A Hybrid MIPv6 and PMIPv6 Distributed Mobility Management: the MEDIEVAL approach

Fabio Giust*†, Carlos J. Bernardos†, Sérgio Figueiredo‡, Pedro Neves§, Telemaco Melia¶
* Institute IMDEA Networks, Spain
E-mail: fabio.giust@imdea.org
† Universidad Carlos III de Madrid, Spain
E-mail: cjbc@it.uc3m.es
‡ Instituto de Telecomunicações de Aveiro, Portugal
E-mail: sfigueiredo@av.it.pt
§ Portugal Telecom Inovaçao, Portugal
E-mail: pedro-m-neves@ptinovacao.pt
¶ Alcatel-Lucent Bell Labs, France
E-mail: telemaco.melia@alcatel-lucent.com

***Abstract*—Video is a major challenge for the future mobile Internet as it is foreseen to account for close to 64% percent of consumer mobile traffic by 2013. However, the current Internet, and in particular the mobile Internet, was not designed with video requirements in mind and, as a consequence, its architecture is very inefficient when handling this type of traffic. This paper presents a novel mobility architecture inspired by the Distributed Mobility Management paradigm, capable of coping with the future video traffic demands, in a distributed and more scalable way. In the proposed solution, mobility support services are spread among several nodes at the edge of the network, thus realizing a flatter architecture and pushing services closer to the terminals. Our approach overcomes some of the major limitations of centralized IP mobility management solutions, by extending existing standard protocols.**

I. Introduction

Future mobile networks are expected to experience higher traffic demands from users and will need to be tailored for video traffic, which is foreseen to account for 64% of the overall mobile traffic by 2013 [1]. Already today, operators are suffering from the increasing number of wireless mobile subscribers accessing data services, and this is expected to increase even more in the near future. The enormous success of mobile multimedia-capable handsets equipped with 3G + WLAN interfaces, together with the flat rates offered by most of the mobile operators, have increased the demand for ubiquitous connectivity.

Operators are migrating their infrastructure to full-IP based networks – for both voice and data – and therefore they need efficient IP mobility solutions that could be used to handle user device mobility, not only between access networks of the same technology, but also between different networks of different technologies (e.g., to enable to opportunistically offload their congested 3G infrastructures to WLAN accesses).

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).

The EU project MultimEDia transport for mobIlE Video AppLications (MEDIEVAL[1]) aims to evolve today's mobile Internet architecture to more efficiently support the upcoming growth of video services. As part of this ambitious effort, current standardized IP mobility management solutions are being revisited, evolving into a new generation of mobility support which better meets current requirements while posing less scalability issues.

Most of the currently standardized IP mobility management solutions (which up to date have shown little or no deployment penetration), like Mobile IPv6 [2], or Proxy Mobile IPv6 [3] rely to a certain extent on a centralized mobility anchor entity. This centralized node is in charge of the mobility control and the users' data forwarding – that is, it is both the central point for data and user plane – therefore making current mobility solutions prone to several problems and limitations [4]. This has triggered big mobile operators to look for novel mobility management approaches which are more distributed in nature, and that allow to enable mobility on demand for particular types of traffic (instead of mobility enabled by default for all the traffic of a particular user). This effort has crystallized in what is known as *Distributed Mobility Management* (DMM).

In this paper we present the mobility architecture which is currently being defined within the MEDIEVAL project. Main characteristics of this evolved mobility architecture are: *i)* it follows a DMM approach, where mobility is anchored at the very edge of the network, *ii)* it adopts an hybrid approach, where network-based mobility management solutions (i.e., PMIPv6-alike) are used whenever possible, and client-based solutions are used otherwise (e.g., between different domains), and *iii)* due to the video-centric nature of the project, multicast traffic delivery and content distribution aspects are fully supported and integrated in the mobility management solution.

The rest of the paper is organized as follows. In Section II

[1] http://www.ict.medieval.eu/

we provide an overview of the most common examples of centralized mobility management, with an emphasis of the main limitations caused by such approach. Section III is dedicated to the detailed description of the hybrid distributed solution adopted in the MEDIEVAL architecture. Finally, Section IV concludes the paper.

