

# IEEE 802.21 and Proxy Mobile IPv6: A Network Controlled Mobility Solution<sup>1</sup>

Telemaco Melia<sup>1</sup>, Fabio Giust<sup>2,4</sup>, Riccardo Manfrin<sup>3</sup>, Antonio de la Oliva<sup>4</sup>,  
Carlos J. Bernardos<sup>4</sup>, Michelle Wetterwald<sup>5</sup>

<sup>1</sup>*Alcatel-Lucent Bell Labs, France, Email: telemaco.melia@alcatel-lucent.com*

<sup>2</sup>*Institute IMDEA Networks, Spain, Email: fabio.giust@imdea.org*

<sup>3</sup>*Univerisità di Padova, Italy, Email: riccardomanfrin@gmail.com*

<sup>4</sup>*Universidad Carlos III de Madrid, Spain, Email: {aoliva, cjb} @it.uc3m.es*

<sup>5</sup>*Institute EURECOM, France, Email: michelle.wetterwald@eurecom.fr*

**Abstract:** IP Mobility has been deeply investigated in the past years and standardization bodies (e.g., IETF, 3GPP and IEEE) have specified a wide suite of protocols enabling seamless mobility across heterogeneous wireless access technologies. However, such mobility helping technologies are not yet widely spread as compared to other emerging technologies like WiFi hotspots. This paper aims at filling this gap between research and real deployments by specifying and implementing a scheme for mobility support in wireless heterogeneous environments. In our solution, mobility management is achieved via the Proxy Mobile IPv6 protocol while optimized handover control is provided by the integration of the IEEE 802.21 framework with Proxy Mobile IPv6. The paper also includes the performance evaluation of the proposed platform, shows results obtained through live experiments on the field.

**Keywords:** IEEE 802.21, PMIPv6, network-based mobility

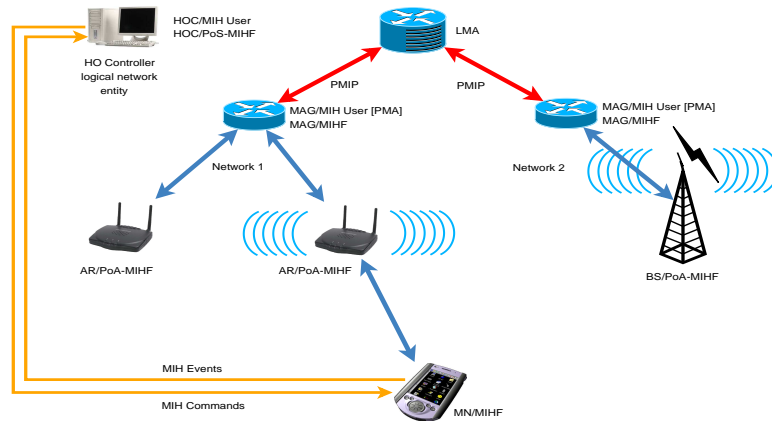
## 1. Introduction

The demand of data services offered by the mobile wireless networks is increasing every year, and the trend is not likely to stop. This growth is due to the availability of 3G and WiFi access which nowadays subscribers are very familiar with, both because of the widespread combined coverage in developed countries and because most handheld devices are 3G and WiFi capable. Besides, the number and popularity of applications for smart-phones that make use of Internet connectivity is getting larger every day, contributing to an increase of market penetration of such devices.

As a consequence, Mobile Operators are migrating their networks to full IP-based networks triggering a real need to adopt an efficient mobility management scheme (e.g., Mobile IPv6 [1], Proxy Mobile IPv6 [2] and their relative extensions/enhancements), while minimizing the extra software required on multi mode mobile devices.

This paper proposes and presents performance results of a network-based mobility solution that exploits the integration of Proxy Mobile IPv6 (PMIPv6) with IEEE Media Independent Handover (MIH) protocol [3]. The main objective of this work is two-fold: *i*) to provide an integrated architecture supporting network-based mobility and network-controlled handover and *ii*) to steer future deployment of network-based mobility technologies by showing encouraging performance results.

