A first evaluation of IP based network architectures

Klaus David[1], Philip Eardley[2], Dirk Hetzer[3],
Andrej Mihailovic[4], Tapio Suihko[5], Martin Wagner[1]

[1]University of Kassel, Germany, [2]BT, Advanced Communications Technology Centre
[3]T-Nova, Germany, [4]King's College, London, [5]Nokia/VTT Information Technology

david@uet.e-technik.uni-kassel.de, philip.eardley@bt.com, Dirk.Hetzer@telekom.de,
andrej.mihailovic@kcl.ac.uk, Ext-Tapio.Suihko@nokia.com, mwagner@uet.e-technik.uni-kassel.de

Abstract

The BRAIN project is investigating a broadband IP-based network solution to complement UMTS. For this to become a reality, both macro and micro-mobility functionalities have to be supported. While macro-mobility will be done by Mobile-IP, there are several proposals for supporting micro-mobility. The first section of this document will present the Mobile-IP protocol, together with its known problems and possible solutions. The second section will provide an initial comparison of recent proposals of micro-mobility protocols.

1. Introduction

The interest of this paper is, how several functionalities, detailed in table 1, have to be supported. This paper discusses these functionalities and will provide an evaluation of different architecture issues.

Table 1: principal functionalities of mobile networks

Functionality	GSM/UMTS	BRAIN
Location Management (Macro-Mobility)	MAP	Mobile IP
Handover	MAP	open, proposals
Security features	MAP+	open, proposals
Protocol interworking	open	open

The main problem is how host mobility (also known as terminal mobility) is realised in an IP network. The principal problem is: when a mobile host[1] (MH) moves onto a new Access Point (AP), how do we route packets to its new destination? We would like a solution that:
- keeps the break in communication during the handover as short as possible. No (or only a few) packets should be lost. Hence all applications, including the real-time ones, are supported.
- lowers the overhead from messaging to achieve the re-routing. Included here is minimising the signalling load and latency, and also the storage and processing requirements at each router.
- is compatible with other internet protocols, e.g. it does not interact adversely with Quality of Service (QoS) protocols.
- is scaleable, e.g. we can apply it whether we have a small or large number of MHs.

The basic mobility problem is, how to know where a MH is connected to the Internet and to route all packets destined to it to its temporary access point. A well known solution for that is Mobile-IP [1], which solves the problem using two IP addresses per MH - one acts as its permanent identifier, whilst the other acts as its temporary routable address (CoA, care-of-address). Mapping between these two is stored at its Home Agent (HA). Due to the known limitations of Mobile-IPv4 [2] (limited address space, need of foreign agent, security problems...), Mobile-IPv6 [3] is the more preferable solution. However, MIPv6 is a long way from the ideal solution outlined above. For example:
- Handovers may not be fast and smooth, because the MH must signal its change of CoA to the HA. This may take a long time if the HA is far away, perhaps in a different country.

[1]Also called mobile terminal or node

- The messaging overhead may be significant particularly if the HA is distant, as this will induce signalling load in the core of the internet.
- MIP may interact with QoS protocols (DiffServ, IntServ), so making QoS implementation problematic. For example, MIP uses tunnels, so packet headers, which contain QoS information, become invisible.

However, MIP is relatively simple and robust and is likely to be ubiquitous. It thus appears to be a good way of handling macro mobility between different operators. Section 2 describes the design principles of the Mobile-IPv6 protocol.

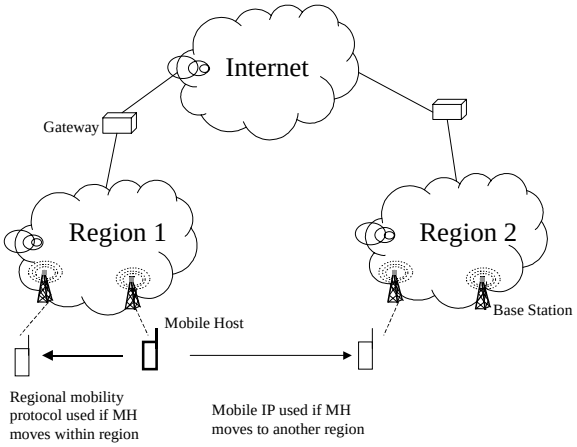

Figure 1: Macro vs micro-mobility management

Meanwhile, more optimised solutions are developed for micro-mobility. These add fine scale localisation to the raw localisation done by MIP, thus reducing the signalling load in the core of the network and improving re-routing latency. Our overall solution therefor consists of MIP, to handle macro mobility, bolted onto a specialised micro-mobility scheme (Figure 1). In Section 3 we compare various micro-mobility proposals.