II. Background and Motivation

A. Centralized Mobility Management: Mobile IPv6

Mobile IPv6 (MIPv6) [2] provides mobility support enabling global reachability and session continuity. A key component in this architecture is the Home Agent (HA), a server located at the Home Network of the Mobile Node (MN) which anchors the permanent IP address used by the MN, called Home Address (HoA). When away from its home network, the MN configures a temporal IP address from the foreign network's address space - called Care-of Address (CoA) - and updates its current location at the HA by means of a Binding Update (BU) message. Upon receiving the BU, the home agents responds with a Binding Acknowledgment (BA) message and an IP bi-directional tunnel between the MN and the HA is established, used to redirect traffic from and to the MN. An optional support to avoid routing packets through the HA, called Route Optimization (RO), was designed to allow the MN to also inform its communication peers - called Correspondent Nodes (CNs) - about its current location.

B. Centralized Mobility Management: Proxy Mobile IPv6

Unlike MIPv6, where the mobile node signals its location changes to the HA, Proxy Mobile IPv6 [3] provides mobility support to moving hosts without their involvement. This is achieved by relocating relevant functionality for mobility management from the MN to a network node called the Mobile Access Gateway (MAG), that is responsible of the mobility signaling to the Home Agent on the MN's behalf. MN's traffic is encapsulated and tunneled between MAGs and the MN's Home Agent, that in PMIPv6 is renamed as Local Mobility Anchor (LMA). In PMIPv6, the network learns through standard terminal operation, such as Router and Neighbor Discovery [5], or by means of link-layer support, about an MN's movement and coordinates routing state updates without any mobility specific support from the terminal. While moving inside the PMIPv6 domain, the MN keeps its IP address, and the network is in charge of updating its location in an efficient manner.

C. Limitations of centralized mobility management solutions

As described in previous section, current mobility management solutions, such as Mobile and Proxy Mobile IPv6, rely on the existence of a central entity anchoring both control and data plane. That is, the HA and LMA are in charge of tracking the location of the mobile nodes and redirecting traffic towards their current topological location. While these solutions have been fully developed during the past years, there are also several limitations that have been identified [4]:

- **Sub-optimal routing.** Data traffic always traverses the central anchor, regardless the current geographical position of the communication end-points. A video related example of the impact of this behavior is the following. Current content providers tend to push data to the edge of the network to optimize performance, but the use of a centralize mobility management approach would make user traffic to go first through the anchoring point, and then to the actual content location (hence vanishing the benefit of having a close content server). With a distributed mobility architecture, the anchors are located at the very edge of the network, so data paths tend to be shorter, both when the endpoints are in the same domain as in the example before, and for any other scenario.
- **Scalability problems.** In current mobility architectures, network links and nodes have to be provisioned to manage all the traffic traversing the central anchors. This poses several scalability and network design problems, with the growing number of mobile users. A distributed approach is more scalable, as the tasks are shared among several network entities, and not delegated to a powerful central node.
- **Reliability.** Centralized anchoring points (i.e., HAs and LMAs) represent a potential single point of failure.
- **Lack of fine granularity on the mobility management service.** Current solutions define mobility support on a per user basis. That is, the service is provided to user's communications as a whole. A finer granularity would allow, for example, that only those IP flows that really require it to benefit from session continuity.
- **Signaling overhead.** This is related to the previous limitation because mobility management involves a certain amount of signaling. If mobility support can be dynamically enabled and disabled on a per application basis, some location updates can be saved, as well as the associated handover latency. However, this is strictly related to the particular scenario and usage pattern, as a distributed mobility solution can also lead to a higher signaling load, in situations in which all the flows demand session continuity.

III. The MEDIEVAL mobility solution

The MEDIEVAL mobility architecture leverages on the concept of Distributed Mobility Management [4], for the development of both network-based and host-based mobility management. The access network is organized in Localized Mobility Domains (LMDs) in which the network-based scheme inspired by [6] is applied. Users are expected to be most of the time roaming within a single LMD, but, for those cases where this is not possible (e.g., roaming to a network owned by a different operator or running a different mobility support scheme), a host-based DMM approach is followed (e.g., based on [7]). In order to integrate both approaches, so that a mobile node can simultaneously have sessions managed by a network-based ("PMIPv6 alike") approach and a host-based ("DSMIPv6 alike") approach, we introduce a novel

architectural element called Mobile Access Router (MAR). An MAR is a network entity implementing all the functionalities of its counterparts in the standard mobility protocols (MIPv6 and PMIPv6), so it is able to play the role of plain access router, home agent, local mobility anchor and mobile access gateway on a per address basis.

