Performance analysis of a network-based protocol for localized IP mobility management

F. Miconi, I. Guardini, and G. Giaretta, Telecom Italia Lab

Abstract—In this paper a new protocol for IP mobility management is described, which follows a network-based approach and fulfills the requirements of optimized usage of radio spectrum and minimum involvement of the terminal. The performance of this solution has been analyzed using the OMNeT++ simulator and a comparison with other well-known protocols, like Mobile IPv6 and Hierarchical MIPv6, has been carried out. Finally, the results of the simulations are presented and discussed in terms of handoff latency, data transport overhead, and signaling volume over the air interface.

I. INTRODUCTION

The increasing popularity of Wireless LANs, the next advent of Wireless MANs (e.g., WiMAX) and the development of cellular networks optimized for IP traffic exchange are giving more emphasis to the problem of mobility management across IP subnets, so that there are currently a lot of protocols under study or under way of development. Nowadays, the most efficient, stable, and well-known solution for IP-based mobility management is Mobile Internet Protocol (Mobile IPv6), that has been standardized by the Internet Engineering Task Force (IETF) in two versions, 4 and 6[1].

Nonetheless, the improvement of technology and the continuous upgrade of user equipment demand for higher performance and consequently better solutions. For this reason, new approaches are being investigated both to improve the efficiency of Mobile IP (in particular Mobile IPv6) and to develop novel mobility management architectures better suited for the widespread deployment in cellular environments, where the minimization of the overhead on the radio access and the capability to manage a fast-growing number of heterogeneous terminals (phones, PDAs, sensors, etc.) are fundamental requirements.

This led to the definition of the concept of network-based localized mobility management. Differently from Mobile IPv6 and its extensions (e.g., Hierarchical Mobile IPv6), that are global mobility management solutions mostly controlled by the terminal, protocols falling in this category are designed to provide seamless mobility inside localized network domains (e.g., the entire network of an operator or a network district) with minimum involvement of the terminal.

This paper compares a solution proposed for NETWORK-based Localized Mobility Management (NETLMM) with Mobile IPv6 and its hierarchical extensions (Hierarchical Mobile IPv6).

The comparison has been performed using a simulator called OMNeT++ (version 3.2), a public-source, component-based, modular and open-architecture simulation environment, freely available for download on [2]. OMNeT++ is an object-oriented, modular, discrete event network simulator, based on the C++ language, that allows to simulate telecommunication networks and other parallel/distributed systems.

The simulation work was carried out exploiting the INET and IPv6SuiteWithINET frameworks of OMNeT++, that have been used to model the basic mechanisms of IPv6 networks (e.g., Neighbor Discovery) and protocols like Mobile IPv6 (MIPv6) and Hierarchical Mobile IPv6 (HMIPv6). Instead, some extra code was implemented in order to simulate the NETLMM protocol devised by the mobile networking research group of Telecom Italia Lab (TILab), that is described in Chapter III.

II. PROBLEM STATEMENT

The continuous increase of the number of the mobile users and of their expectations in terms of quality of service, especially for real-time applications (e.g., VoIP), is pushing the development of new mobility management protocols capable to improve performance and scalability of Mobile IP (v4 and/or v6) and its various extensions (e.g., HMIPv6).

Being a terminal-based solution, Mobile IPv6 requires that the Mobile Node (MN) registers across movements with its peer entities, namely the Home Agent (HA) and Correspondent Nodes (CNs). Depending on the position of the nodes within the network, and their topological distance, this end-to-end registration procedure may generate a relevant handoff latency, that is the time necessary to re-establish IP connectivity after any mobility event. Moreover, it involves the exchange of a large amount of control signaling, which is not desirable neither in the core network nor on the radio interface.

The former issue can be mitigated through some ad hoc solutions, like the allocation of a HA very close to the MN’s point of attachment (i.e., local HA), or through other state-of-the-art optimizations, such as Optimistic Duplicate Address Detection [3], designed to minimize specific components of the handoff latency (e.g., movement detection delay).

