A Novel Fast Local Mobility Protocol for Next Generation Mobile Networks

Nuno G. Ferreira, Rui Aguiar, Susana Sargento

***Abstract* - In the current mobile cellular networks the terminal mobility support is based on layer-1 and homogenous layer-2 mechanisms. This mobility support is sufficient for current numbers of mobile terminals, however in the future it is expected that this number will significantly increase. In order to handle the increasing number of mobile terminals with distinct layer-2 interfaces and also to support the paradigm of "Internet Everywhere", the next generation networks will be entirely based on Internet Protocol (IP). Nonetheless, IP does not support mobility per se, thus, it is essential to develop efficient mechanisms to guarantee this fundamental requirement. This paper presents a possible solution for this problem and also demonstrates, with implementation results, that this new vision is fairly possible to be used in Next Generation Mobile Network.**

I. INTRODUCTION

Next generation mobile network users will expect a complete integration of internet services, internet everywhere and always best connection paradigms in their future. The current IETF-sponsored mobile solution is Mobile IP [1] that is also becoming a standard for IP mobility in mobile networks. Mobile IP applied to IPv6 networks, also known as Mobile IPv6 [1], defines a new entity called Home Agent (HA). This mobility entity is responsible to handle all the packets on the home network on behalf of the Mobile Terminal. In these mobility solutions the Mobile Host has two different IPv6 addresses, the *home address*, referring to address in the home network, and the care-of-address, referring to the address in the foreign network. Packets destined to the Mobile Host are intercepted by the Home Agent and tunnelled towards the Mobile Host in the foreign network using its care-of address. This mechanism allows the users to roam outside their home networks to other networks. However, the Mobile IP strategy it is not perfect and can fall, e.g., in inefficient routing paths or in triangular routing paths. Thus, Mobile IP provides support for IP mobility but does not make efficient use of network resources.

The Mobile IP paradigm has been enhanced to provide robustness and efficient usage of network resources. As extensions, these Routing Optimizations guarantee the direct communication between the Mobile Host and the Correspondent Terminal, and as a result a better and efficient routing path between both. Still, the mobile device's care-of address changes each time the user moves between neighbouring base stations, resulting in consequent notifications to the Home Agent and the Correspondent Terminals on every handoff by a Binding Update message. In addition, if the Mobile Host is quality-of-service (QoS) enabled, acquiring a new care-of address on every handoff would trigger the establishment of new QoS reservations from the Home Address to the care-of-address even if most of the path remains unchanged.

Since Mobile IP *per se* could not respond to the needs of next generation mobile networks, many protocols were developed trying to overcome its faults. Hierarchical Mobile IPv6 (HMIPv6) [2] is a mobility protocol based on hierarchical relations between mobility agents called Mobility Anchor Points (MAP). In this type of architecture the Mobile Host can acquire a Regional Care-of-Address (RCoA) that allows it to move in the same region without changing its global mobility Care-of-Address (CoA). This mechanism addresses a better way to handle mobility signalling, providing better performance during the handover and reducing the overhead caused by the global mobility signalling messages. This enhancement occurs because the Mobile Host does not need to send a Binding Update message to its Home Agent after the handover execution between Access Routers (AR) in the same HMIP region. On the other hand, HMIPv6 compels the Mobile Host to acquire a new RCoA after the handovers, and a global mobility Care-of-Address after an inter-region handover. Still, HMIPv6 reduces the global signalling during the handovers, but harms the handover timings when the Mobile Host moves between different HMIP regions due the time wasted updating all the MAPs on the network.

Fast Mobile IPv6 (FMIPv6) [3] is a mobility protocol developed to accelerate the handover procedure allowing the reduction of handover time. In opposite to HMIPv6, the FMIPv6 architecture is not hierarchical and does not organize its agents in regions, but it reduces the effective packet loss during handover. FMIPv6 integrates a mechanism of predictive handover that enables the network to prepare the new AR to the Mobile Host arrival. Thus, the Mobile Host context is transferred between the old AR and new AR and the Mobile Host is prepared and pre-configured to be compliant with the new network configuration before the handover execution. This predictive mechanism allows the seamless handovers between Access Routers and avoids the Mobile Host configuration time right after the handover. Nevertheless,

FMIPv6 is an enhancement of MIP with fast and predictive handovers but this is not enough to fulfil the fast local mobility requirements: when a Mobile Host moves between Access Routers, it needs to acquire a new CoA and send a Fast Binding Update (FBU) to its Home Agent. This fact compels the Mobile Host to reconfigure its IP configuration increasing the blackout time. Besides, this also increases the signalling traffic in the global network and especially in the access network wasting core network resources and radio resources.

