UNIFIED LOCAL MOBILITY MANAGEMENT

Jukka Manner,[1] Tapio Suihko,[2] and Kimmo Raatikainen[1]

[1] *University of Helsinki, Department of Computer Science,*
P.O.Box 26, 00014 University of Helsinki, Finland
jukka.manner,kimmo.raatikainen@cs.helsinki.fi

[2] *VTT Information Technology*
P.O. Box 1203, FIN-02044 VTT, Finland
tapio.suihko@vtt.fi

Abstract

To enhance the mobility of nodes within an access network, various local mobility management protocols have been suggested. All these protocols have their strengths and drawbacks. The deployment of these protocols is a chicken and egg problem, since the access network and the mobile nodes must support the same protocol. This paper presents a new protocol designed to replace the communication between the access network and the mobile nodes in existing and future local mobility management schemes. The protocol allows mobile nodes to log into and roam within any access network regardless of the local mobility scheme used internally in the network.

Keywords: Local mobility management, micro mobility, Mobile IP

1. Introduction

The mobility management of IP-based mobile nodes (MN) has been a popular research topic for many years. The most well-known mobility management protocol is Mobile IP (MIP) (Perkins, 2002) (Johnson et al., 2004). MIP is not a perfect solution, and has, e.g., latency issues with handovers. These shortcomings have triggered work towards localizing the mobility management of MNs.

Local mobility management (LMM) protocols seek to enhance the mobility of MNs within the local domain, and hide the movement of MNs from correspondent nodes. These protocols operate within the ac-

cess network (AN), and between access routers (AR) and MNs. The various schemes can be roughly divided in two groups, protocols based on MIP, and standalone protocols. The former group includes protocols like Hierarchical Mobile IP (Soliman et al., 2004), and Fast MIP (Koodli, 2003). The latter group includes protocols, such as, Cellular IP (Campbell et al., 2000; Shelby et al., 2000), the Edge Mobility Architecture (EMA) (O'Neill et al., 2001), and the BRAIN Candidate Micro Mobility Protocol (BCMP) (Boukis et al., 2003). The Handoff-Aware Wireless Access Internet Infrastructure (HAWAII) (Ramjee et al., 1999) belongs to both groups. The differences in all these protocols can be seen in the general operation of the protocols, the algorithms and logic they use, and, most of all, on the messages needed to support the mechanisms.

Deployment of LMM is difficult since the MNs and the AN must implement the same protocol. The question is, which protocol should be used? All protocols have their weaknesses and strengths, and are suitable for different networks and user base. In order to deploy LMM, MNs and ANs may need to implement more than one protocol. Moreover, when a new MN requests services from an AN, the parties must be able to agree on the LMM protocol used.

The deployment of LMM would be much easier if there were a unified protocol between the AN and the MNs. This would allow the AN operator to deploy the LMM protocol that best suits the network. The MNs would have a standard way to log into any AN and request services, including the management of the mobility of the MN. Moreover, a unified protocol allows experimenting with different AN-internal mobility management without requiring changes to MNs.

This paper presents the Local Mobility Management Protocol (LMMP) that works between the ARs and MNs. With this protocol MNs can log in to an AN, and perform handovers in a controlled manner. The design of LMMP is based on an analysis of existing LMM schemes, and the messages they pass between ARs and MNs. The set of protocol messages and functions available in LMMP is intentionally large in order to accommodate different LMM schemes within ANs. The AN-internal operations triggered by LMMP messages depend on the AN.

This paper is structured as follows. In Section 2 we present an analysis of four LMM protocols and identify the protocol messages they send over the wireless link. Based on this analysis, in Section 3 we present the LMMP messages, and discuss the operation of the protocol when the MN logs into the AN and goes through handovers. We conclude Section 3 by discussing security issues in using LMMP, and describe our initial open source implementation.

2. Review of Existing Protocols

Research in local IP mobility management has resulted in a number of different protocols and schemes. In this section we take a look at four different protocols to handle the local mobility of MNs. The basic framework architecture for local IP mobility is presented in Figure 1. The architecture includes at least two components, mobile nodes (MN) and access routers (AR), but may also include a Mobility Anchor Point (MAP). ARs are the default routers for the MN, but, usually, include more functionality than just basic IP routing. The role of a MAP can be to co-ordinate the management of IP addresses to MN, and act as a boundary router towards external networks.