The latter aspect, instead, requires deeper revisions of the overall architecture, such as the introduction of a mobility management hierarchy. The key idea is that mobility within

1 For this paper the focus is only the protocol Mobile IPv6.
a Localized Mobility Domain (LMD), that is a network area with well known boundaries, such as a corporate, is managed locally, without involving any distant entity, like the Mobile IPv6 Home Agent (HA). Instead, Mobile IPv6, or other global mobility management protocols (e.g. HIP), are activated only in case the user leaves the localized domain. This has the advantage of minimizing the volume of signaling within the core network, since local mobility does not generate mobility management signaling outside the visited domain. Moreover, this approach slightly reduces the handoff latency, since local movements are handled by local mobility agents, that are normally very close to the terminal (i.e. low Round Trip Time). A well known implementation of this architecture is Hierarchical Mobile IPv6 [4], that introduces the concept of Mobility Anchor Point (MAP) to hide local mobility to the HA located in the home domain.

Nonetheless, localized mobility management is not by its own enough to fulfill the strict requirements raised by the evolution of cellular networks towards 4th generation systems (4G) [5], that are summarized here below:

- the volume of signaling exchanged during an handover has to be minimized in any network segment, and particularly on the air interface;
- despite the advances in wireless technology, the radio spectrum remains a limited resource, so it is necessary to reduce the amount of the per-packet overhead necessary for routing of data traffic;
- the mobility protocol should be able to support any available radio access technology (IEEE 802.11, WiMAX, upcoming cellular accesses, etc.);
- the architecture should be best suited also for terminals with very limited processing and storage capabilities (e.g. machine-to-machine equipment).

HMIPv6 does not satisfy all the requirements listed above, since, compared to MIPv6, it does not provide benefits on the amount of signaling on the air interface and requires multiple levels of tunneling between terminal and network to achieve proper routing of data traffic while on the move.

These drawbacks can be overcome performing localized mobility management in a network-based fashion. According to that, localized mobility management is handled by the routers as part of the basic connectivity service offered to the user. In this way the mobile user needs minimal software support on the terminal, mostly limited to the movement detection procedure.

III. DESCRIPTION OF THE SOLUTION

A network-based localized mobility management protocol following the design principles described in the previous section has been developed by the mobile networking research group of TILab and is specified in [6]. It can be used to handle IP mobility within a Localized Mobility Domain (LMD) spanning a whole administrative domain (e.g. an operator’s network) or part of it. The edge of the LMD is made of Access Routers (ARs). An AR can manage one or more IP links (i.e. layer 2 access networks), each one univocally associated with at least an IPv6 prefix.

As long as the mobile node remains within the same LMD, it can keep on using the same IP address even if it happens to change the AR it is attached to. Proper routing of IP packets while on the move is ensured by the AR where the mobile node has switched on, the Home Anchor Router (HAR), that works as anchor point for data traffic and forwards it to the AR which the mobile node is currently attached to, the Visited Access Router (VAR). Data forwarding is carried out through a bi-directional tunnel between HAR and VAR, and the mobile node is only responsible for movement detection.

In detail, when the mobile node powers up (or enters) in the LMD it gets an address through an address configuration mechanism (e.g. stateless autoconfiguration or DHCPv6). The address configured by the host is topologically correct, since it belongs to the network prefix announced by the AR on the visited link. Therefore the host can communicate with any other node using standard IP routing.

When the host moves to another link and changes default router, it sends an Activate message to the new access router with an indication of the IP address used on the previous link. This is not intended to be a novel mobility management message, but can be an existing message delivered by the terminal as part of the usual procedures performed when attaching to a new link. For example, the Activate message can be a Neighbor Discovery message, a DHCPv6 message or the signaling exchanged to gain authenticated access to the network (i.e. AAA). Another viable option is to discover the presence of the mobile node exploiting L2 protocols, or triggers, specific of the radio technology employed in the access network. In the OMNeT++ implementation developed as part of this work, the activate message is a Router Solicitation (RS) with a special option, called Global Address Option, including the global address of the host.