HMIPv6 with Fast Handovers (FHMIPv6) [12] is an extension of classical HMIPv6 with fast handover capabilities. This enhancement provides the ability of predict the handover inside and outside the HMIPv6 regions. Consequently, it is possible to prepare the new AR with the Mobile Host context and also pre-configure the Mobile Host to be compliant with the new IPv6 network configuration. These improvements will minimize the handover time between different AR and will almost avoid the blackout time. The combination of HMIP and FMIP is almost perfect; still, as the Mobile Host needs to change its RCoA whenever it moves between ARs, it will send a Fast Binding Update packet every time its IPv6 configuration changes. This procedure will waste network resources especially radio network resources, and after all, it does not fulfil the efficient use of network resources requirement.

On the other hand, micro-mobility protocols such as Cellular IPv6 (CIPv6) [4] and Handoff-Aware Wireless Access Internet Infrastructure (HAVAII) [5] attempt to provide better mechanisms to support IP mobility based in the assumption that Mobile Terminals constantly move inside a restricted and small micro areas, also known as micro-domains. Cellular IPv6 is an extension to the MIPv6 protocol, and its main objective is to provide better results in handover timings while the Mobile Host moves in nearby regions. In Cellular IPv6 the Mobile Host does not change its IPv6 address while it moves between Base Stations (BS) of the same cell. This fact improves the handover procedure since the handover signalling and handover signalling propagation timings do not exist. Nonetheless, Cellular IPv6 (as well as the HAVAII) needs to solve the latency applied in the packet transition while travelling along the micro-domain network, as well as substantial wireless resources wasted caused by the micro-mobility related signalling. These two facts reduce significantly the performances of the access network and waste to much radio resources in 4G scenarios making it difficult to handle traffic flows like multimedia and real-time IP traffics with several users under high mobility.

Typically, Mobile IP and its mobility extensions are fairly poor efficient when applied to wide-area wireless networks under high mobility scenarios with QoS requirements. In this paper we present a new approach to solve these limitations, which hinges on the assumption that most user mobility is local. Consequently, our approach, Local-centric Mobility System (LMS), extend the concept of local mobility with cellular network concepts such as paging and idle/active Mobile Host modes. It implements a localized mobility management architecture that aims for the: minimization of the handover timings and related signalling; reduction of packet losses during the handover; increased efficiency in wireless and core network resources usage; increased efficiency in wireless and core network resources usage; and integration of mechanisms for AAAC support

II. DESIGN GOALS

In our approach, LMS, we had five goals:

- *Fast, Predictive and Seamless Handovers* – architect a new mechanism to provide predictive handovers with context transfer between Access Routers in order to prepare the foreign network to receive the Mobile Terminal, resulting in seamless and fast handover.
- *Moving without changing the IPv6 address* – design a network architecture that provides support for mobility without changing IPv6 address, resulting in less signaling and fast handovers between Access Routers.
- *Provide scalability* – Network architecture able to be scalable and also able to support many Mobile Terminals.
- *Enhance the security and robustness of the protocol* – design security mechanisms to prevent attacks against the normal functioning of the protocol and also prevent personification and privacy attacks.
- *Access control, Authorization, Accounting and Charging (AAAC)* – provide access control during the registration and handover procedures; authorization for actions, for a instance, handover request; accounting of network usage and charging.

III. LOCAL-CENTRIC MOBILITY SYSTEM ARCHITECTURE

In network operator scenarios, network architecture is one of the more important aspects that should be correctly designed to minimize IP routing paths, propagation delays and to increase robustness and scalability. Typically in the current cellular networks, defined by 3rd Generation Partnership Project (3GPP), the architecture is hierarchically designed to handle different cells with multiple mobile terminals. In 3G networks, the Gateway GPRS Support Node (GGSN) is on top of the routing path hierarchy with several Service GPRS Support Nodes (SGSN) at its bottom, serving different base stations. This hierarchy provides a stable and scalable architecture that can handle millions of mobile terminals along considerable distances. In the LMS architecture we inspire our approach in this concept in order to guarantee the maximum scalability, stability and robustness. The LMS architecture is based in three different levels: access

wireless network; micro-domain core network; backbone core network.

In each architectural level there is a different type of agent. The LMS agents are:

1 .*MT – Mobile Host@Access Network*: this agent is responsible to enable the terminal to get connected in the access network.

2. *BS – Base Station@Access Network*: this agent is responsible for the packet filtering between the core access network and the edge access network. The core access network connects all access agents, all BS and the MAP; the edge access network connects all Mobile Hosts and BS.

3 .*MAP – Mobility Anchor Point@Micro-Domain:* this agent is responsible for the management of all the intra-domain tasks. These tasks concern the access control during the intra-domain handovers and accounting procedures during the intra-domain hosting. This agent is also responsible for all the BS state-full auto-configuration.

4 .*MMP – Mobility Management Point@Core Network*: this agent is responsible for the management of all the authorization, inter-domain authentication, accounting aggregation and charging related tasks. This agent is also responsible for all MAPs state-full auto-configuration.