<sup>1</sup>The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7-ICT-2009-5) under grant agreement n. 258053 (MEDIEVAL project). Carlos J. Bernardos has also received funding the Ministry of Science and Innovation of Spain, under the QUARTET project (TIN2009-13992-C02-01).



**Figure 1: Architecture Model**

The remainder of the paper is organized as follows. section 2. presents the implemented architecture, section 3. gives a deep insight on the experiments driven and their results and section 4. is dedicated to the conclusions.

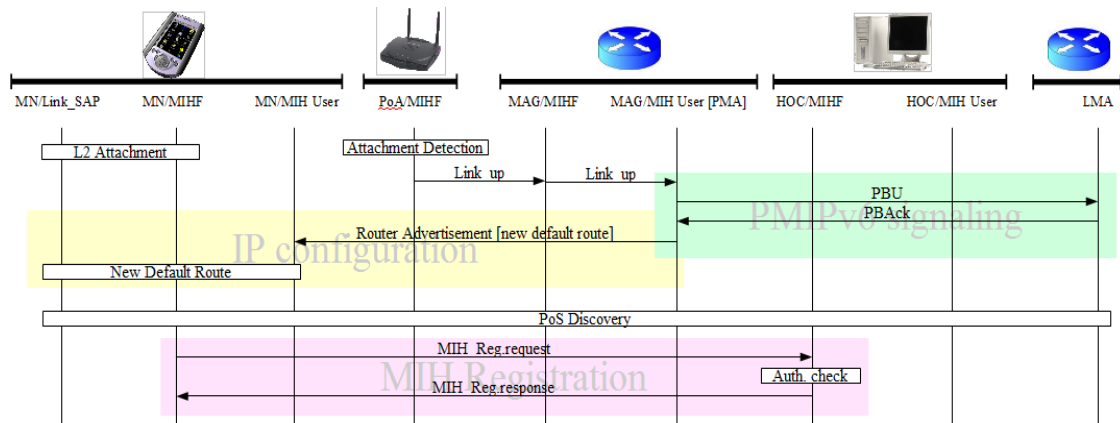
## 2. System Design

In order to reach a fully network-based mobility support we leverage on Proxy Mobile IPv6, for which a Mobile Node (MN) is completely unaware of the layer 3 changes while it is roaming in the mobility domain. In parallel, according to MIH, the functions installed in mobile devices and network nodes lead to a co-operative behavior for which both MNs and network operators share information and commonly agree on handover target selection.

Similarly to what happens in PMIPv6, where a central server (Local Mobility Anchor - LMA) coordinates the Access Routers (AR) by means of an entity installed on them called Mobile Access Gateway (MAG), MIH-Functions (MIHF) are implemented both in the AR or Base Stations (MIH Points-of-Access - PoA) and in a central entity (MIH Point-of-Service - PoS), here called Handover Controller (HOC), that retains the complete vision of the access network, i.e., it is aware of all the connected MNs, all the PoAs and all the MAGs deployed in a certain area together with the binding relationships existing between such elements. It knows to which access networks PoAs and MAGs belong to: such database is statically configured in the HOC. In addition, MIH services are also in the MN, and the HOC is able to communicate with it through the terminal's active interface. Figure 1 depicts the architecture described.

As explained above, all elements in the network: ARs, MNs and HOC contain an MIHF. Each of the network entities exploit the MIHF functionality in a different way by providing a control module interacting with the MIHF as a MIH User. The MIH User located in the HOC is responsible to coordinate the handover, hence providing the required intelligence. It exploits the rest of the MIH enabled entities in the network by receiving MIH Events and sending MIH Commands. The MIH User located in the ARs, is in charge of triggering the PMIPv6 registration with the LMA upon reception of a MIH\_Link\_Up event. The MIH User located in the terminal is in charge of executing the commands received from the HOC, who is managing the terminals mobility.