The router that receives the Activate message acts as VAR for the mobile host and begins a procedure of host registration sending a Location Update (LU) to the previous access router, which acts as Home Access Router (HAR). The HAR maintains in a Location Cache the binding between the address of the host and his position (i.e. the address of the VAR) and replies to the VAR with a Location Acknowledgement (LA) message. After that, the HAR starts intercepting all the packets addressed to the host and forwards them via bi-directional tunneling to the VAR.

At the next movements of the mobile node, the HAR, after having received the LU message, must also notify the old VAR that the host moved to another access router by sending a Move Notify message.

This strategy allows to satisfy the requirements of an efficient usage of the air interface. In fact, control signaling is exchanged only between the access routers, without involving the host; which means that it doesn’t traverse the
wireless link. Moreover, all the packets addressed to the host are routed through the tunnel between HAR and VAR and are then forwarded to the host through standard IP routing; in this way the message overhead on the air interface is decreased, since there is no tunneling towards the terminal.

IV. EXPERIMENTAL RESULTS

Purpose of the work described in this paper was to carry out a simulative analysis to compare the performance of the network-based localized mobility management protocol presented in section III with the one of other state-of-the-art terminal-controlled solutions, that are:
- Mobile IPv6 with a centralized Home Agent;
- Mobile IPv6 with a local Home Agent (i.e. within the visited domain);

The reported measurements analyze three aspects of mobility management: handoff latency, per-packet overhead on data traffic and volume of control signaling exchanged by the mobile node on the wireless link. The simulations have been performed through the OMNeT++ simulator.

A. Network Scenario

![Network Scenario](image)

The reference network scenario for all the simulations is represented in Figure 1: the network has an hierarchical structure, in which the local domain is compounded by one gateway (that, in the case of HMIPv6, acts as MAP) and five access routers connected to one or more Wireless LAN Access Points, that represent the points of attachment to the network for the mobile nodes (MNs). During the simulations the MNs communicate with a Correspondent Node (CN) located within an IP backbone placed behind the gateway.

B. Configuration Parameters

The number of the mobile nodes moving within the local domain is variable: 5 or 10 MNs. This means that there are 8 simulation scenarios, 2 for each protocol (i.e. one run with 5 MNs and one run with 10 MNs).

For each scenario the variable parameters are: the delay introduced by the IP backbone and the activation of the Optimistic DAD (Duplicate Address Detection) procedure. According to [7], the delay of the packets on the Internet can be modeled with a shifted Gamma statistical distribution having a mean of 9.662 ms for a local network and 108.232 ms for a geographical network. How these parameters are configured in the simulations is explained in Table I.

<table>
<thead>
<tr>
<th>Simulation</th>
<th>IP Backbone mean delay</th>
<th>ODAD</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>9.662 ms</td>
<td>off</td>
</tr>
<tr>
<td>2</td>
<td>108.232 ms</td>
<td>off</td>
</tr>
<tr>
<td>3</td>
<td>9.662 ms</td>
<td>on</td>
</tr>
<tr>
<td>4</td>
<td>108.232 ms</td>
<td>on</td>
</tr>
</tbody>
</table>

The length of each simulation is 2400 seconds. The implemented DAD algorithm is based on sending one Neighbor Solicitation message and then waiting for a time-out of 120 ms, before considering the address under detection unique on the link.

Each MN, while it is moving, performs a VoIP call with the CN and establishes two FTP connections with it for downloading 2 files of 3 MBytes each. In order to take into account that a phone call is usually a combination of speech and periods of silence, the VoIP call is simulated through a sequence of 10 UDP flows (separated by a pause) having an exponential length with mean of 30 seconds [8]. The reference voice codec assumed for the simulations is G.729, which implies that each UDP packet has a payload length of 32 bytes (including 8 bytes of RTP header) and is sent every 0.05 seconds.

