QoS in Next Generation Mobile Networks: An Analytical Study

Javier Carmona-Murillo, José-Luis González-Sánchez, David Cortés-Polo, and Francisco-Javier Rodríguez-Pérez

GITACA Research Group, University of Extremadura, Spain

Abstract. Two of the major challenges for next-generation mobile systems are to achieve seamless mobility management in next generation wireless networks and to manage resources efficiently given the exponential growth that mobile data traffic has experienced over the last few years. To track host mobility, the IETF has made important efforts to develop mobility management protocols such as Mobile IPv6 and Proxy Mobile IPv6. These protocols establish a tunnel to connect the mobile node with its correspondent node. The tunneling method provided by MPLS can be profitably used to take advantage of MPLS traffic engineering capabilities in order to achieve faster re-routing when a mobile node changes its point of attachment to the network. Moreover, in order to deal with increasing mobile traffic demand, mobility management network architectures are being redesigned towards a more distributed operation. Given these scenarios, service disruption during handoffs continues to cause excessive packet loss that needs minimizing in order to support quality of service requirements for emerging applications. In this paper, a qualitative and quantitative analyses of the most representative host-based and network-based mobility management approaches is presented, including recent distributed mobility management approaches.

1 Introduction

The design of Next Generation Wireless Networks (NGWN) has two main goals. First of all, the possibility of maintaining connectivity while a user moves among heterogeneous networks. Secondly, the ability to provide a similar level of QoS (Quality of Service) while the node moves between these networks [1]. In order to achieve the first goal, the Internet Engineering Task Force (IETF) designed Mobile IPv6 [2] and Proxy Mobile IPv6 [3] to overcome the problems caused by handover in heterogeneous networks. Mobile IP (MIP) and Proxy Mobile IPv6 (PMIP) are widely accepted as the most appropriate protocols for addressing IP mobility management in future wireless mobile networks.

The second problem, related to the provisioning of enough network resources, has largely been studied in both wired and wireless environments. There are three general models used to provide network resources for quality of service (QoS) guarantees in the Internet: integrated services (IntServ), differentiated services (DiffServ) and MPLS (Multi-Protocol Label Switching) [4]. IntServ can provide quantitative QoS

C.X. Mavromoustakis et al. (eds.), *Resource Management in Mobile Computing Environments*, Modeling and Optimization in Science and Technologies 3,
DOI: 10.1007/978-3-319-06704-9_2, © Springer International Publishing Switzerland 2014

guarantees to individual flows and DiffServ can provide qualitative QoS guarantees to multiple flows in an aggregate way. For its part, MPLS is a QoS technology with traffic engineering (TE) introduced to enhance the performance of the Internet's datagram model in terms of both management and delivery [5].

The integration of Mobile IP and Multiprotocol Label Switching has worked successfully due to the ability of MPLS to engineer efficient traffic tunnels, including constraint-based routing, survivability and recovery, thus avoiding congestion and enabling an efficient use of the available bandwidth. These features highlight the potential of MPLS for solving MIP's operational and architectural shortcomings such as: high handoff latency [5] and packet loss or high global signaling load and scalability issues. MPLS could also be viewed as a tunneling technology that overcomes the tunneling techniques proposed in Mobile IP standard. For this reason, it has been proposed to use both technologies together [7-10].

Moreover, these mobility management schemes developed for IP and cellular networks rely on a centralized mobility anchor entity, responsible for both the mobility signaling and user data forwarding. This traditional centralized approach is likely to have several issues or limitations which require costly network dimensioning and engineering to resolve. The IETF (Internet Engineering Task Force) has recently chartered the distributed mobility management (DMM) working group [11] with identifying limitations in the existing IP mobility support protocols and developing distributed mobility management protocols based on the existing IP mobility support protocols such as MIPv6 and PMIPv6.

This chapter presents qualitative and quantitative analyses on mobility management protocols and MPLS integration. In addition, the objective of this chapter is to provide a comprehensive comparison of the main alternatives and addresses the most important strong and weak points of each of these well-known mobility support protocols through numerical results. The rest of the chapter is organized as follows. In section 2, we present background knowledge about mobility management protocols. We have developed an analytical model used to derive the signaling cost function of registration update, link usage and packet loss. This is presented in section 3. In section 4 the numerical results are shown. Finally, concluding remarks are given in section 5.

2 Mobility Management in the Internet

Mobility management in the Internet is a key aspect of mobile communications and is the next step in the Internet evolution. It is practical now for a mobile node to roam between different access technologies and, in addition, it is reasonable to expect address continuity and session persistence across these handoffs. Anticipating these requirements, Mobile IPv6 protocol has been developed by the IETF. It is a host-based mobility management protocol requiring the participation of the host in all aspects of mobility management. An alternative approach is network-based mobility management protocols, where the host does not participate in any mobility related signaling. The main network-based protocol, recently developed by the IETF, is Proxy Mobile IPv6.

2.1 Host-Based Schemes

Until now, Mobile IP is the most representative mobile management scheme developed by the IETF on the way towards next generation mobile networks.

Mobile IPv6 allows nodes to remain reachable while moving around in IPv6 networks. Without specific support for mobility, packets destined to a mobile node would not be able to reach it while the mobile node is away from its home link. In order to continue communication in spite of its movement, a mobile node could change its IP address each time it moves to a new link, but the mobile node would then not be able to maintain transport and higher-layer connections when it changes location. Fig. 1 illustrates an overview of Mobile IPv6 and its basic terminology. Next, a brief description of the protocol is given.