It is worth noting that through the use of the IEEE 802.21 standard and the coordination between the different MIH functions in the PoAs (ARs), MNs and PoS (HOC),



**Figure 2: MIH bootstrap signaling**

we are able to follow a make-before-break approach.

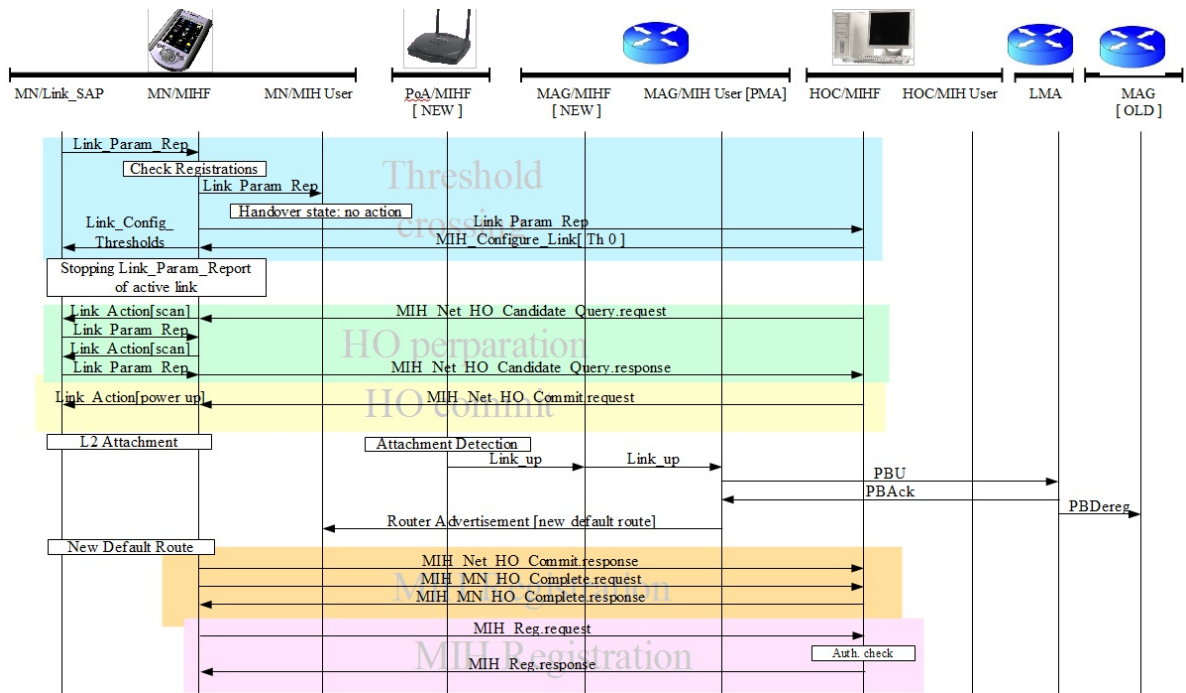
As IEEE 802.21 provides a very flexible set of services, the reporting of the status of radio conditions and other operations are performed in an asynchronous manner based on exchanging MIH messages between the MIH entities across the domain. The following subsections detail the protocol behavior.

### 2.1 Discovery and Bootstrapping

Bootstrapping in this context is regarded as power up procedure and consists of *i*) powering on a network interface, *ii*) selection of the best PoA based on RSSI, *iii*) network attachment and IP address configuration, and *iv*) MIHF registration. Regarding *iv*), before a control communication channel is setup between two MIH peers (typically MN and PoS), the MIH user in the MN should start a discovery process, that can be processed either at layer two or at layer three. IEEE 802.21 standard describes procedures for layer two based discovery while here the approach suggested in [4] is followed, hence executing it either via DNS [5], or via DHCP [6]. No assumptions are made on the timing of such discovery procedure (it could happen while access authentication is performed). The address of the PoS is therefore used during the bootstrapping phase for MIHF registration between the HOC and the MN.