Nevertheless, MEDIEVAL project poses new challenges in distributing video content with defined Quality of Experience (QoE) requirements. In order to be able to always guarantee these requirements, users' traffic might be redirected or offloaded looking for the best network and terminal conditions for video transmission. This feature affects the mobility architecture because some controllers in the terminal and in the network are needed to monitor the status of the connection and to take handover decisions if necessary. These controllers are the Connection Manager in the user terminal and the Flow Manager in the MAR. We will describe in the following subsections the details of these controllers and the operations performed to support unicast and multicast mobility.

A. Connection Manager

The Connection Manager (CM) runs in the mobile terminal only, and is devoted to trigger/coordinate the Mobility Engines and to interact with other functional blocks of the general architecture, fulfilling several tasks to optimize both the handover phase and the video transport.

The CM is an IEEE 802.21 [8] MIH user implemented to enable vertical handover in the terminal, i.e. to switch from one radio interface to another (or eventually use both) and thus collects information from below IP layers which may help in handover decisions and flow mobility handling. This information includes the availability of access networks in a geographical area, link-layer parameters information to assist in network selection, information related to 802.21, such as Point of Access (PoA) capabilities and indication of supported high-layer services (e.g., indication that a PoA supports some kind of multicast optimization and/or is able to provide specific transport optimizations).

The Connection Manager also supports ALTO protocol [9] functionalities to discover which is the optimal content cache from available ones. This ALTO interaction between the CM and functional blocks in the network is activated in the preparation phase of the handover or when a new PoA is available (e.g., on a different radio interface). Finally, the CM runs a decision engine in charge to take flow handover decisions triggered by user mobility. Using the information collected by the aforementioned functions, the CM is able to determine what is the best scenario for the terminal in terms of both radio conditions and network usage.

B. Flow Manager

The Flow Manager (FM) is responsible for controlling all the handover phases at a flow-level, including the always critical target network selection, as well as the interface with the distributed mobility management protocol. The mobility procedures are only activated for flows/services that effectively require session continuity. From the architecture point of view, to comply with the distributed mobility management approach, the FM is a distributed network-side entity running on each MAR. It interacts with a Content Adaptation module to adapt the flow to the network conditions of the target network. Moreover, it interfaces with the Content Delivery Network (CDN) controller to receive mobility triggers when the caches are overloaded. The FM interfaces are extended versions of the 802.21 and the ALTO standardized protocols. Figure 1 provides a high-level overview of the FM main functionalities and interactions.

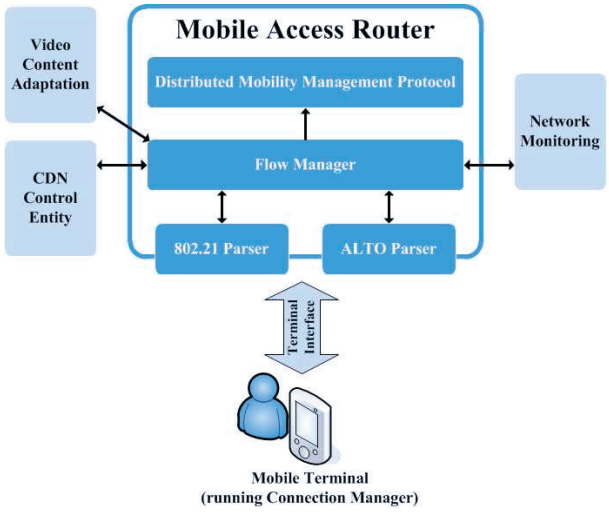

Fig. 1. Flow Manager Architecture

Hereafter a handover procedure due to network congestion is depicted to describe the role of the FM in the overall procedure. The CDN controller detects that a cache is overloaded and informs the FM to move a specific set of flows that are crossing the CDN. The FM looks for the available surrounding networks and queries their resources availability. Thereafter it provides the resulting set of candidate access networks to the CDN controller, which weights each one of the provided candidate networks (based on CDNs availability) and sends the ordered list back to the FM. Finally, the FM triggers the distributed mobility management protocol on the network side (e.g., PMIPv6) or on the client side (e.g., DSMIPv6) through the CM.