Figure 1 shows how a LMS network is organized in a top down point of view, starting at the HA (Home Agent) in the global mobility area and ending on the Mobile Host that is embedded in the LMS micro-domain.

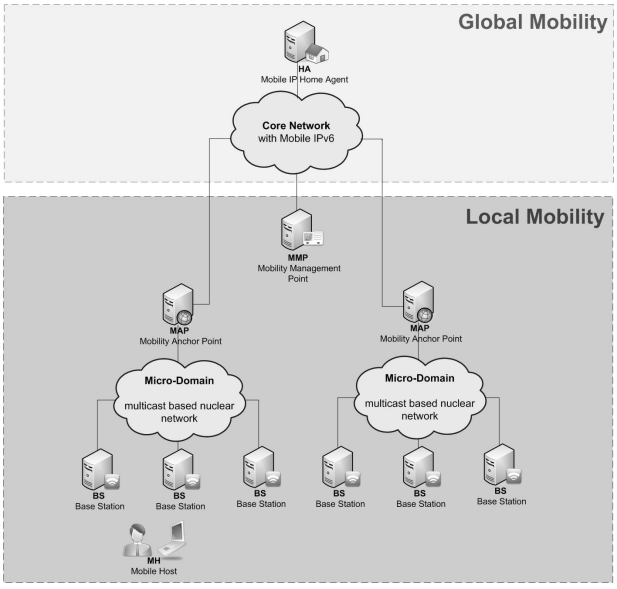

Figure 1 – Global Mobility and Local Mobility in LMS

As shown in Figure 1 the LMS architecture provides a distributed organization of the micro-domains in the operator network. In LMS networks, each micro-domain could be controller as an autonomous administrative domain based on the MMP policies. The MMP agent stores policies regarding security and Quality-of-Service (QoS) for each micro-domain and also for each mobile user on the network. Compared with the current Third Generation Partnership Project (3GPP) [15] definition in LMS architecture the MMP agent is similar to the 3GPP Home Subscriber Server (HSS), however the MMP agent has also additional functionalities over the HSS base capabilities.

IV. MICRO-DOMAINS IN LMS ARCHITECURE

The LMS architecture is organized in several micro-domains, each one can be autonomously managed. LMS architecture also defines two types of micro-domains, "restricted" and "public" micro-domains. A public micro-domain can be accessed by any mobile host registered on the network and does not had any type of access control. On the other hand, a restricted micro-domain can only be visited by authorized mobile hosts. This control is provided based on MMP policies and can be fully defined by the network operator per user and micro-domain.

Figure 2 shows how LMS cells can be organized in a heterogeneous type of access areas, as can be seen in the black areas in the figure. This strategy improves the security scalability of operator network architectures and also the differentiated network service since all the access conditions are based on MMP policies managed in the central data base.

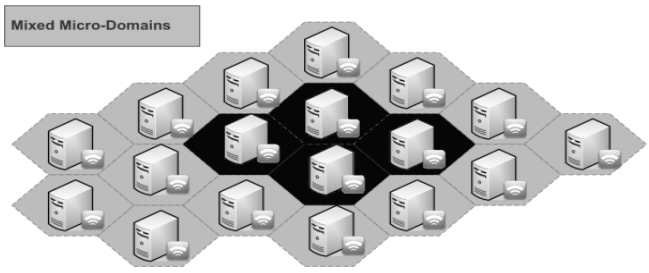

Figure 2 – Global Mobility And Local Mobility in LMS

In the LMS architecture, a micro-domain is not necessarily continuous in a geographical area. The micro-domains are constituted by several paging areas and each one by several cells. The communication between cells and between paging areas is provided in virtual link basis. Thus, the relation between cells and paging areas in the micro-domain are always logical and can be geographically distinct.

The network topology of a micro-domain is hierarchical and it is based in two levels. On the top level there is the MAP that manages all the micro-domain tasks and also forwards the data packages to the core network. At the lower level there are BSs that make the connection between Mobile Hosts and core micro-domain network. The BS's in the micro-domains are further grouped in paging areas. Each paging area is used to group mobile hosts in sub-regions in the micro-domains: this is especially important when the Mobile Host is in idle mode and it is necessary to route IP packets to it. We support the

wireless concept of paging that can be mapped to paging at the L2 layer at each BS. The duality Active/Idle in the terminals also improves the power resource management that is one of the main concerns in next generation operator networks.