Figure 2 describes the whole bootstrap signaling flow operation. When the node powers up its interface(s), the terminal starts layer 2 attachment procedure, which includes also the authentication of the MN in the Access Network and can be processed through layer two credentials provided by the MN to the PoA, that are used to query the AAA infrastructure. Upon completion of layer two attachment procedure, the Access Point (MIHF@AP) sends a MIH\_Link\_up message to the MIHF@AR that forwards it to MIH-User@AR. This message triggers the PMIPv6 registration: a Proxy Binding Update (PBU), carrying the MN identifier, is transmitted from the MAG to the LMA and a PBAck acknowledges the handshake exchange. The PBAck received in the MAG triggers a unicast Router Advertisement that is received by the MN and allows the IP configuration procedure (including the new IPv6 default route).

As soon as the MN has obtained a valid default route, a MIH peer discovery procedure takes place. Subsequently, the MIHF@MN initiates the MIH Registration procedure sending an MIH\_Register.request to the MIHF@HOC entity. The HOC shall check the MN MIHF\_ID, allocate its MIH registration entry and finally reply with



**Figure 3:** MIH proactive handover signaling

a MIH\_Register.response message. In case of successful MIH registration, after the MIH\_Register.response, the MIHF@HOC also sends a MIH\_Configure.Link message to the MIHF@MN, to configure various parameters related to the active link. One of such parameters is the threshold used to detect the worsening of the active link radio conditions.

The MIH\_Configure.Link concludes the Bootstrap procedure, as the MN has IP connectivity and can roam across the domain without experiencing any session discontinuity, taking advantage of the MIH functionalities offered by the MIHF@HOC which it has registered to.

## 2.2 Handover Procedure

The handover (HO) procedure is shown in Figure 3. The MN periodically triggers measurement reports about the condition of the active radio link. Upon crossing the previously configured threshold, the MIHF@MN sends a MIH\_Link\_Parameter\_Report to the MIHF@HOC informing about the event, and consequently, the MIHF@HOC initiates the handover preparation by replying with a MIH\_Net\_HO\_Candidate\_Query.request message. When the MN receives the Candidate Query, a series of Link action.request are sent from the MIHF@MN to the Link\_SAP (i.e., the interface between MIH and the NICs drivers) to query for the radio conditions detected for the different potential candidate target PoAs. The lower layers (device technology drivers) collect the required information and reply back to the MIHF@MN, which generates and sends to the HOC a MIH\_Net\_HO\_Candidate\_Query.response with the list of found PoAs, ordered by the best received signal strength.

When the MIHF@HOC receives the response, it can correlate the received data with other information it has regarding the available access networks in the domain. Based on different criteria and on the intelligence implemented in the MIH-User@HOC,

the MIHF@HOC sends a MIH\_Net\_HO\_Commit.request message to the MN (different parameters can be sent taking into account policies for resource allocation, user profile, application requirements). Upon receiving the Commit.request, the MIHF@MN triggers a Link\_action.request primitive towards the Link\_SAP with link action set to Power\_up. The Link\_SAP then translates the primitive in the specific technology one in order to perform the attachment to the target link.

As the presence of a new attached MN is detected by the new PoA, a MIH\_Link\_up message is sent to the MAG it is attached to in the Access Network, and then the normal PMIPv6 signaling is triggered. After the new IP configuration is completed (unicast Router Advertisement is received and default route is configured) the MN can send the MIH\_Net\_HO\_Commit.response message to the HOC to inform it about the new attachment result. Additionally the MIHF@MN sends a MIH\_MN\_HO\_Complete.request message to ensure that on the network side the procedure is also complete. Upon receiving the message the MIHF@HOC can update the cache with the new location of the handed-over MN. After the MIH\_MN\_HO\_Complete.response is sent back to the MIHF@MN, a new registration is triggered between the MN and the HOC. The registration is used, in this specific case, to simply renew the old expiration time and data, therefore it could be theoretically skipped or postponed. It should be noted that in case of changing the HOC, a discovery and registration would be needed in order to proceed with any further new communication. After the registration is complete and the MN receives from the HOC the settings for the thresholds by means of the MIH\_Configure\_Link\_message, the MIHF@MN state turns to idle and the terminal is ready to restart this procedure once again and report measurements periodically.