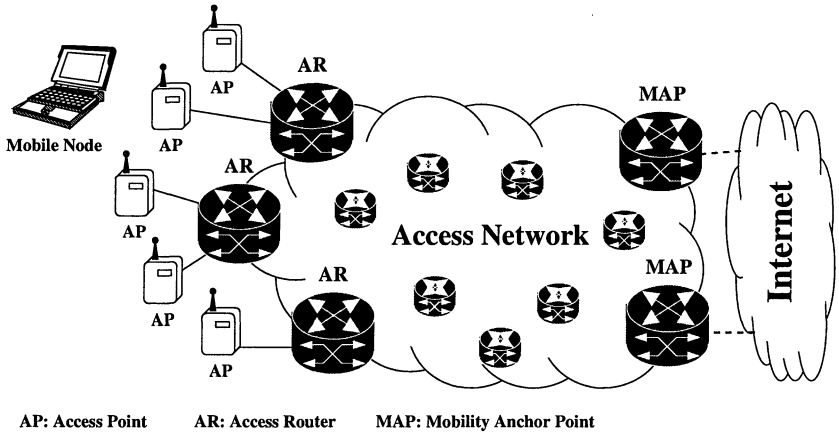

Figure 1. A framework architecture for local mobility management.

2.1 Cellular IP

One of the most well-known LMM schemes is Cellular IP (CIP) (Campbell et al., 2000; Shelby et al., 2000). CIP is a per-host routing protocol, which means that routers store per-host routing entries. The protocol is integrated efficiently with MIP. The MNs operate a little differently depending on the IP protocol version, namely the IP address management differs. CIP does not have its own address management.

Routing and addressing in CIP for IPv4 is based on the use of the home address of the MN. MNs use the address of a gateway as their MIP care-of-address. Inside the AN, the MNs are identified by their home address. Routers within the AN store per-host routing entries, where the routing table stores the next-hop closer to the MN. The routing entries are set up by the MN. When the MN enters the AN, packets sent from

the MN (*uplink*) are used to establish the location information in routing caches in routers. Packets going toward the MN (*downlink*) then use the reverse route. If the MN does not have data to send, it periodically sends CIP routing refresh messages. Uplink and downlink routing paths are symmetric. In IPv6 networks, MNs use the IPv6 stateless address auto-configuration.

CIP supports both unplanned and planned handovers. Handovers are initiated by MNs. In an unplanned handover, the MN switches to a new AR (called *base station*) and sends a routing refresh message, or data packets, which updates the routing caches within the AN.

Handovers can be planned to lower the packet loss and packet delivery latencies. Planned handovers require the knowledge of the next AR. In CIP, a planned handover requires that the MN is able to send messages to the current and new AR. In this handover the MN switches temporarily to the new AR, and sends a routing refresh message. It then switches back to the old AR for a short duration, after which it makes a permanent handover to the new AR. During this time the routing caches have been updated and the data packets are being routed to the new AR.

CIP has also support for IP paging. When MNs have no data to send or receive, they stop sending routing refresh messages, and enter an idle mode for saving power. During idle mode, MNs periodically send paging refresh messages, which store paging location information in paging caches. Paging and routing caches may be located in different routers. When the AN has data packets to be sent to the MN, a paging query is broadcast in the paging area the MN has last registered in. The MN eventually receives the page and responds by updating its routing information in the AN.

2.2 HAWAII

HAWAII (Ramjee et al., 1999) is a per-host routing protocol. HAWAII is tied to MIP in that the protocol does not specify its own messages over the wireless link but instead relies on MIP. An MN entering a new domain registers using MIP and is assigned a collocated care-of-address. The MN keeps this care-of-address unchanged while moving within the foreign domain, thus, handovers are not noticed outside the AN.

Location information is created, updated, and modified by explicit MIP signaling messages sent by MNs. HAWAII defines four alternative path setup schemes that control handovers between ARs, both planned and unplanned handovers. The appropriate scheme is selected depending on the operator's priorities between eliminating packet loss, mini-

mizing handoff latency, and maintaining packet ordering. HAWAII also supports IP paging through IP multicasting (Ramjee et al., 2000).

2.3 MER-TORA

Edge Mobility Architecture (EMA) (O'Neill et al., 2001) discusses the management of local mobility on the edges of fixed IP networks, as opposed to Mobile Ad-hoc Networks (MANET) where all nodes can move relative to each other. The edge mobility is called Mobile Enhanced Routing (MER). The EMA architecture and the MER concept is a framework, which does not specify the exact messages or protocols used. The mobility management is done with prefix-based routing up to a cross-over AR allocated initially to an MN, and from there by using per-host routing. Paging is discussed, and MIP can be integrated with the framework.