C. Results

The data measured during the simulations are:
- handoff latency,
- per-packet overhead on the wireless link,
- volume of control signaling on the wireless link.

Handoff latency

The implemented movement detection algorithm is the same for all the 4 protocols (network-based localized mobility management, Mobile IPv6 with centralized HA, Mobile IPv6 with local HA and Hierarchical Mobile IPv6), so that the differences in the measurements are due only to the different peculiarities of the protocols. The algorithm is based on a Layer 2 trigger, which notifies the MN when it

2 The DAD algorithm allows to check if the address is unique on the link. The ODAD algorithm, instead, allows to use the address as source for the messages even if the DAD procedure is not yet completed.
has changed the Access Point: when the L2 trigger is received, the MN detects that there may have been a potential change of IP subnet and sends a Router Solicitation message, in order to discover the new Access Router; the AR replies with an unicast Router Advertisement message. In this way the ARs do not need to send unsolicited RAs over the wireless link, which allows not to waste resources over the radio interface. Both RS and RA messages include a special option, named Global Address Option, containing the host’s global IP address.

Concerning the MIPv6 and HMIPv6 protocols, the handoff latency can be subdivided in the following three components:
1) $T_{MD}$ (Movement Detection Delay): time needed to detect the movement to a different subnet;
2) $T_{CoA}$ (Care-of Address Configuration Delay): time needed to configure the new Care-of Address,
3) $T_{HARReg} / T_{MAPReg}$ (HA / MAP Registration Delay): time needed to complete the registration (i.e. sending BU and receiving BA) with the peer entity, that is the HA for MIPv6 and the MAP for HMIPv6.

Instead, with the NETLMM protocol, the handoff latency can be characterized as follows:
1) $T_{MD}$ (Movement Detection Delay), same as above;
2) $T_{HARReg}$ (HAR Registration Delay): time needed to complete the registration with the Home Anchor Router (i.e. sending LU and receiving LA);

In Figure 2 the average values of the handoff latency are shown for the 4 protocols in each simulation, distinguishing the three components just described.

It is possible to observe that for all protocols the predominant component of the handoff latency is the HA (or MAP or HAR) Registration Delay ($T_{HARReg}$, $T_{MAPReg}$ or $T_{HARReg}$). In Figure 2(a), referring to MIPv6 with centralized HA, the measurements registered in the second and fourth simulation present a bigger value of the $T_{HARReg}$ component than in other simulations: this is due to the fact that in those simulation scenarios the HA is located behind a geographical IP backbone, which introduces a relevant delay on signaling and data traffic. For the other protocols, instead, this parameter does not have any influence on the handoff latency results since the mobility is managed locally.

For MIPv6 and HMIPv6 protocols, the Optimistic DAD (ODAD) procedure leads to a reduction of the mean handoff latency, while for the NETLMM protocol it has a much smaller influence. This is due to the fact that with NETLMM the host doesn’t have to wait for the DAD procedure after an handover, because it does not have to configure a new address, so ODAD doesn’t introduce any benefit.

Figure 3 shows a comparison between the mean values of the handoff latency for the 4 protocols in the 4 simulation scenarios presented in Table I. It can be noted that HMIPv6 provides the best result: this is due to the optimal position of the MAP within the local domain (i.e. the access gateway), while for the other protocols, the mobility agent is either an AR (MIPv6 with local HA and NETLMM protocol) or a node outside the LMD (MIPv6 with remote HA). However, the mean values of the handoff latency for the NETLMM protocol are also acceptable, because, as it is shown in Table II, the difference between the measured mean values for HMIPv6 and NETLMM protocol is 30 ÷ 75 ms. So the performance, in terms of latency, is pretty much comparable.
Finally, comparing the handoff latency values of MIPv6 (with centralized or local HA) and NETLMM protocol, the latter results to be the best, even if host’s ODAD support is activated. The latency reduction for NETLMM protocol is at least 40 ms: this is due to the fact that the path of the mobility management messages is shorter, as the end-point is the AR, not the host (i.e. the radio link is not involved).