### 3. Evaluation and Results Analysis

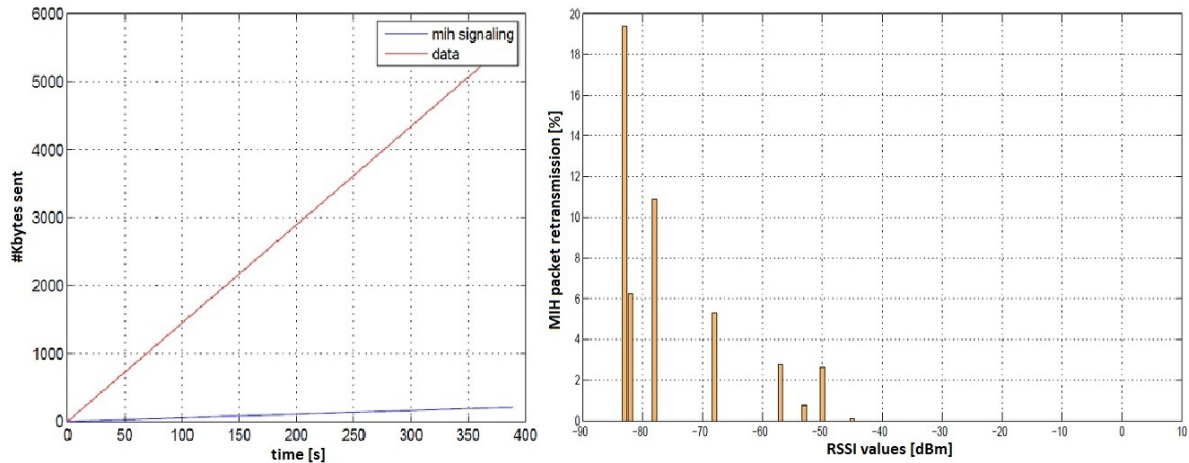
The architecture proposed in section 2. has been set up using an IPv6 network comprising three MAGs, an LMA, and a MN (the nodes are PCs running Linux kernel 2.6.16, and all the MIH functions/signaling was implemented in C). Due to testbed limitations in our scenario we only built a IEEE 802.11g wireless access, thus replicating a WiFi-to-WiFi intra-technology handover. To emulate large network delays the Imunes<sup>1</sup> platform has been configured between the MAGs and LMA to artificially increase/decrease the end-to-end RTT between the MN and the LMA. The LMA further implements the HOC controller for network controlled handovers.

#### 3.1 Congestion and Retransmissions Control of MIH signalling

The proposed platform exploits two different protocols to achieve a cross-layer mobility management; the goal of both is to minimize the over-the-air signaling thus reducing the associated bandwidth consumption.

Since the PMIPv6 protocol runs only between network components, the study focuses on the MIH messages sent through the wireless interface between the MN and the network. The simulation study in [7] computes the required message size and an average of the consumed bandwidth. To prove that our system provides similar results in a real scenario, we analyzed the required signaling to perform handovers between the three MAGs. The left graph of Figure 4 represents a number of more than 200 handovers performed in 400 seconds. We captured both the signaling data and the

<sup>1</sup><http://old.tel.fer.hr/imunes/>



**Figure 4:** Experiment results: ratio between a VoIP stream and the MIH signaling over IEEE 802.11g (left), ReTX vs RSSI (right)

VoIP stream running between the MN and a correspondent node in the network and plotted the cumulative function over time. The different slope between the MIH and VoIP lines shows how little the MIH traffic costs over time. We argue that this is the desired effect since it matches the simulated results in [7].