One example of a suitable protocol is the Temporally-Ordered Routing Algorithm (TORA) (Park and Corson, 1997). TORA is an ad-hoc routing protocol, which can be tuned to support edge mobility. TORA operates with respect to the "height" of nodes (relative to a destination node), and each node is assigned a unique identifier. The protocol proactively or reactively builds a directed acyclic graph (DAG) rooted at the destination. When employed in a MER domain, TORA can support unplanned and planned handovers.

2.4 BCMP

One of the most recent protocols to support local mobility is the BRAIN Candidate Micro Mobility Protocol (BCMP) (Boukis et al., 2003; IST-BRAIN Project, 2001; IST-MIND Project, 2002). MNs log in to the network with an explicit message and acquire an IP address. In the common case, this address is used for the whole duration of the visit in the AN. Authentication is handled with the login procedure.

BCMP uses per-host tunneling as its routing mechanism. The IP address of an MN is allocated by a certain MAP (called *anchor*). The IP routing is set up so that all downlink data packets arrive through the allocated MAP, which then tunnels the packets to the AR serving the MN. When the MN switches to a new AR, the tunnel end point is updated. Upstream routing can be handled with a shortest path route, or symmetrically back through the MAP.

Handovers are initiated by the MNs. A handover can be planned, where the MN informs the network about the new AR before the actual handover. The current and new AR then set up a tunnel, and all IP packets destined to the current AR are also copied to the new AR.

When the tunnel is set up, the MN is informed. It can then perform the handover and register at the new AR. In the unplanned handover, the MN just appears under a new AR, and updates its location information. If the MN moves far away from the initial MAP, BCMP has a functionality to switch MAPs. This should only be done when the MN is not actively sending or receiving data, as it involves changing the IP address assigned to the MN. BCMP also supports IP paging.

2.5 Summary of Functionality

The previous sections provided a short overview of the main protocol features found in some of the most well-known micro mobility protocols. Based on the evaluation, we present in Table 1 a summary of the functions in each protocol. Table 2 lists the messages used in the protocols over the wireless link

Table 1. Summary of the functionality in the presented LMM schemes.

Function	Cellular IP	HAWAII	MER-TORA	BCMP
Address management	Use HoA or addr. autoconf.	Part of MIP	Obtain addr. through login	Obtain addr. through login
Explicit login	MIP or separate	Part of MIP	Yes	Yes
Explicit logout	Refresh timeout	Part of MIP	Discussed	Yes
Routing	Per-host	Per-host	Prefix&per-host	Per-host tunnel
Unplanned HO	Yes	Yes	Yes	Yes
Planned HO	Yes	Yes	Yes	Yes
Handover init	by MN	by MN	by MN	by MN
Route refresh	Yes	Yes	Not specified	Not specified
Paging	Supported	Supported	Discussed	Supported

Table 2. Messages passed over the wireless link.

Protocol	Messages
Cellular IP	Beacon signal, route update (register option in route update), paging update, paging teardown
HAWAII	MIP messages (register and reply), paging request, refresh, update
EMA	Depends on the MER protocol, still, similar to BCMP
BCMP	Login request and reply, handover preparation, handoff and acknowledgment, paging, logout

3. The LMM Protocol

This section presents the Local Mobility Management Protocol (LMMP). LMMP is meant to replace the communication over the wireless link in existing and future LMM schemes. The basic operation of the LMM schemes remain unchanged within the AN.

Our design is based on the analysis of existing protocols. The functions designed into LMMP are intentionally larger than in any of the protocols presented. When LMMP is integrated with an existing LMM scheme, not all the functions available in LMMP need to be implemented by the AN; for instance, IP paging, or all authentication mechanisms discussed later in this paper. MNs must implement the whole specification.

LMMP supports network- and mobile-initiated handovers, planned and unplanned handovers, re-initialization of MNs, and paging. An unplanned mobile-initiated handover is the basic case, but the network can also suggest or force the MN to do a handover. The new location can be left unspecified, or the network can indicate a target. Planned handovers can be performed if the network or the MN has the information about the next point of attachment, e.g., using a Candidate Access Router Discovery mechanism (Liebsch et al., 2004).