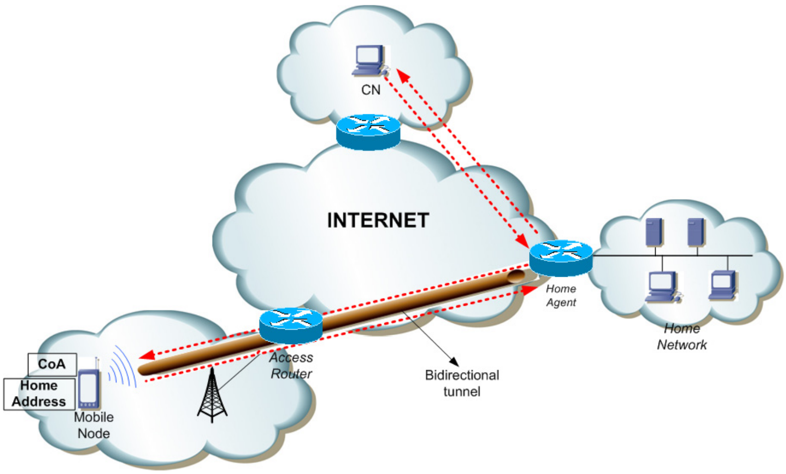

Fig. 1. Overview of Mobile IPv6

Mobile IPv6 basic operation is as follows. The Mobile Node (MN) establishes a connection with the Correspondent Node (CN). A Home Agent (HA) serves as the anchor node in the Home Network that tracks the network connection point (location) of a user as the user moves. Periodically, or whenever the user changes their point of attachment to the network, the user registers with the HA through Binding Update (BU) messages, informing of the user's current location and establishing a tunnel (IP-in-IP or GRE) between the HA and the MN located in a visited network. With this registration, the MN obtains a new address, called Care of Address (CoA), that belongs to the foreign network. The Home Agent is the critical part of the system since it is on the critical path of both signaling and data for mobile users.

The other alternatives based on Mobile IP, which integrate mobility and MPLS, are Mobile MPLS [7], FH Micro Mobile MPLS [8] and LinkWork Mobile MPLS [12]. All these schemes are briefly explained next.

Mobile MPLS was one of the first proposals to integrate Mobile IP and MPLS protocols. It aims to improve the scalability of the Mobile IP data forwarding process by removing the need for IP-in-IP tunneling from Home Agent (HA) to Foreign Agent (FA) using Label Switched Paths (LSPs).

FH Micro Mobile MPLS overcomes some limitations of Mobile MPLS. In this scheme the fast handoff mechanism anticipates the LSP procedure setup with an adjacent neighbor subnet that an MN is likely to visit. The main idea behind FH Micro Mobile MPLS is to set up an LSP before the MN moves into a new subnet to reduce service disruption. In this context, the authors consider active and passive LSPs. The active LSP is the one from the LERG (the root of the MPLS domain) to the current serving LER in the visited network. This LSP is used to transfer data. Passive LSPs are those from the LERG to the neighboring LER of the current foreign agent. These LSPs will not be used except when the MN moves to its own network. In this moment, the MN establishes its new active LSP and passive LSPs with neighboring subnets.

The last host-based proposal is LW Mobile MPLS, a proposal aimed to solve some problems detected in the previous alternatives. From our point of view, the need to setup a complete LSP after each movement increases the signaling over-head and reduces the overall performance of the network. In our proposal, we handle mobility efficiently by reducing the signaling overhead in an MPLS domain. This solution is based on the forwarding chain concept (set of forwarding paths). We introduce some special nodes in the MPLS, called Linkage Nodes (LN), which are responsible for the redirection of the LSP. This way, the LSP is composed of a set of forwarding paths that allow the signal to be localized and adapt in order to track host mobility. Fig. 2 shows the basic operation of this scheme.

Initially, when a mobile node moves to an adjacent network it disconnects from its previous LER/Access Router (AR) called PELER (Previous Egress LER) and it attaches to a new LER/AR called NELER, (New Egress LER) establishing a new LSP towards this router.

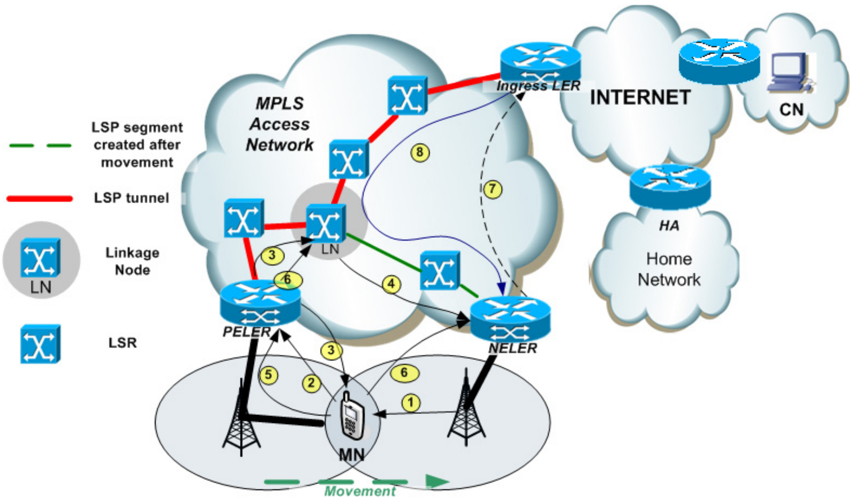

Fig. 2. LinkWork Mobile MPLS operation

When the MN moves to an adjacent network, it proceeds as follows. The MN enters an overlapped area of an adjacent subnet, it receives an L2 (layer 2) signal from the potential new base station (BS) (step 1). Next, the MN notifies the PELER of the possibility of a handoff by sending a HI (Handover Initiate) message which contains the new Base Station identifier. This information is going to be used to obtain the NELER IP address, thanks to a data structure that maintains a match between this identifier and each adjacent LER IP address (step 2). These 2 steps of the LW Mobile MPLS architecture are similar to those proposed in the FH-Micro Mobile MPLS scheme.