C. Unicast mobility support

As early mentioned, the MEDIEVAL mobility architecture adopts a distributed approach using a special network entity called MAR. A MAR can be deployed at various levels of the network hierarchy, achieving different degrees of distribution. For instance, having as a reference the Evolved Packet System (EPS) architecture, the number of deployed anchors would range from a few – if MARs are deployed in the Packet Data Network Gateway (PGW) – to a larger number as pushing them to the network edge – for example if MARs are implemented in the Serving Gateway (SGW) or even in the evolved Nodes B (eNB). In the rest of the paper we assume

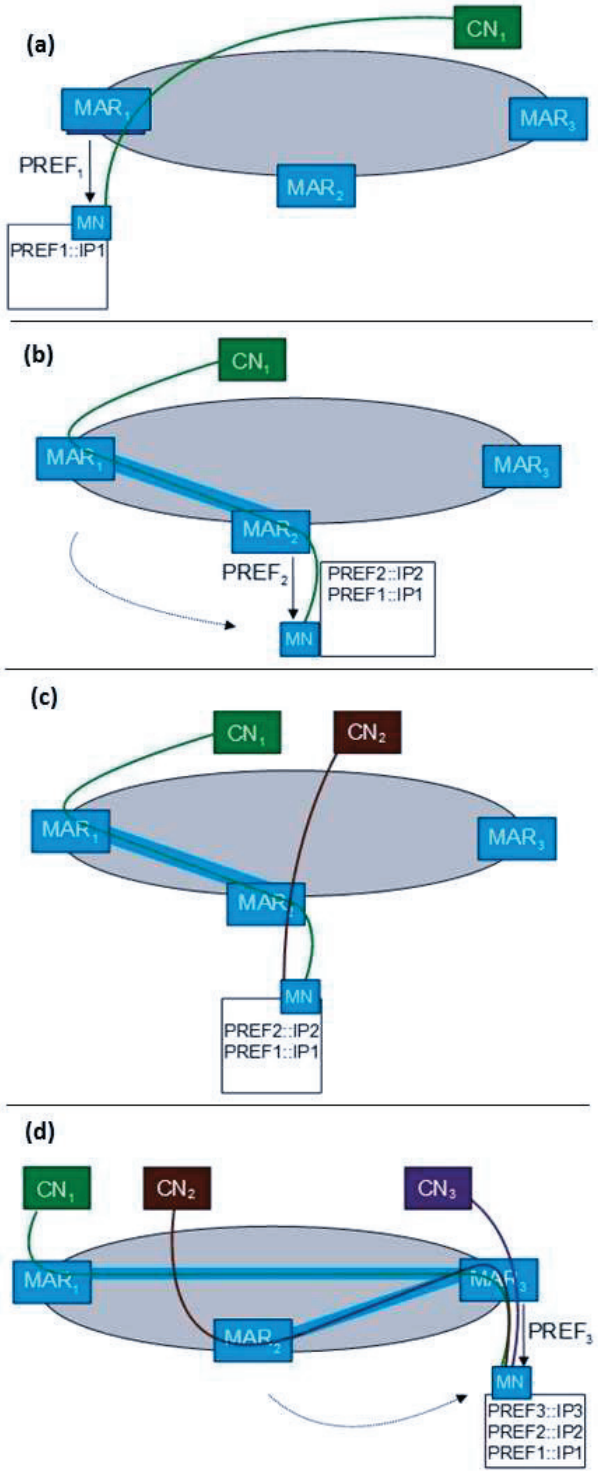

Fig. 2. Distributed Localized Mobility Domain and example scenarios

the MAR is deployed in the access router of the mobile nodes, that is, the first hop router of the terminals.

The MNs are assumed to spend most of the time within an LMD (at least for the same service). While an MN is in an LMD domain, it gets a different set of IP addresses when changes its point of attachment, as compared to what happens in PMIPv6. In fact, upon layer-2 attachment, the MN learns, through standard Neighbor Discovery operations [5], the MAR to which it has attached, and consequently configures an IPv6 address using the prefix advertised by the MAR. For the sake of simplicity we consider that the MN configures only one address per each visited MAR. When the MN starts a communication (an IP flow) with a Correspondent Node (CN), it selects as source the IP address that has just been configured at its current MAR. In this sense, the new IP flow is topologically anchored at the MAR which advertised the prefix the MN is using, and normal IPv6 routing takes place, without any tunneling nor special packet handling performed by the MAR, see Figure 2-a.