3.1 Protocol Messages

LMMP includes 15 message types. Individual messages are used to log into the network, to log out, to initiate a handover, to execute a handover, and to send acknowledgments and asynchronous messages, such as, routing and paging refresh. LMMP messages are transported using the new Experimental ICMP Mobility type. The LMMP message types are described below:

Login is sent by the MN. It includes authentication information and an IP address of the MN. The IP address is either the home address of the MN, or an address received through auto-configuration.

Login Ack is used to confirm a successful login procedure. The message carries a session identifier (SID), and may also carry a new IP address that the MN must assign to its interface.

Logout is used to log out from the network in a controlled fashion. Both the MN or the AR can send this message to initiate the logout procedure.

Init Handover is used by either the AR or the MN to inform the other party that a handover should or must be executed. The message may carry information relevant to choosing the new point of attachment, e.g., a link layer address of the new point of attachment, the IP address of the new AR, or an IEEE 802.11 wireless LAN network name (ESSID).

Handover is sent by the MN to the new AR to inform that it just handed over from another point of attachment. The message may carry the IP address of the

previous AR. If paging is used, the message is also an answer to a paging query when the MN is in idle mode.

Re-Init is used to re-initialize the local mobility management information at the MN. The message may carry a new IP address for the MN, new routing and paging refresh intervals, and a new paging area ID (PID). The message can either suggest or force the MN to re-initialize its data structures.

Re-Init Done is used to confirm the update of the mobility management information at the MN and carries the sequence number of the Re-Init message being confirmed.

Routing Refresh is used by MNs to periodically inform of themselves, that they still require the IP connectivity.

Paging Refresh is used to update paging information in the AN.

Paging Query is broadcast from ARs to trigger an MN in idle state to update its local mobility management state in order to start receiving downlink data packets. The update is done with a *Handover* message.

AR Advertisement is used to broadcast information about the AN to the MNs. The advertisements may carry IDs of one or more PIDs the AR belongs to, information about how the MN must configure an initial IP address, paging and routing refresh intervals, and information about the authentication method used in the login procedure, if any.

Key Exchange Request/Reply are used in a built-in key exchange mechanism if no other mechanism is available. These are discussed later.

Ack is used to acknowledge a message received. The message carries the sequence number of the message being acknowledged.

Error is used to report error situations.

All messages, except the *Login* , *AR advertisement*, and *Key Exchange Request/Reply* carry a unique session identifier (SID). The SID is used to refer to the session established between the MN and the AN for the whole duration the MN stays in the AN. Even if the IP address of the MN changes, the SID remains. The SID is chosen by the AN.

All messages carry a sequence number, and may be secured with IP-level mechanisms, The information carried by the *AR advertisement* can also be broadcast with IP router advertisements. Table 3 provides a summary of the LMMP messages and the payloads they carry, and Figure 2 shows the generic structure of LMMP messages.

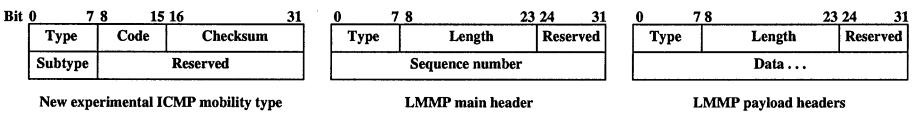

Figure 2. The generic structure of LMM message.

Table 3. Summary of LMMP messages and their possible payloads.

Message	Sender	Payload
Login	MN	Initial IP address
Login Ack	AR	SID, new PID
Logout	MN/AR	SID
Init Handover	MN/AR	SID, IP address of new AR, L2 address of new AP, IEEE 802.11 ESSID etc.
Handover	MN	SID, IP of old AR (if known)
Re-Init	AR	SID, IP address, PID, intervals for routing and paging
Re-Init Done	AR	SID, Sequence number of Re-Init
Routing refresh	MN	SID
Paging refresh	MN	SID, Paging area ID
Paging query	AR	SID (of MN being paged)
AR adv.	AR	Login and authentication information, intervals for paging and routing, PID(s)
Key Ex. Request	MN	Public key of MN
Key Ex. Reply	AR	Nonce N1, public key of AR
Ack	MN/AR	SID, Sequence number of the received message
Error	MN/AR	SID, Error code

3.2 Protocol Operation

ARs periodically transmit *AR advertisements.* These messages give new MNs necessary information about how to log into the network. In an IPv4 AN, the advertisements may instruct the MNs to use DHCP to acquire an initial IP address, or to use their home address in the login procedure. An IPv6-enabled MN could use the IPv6 stateless address auto-configuration or DHCPv6.