Once the PELER knows the subnet which the MN is going to move to, it sends a message upstream to the selected LN, notifying of a possible L3 handover, and beginning the setup of a new section of the LSP from LN to NELER (step 3) with the required QoS, using RSVP-TE. In this step, the PELER also informs the MN of the NELER IP address through a Neighbor Discovery message. At this moment, a new section of the LSP tunnel could be set up so data traffic can be forwarded towards the new location of the MN (step 4). When the signal strength received from the current base station falls below a certain threshold level, the MN notifies of the handoff to the PELER. Now, the PELER starts the mechanism responsible for minimizing packet loss (step 5).

Once the L2 handover is performed, the L3 (layer 3) handover is initiated by the MN with the NELER through MIPv6 registration process (step 6). The new LSP section from the LN to the new egress router will be used when the LN is aware of the movement. This happens when the PELER starts to return data packets back to the LN, which will be forwarded to the NELER through the new LSP section together with buffered packets according to the recovery mechanism. Finally, the NELER sends the Mobile IPv6 Binding Update message to ILER (step 7). The ILER will reply to the MN which is located in the new subnet.

2.2 Network-Based Schemes

As we have detailed in the previous section, host-based mobility management requires client functionality in the IPv6 stack of a mobile node. Exchange of signaling messages between the mobile node and the home agent enables the creation and maintenance of a binding between the mobile node's home address and its care-of address. Mobility in Mobile IPv6-based solutions requires the IP host to send IP mobility management signaling messages to the home agent, which is located in the network. This means that the protocol requires stack modification of the mobile node in order to support the mobility improvements. In addition, the requirement for the modification of mobile nodes may cause them to become increasingly complex. On the other hand, in a network-based mobility management approach, the serving network handles the mobility management on behalf of the mobile node; thus, the mobile node is not required to participate in any mobility-related signaling.

With these design goals, the IETF developed a network-based mobility management protocol which aims to cover:

- Support for unmodified Mobile Nodes: Unlike host-based mobility management protocols, the network-based protocol should not require any software modification for IP mobility support on the mobile nodes.
- Efficient use of wireless resources: The network-based protocol should avoid tunneling overhead over the wireless link, so it should minimize overhead with-in the radio access network.
- Reduction in handover-related signaling volume: Considering MIPv6, whenever an MN changes the subnets, various signaling messages are required. Therefore, in the network-based protocol the handover-related signaling should be performed as infrequently as possible.
- Support for IPv4 and IPv6: Although the initial design of the network-based protocol uses an IPv6 host, it is intended to work with IPv4 or a dual-stack host as well.

Compared to host-based mobility management approaches such as MIPv6 and its enhancements, a network-based mobility management approach such as Proxy Mobile IPv6 has several advantages.

From a deployment perspective, network-based mobility management does not re quire any modification of mobile nodes. This requirement can be considered one of the primary reasons Mobile IPv6 has not been widely deployed in practice.

From a performance perspective, due to the fact that wireless resources are very scarce, the efficient use of wireless resources can result in enhancement of network scalability. In host-based approaches such as MIPv6, the mobile node is required to participate in mobility related signaling. Thus, a lot of tunneled messages as well as mobility-related signaling messages are exchanged via the wireless links. Considering the explosively increase in the number of mobile subscribers, such a problem would cause serious performance degradation. On the contrary, in a network-based approach the serving network controls mobility management on behalf of the MN, so tunneling overhead as well as a significant number of mobility-related signaling message exchanges via wireless links can be reduced.

Another advantage is from a network service provider perspective. Network-based mobility management can enhance manageability and flexibility by enabling network service providers to control network traffic and provide differentiated services, among other things. In fact, some cellular systems such as IS-41 and Global System for Mobile Communications (GSM) can be considered network-controlled systems. Moreover, General Packet Radio Service (GPRS) has some resemblance to Proxy Mobile IPv6 in that they are both network-based mobility management protocols and have similar functionalities. Recently, the Third Generation Partnership Project's (3GPP) Evolved Packet System (EPS), commonly referred to as the 4G (Fourth Generation) Long Term Evolution (LTE) has adopted the Proxy Mobile IPv6.

PMIPv6, the main network-based protocol, shown in Fig. 3, is based on MIPv6 in the sense that it extends MIPv6 signaling and reuses many concepts such as HA functionality. The new principal functional entities of PMIPv6 are the mobile access gateway (MAG) and local mobility anchor (LMA). The MAG typically runs on the AR. Its main role is to detect the MN's movements and initiate mobility-related signaling with the MN'LMA on behalf of the MN. In addition, the MAG establishes a tunnel with the LMA to enable the MN to use an address from its home network prefix and emulates the MN's home network on the access network for each MN. On the other hand, the LMA is similar to the HA in MIPv6.

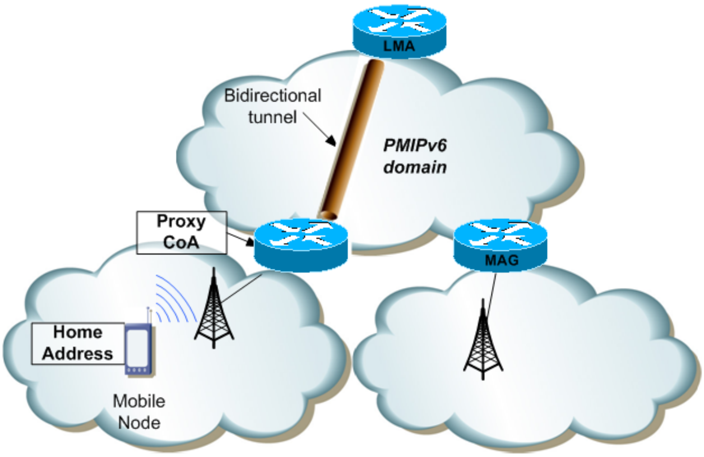

Fig. 3. Overview of Proxy Mobile IPv6

Its main role is to maintain access to the MN's address while it moves and to store information necessary to associate an MN with its serving MAG, enabling the relationship between the MAG and LMA to be maintained.