Overhead over the application data

One of the advantages of a network-based approach is the reduction of per-packet overhead on application data. This is because the traffic is tunneled only in the path from HAR to VAR, while for MIPv6 and HMIPv6 protocols the end point of the tunnel is the MN. So, for NETLMM protocol, all the packets transmitted over the wireless link are encapsulated into a single IP datagram, with an overhead of 40 bytes (i.e. length of the IPv6 header). Instead, with MIPv6 each data packet addressed to, or transmitted by, the host is encapsulated into two IP datagrams, that become three IP datagrams with HMIPv6, since the traffic undergoes a double tunneling, between the MN and the HA, for global mobility, and between the MN the MAP, for local mobility.

Table III shows the proportional increase of the message length due to per-packet overhead. The value for the VoIP data is bigger then the one for the FTP data, because the UDP packets have a length of 40 bytes, while the length of a TCP segment is 1024 bytes.

<table>
<thead>
<tr>
<th>Application</th>
<th>Protocol</th>
<th>Proportional increment of the data traffic</th>
</tr>
</thead>
<tbody>
<tr>
<td>FTP</td>
<td>MIPv6</td>
<td>7.81 %</td>
</tr>
<tr>
<td></td>
<td>HMIPv6</td>
<td>11.72 %</td>
</tr>
<tr>
<td></td>
<td>NETLMM</td>
<td>3.91 %</td>
</tr>
<tr>
<td>VoIP</td>
<td>MIPv6</td>
<td>200 %</td>
</tr>
<tr>
<td></td>
<td>HMIPv6</td>
<td>300 %</td>
</tr>
<tr>
<td></td>
<td>NETLMM</td>
<td>100 %</td>
</tr>
</tbody>
</table>

In Figure 4(a) and (b), the volume of per-user FTP and VoIP data traffic for the 4 protocols is shown for the first two simulation scenarios. The ratio between the payload length and the header length reflects the percentages of Table III (also for the simulations 3 and 4, whose results aren’t here visualized). Concerning the VoIP traffic, we can observe that the NETLMM protocol is much more efficient then the other protocols, because, due to the very small length of a VoIP packet, reducing the IP overhead results to be essential to constrain the waste radio resources.

It is however necessary to remind that, in the case of MIPv6 and HMIPv6, the results are collected assuming the MNs communicate with the CN in Bidirectional Tunneling. With Route Optimization it would be possible to avoid one level of encapsulation, since all traffic would not pass through the HA. However, the usage of Route Optimization would induce a bigger volume of the handover-related signaling, as it will be explained in the following.

**Signaling volume**

For MIPv6 and HMIPv6 protocols, the signaling messages transmitted on the radio interface include Router Solicitation, Router Advertisement, Binding Update and Binding Acknowledgement. With NETLMM protocol, instead, the only messages that traverse the radio interface are RS and RA, because the mobility management messages are exchanged only between the routers of the LMD and do not regard the MN. Nevertheless, in this case the RS and RA messages have a bigger length, because they include the Global Address Option with the MN’s global IP address.

Figure 5 shows the mean value of the signaling traffic volume per user and per handover exchanged between host and AR, measured in the simulations 1 and 3 (where the ODAD support is set respectively to “off” and “on”)\(^3\).

The minimum value of signaling volume has been obtained with NETLMM protocol (in average 212 bytes for

\(^3\) The results registered in the other two scenarios are definitely comparable; in fact, the only difference in the parameters is the IP backbone delay, which doesn’t have any influence on the signaling traffic volume.
each simulation), while the maximum one with HMIPv6 (in
average 325 bytes): this is due to the MAP Option that each
RA message has to include in order to notify to the terminal
the global address of the MAP.