The LMMP login procedure is presented in Figure 3, and the controlled logout procedure is presented in Figure 4. The LMM protocol deployed within the AN must also support a timeout-based logout, so that data structures related to an MN are removed if the MN has disappeared. The network can also send the logout message to the MN informing that the connectivity will be dropped.

In order to perform a mobile-initiated planned handover, LMMP prehandover procedure, as presented in Figure 5, is carried out before the actual link-layer handover. After this phase, or to just perform an unplanned handover, messages are exchanged as presented in Figure 6.

Figure 7 presents the messaging when the network initiates a handover. The *Init Handover* message sent by the network may suggest that the MN should change its point of location, or force the MN to

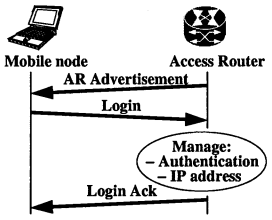

Figure 3. Login procedure.

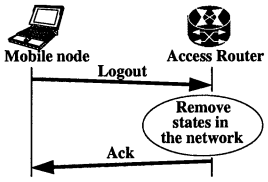

Figure 4. Logout procedure.

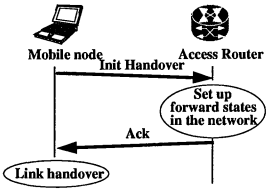

Figure 5. Pre-handover procedure.

move elsewhere. The message can indicate a specific target for the handover.

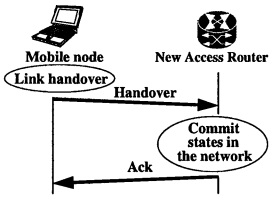

Figure 6. Handover procedure.

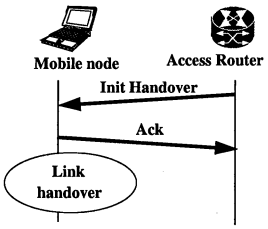

Figure 7. Network-initiated handover procedure.

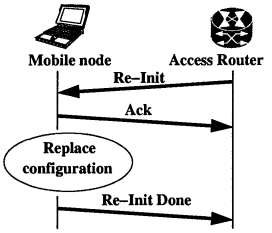

Figure 8. Forced re-initialization procedure.

A *Re-Init* message can indicate that the MN must or should update its data structures. If the update is mandatory, the MN changes its data structures and replies with the *Re-Init Done* message. Changing the IP address assigned to the MN may have many consequences, e.g.,

- Session Initiation Protocol-based sessions will need to issue a Re-Invite to the new IP address,
- Datagram Congestion Control Protocol-based transfers must send a Move message, and
- If MIP is not used, UDP- and TCP-based transfers must be restarted.

The re-initialization can also be delayed, e.g., until all existing transfers have concluded. This kind of feature would be needed, e.g., with the BCMP protocol. The more the MN moves away from its original BCMP anchor point, the more the routing paths become sub-optimal. Therefore, in order to optimize routing, the MN should at some point in time switch to a new anchor point and start to use an IP address

that belongs to this new anchor. Figure 8 shows the messaging for a suggested re-initialization of the MN.

Some mobility management technologies require that MNs periodically refresh their routing state. Therefore, LMMP includes routing refreshment, but this functionality is not needed in all networks.

To our best knowledge, IP paging has not been deployed yet, but the LMMP specification includes a basic IP paging functionality. ARs may advertise more than one PID, because the paging areas may overlap, and an AR may simultaneously belong to several paging areas. An MN chooses by itself one PID during the login, or the AN can indicate one. When the MN wants to enter idle mode, it sends a *Paging refresh* message. The MN sends these messages also periodically. If the MN goes through a handover and receives an AR advertisement that does not include the PID, it will choose a new paging area, and sends a new paging refresh. When the network has data packets destined to the MN and does not have accurate location information, the MN is paged. The mechanism to do this paging within the AN is out of scope of this specification, but once an AR wants to reach the MN, it sends a *Paging query* message to the MN. The MN responds with a *Handover*.

3.3 Security Issues

The LMMP protocol includes many functions that are critical to security. The minimum level is message authentication. Without message authentication a third party can masquerade as the AR or as the MN, and send malicious messages, e.g., a logout message.