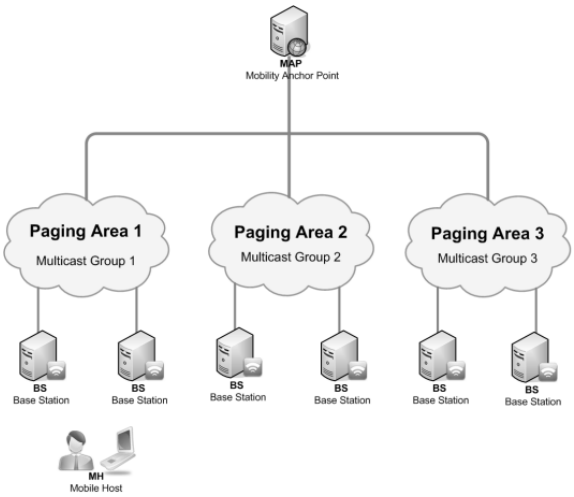

Figure 3 – LMS micro-domain architectural view

V. DATA TRANSMISSION INSIDE THE MICRO-DOMAIN

One of the most important issues in operator networks is resource optimization - efficient use of link resources. Thus, in LMS we developed a new mechanism to deliver data among the entire micro-domain avoiding data replication and improving the efficient use of network resources. This mechanism is based in IP Multicast tunnelling in a label switch basis that allows point to multi-point and also point to point data communication between micro-domain agents.

Figure 4 presents the main capabilities of this mechanism. Using multicast to transmit data allows several BS on the micro-domain to be reached without packet replication. This type of feature is very useful during the intra-micro-domain handovers of terminals running multimedia sessions. The architecture makes also possible the forwarding of packets of unicast sessions over this protocol reducing the use of the network resources, while reducing packet loss in handover. The packets that need to travel over the micro-domain network are encapsulated IP-over-IP in a multicast channel for the corresponding paging area. Each paging area is connected to MAP via a multicast channel that aggregates one set of BS. The multicast channels are managed by the MAP of each micro-domain that creates or removes the BS from the multicast groups dynamically. With this mechanism running on the LMS network it is possible to optimize the packet transmission during unicast and multicast sessions and improve the efficient use of network resources specially in handover situations.

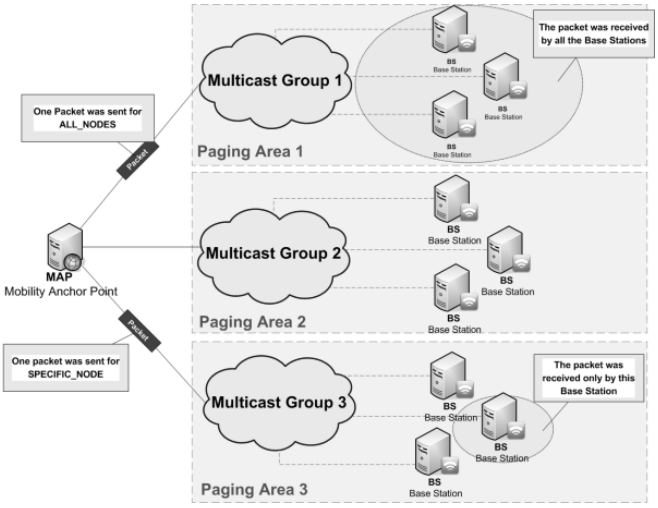

Figure 4 – LMS micro-domain core protocol

VI. SECURITY AND QUALITY OF SERVICE IN LMS

LMS aims to be an operator technology that provides fast local mobility, security and QoS functionalities. During the very first Mobile Host registration, the user profile is store in the central data base and can be always consulted by the MMP agent. This profile stores information regarding QoS reserved for this user and also security considerations.

The LMS does not integrate any extra security for Mobile Host data transmission but rely on existing security layers. Nevertheless, the LMS integrates cryptographic capabilities for internal signalling. The signaling packets of the protocol sent by Mobile Host are always authenticated with its PID. The PID is derived from the secret cryptographic key of the micro-domain network and it is generated by the MMP during the access registration on the micro-domain. This PID is generated applying a MD5 hash function on a set of bits that represent the Mobile Host (128 bits) and the network key (128 bits). The packets that contain confidential content are always encrypted and authenticated. This type of procedure ensures that most of the typical attacks over the access and control tasks of the micro-domain networks are avoided and the Mobile Hosts authenticity is secured.

When the Mobile Host wants to connect to the network it starts sending a Registration Request message that contains is personal identification that is encrypted with the private cryptographic key. This request is processed by the MMP that makes the decision based in the micro-domain restrictions (public/restrict access) and also based on the user profile stored in the central data base. If the Mobile Host is allowed to connect to the network, the MMP agent sends the correct policies to the specific micro-domain where it is attached on. Based on these policies the MAP agent can provide QoS functionalities in its micro-domain. When the Mobile Host aims to moves inside its micro-domain, the QoS policies

do not change and it is not necessary to request information from MMP; however when it moves to another micro-domain the MMP is contacted before the handover in order to provide authorization and also to notify the new micro-domain about the correct QoS policies.