![Figure 5](image)

**Figure 5**

Mean value of the signaling traffic volume per user per
handover measured in simulation 1 (a) and 3 (b).

The eventual support of Route Optimization for MIPv6
would lead to an increase in the measured values, because
the host would be forced to repeat the binding registration
procedure, and the signaling for managing the correspondent
security association, for each CN it is communicating with.

**TABLE IV**

<table>
<thead>
<tr>
<th>Sim</th>
<th>MIPv6 centr. HA</th>
<th>MIPv6 local HA</th>
<th>HMIPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>28.33 %</td>
<td>28.16 %</td>
<td>35.46 %</td>
</tr>
<tr>
<td>2</td>
<td>26.33 %</td>
<td>25.42 %</td>
<td>32.94 %</td>
</tr>
<tr>
<td>3</td>
<td>27.80 %</td>
<td>26.91 %</td>
<td>34.40 %</td>
</tr>
<tr>
<td>4</td>
<td>28.46 %</td>
<td>27.36 %</td>
<td>36.20 %</td>
</tr>
</tbody>
</table>

Finally, in Table IV it is shown the proportional reduction
of the signaling traffic volume involved by NETLMM
protocol with respect to the other protocols. The benefits are
relevant, as the reduction of the per-handover volume varies
between 25% (against MIPv6) and 36% (against HMIPv6).

**V. CONCLUSIONS AND NEXT STEPS**

The performance of the protocols for local mobility
management has been evaluated against the requirements of
next generation cellular networks (4G), in particular the
need to minimize the handoff latency and the waste of
resources on the air interface.

The network-based localized mobility management
protocol described in this paper results satisfy the
requirements, because it leads to a more efficient use of the
radio spectrum, reducing the handover-related signaling
traffic and especially the overhead on data packets.
Furthermore, the performance in terms of latency is
comparable with that one of other terminal-based solutions,
like MIPv6 with local Home Agent and HMIPv6.

The IETF NETLMM Working Group is currently
standardizing a protocol following the design principles
described in this paper. The resulting solution is expected to
be more complete and efficient than the one evaluated in our
work, including enhanced capabilities like dead peer
detection, autoconfiguration, etc.

Implementing the standard track solution in OMNeT++ is
a possible prosecution of our effort, but it is expected the
results will be definitely similar, especially concerning the
overhead on data packets and the signaling traffic volume,
since the philosophy at the basis of the protocol will be the
same assumed in this paper. The work should be coupled with
an extension of the performance analysis to more
complex scenarios, such as the case of a big population of
users moving around relying on a wide area radio coverage.
Moreover, it will be necessary to study in deeper detail how
to combine a network-based localized mobility management
solution with a global mobility management protocol like
Mobile IPv6, in order to end up with a complete architecture
capable to handle with maximum efficiency any kind of,
global or local, mobility scenario.

**REFERENCES**

Engineering Task Force, RFC 3775, June 2004
Internet Engineering Task Force, draft-ietf-ipv6-optimistic-dad-06.txt,
September 2005
Mobile IPv6 Mobility Management (HMIPv6)”, Internet Engineering
Task Force, RFC 4140, August 2005
“Requirements and Gap Analysis for IP Local Mobility”, Internet
Engineering Task Force, draft-kempf-netlmm-nohost-req-00.txt, July
2005
Engineering Task Force, draft-giaretta-netlmm-00.txt, September 2005
Packet Delays”, Internet Engineering Task Force, draft-Corlett-
Statistics-of-packet-delays-00.txt, March 2002
and cellular mobile networks”, SIGNET Research Group,
Dipartimento di Ingegneria dell’Informazione, Università di Padova,
February 2005