We have identified three schemes to secure the LMMP messaging. The first one is to use a separate authentication protocol, such as, the Protocol for Carrying Authentication for Network Access (PANA) (Forsberg et al., 2004), before the MN is about to log into the network. PANA is the most recent IETF effort to define a common link-layer independent transport protocol for Extensible Authentication Protocol (EAP) (Blunk et al., 2004) so that network access can be authenticated. PANA can carry any authentication method that can be specified as an EAP method. The mechanism also allows negotiation of all keying material to be used with securing LMMP exchanges. The second scheme is to omit IP layer authentication and to trust link layer specific mechanisms. This would be possible, e.g., with a secure IEEE 802.11 wireless LAN.

The third scheme is the following hybrid IP-layer key distribution scheme built from (Needham and Schroeder, 1978) and (Shelby et al., 2000). Public key cryptography is used to secure the key exchange between the MN and AR. During this handshake a per-session shared secret

key is built (K_{an-mn}). This key is used to authenticate all further messages in a LMMP session. The scheme requires that each AR has its own public (PK_{ar}) and secret key (SK_{ar}), the MNs all have their own public (PK_{mn}) and secret key (SK_{mn}), and there exists a secret key shared by all ARs in the AN (K_{an}). The operation of the scheme is the following:

1 When an MN wants to log in to the network, it first sends its PK_{mn} to the AR in a *Key Exchange Request.*

2 When the AR receives the message, it chooses a nonce N_1, adds its own PK_{ar}, encrypts these two pieces of information with the received PK_{mn}, and sends these then to the MN in a *Key Exchange Reply.*

3 When the MN receives this message, it decrypts N_1 and PK_{ar} with its own SK_{mn}, chooses a second nonce N_2, encrypts both nonces with PK_{ar} in a *Login* message, and sends it to the AR.

4 When the AR receives the *Login*, it can decrypt N_1 and N_2 using SK_{ar}, and verify N_1. During the login procedure, a session ID (SID) is chosen for this MN. The AR then calculates an MD5 hash from $\{K_{an}, SID\}$. This is the secret key K_{an-mn} shared between the MN and the AN. K_{an-mn} and the nonce N_2 are then encrypted using PK_{mn}, and sent to the MN in the *Login Ack* message.

5 Finally, the MN can verify the nonce N_2 received in the *Login Ack.*

Further LMMP messages belonging to this session carry a Message Authentication Code (MAC) calculated from all the LMMP fields with a key exchanged previously. If the presented third scheme is used, the authentication is calculated with K_{an-mn}. When the MN makes handovers and appears under a new AR, the new AR can extract the unencrypted SID from the message, calculate by itself the K_{an-mn}, and verify the authenticity of the message. The default algorithm for calculating the MAC is HMAC-MD5.

3.4 Implementation

In order to validate our design, we have implemented LMMP as open source. The software implements the LMMP messaging with the internal authentication scheme, and provides hooks to integrate the software with existing LMM protocols[1]. The LMMP is implemented as a library, and

[1]The software, and the encoding and full structure of the LMMP messages can be found at `http://www.cs.helsinki.fi/Jukka.Manner/`.

we have two client software, one for MNs and for ARs, that make use of the library calls to send and receive ICMP messages with LMMP payloads. All state keeping is done by the client software, e.g., ARs store a list of data structures that hold information about each MN, e.g, the SID, the shared authentication key, the IP address, the LMMP protocol state of the MN, and when it was last heard.

Integration of LMMP with existing LMM schemes, such as CIP or BCMP, would be quite straightforward. A CIP-based AN would need the ARs to be modified, but the core of the AN would remain. The biggest change would be the addition of the concept of a session identifier, and the key exchange. A basic LMMP-CIP implementation would not need to implement the re-initialization of an MN, and the network-initiated handover. The messaging in BCMP is already quite close to LMMP, and only requires minor modifications.

We have not performed any performance analysis targeted at LMMP. Our work is about an interface specification, and validation of the operational logic. Transmission times and the processing of the messages is in direct relation to the available link bandwidth, and to the processing power of the nodes. However, there are certain design considerations that can affect the operation of LMMP, e.g., when messages are lost, what should the retransmission strategy be for each message type? Some messages, e.g., a forced *Re-Init*, should be resent more aggressively than others, e.g., a suggested *Re-Init*. Also, how many routing or paging refresh messages could be lost before the AN decides that the MN has disappeared? Our open source implementation allows anyone to evaluate LMMP to see whether it would fulfill the goal of a unified local mobility management protocol.