Other network-based proposals used in this analysis are FHPMIPv6 [13] and MPLS-PMIPv6 [14]. FHPMIPv6 is a fast handover extension for PMIPv6. The main idea behind this option is to establish a bi-directional tunnel between the PMAG and the NMAG so packets destined for the MN are forwarded from the PMAG to the NMAG through this tunnel.

MPLS-PMIPv6 is the first scheme which proposes MPLS as an alternative tunnel technology between a MAG and a LMA. Two kinds of labels are employed: a classical tunnel label and a Virtual Pipe label. The latter is introduced as a means to differentiate traffic with the same MAG-LMA end-points according to the operators of the various MNs served by the same MAG.

Fig. 4 shows the message flow of the operation in MIPv6 and PMIPv6, the most representative host-based and network-based mobility management protocols.

2.3 Distributed Mobility Management Approach

The mobility management proposals described in the previous section are based on a centralized mobility agent (Home Agent in Mobile IPv6 or LMA in Proxy Mobile IPv6) that allows a mobile node to remain reachable during its movement. Among other tasks, this anchor point ensures connectivity by forwarding packets destined to, or sent from, the mobile node.

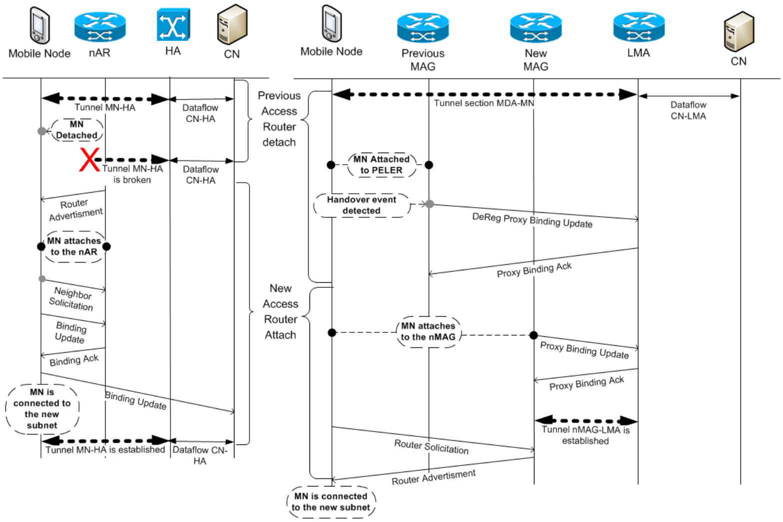

Fig. 4. Message flow in MIPv6 and PMIPv6

Nowadays, most of the deployed architectures have a small number of centralized anchors managing the traffic of millions of mobile users. This centralized approach brings several limitations such as non-optimal routing, scalability problems and reliability:

- Suboptimal routing: Since the (home) address used by an MN is anchored at the home link, traffic always traverses the central anchor, leading to paths that are, in general, longer than the direct one between the MN and its communication peer. This is exacerbated by the current trend in which content providers push their data to the edge of the network, as close as possible to the users, as for example by deploying content delivery networks (CDNs). With centralized mobility management approaches, user traffic will always need to go first to the home network and then to the actual content source, sometimes adding unnecessary delay and wasting operator resources.
- Scalability problems: Existing mobile networks have to be dimensioned to support all the traffic traversing the central anchors. This poses several scalability and network design problems, as central mobility anchors need to have enough processing and routing capabilities to be able to deal with all the user traffic simultaneously. Additionally, the entire operator's network needs to be dimensioned to be able to cope with all the user traffic.
- Reliability: Centralized solutions share the problem of being more prone to reliability problems, as the central entity is potentially a single point of failure.

Recent IP network usages such as multimedia content access and video streaming contribute to an exponential growth in bandwidth usage. The architectural limitation of centralized topologies require that data must first be routed to the HA or the LMA (centralized agents) which may be geographically far away from the mobile node, and then tunneled to the mobile node. Therefore, these limitations become clearer when the centralized mobility management needs to support mobile videos, which demand a large volume of data and often require quality of service (QoS) such as session continuity and low delay.

This motivates distributed mobility management solutions to efficiently handle ever increasing mobile traffic, the major portion of which carries video traffic [15]. Moreover, the IETF has recently created a working group called DMM (Distributed Mobility Management) that is identifying the limitation and defining the problem statements for achieving DMM with the existing IP mobility support protocols. A further description of the main DMM proposals can be found in [16] and [17].

3 Qualitative Analysis

In this section we investigate the qualitative model used to compare various existing well-known mobility support protocols, both host-based and network-based. This analysis is based on various evaluation criteria such as the cost functions of registration updates, total packet loss during a session, buffer size metrics and tunneling overhead. In order to evaluate the performance of these mobility protocols when an MPLS access network is introduced, some MPLS-based proposals are compared with non MPLS-based ones.

As we can see in the Table 1, we compare seven mobility protocols. However, not all of them are integrated with MPLS. Despite this, we consider them in our analysis due to their importance, given that Mobile IP and PMIPv6 were developed by IETF as the main Internet mobility solutions and 3GPP has used them to achieve mobility in the LTE (Long Term Evolution) evolved packet core [18].