In case the MN changes its point of attachment (see Figure 2-b and c) due to user movement or triggered by the network, a different prefix is advertised by the new MAR and the MN configures another IP address. This address is used to start new communications, while the old address can be kept if the MN wants to maintain previous IP flows alive. Since ongoing flows are anchored at the previous MAR, a tunnel is built between the old MAR and the current one, so that packets can be redirected to the current location of the MN. Note how this behavior resembles PMIPv6: previous MAR acts as the LMA anchoring the prefix it advertised, while the serving MAR plays the role of a MAG when handling traffic using that prefix, but, in addition to PMIPv6, it also behaves as a standard router for the flows started with the new address. The node acting as LMA has to store an entry with the binding between the MN's current location and the prefix it advertised. This data structure can be inherited from PMIPv6 protocol, as well as the signaling between the nodes needed to perform the tunnel creation and location update (Proxy Binding Update/Proxy Binding Acknowledgment handshake).

When another handover occurs, previous MARs establish a tunnel with the serving MAR if the ongoing flows must be maintained, while new communications are started with the prefix advertised by the current MAR (Figure 2-d). This mechanism allows maintaining mobility sessions on a per flow basis, that is, only for those IP flows that really require mobility support, and can be extended to allow flow mobility for load balancing or traffic offloading.

The MEDIEVAL architecture comprises the use of IEEE 802.21 standard to assist the mobile node in the handover phase. The Media Independent Handover protocol both provides support to vertical handover and network selection, as seen in previous subsections, but in this context it is also used to propagate useful information to the MARs, such as source and target MARs' IP addresses, without introducing new mobility options nor mobility messages in the sets already defined in [2], [3]. For instance, without this mechanism, since no central mobility agents are used, a MAR serving a new MN should query (eventually by flooding) neighboring MARs to discover if the MN has already active sessions anchored to them.

A mobile node changes address while moving among different access networks and poses some issues in reachability

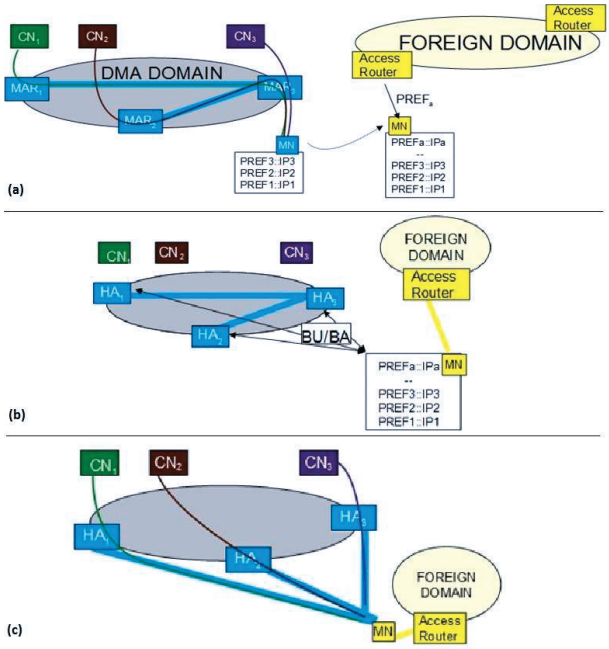

Fig. 3. Distributed host-based mobility management

when it is contacted as a server. Indeed, in the description above it is assumed that the MN starts the communication first, so the correspondent node learns the MN's address automatically and keeps on using that address for the whole duration of the flow. In order to keep the MN always reachable, a rendez-vous infrastructure can be used, in which the address configured after the first attachment is stored, in association with the MN's current location, and subsequently updated by the MN itself after moving. Alternatively, the MN can use Dynamic DNS mechanism [10].

There might be a case in which the MN moves outside the current LMD, attaching to a new network (the yellow one in Figure 3-a) that either belongs to another operator, or does not support the mobility management described. In such situation the connection manager in the terminal deviates from the mechanism described before and activates a client for mobility management similar to MIPv6. By doing this, instead of moving the tunnels to another router, they are moved to the MN itself, with the MARs acting as home agents, as shown in Figures 3-b,c, and the MN performing the required signaling instead of the serving MAR. [7] provides a complete description for host-based distributed mobility management, and that solution can be applied with minor variations to this scenario.