It is worth noting that packet loss over the wireless medium is often a reason for performance decay in telecommunications systems, thus a packet retransmission mechanism should be implemented. To fulfill this requirement we followed the approach suggested in [4], that, instead of using TCP reliability to carry the MIH messages, leverages on the MIH built-in request/response scheme over UDP datagrams. The system has been tested in different radio environments spanning from very good conditions to very poor link quality.

While the left plot of Figure 4 accounts for experiments run with optimal link quality (i.e., small packet loss), the right one shows the relationship between the number of retransmissions and the RSSI.

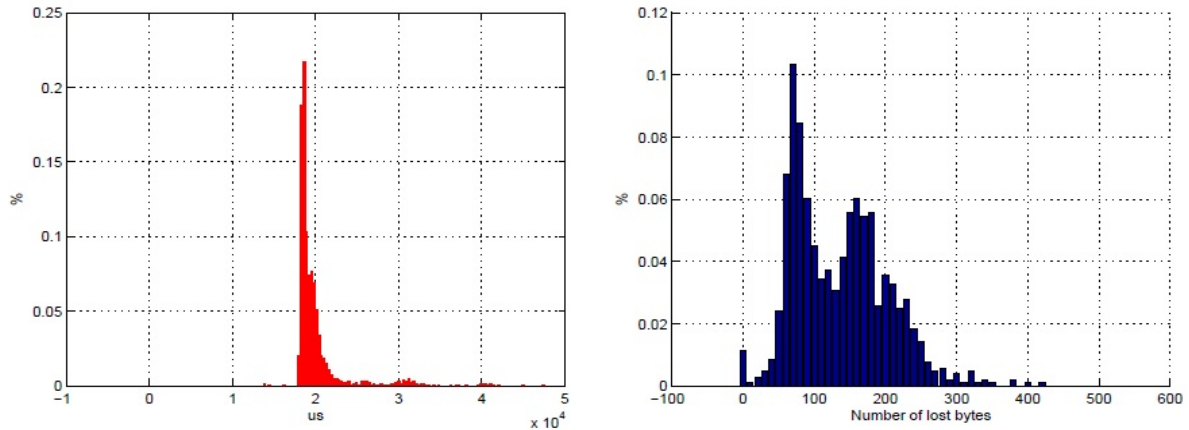
It's important to notice that in the tests we did, most of the retransmissions were in the form of bursts generated by the same packet retransmitted several times (up to 4 or 5). Those tests were repeated several times and produced slightly different results, but the trend was constant and proved the importance of the acknowledgment mechanism effectively increasing the efficiency of MIH operations. The plot supports the considerations given above showing where retransmissions take place.

### 3.2 Handover Latency and Packet Loss

Handover latency is here regarded as the time required to switch link as well as to configure the link for IP communication.

To evaluate handoff latency we introduced timestamps in the code executed in MIHF@MN process and we logged the operations flow. We can see from the collected data shown in the left part of Figure 5 that the average handover delay is about 20ms, no handover takes less than 15ms and very few more than 35ms. The main contribution is given by the time required by the physical layer to attach to the new link, since we deployed the PMIPv6 nodes such to have a delay between LMA and MAGs of 1 ms.

The time required to switch link has an impact in the time the terminal is not



**Figure 5:** Results of handovers over a VoIP stream: delay distribution (left) and packet loss (right)

reachable and packets cannot be delivered. To measure the packet loss during handovers we first evaluated the average packet loss due to standard medium behavior: this was conducted while the MN was attached to a single PoA and sending ICMP ping requests as well as datagrams to the network with best radio conditions.

An average of 0.4% packet loss was measured. Taken into account this basic packet loss, in the right graph of Figure 5 we can see the distribution of packet loss for the VoIP data stream due to a single handover. This was calculated by sending a standard VoIP stream (100 pk/s, 100 B/pk), and calculating the amount of received data every 100 ms. We argue an average of 300 bytes lost per handover is an acceptable result for real time multimedia communications.