Table 1. Protocols features

	Mobile IP-based protocols				Proxy Mobile IP-based protocols		
Protocol criteria	MIPv6	Mobile MPLS	FH Micro Mobile MPLS	LW Mobile MPLS	PMIPv6	FH PMIPv6	PMIPv6-MPLS
Required infrastructure	HA	HA-FA	LERG-FA	ILER-PELER / NELER	LMA MAG	LMA MAG	LMA MAG
Mobility Scope	Global	Global	Local	Local	Local	Local	Local
Tunneling protocols	IP-IP, GRE	MPLS	MPLS	MPLS	IP-IP, GRE	IP-IP, GRE	MPLS
MPLS integration	No	Yes	Yes	Yes	No	No	No

In order to simplify the analytical study, we suppose that every subnet is equidistant from the ingress LER in the MPLS domain, with a distance of δ (in terms of number of hops). In the same way, we do not consider the cost of the process that periodically updates the link (binding update) between the MN and the HA in order to update the cache, as is shown in [19]. We analyze the mobility behavior of the MN, keeping in mind a topology where a terminal could move to every neighbor network with the same probability. The parameters to be used are the following:

Parameters:

- t_s Average connection time for a session;
- t_r Average stay time at a visited network;
- T_{ad} Time interval between Agent Advertisements messages;
- N_h Average number of level 3 handover in a session ($N_h = t_s/t_r$);
- N_g No. of remaining neighbors of the new LER not notified in a handover;
- s_u Average size of a signaling message for record update;
- s_l Average size of a message for LSP establishment;
- h_{x-y} Average number of hops between x and y in the wired network;
- B_w Bandwidth of the wired link;
- B_{wl} Bandwidth of the wireless link;
- L_w Latency of the wired link (propagation delay);
- L_{wl} Latency of the wireless link (propagation delay);
- P_t Routing or label table lookup and processing delay;
- λ_d Transmission ratio for a downlink packet;
- T_{inter} Time between arrivals of consecutive data packets.

On the other hand, $t(s,h_{x-y})$ is the time spent for a packet with size *s* to be sent from *x* towards *y* across wired and wireless links. $t(s,h_{x-y})$ can be expressed in the form:

$$t(s,h_{x-y}) = c + h_{x-y} \cdot \left(\frac{s}{B_w} + L_w \right) + (h_{x-y} + 1) \cdot P_t$$

$$where \qquad c = \begin{cases} \dfrac{s}{B_{wl}} + L_{wl} & if \quad x = MN \\ 0 & if \quad x \neq MN \end{cases}$$

3.1 Signaling Cost

The total signaling cost of registration update for a session can be defined as C_u. This value depends on the traffic load when signaling messages are sent, i.e., this cost depends on the size of signaling messages and the number of hops in every level 3 handoff process during the time interval that communication of MN remains active. Therefore, the cost is defined by the messages size multiplied by the number of needed hops.

Each movement between neighboring subnets implies sending several signaling messages. In Mobile IP and Mobile MPLS cases, the registration update with the HA is needed, whereas in FH, LW and PMIP cases, the update is local with the root of the domain. Apart from signaling of the mobility management protocol, some proposals also add the cost of the LSP procedure set-up. This is the case of Mobile MPLS, FH-Micro Mobile MPLS, LW Mobile MPLS or PMIP-MPLS.

This way, we obtain the following values for the signaling cost when the registration update process occurs:

$$C_u(Mobile\,IP) = 2 \cdot s_u \cdot h_{MN-HA} \cdot N_h$$
$$C_u(Mobile\,MPLS) = 2 \cdot s_u \cdot h_{MN-HA} \cdot N_h + 2 \cdot s_l \cdot h_{FA-HA} \cdot N_h$$
$$C_u(FHMMM) = 2 \cdot s_u \cdot h_{MN-LERG} \cdot N_h + 2 \cdot s_u \cdot h_{FA-FA} \cdot N_h + 2 \cdot s_l \cdot h_{FA-LERG} \cdot N_g \cdot N_h$$
$$C_u(LW\,Mobile\,MPLS) = 2 \cdot s_u \cdot h_{MN-ILER} \cdot N_h + 2 \cdot s_l \cdot h_{LN-NELER} \cdot N_h$$
$$C_u(PMIP) = 2 \cdot s_u \cdot h_{MAG-LMA} \cdot N_h + 2 \cdot s_u \cdot h_{nMAG-LMA} \cdot N_h$$
$$C_u(FHPMIP) = 2 \cdot s_u \cdot h_{nMAG-pMAG} \cdot N_h + 2 \cdot s_u \cdot h_{nMAG-LMA} \cdot N_h$$
$$C_u(PMIP-MPLS) = 2 \cdot s_u \cdot h_{pMAG-LMA} \cdot N_h + 2 \cdot s_l \cdot h_{nMAG-LMA} \cdot N_h$$

3.2 Packet Loss during a Session

Packet loss during a session (P_{loss}) is defined as the sum of lost packets per MN during all handoffs. Apart from FH, LW and FHPMIP, in the other schemes all in-flight packets will be lost during the handoff disruption time due to the lack of a buffering mechanism.

Our LW Mobile MPLS proposal also has a recovery mechanism that minimizes the packet loss. Its operation is explained briefly. When the MN informs PELER of an L2 handoff, this edge router does not send any more packets to the MN; instead it sends the packets back to the LN. When the first packet arrives back to the LN, it tags the next packet received and sends it and buffers all incoming packets from the PELER. Once the LN receives the tagged packet from the reverse path, it removes the tag, sends it through the new section of the LSP through the NELER. Once all incoming packets from PELER have been sent, buffered packets are forwarded to the NELER. This is how we avoid packet disorder and minimize packet loss. The main advantage of this alternative is that the packets are sent towards the new location of the MN in order so the MN task of reordering the information is significantly reduced.

Fig. 5 shows an example in which the path that a packet involved in the recovery mechanism follows ca be observed. d and d' are the distance between LN and the PELER and the distance between the LN and the NELER respectively.