D. Multicast mobility support

Multicast is increasingly being seen as a key mechanism for big data delivery, in particular video: the larger the content, the worst its effect when replicated in the network.

Regarding MEDIEVAL's architecture, the Multicast Mobility Engine (MME) is the logical block responsible for multicast operations. The considered multicast routing protocol is Protocol Independent Multicast Sparse-mode (PIM-SM), using either any-source or source-specific models. Only intra-LMD mobility is considered, which maps to network-based mobility scenarios. As such, the Flow Manager triggers MME for multicast flow mobility, which should result in different operations for multicast sources and listeners: for instance, the mobility of a listener may trigger a Context Transfer by the MME, while the mobility of a source could lead to a (source-aware) modified PBU being sent to a MAR. Thus, the MME acts on behalf of the Flow manager, which is responsible for storing information about multicast flows properties, such as IP multicast group addresses, corresponding sources (in PIM-SSM) and multicast trees Rendezvous Points (RPs). Below, multicast mobility both from the video listener and from the source perspective are analyzed.

1) Multicast Listener mobility: Significant standardization efforts are currently being dedicated to the study of multicast support in mobility scenarios. Within IETF's MULTIMOB WG a base solution for PMIPv6 has been defined [11], which consists in the MAGs acting as MLD proxies and the LMAs as multicast routers, with the PBU/PBA triggering the multicast information update with little or no intervention from the MN. However, this approach does not avoid non-negligible delays in the multicast service during the MN handover, and raises the tunnel convergence problem.

While the application of DMM concepts helps in solving some multicast-related issues, it also raises or exacerbates others. Namely, PMIPv6 mechanisms cannot be trivially used in DMM because the tunnel convergence problem would become a dominant side-effect. The PMIPv6 tunnel convergence problem appears when an MN handoffs to a new MAG which is also relaying the same multicast stream to multiple users associated to different LMAs. As for each LMA a different tunnel will exist, this behaviour is against the multicast principle for which a node in the multicast tree should receive the multicast stream only once. While this is a moderate problem in PMIPv6 since the deployment estimation is about 4 LMAs for 10^6 users, applying DMM concepts will lead to a large number of MARs per network. Thus, the convergence problem becomes more severe with the number of more flows keeping mobility state, as more replication per MAR would exist.

In order to tackle multicast support in DMM, the following requirements within MEDIEVAL were identified:

- All the MARs implement multicast router instances according to the MLD suite.
- A message exchange between MARs must occur in order to allow multicast context transfer.

With the above, an MN is able to receive multicast traffic while moving, as the MAR it is currently attached to is responsible of managing the MN's multicast subscription, with minimal or no intervention from the MN (even after handoff). Specific issues that need to be tackled include:

- The multicast context transfer message format, which can be similar to the one in [12].
- When the MN goes out of the DMM domain it might happen that the MN must restart the MLD procedure

because the new attaching point either is not a multicast router or, for any reason, is not capable to interpret multicast context transfer.

2) Multicast Source Mobility: MEDIEVAL is also investigating source multicast mobility within PMIPv6. While the use of this protocol exempts the MN from sending mobility signaling, it also results in other problems, such as triangular routing in scenarios where multicast listeners connect to the same MAG as the multicast source. Within a scenario of source specific multicast (SSM), mobility results in problems such as tree reconfiguration and packet loss. In [13], two schemes for source mobility support are proposed: LMA-based and MAG-based. The former is the easiest to deploy and brings more advantages in mobile scenarios, but when to use Rendezvous Point Tree (RPT) or Shortest Path Tree (SPT) needs to be evaluated; the latter for example, allows for setting the LMA as the RP, preventing the tree reconstruction in case of mobility.

Using a DMM-based solution brings some of the advantages of PMIPv6. By setting the mobility anchor as the router where the flow was initially created, any mobility process leads to a stage where the current MAR is analogous to the MAG, while the anchor MAR is analogous to the LMA for the considered flow, which is beneficial from a multicast source point of view. A possible solution is the use of a tunnel between the current MAR and the MAR that is anchoring the address used as source address of the multicast transmission. The combination of the mobility anchor with the multicast tree RP, similarly to setting the LMA as RP in PMIPv6, will be evaluated. In this way, multicast tree reconstruction, which brings severe latency and packet loss, can be avoided.