The LMS architecture is based in two layers, the lower layer is constituted by all MAPs and manages the lower layer tasks like: Mobile Hosts flow control for accounting and intra-domain authentication control. Note that, as mentioned before, micro-domains can have access control, with a Mobile Host granularity. The higher layer is constituted by the MMP that merges all services reports from the MAPs, and manage all this information with any centralized agent.

MMP can be made compliant with protocols like Remote Authentication Dial in User Service (RADIUS), or can communicate directly with a LMS central data base. This data base can be a SQL based DBMS (Data Base Management System) that contains information about the micro-domains (MAPs and BS) for auto-configuration services; it can also contain information about Mobile Host authentication control, authorization services, accounting and charging. The main advantage of the usage of a central data base is that it can also store information about network agents' information (auto-setup info and agent info)

VII. LMS MOBILE HOST REGISTRATION

The registration of the Mobile Host occurs in two phases: operator database registration and network connection registration. The first phase occurs before any attempt of network connection. The Mobile Host makes a registration on the central database of the operator, storing its NAI and a Ticket_Key (alternatively this Ticket_Key may be a credential delivered by the operator to the Mobile Host, e.g. by a SIM card). These two fields can univocally identify this Mobile Host and will be used during authentication and authorizations requests.

The second phase occurs when the Mobile Host connects to the network. The Mobile Host sends an authenticated Registration Request to the network with the confidential information encrypted. The packet is forwarded to the MMP, as the BS and the MAP are not able to decrypt confidential information. For security reasons, the MMP is the only agent that can directly communicate with the operator database and, then, knows the TicketKey to decrypt the Registration Request packet.

After decrypting the packet, the MMP verifies if the Mobile Host is authorized to entry in that specific micro-domain. If not, the MMP sends a Registration Response with access denied. In the positive case, the MMP generates a PID for the Mobile Host and makes its registration on its caches and database. After this process, the MMP generates a new IPv6 for the Mobile Host based on the network-prefix IPv6 of the micro-domain and its MAC address. The MMP sends back the Registration Response with this information to the Mobile Host. While the packet travels the micro-domain network, the MAP will make the Mobile Host registration on the specific paging area that it aims to bind.

When the Mobile Host receives a positive registration response, it automatically sets up its configuration and starts to send heart beat packets to the network, necessary to avoid soft-state termination.

VIII. LMS HANDOVER MECHANISM

In the LMS architecture there are two types of handovers, the Intra Micro-Domain Handover, and the Inter Micro-Domain Handover.

A) Intra-micro-domain handover occur when a Mobile Host moves between two different BS on the same micro-domain. When the Mobile Host intends to initiate the handover, it sends a Handover Request message for the network. The Handover Request is an authenticated packet that informs the network about the new BS, new paging area and new network ID where the Mobile Host aims to move. The packet is sent for the old BS and it is forwarded to the MAP requesting a decision. When the MAP receives the packet, it knows that the Mobile Host intends to move on the same micro-domain network, because the new network ID in the Handover Request packet is the same of the current network ID.

In this type of handovers, the MAP does not need any third-party authorization from MMP to process the Handover Response. Thus, the MAP processes a Mobile Host registration on the new paging area of the micro-domain and sends a Paging Update packet to it over multicast channel. When a BS in this paging area receives the Paging Update, it makes a registration in its caches allowing this Mobile Host to bind in. The caches on the agents implement soft-states; after the Mobile Host chooses one, the others will be removed after some time.

After the Paging Update, the MAP sends a Handover Response allowing the Mobile Host to complete its handover to the new BS. The Mobile Host receives the packet, moves to the new BS, but does not need to change its network setup configuration (it only needs to change its routing table redirecting its traffic to the new BS). After this process, the Mobile Host sends periodically a heart beat packet to the new BS refreshing the soft-states.

If the Mobile Host is not able to predict its handover and send Handover Request related signalling, it can simply move to another BS and start its registration on the network again. In these cases, as the new BS does not know who the Mobile Host is, it needs to start a new registration. After its completion, the new registration on the network overlaps the previous one.

B) The inter-micro-domain handover happens when a Mobile Host moves between BS in different micro-domains. When the Mobile Host intends to initiate the handover, it sends a Handover Request to the old BS, as

before, which again forwards it to the MAP requesting a decision. The MAP, after receiving the Handover Request, knows that this handover is an inter-micro-domain handover through the new Network ID. In this case, the MAP needs to delegate this decision task to the MMP agent and forwards the packet towards it. When the MMP receives the packet, it verifies if this Mobile Host can access the new micro-domain network. In negative case, the MMP generates a Handover Response with an access denied response and sends it back to old MAP. In positive case, the MMP notifies the new MAP that a new Mobile Host will move to its micro-domain. If the new MAP is able to register the Mobile Host on its micro-domain, then it will send a message with positive information to MMP notifying it that the registration was made successfully; otherwise, it will send a negative response to it. Based on the new MAP response, the MMP generates a new PID and a new IPv6 address based on IP network prefix of the new micro-domain, and sends a Handover Response back to the old MAP. When the old MAP receives the Handover Response from MMP, it forwards the packet to the Mobile Host. In the case of a positive Handover Response, the MAP also removes this Mobile Host from its caches.