FHPMIPv6 buffers data packets until the tunnel is established between the pMAG and the nMAG. Therefore, the value P_{loss} for each proposal is:

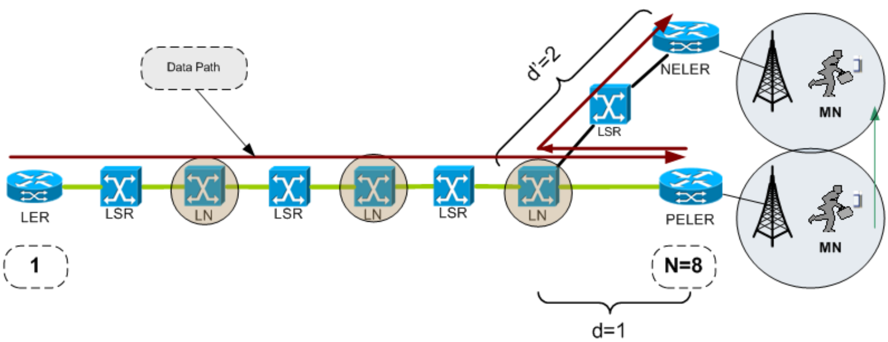

Fig. 5. Path followed by a packet involved in the recovery mechanism

$$P_{loss}(Mobile\,IP) = \left[\left(\frac{1}{2}T_{ad}\right) + T_c(MobileIP)\right] \cdot \lambda_d \cdot N_h$$

$$P_{loss}(Mobile\,MPLS) = \left[\left(\frac{1}{2}T_{ad}\right) + T_c(MobileMPLS)\right] \cdot \lambda_d \cdot N_h$$

$$P_{loss}(FH\ Micro\,Mobile\,MPLS) = t(s_u, h_{MN-FA}) \cdot \lambda_d \cdot N_h$$

$$P_{loss}(LW\ Mobile\,MPLS) = t(s_u, h_{MN-NELER}) \cdot \lambda_d \cdot N_h$$

$$P_{loss}(PMIP) = \left[\left(\frac{1}{2}T_{ad}\right) + T_c(PMIP)\right] \cdot \lambda_d \cdot N_h$$

$$P_{loss}(FHPMIP) = t(s_u, h_{MN-pMAG}) \cdot \lambda_d \cdot N_h$$

$$P_{loss}(PMIP - MPLS) = \left[\left(\frac{1}{2}T_{ad}\right) + T_c(PMIP - MPLS)\right] \cdot \lambda_d \cdot N_h$$

where T_c is the average time of the handover completion, which is defined as the sum of three terms: interruption time, establishment time and $T_{inter}/2$.

3.3 Buffer Size

The buffer for storing in-flight packets is located at the Linkage Node (LN) in the LW Mobile MPLS whereas in the FH-Micro Mobile MPLS the buffer is located in the LER/FA nodes. As for FHPMIP, the buffer can be found in the pMAG node. Therefore, the buffer size requirement (B_{size}) is listed as follows:

$$B_{size}(FH\ Micro\,Mobile\,MPLS) = \left(\frac{1}{2}T_{ad}\right) + t(s_u, h_{MN-FA} + h_{FA-FA}) \cdot \lambda_d$$

$$B_{size}(LW\ Mobile\,MPLS) = \left(\frac{1}{2}T_{ad}\right) + t(s_u, h_{LN-PELER} + h_{PELER-LN}) \cdot \lambda_d$$

$$B_{size}(FHPMIP) = \left(\frac{1}{2}T_{ad}\right) + t(s_u, h_{MN-pMAG} + h_{pMAG-nMAG}) \cdot \lambda_d$$

3.4 Tunneling Overhead

As we have seen in the previous sections, host-based and network-based mobility management protocols establish a tunnel to forward data packets. The IETF advises the use of IP-in-IP or GRE (Generic Routing Encapsulation) as tunneling methods. In this section we take a look at these technologies and compare them with MPLS tunnels.

IP-IP (IP in IP) is a protocol by which an IP datagram may be encapsulated (carried as payload) within an IP datagram, by adding a second IP header to each encapsulated datagram. However, IP-in-IP tunneling increases the overhead, because it needs an extra set of IP headers. Typically, a pure IP-over-IP tunnel configured with tunnel mode IP-IP has a 20-byte overhead, so if the normal packet size (MTU) on a network is 1500 bytes, a packet that is sent through a tunnel can only be 1480 bytes big.

GRE (Generic Routing Encapsulation) is another tunneling method that encapsulates any network layer packet. GRE requires the IP-in-IP encapsulation with the extra IP-IP header (20 bytes), but it also adds another 4 bytes of the GRE header to a packet, resulting in 24-byte overhead. After this increase the packet may need to be fragmented because it is larger than the outbound Maximum Transmission Unit (MTU).

On the other hand, an MPLS LSP tunnel has one label (4 bytes) or a stack of overhead labels (for example, when using Link Protection Fast reroute). MPLS adds four bytes to every datagram but, unlike GRE tunnel, MPLS does not change the IP header. Instead, the label stack is imposed on to the packet that takes the tunnel path.

The three approaches can also be compared in terms of the overhead they generate during data packet forwarding operations, i.e. when the MN communicates with the CN while remaining attached to the same foreign network access router. Table 2 shows this operational overhead.

From our analysis it emerged that MPLS can be profitably used to complement PMIPv6, as it enhances the tunneling paradigm with fast forwarding techniques and the potentially allows Traffic Engineering support. We showed that MPLS adds no extra overhead to MIPv6/PMIPv6; conversely it may even contribute to reductions in both handover delay and the operational overhead.

4 Numerical Results

In this section we focus on a quantitative analysis among the technologies presented in section 2. The parameter settings in our experiments are listed in Table 3. The settings of the distances $d_{x\text{-}y}$ values are represented by Fig. 5.

Fig. 6 presents the comparison of registration cost vs. resident time when parameters have their default settings.

Table 2. Operational overhead

Tunneling mechanism	Overhead
IP-IP	20 Bytes
GRE	24 Bytes
MPLS	4 Bytes

Table 3. Parameter settings

Parameter	Value
t_s	1000 sec.
t_r	5~50 sec (default 20)
t_{ad}	1 sec.
s_u	48 Bytes
s_l	28 Bytes
B_w	100 Mbps
B_{wl}	11 Mbps
L_w	1 msec.
L_{wl}	2 msec.
P_t	10^{-6} sec.
N_g	1
λ_d	64 Kbps

In this case, the Mobile MPLS scheme is the costliest alternative due to the need to establish a complete LSP tunnel from mobile node to HA separate from the specific Mobile IPv6 signaling. On the contrary, LW Mobile MPLS uses the resources in the MPLS access network efficiently as it reduces signaling to an area, and therefore doesn't overload links and nodes near ILER. This way, LW Mobile MPLS can significantly reduce the registration cost particularly when the MN hands off frequently (i.e. the resident time in each subnet is short). The introduction of LN nodes in the MPLS domain allows the signaling exchange to be reduced by the creation of a linkworked LSP that allows local registration.