As referred in previous sections, MEDIEVAL's architecture is supported by 802.21 MIH, and will also aim to enhance the standard (e.g., by adding new Information Elements). One of these enhancements is the proposal of multicast transport for 802.21 signaling [14]. Such mechanism is scoped for scenarios where multiple users within the same area have a common attribute (e.g., use the same application). Issues that need to be addressed include reliability, where one possible solution is the aggregation of MNs responses in bitmaps.

IV. Conclusion

While mobile network's data traffic is expected to greatly increase in the upcoming years, current mobility management solutions might not be able to provide the support in an efficient way, due to their centralized nature relying on a cardinal anchor in charge of both data and control plane.

In this paper we investigated a mobility management scheme inspired by the *Distributed Mobility Management* approach, that leverages on the hybrid use of PMIPv6 and MIPv6 in their distributed and dynamic flavors that are currently being proposed in the IETF research community.

The proposed solution is currently being defined and refined within a more ambitious effort: the MEDIEVAL project, which aims at optimizing video transport in mobile networks. Within this scope some extra entities and functional blocks are needed in order to communicate with the mobility stack and the other architectural elements. For this purpose we introduced the Connection Manager on the terminal side and the Flow managers on the network side, that with a wise coupling of 802.21 MIH features and other sophisticated techniques are capable to assist and coordinate the mobile terminal during its consumption of video traffic, aiming at optimize video transport according to the best joint network usage and radio conditions. The MEDIEVAL project will evaluate, implement and validate some of the mobility mechanisms proposed in this paper, as well as propose the defined extensions in the appropriate standardization bodies.

References

[1] E. Schonfeld, "Cisco: By 2013 Video Will Be 90 Percent Of All Consumer IP Traffic And 64 Percent of Mobile," Jun. 2009. [Online]. Available: http://techcrunch.com/

[2] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," RFC 3775, Jun. 2004.

[3] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, "Proxy Mobile IPv6," RFC 5213, Aug. 2008.

[4] H. Chan, "Problem statement for distributed and dynamic mobility management," Internet-Draft (work in progress), draft-chan-distributed-mobility-ps-02.txt, Mar. 2011.

[5] T. Narten, E. Nordmark, W. Simpson, and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)," RFC 4861, Sep. 2007.

[6] P. Seite, "Dynamic Mobility Anchoring," Internet-Draft (work in progress), draft-seite-netext-dma-00.txt, May 2010.

[7] F. Giust, A. De La Oliva, and C. J. Bernardos, "Flat access and mobility architecture: an IPv6 distributed client mobility management solution," in *2011 IEEE INFOCOM MobiWorld Workshop*, Apr. 2011.

[8] 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.

[9] R. Alimi *et al.*, "Alto protocol," Internet-Draft (work in progress), draft-ietf-alto-protocol-07.txt, Mar. 2011.

[10] P. Vixie, S. Thomson, Y. Rekhter, and J. Bound, "Dynamic Updates in the Domain Name System (DNS UPDATE)," RFC 2136 (Proposed Standard), Apr. 1997.

[11] T. C. Schmidt, M. Waehlisch, and S. Krishnan, "Base deployment for multicast listener support in pmipv6 domains," Internet-Draft (work in progress), draft-ietf-multimob-pmipv6-base-solution-07, Dec. 2010.

[12] L. M. Contreras, C. J. Bernardos, and I. Soto, "Rapid acquisition of the mn multicast subscription after handover," Internet-Draft (work in progress), draft-contreras-multimob-rams-00.txt, Jun. 2010.

[13] H.-K. Zhang, Z.-W. Yan, S. Gao, L.-L. Wang, Q. Wu, and H.-W. Li, "Multicast source mobility support in pmipv6 network," Internet-Draft (work in progress), draft-zhang-multimob-msm-02.txt, Mar. 2011.

[14] D. Corujo, S. Figueiredo, and R. L. Aguiar, "Media-Independent Multicast Signaling for Enhanced Video Performance in the MEDIEVAL Project," in *Future Internet and Mobile Summit 2011*, Jun. 2011.