After receiving the Handover Response packet, the Mobile Host knows if it can move or not to the new micro-domain. In a positive case, the Mobile Host changes its setup configuration and after all, it moves to the new BS (it also keeps sending heart beat packets periodically). If this handover cannot be predicted, the Mobile Host needs to start a new registration on the network.

IX. LMS MAIN FEATURES

As we presented in this paper, the Local-centric Mobility System provides several advantages, which can be summarized as:

- *Localized architecture* – the LMS network is organized in semi-autonomous micro-domains providing very efficient local mobility support: the Mobile Host can move in the same micro-domain without changing the IPv6 address.
- *Low handover-related signalling* – in LMS, the handover-related signalling traffic is very low. As result, this technique especially improves the handover timings and network resources exploitation.
- *Handover improvements* – fast and seamless handover mechanisms with make-before-break techniques with very low (zero) packet losses are supported.
- *Efficient use of access resources* – the signalling packets across access network, shared between Mobile Hosts and BS, are small, improving the efficient use of wireless resources.
- *Efficient use of core resources* – LMS integrates a new packet-forwarding mechanism based on multicast services to improve core-network resources.
- *Support for heterogeneous access link technologies* - LMS is completely independent from the L2 technology, and can support multiple heterogeneous network link technologies.
- *Secure mobility management* – LMS supports security at the signalling level.
- *Access control on mobility actions* – LMS performs an explicit authorization before handovers to different micro-domains.
- *AAAC integrated services* – LMS provides intrinsic support for AAAC services.

X. PROTOTYPE TESTS AND RESULTS

The proposed LMS mechanism was prototyped for i386 machines, running GNU/Linux environments. The network was built with heterogeneous link technologies such as IEEE802.11 [16] and Ethernet. The IEEE802.11 link was used between the Mobile Host and Access Routers, the Ethernet links were used in the core network inside the micro-domain at 100MBit/s and outside with 10Mbit/s. All machines were set up in a laboratory, and therefore link propagation times were small – which may slightly bias the results. The machines in the test bed have the following hardware features:

- MH – Pentium DualCore (1.6GHz);
- BS – VIA (1.2GHz);
- MAP – AMD AthlonXP (1.9GHz);
- MMP – AMD AthlonXP (1.9GHz) ;
- CN – Pentium III (300MHz)

Figure 5 presents the network architecture used in the LMS prototype test bed.

The tests made in the test bed provided information about the impact of the handover in the Mobile Host connections for UDP and TCP traffic. The tests were made with network performance test tools, such as iPerf and mGen. We used the iPerf tool to test the network for real TCP traffic and study the impact of the handover in the TCP sequence numbering. The mGen packet generator was used to generate UDP traffic and measure the blackout experience during the handovers.

Figure 6 shows how real TCP traffic is affected by the handover situations in LMS. In the graphic of Figure 6 we can see that the handover does not affect too much the TCP sequence number, and therefore minimizes the TCP traffic disruption in the handoff moment.

Figure 7 shows how LMS handover affects UDP communications. The graphic shows the jitter (in seconds) of the UDP packets during the 5 (five) handovers. Since the jitter (in data packet communications) represents the time difference betweens two packets in the transmission, this graphic shows that during the handover the jitter between two packets is (in average) 68.7ms. This time also represents the real blackout time during the handovers in out LMS test bed.