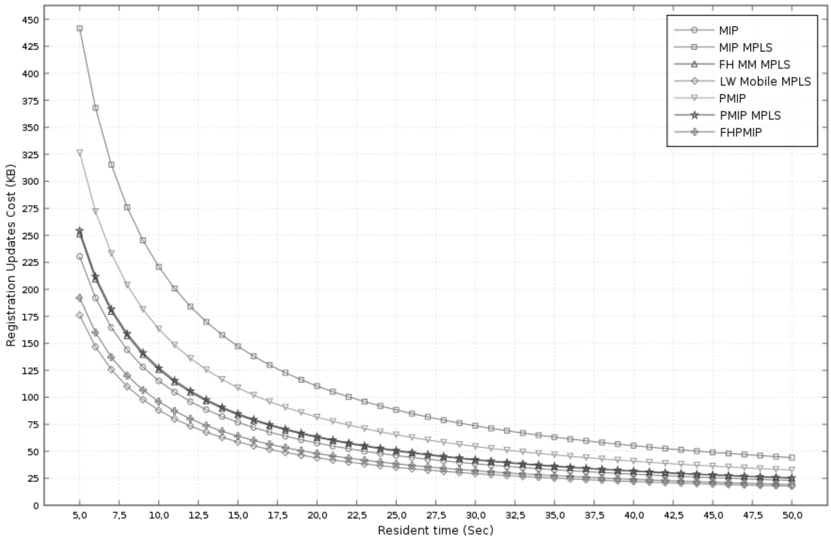

Fig. 6. Registration update cost

Fig. 7 shows the amount of lost packets during the whole connection session for different approaches. These results show the high difference between the proposals which have buffering mechanisms and those which do not. Both PMIP MPLS and Mobile MPLS have the largest amount of lost packets due to the higher establishment time (Tc) needed to setup an LSP between the HA / LMA and the new serving agent in the visited network.

In contrast, FH Micro Mobile MPLS, FH-PMIP and our proposal, LW Mobile MPLS, provide the best results thanks to the buffering and recovery mechanisms. Note the similar level of packet loss as all three proposals initiate the buffering mechanism at the same time. However, there are significant differences between them that explain the difference in the registration update cost performance. First of all, the LW Mobile MPLS approach performs the forwarding LSP chain in LN nodes, which are internal routers of the domain. In our opinion, the flexibility of the architecture can be improved by using a few nodes inside the domain as LNs which could also be easily adapted to the needs of the service provider. Secondly, the recovery mechanism proposed in our LW Mobile MPLS architecture is designed to deliver recovered packets in the correct order; this means that our proposal saves the upper transport layer from doing this task.

With respect to buffer size requirements, a buffer is needed to store in-flight packets during each handoff operation. As stated before, only LW Mobile MPLS, FHPMIP and FH Mobile MPLS do this. In this case, the LW proposal needs a smaller buffer than the others. This difference is based on the fact that the time in which the in-flight packets are stored is less than in the other proposals. Fig. 8 shows the buffer size vs. the bandwidth of the MPLS access network. In this graph we can observe that from 200 Mbps the size of the buffer remains rather stable, around 1,25~1,50 Kb.