4. Conclusions

This paper presented a design for a universal local mobility management messaging between MNs and ARs. The LMMP protocol only discussed the messaging over the wireless link, and leaves out the messaging within the AN. This allows experimenting with different access network internal LMM schemes.

Future work around LMMP should focus on a more thorough analysis of how the protocol could be integrated with PANA. Also, it would be interesting to integrate LMMP with the IETF Context Transfer (Loughney et al., 2004) and Candidate Access Router Discovery (Liebsch et al., 2004) protocols. Moreover, the *Login* message could be extended to allow requesting more than one IP address or a subnet prefix for nodes within a mobile network.

References

Blunk, L., Vollbrecht, J., Aboba, B., Carlson, J., and Levkowetz, H. (2004). Extensible authentication protocol EAP. Internet draft (work in progress). (draft-ietf-eap-rfc2284bis-09.txt).

Boukis, C., Georganopoulos, N., and Aghvami, H. (2003). A hardware implementation of BCMP mobility protocol for IPv6 networks. In *Proceedings on the IEEE Global Communications Conference (GLOBECOM)*.

Campbell, A. T., Gomez, J., Kim, S., Tyranyi, Z., Wan, C.-Y., and Valko, A. (2000). Design, implementation and evaluation of cellular IP. *IEEE Personal Communications*, 7:42–49.

Forsberg, D., Ohba, Y., Patil, B., Tschofenig, H., and Yegin, A. (2004). Protocol for carrying authentication for network access (PANA). Internet draft (work in progress). (draft-ietf-pana-pana-03.txt).

IST-BRAIN Project (2001). Deliverable D2.2: BRAIN architecture specifications and models, BRAIN functionality and protocol specification. (Available from: `http://www.ist-brain.org`).

IST-MIND Project (2002). Deliverable D2.2: MIND protocols and mechanisms specification, simulation and validation. (Available from: `http://www.ist-mind.org`).

Johnson, D. B., Perkins, C., and Arkko, J. (2004). Mobility support in IPv6. Request for Comments (Standards Track) 3775, Internet Engineering Task Force.

Koodli, R. (2003). Fast handovers for mobile IPv6. Internet draft (work in progress). (draft-ietf-mipshop-fast-mipv6-00.txt).

Liebsch, M., Singh, A., Chaskar, H., and Funato, D. (2004). Candidate access router discovery. Internet draft (work in progress). (draft-ietf-seamoby-card-protocol-07.txt).

Loughney, J., Nakhjiri, M., Perkins, C., and Koodli, R. (2004). Context transfer protocol. Internet draft (work in progress). (draft-ietf-seamoby-ctp-10.txt).

Needham, R. and Schroeder, M. (1978). Using encryption for authentication in large networks of computers. *Communications of the ACM*.

O'Neill, A., , and Tsirtsis, G. (2001). Edge mobility architecture - routeing and handoff. *British Telecom Technology Journal*, 19. (Available at: `http://www.btexact.com/ideas/bttj?doc=42522`).

Park, V. D. and Corson, M. S. (1997). A highly adaptive distributed routing algorithm for mobile wireless networks. In *Proceedings of IEEE INFOCOM*.

Perkins, C. (2002). IP mobility support. Request for Comments (Standards Track) 3344, Internet Engineering Task Force.

Ramjee, R., Porta, T. L., and Li, L. (2000). Paging support for ip mobility using HAWAII. Internet draft (work in progress). (draft-ietf-mobileip-paging-hawaii-01.txt).

Ramjee, R., Porta, T. L., Thuel, S., Varadhan, K., and Wang, S. (1999). HAWAII: a domain-based approach for supporting mobility in wide-area wireless networks. In *Proceedings of the Seventh International Conference on Network Protocols (ICNP)*, pages 283 – 292.

Shelby, Z., Gatzounas, D., Campbell, A., and Wan, C. (2000). Cellular IPv6. Internet draft (work in progress). (draft-shelby-seamoby-cellularipv6-00).

Soliman, H., Castelluccia, C., El-Malki, K., and Bellier, L. (2004). Hierarchical MIPv6 mobility management. Internet draft (work in progress). (draft-ietf-mipshop-hmipv6-01.txt).