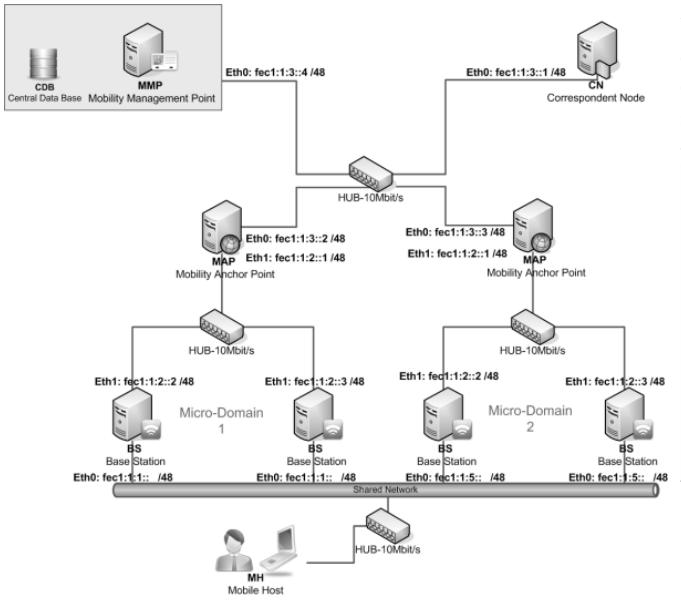

Figure 5 – LMS test bed architecture

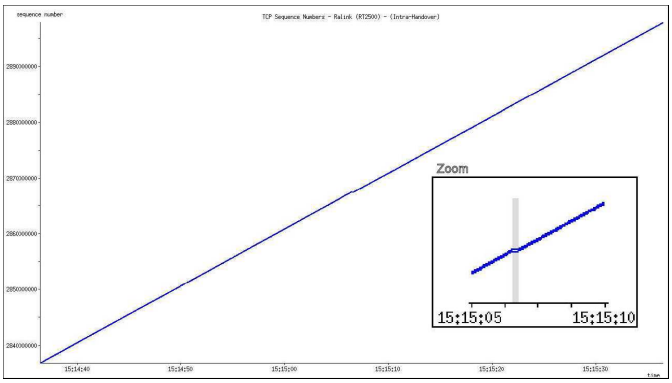

Figure 6 – Handover impact in TCP session

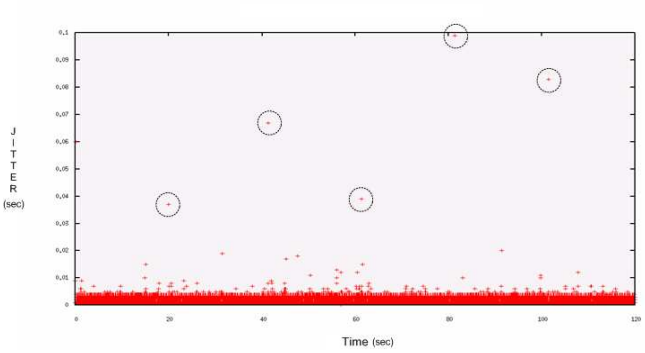

Figure 7 – Handover impact in UDP traffic. (Jitter)

The graphic of Figure 8 presents the packet loss relation in UDP traffic during 5 (five) handovers. As can be seen in the graphic the packet loss is always less than 10% (ten percent) which can provide seamless handovers with minimum service disruption. This also proves that LMS can provide a reliable, fast and seamless mechanisms for high mobility scenarios for next generations networks, allowing the terminals to receive multimedia content even during the handovers with a minimal impact on the service.

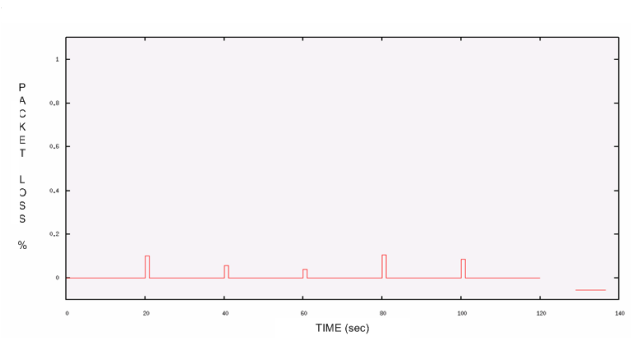

Figure 8 – Handover in UDP traffic. (Packet Loss)

The diagram of Figure 9 is a UML sequence diagram and presents the inter Micro-Domain handover procedures and also the times spent in each step

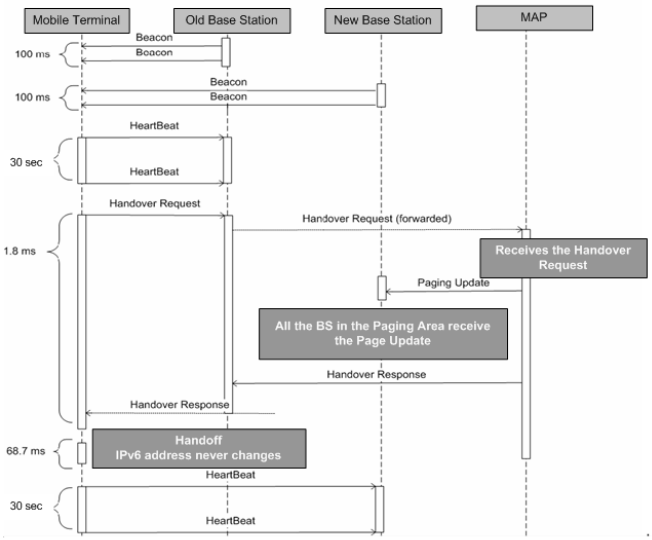

Figure 9 – Handover times in LMS scenarios

As can be seen in the diagram, the handover signalling and authorization process is completed after 1.8 ms. After, the radio handoff (blackout time) takes 68.7ms to be completed and in some cases case was higher that 100 ms. This time represents all the L2 (Layer 2) authentication and association mechanisms needed in wireless technologies (in this case IEEE802.11), and is independent of the LMS operation.