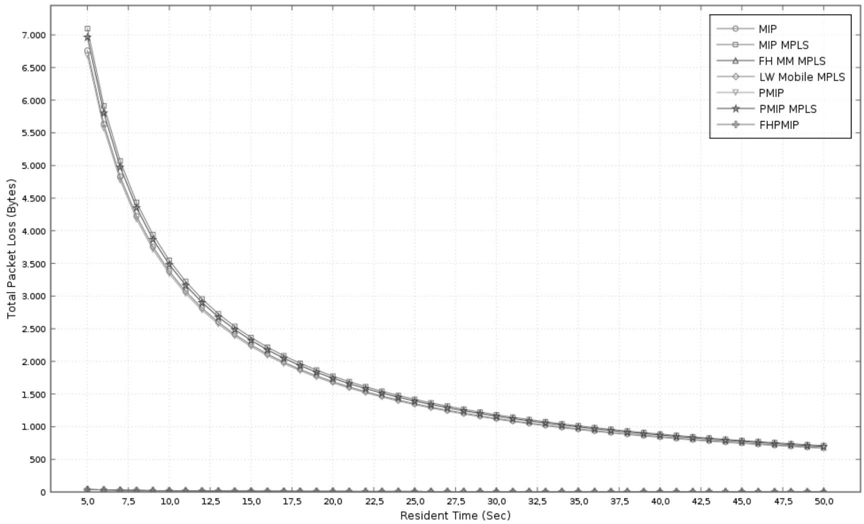

Fig. 7. Total packet loss during a session

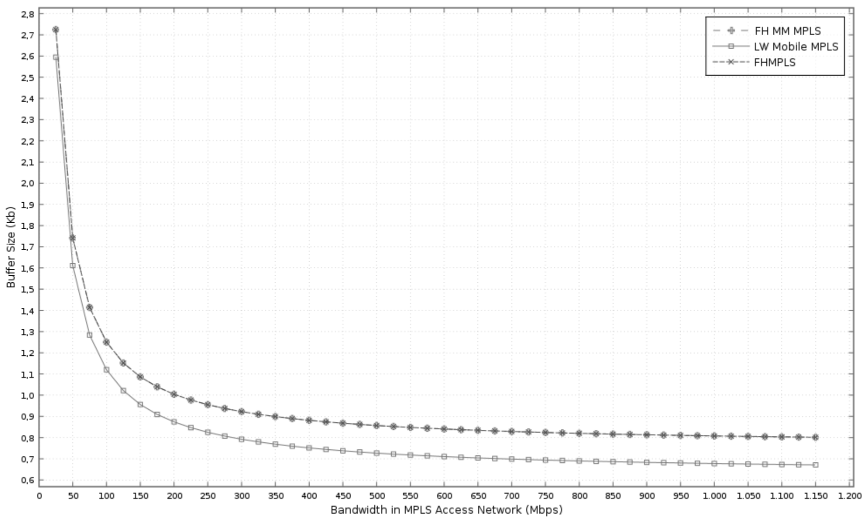

Fig. 8. Buffer size vs. bandwidth in MPLS access network

5 Conclusion

In this chapter, various well-known IP mobility support protocols have been evaluated and their performance has been measured when an MPLS domain is introduced into the access network. One of these schemes is called LinkWork Mobile MPLS, an architecture that offers efficient management through the use of special LSR that we call Linkage Nodes (LN). These nodes are responsible for rerouting the LSP tunnel to the LER that serves the mobile node in each handover. Also these nodes retrieve the packets in flight when a service interruption is provoked by a handover.

Through the analytical study and the simulations carried out we obtained the numerical results of seven protocols related to the links, the signaling costs, the packets lost during the movements in each session and the ideal buffer size needed to accomplish the objectives.

We highlight the small signaling cost of LW Mobile MPLS and also the great capacity to minimize the loss of packets compared to the alternatives. The analysis proves the need to use a buffer mechanism to store in-flight packets in order to achieve packet loss improvement.

Finally, from our study it emerged that MPLS can be profitably used to complement mobility protocols, as it enhances the tunneling paradigm with fast forwarding techniques and the possible support of Traffic Engineering. One of the main conclusions of this work is that MPLS adds no extra overhead and it may even contribute to reducing both handover delay and the overhead during data exchange.

References

[1] Langar, R., Bouabdallah, N., Boutaba, R.: A comprehensive analysis of mobility management in MPLS-based wireless access networks. IEEE/ACM Trans. Netw. 16(4), 918–931 (2008)

[2] Johnson, D., Perkins, C., Arkko, J.: Mobility Support in IPv6. IETF RFC 6275 (July 2011)

[3] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., Patil, B.: Proxy Mobile IPv6- RFC 5213 (August. 2008)

[4] Rosen, E., Viswanathan, A., Callon, R.: Multiprotocol Label Switching Architecture. IETF RFC 3031 (January 2001)

[5] Taha, A.-E.M., Hassanein, H.S., Mouftah, H.T.: Extensions for Internet QoS paradigms to mobile IP: a survey. IEEE Communications Magazine 43(5), 132–139 (2005)

[6] Koodli, R.: Fast Handovers for Mobile IPv6. IETF RFC 4068 (July 2005)

[7] Ren, Z., Tham, C., Foo, C., Ko, C.: Integration of mobile IP and multi-protocol label switching. In: Proc. IEEE ICC, vol. 7, pp. 2123–2127 (2001)

[8] Langar, R., Tohme, S., Bouabdallah, N.: Mobility management support and performance analysis for wireless MPLS networks. International Journal of Network Management 16(4), 279–294 (2006)

[9] Sa-Ngiamsak, W., Krachodnok, P., Varakulsiripunth, R.: A Recovery Scheme for QoS Guaranteed Mobile IP Over MPLS Network. In: 2006 1st International Symposium on Wireless Pervasive Computing, January 16-18, pp. 1–5 (2006)

[10] Quintero, A., Del Frutos, E.: MPLS Based Architecture for Mobility and End-to-End QoS Support in Fourth Generation Mobile Networks. Journal of Computer Science 5(4), 255–262 (2009)

[11] IETF DMM working group charter page, `http://datatracker.ietf.org/wg/dmm/charter/` (accesed May 2013)

[12] Carmona-Murillo, J., González-Sánchez, J.L., Rodríguez-Pérez, F.J.: Performance evaluation of an architecture for localized IP mobility management. In: 2010 International Conference on Network and Service Management (CNSM), October 25-29, pp. 386–387 (2010)

[13] Yokota, H., Chowdhury, K., Koodli, R., Patil, B., Xia, F.: Fast handovers for Proxy Mobile IPv6. IETF Internet-Draft (May 2010) (expires November 2010)

[14] Garroppo, R.G., Giordano, S., Tavanti, L.: Network-Based Micro-Mobility in Wireless Mesh Networks: Is MPLS Convenient? In: Global Telecommunications Conference, GLOBECOM 2009, pp. 1–5. IEEE (December 2009)

[15] Zuniga, J.C., Bernardos, C.J., de la Oliva, A., Melia, T., Costa, R., Reznik, A.: Distributed mobility management: a standards landscape. IEEE Communications Magazine 51(3), 80–87 (2013)

[16] Shin, D.-H., Moses, D., Venkatachalam, M., Bagchi, S.: Distributed mobility management for efficient video delivery over all-ip mobile networks: Competing approaches. IEEE Network 27(2), 28–33 (2013)

[17] Lee, J.-H., Bonnin, J.-M., Lagrange, X.: Host-based distributed mobility management support protocol for ipv6 mobile networks. In: 2012 IEEE 8th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 61–68 (2012)

[18] Ali, I., Casati, A., Chowdhury, K., Nishida, K., Parsons, E., Schmid, S., Vaidya, R.: Network-based mobility management in the evolved 3GPP core network. IEEE Communications Magazine 47(2), 58–66 (2009)

[19] Lo, S.-C., Lee, G., Chen, W.-T., Liu, J.-C.: Architecture for mobility and QoS support in all-IP wireless networks. IEEE Journal on Selected Areas in Communications 22(4), 691–705 (2004)