### 3.3 Handover Latency with *Imunes* artificial delays

In order to simulate a real world scenario we employed *Imunes* to increase routing delays between the MAGs and the LMA. Thus we emulated the case of a MN handing over from a link with a small RTT to links with one and two orders of magnitude larger RTT. We configured the *Imunes* machine with the following parameters:

- delay LMA  $\Rightarrow$  MAG1: 1ms (same value of previous tests)
- delay LMA  $\Rightarrow$  MAG2: 10ms
- delay LMA  $\Rightarrow$  MAG3: 100ms

The results obtained in this test nicely match the handover delay results, since what we expected was a longer latency mainly affected by the increased RTT due to the PBU/PBA exchange. In the two sets of tests we got values around 40ms and 220ms, respectively, that is equal to the values already obtained in the previous section plus two times the delays listed above, underlining the impact of a very large RTT on the overall handover latency.

Given the nature of our design, it should be noted that the RTT affects only the attachment to the new link. In fact the optimal threshold configuration for handover initiation allows the HOC to timely start the handover preparation phase while the MN is still attached to the old link. After the MN switches to the new link, the Link\_up message triggers the PMIPv6 registration which is affected by the RTT (registration

requires an handshake between MAG and LMA). Since the HOC knows the health status of the network, it is desirable to consider the RTT as parameter when performing target selection aiming at minimizing the effect of moving from one link with low RTT to a link with a larger one.

#### 4. Conclusions

This paper presented an integrated solution for optimized mobility control across heterogeneous wireless networks exploiting IETF Proxy Mobile IPv6 and IEEE 802.21 Media Independent Handover. The presented work takes inspiration from the simulation results published previously in [7] and shows how network controlled handovers can be achieved in a real deployment case.

Our test network setup lets a mobile device equipped with a IEEE 802.11g card roaming across the PMIPv6 domain. The intelligence implemented in the network controls the mobility of the mobile device and can issue handover commands when necessary. The cross layer design in the mobile device (MIH layer) helps the mobility functions to be timely triggered and optimizes the actions performed by the lower layers.

The tests performed show the low handover latency and give a quantitative measure of the amount of retransmitted signaling based on an application layer acknowledgment mechanism. In presence of good channel conditions the performance of the handover procedure is suitable for real time communications while, with the worsening of the radio channel, handover performance decreases accordingly. To emulate large networks, delays between nodes have been artificially increased aiming at simulating the handoff from a link with small RTT to links with one and two orders of magnitude larger RTT.

We argue that the obtained handover performance matches the requirements for seamless mobility, while the network controlled approach very well addresses the interest of Mobile Operators seeking new paradigms for mobility control. Authors believe that, by means of a real study case, the advances presented in this work significantly help in designing and deploying next generation networks.

#### References

- [1] D. Johnson *et al.*, “Mobility Support in IPv6.” RFC 3775, June 2004.
- [2] S. Gundavelli *et al.*, “Proxy Mobile IPv6.” RFC 5213, Aug. 2008.
- [3] LAN/MAN Committee of the IEEE Computer Society, “IEEE Std 802.21-2008, Standards for Local and Metropolitan Area - Part 21: Media Independent Handover Services,” 2008.
- [4] T. Melia *et al.*, “IEEE 802.21 Mobility Services Framework Design (MSFD).” RFC 5677, 2009.
- [5] P. Mockapetris, “Domain names - implementation and specification.” RFC 1035, Nov. 1987.
- [6] R. Droms *et al.*, “Dynamic Host Configuration Protocol for IPv6 (DHCPv6).” RFC 3315, July 2003.
- [7] T. Melia *et al.*, “Toward IP converged heterogeneous mobility: A network controlled approach,” *Computer Networks*, vol. 51, no. 17, pp. 4849 – 4866, 2007.