XI. PROTOCOL COMPARISION

The table below summarizes the characteristics of some mobility protocols and makes a comparison with the LMS – Local-Centric Mobility System. Note that the LMS architecture can be sufficiently distributed and also scalable enough to support a cellular operator network, and as thus can be seen as providing global mobility, while providing efficient localized mobility inside the micro-domains.

	CIP	HMIP	MIP	F-HMIP	FMIP	LMS
Local / Global	Local	Local	Glob.	Local	Glob.	Local
Fast Handover	**Yes**	No	No	**Yes**	**Yes**	**Yes**
Seamless HO	**Yes**	**Yes**	No	**Yes**	**Yes**	**Yes**
Efficient Use of Core Resources	No	**Yes**	No	**Yes**	No	**Yes**
Efficient Use of Link Resources	No	**Yes**	No	No	No	**Yes**
Minimize CoA changes during Handover	**Yes**	No	No	No	No	**Yes**

XI. CONCLUSIONS

This paper presents a novel approach for local mobility in next generation networks. The new concepts were tested in a test bed scenario and we presented in this paper the measured performance evaluation of LMS. Since the LMS provides a local mobility mechanism, it was designed to provide scalability, fast and seamless handovers, efficient exploitation of network resources and reliability. The LMS also provides some integrated QoS services that allow LMS to be easily integrated with the operator network requirements and also enhance handovers with predictive authentication mechanisms. Furthermore, it has a new mechanism for packet forwarding in the core network of micro-domains that increases the network performance especially during the handover situations. This protocol also presents a signalling mechanism that improves the exploitation of access network resources especially in wireless scenarios. Finally, it has some mechanisms to improve the security of network signalling without add extra security to data flows sent by Mobile Hosts.

The evaluation tests showed how LMS can solve some problematic aspects of the global mobility architecture and protocols. The LMS can minimize the handover timings from some hundreds of milliseconds (in a real mobility scenario) to less than 100ms in wireless scenarios, mostly remaining due to physically layer limitations. Packet loss during handover was also mostly negligible, and the network overhead was also minimized improving the efficient use of the core and wireless network resources. Concluding, the LMS shows that it can be possible to optimize the mobility mechanisms to improve the timings, avoid packet losses and make efficient use of network resources in mobility scenarios.

REFERENCES

[1] D. Johnson, C. Perkins. Mobility Support in IPv6.June 2004, RFC 3775

[2] Hesham Soliman et al. Hierarchical mobile IPv6 mobility management (hmipv6), IETF Internet RFC 4140, Aug 2005.

[3] R. Koodli. Fast Handovers for mobile IPv6, IETF Internet RFC 4068, July 2005.

[4] Zach D. Shelby, et al., Cellular IPv6, Internet draft, draft-shelby-seamoby-cellularipv6-00, November 2000.

[5] Ramjee, R. et al, HAWAII: a domain-based approach for supporting mobility inwide-area wireless network, IEEE/ACM Transactions on Networking, Volume: 10, Issue: 3, Jun 2002, pp. 396-410.

[6] J. Kempf, et all, Requirements and Gap Analysis for IP Local Mobility, draft-ietf-netlmm-nohost-req-01, February, 2006

[7] A.Campbell, J. Gomez, S. Kim, and C. Wan. Comparison of IP micro-mobility protocols. IEEE Wireless Communications, vol 9, pages 72–82, February 2002.

[8] Xavier Pérez-Costa, Marc Torrent-Moreno, Hannes Hartenstein, A Performance Comparison of Mobile IPv6, Hierarchical,Mobile IPv6, Fast Handovers for Mobile IPv6 and their Combination - Volume 7 , Issue 4 (October 2003)

[9] J. Gomez, "Design, Implementation and Evaluation of Cellular IP", IEEE Personal Communications, Vol. 7 No. 4, pg. 42-49, August 2000.

[10] Rui L. Aguiar, et al, Scalable QoS-aware Mobility for Future Mobile Operators, IEEE Communications Magazine, vol 44 n.6 pp 95-102, Jun 2006.

[11] IETF Netlmm Working Group, http://www.ietf.org/html.charters/netlmm-charter.html.

[12] Jung H., et al., "Fast Handover for Hierarchichal MIPv6 (F-HMIPv6)", draft-jung-mobileip-fastho-hmipv6-01.txt, IETF June 200

[13] IEEE Wireless Communications Magazine, vol. 9 - A. C. et. al., Comparison of IP Micro-Mobility protocols – February 2002

[14] D. Tang and M. Baker, Analysis of a Local-area Wireless Netowork ,ACM International Conference on Mobile Computing and Networking (MOBICOM), 2000

[15] 3GPP (04) - Network architecture, 3GPP TS 23.002 V6.4.0, june 2004.

[16] IEEE802.11 – IEEE802.11 Workgroup – URL: http://www.ieee802.org/11/