2. Mobile IPv6

In this section, we outline some basic characteristics of Mobile IPv6. Mobile IPv6 is intended to enable IPv6 nodes to move from one subnet to another. It is both suitable for mobility between subnets across homogenous and inhomogeneous media. The protocol allows a mobile node to communicate with other hosts (correspondent host, CH) after changing its point of attachment from one subnet to another. A mobile node is always addressable by its home address, and packets will be routed to it using this address (Figure 2).

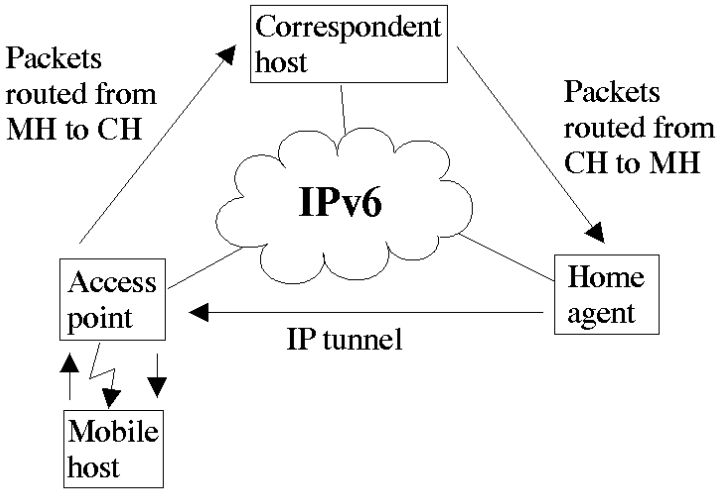

Figure 2: Triangle routing

2.1. Location Management

Mobile nodes will have assigned to their network interface two IPv6 addresses whenever they are away from their home subnet. One is its home address, which is permanently assigned to the mobile node in the same way as any IP node. Mobile IPv6 adds a second address, known as the mobile node's care-of address, which is associated with the mobile node only while visiting a particular foreign subnet.

Each time the mobile node moves its point of attachment from one IP subnet to another, the mobile node will configure its care-of address by methods of IPv6 Neighbour Discovery. The association between a mobile node's home address and its care-of address, along with the remaining lifetime of that association, is known as a binding. The central data structure used in Mobile IPv6 is a cache of mobile node bindings, maintained by each IPv6 node, known as a Binding Cache.

While away from home, a mobile node registers one of its bindings with a router in its home subnet, requesting this router to function as the home agent for the mobile node. While it has a home registration entry in its Binding Cache, it intercepts any IPv6 packets addressed to the mobile node's home address on the home subnet, and tunnels each intercepted packet to the mobile node's care-of-address indicated in this Binding Cache entry. To tunnel the packet, the home agent encapsulates it using IPv6 encapsulation.

In addition, Mobile IPv6 provides a mechanism for IPv6 correspondent nodes communicating with a mobile node, to dynamically learn the mobile node's binding. When sending a packet to any IPv6 destination, a node checks its Binding Cache for an entry for the packet's destination address, and if a cached binding for this address is found, the node routes the packet directly to the mobile node at the care-of-address indicated in this binding; this routing uses an IPv6 Routing header instead of IPv6 encapsulation, as this adds less overhead to the size of the packet. (The home agent cannot use a Routing header, since adding one to the packet at the home agent would invalidate the authentication in any IPv6 Authentication header included in the packet by the correspondent node). If no Binding Cache entry is found, the node instead sends the packet normally (with no Routing header), and the packet is then intercepted and tunneled by the mobile node's home agent as described above.

2.2. Handover

The mobile node detects the unreachability of its default router while the mobile node is actively sending packets either through indications from upper layer protocols that a connection is not making progress (e.g. TCP timing out) or through the failure of receiving any packets (the mobile node may continually probe its default router with Neighbour Solicitation messages if it is not otherwise sending packets to it).

While the mobile node is moving from one cell to another it is configuring a new care-of-address for the new point of attachment, and report it to its home agent (by the way of a Binding Update). Until the Binding update has been successful, it will receive the remaining packets via the old access point or send another Binding Update to the old access point which redirects the data to the new one. The latter technique can be used to reduce the handover latency time rapidly. If one of the micro-mobility protocols discussed in chapter 3 is being used, this time can be reduced even more.

2.3. Security

- Authentication: All packets used to inform another node about the location of a mobile node must be authenticated. Otherwise, traffic intended for a mobile node could be hijacked and redirected to a malicious host. Authentication is being done by an IP Authentication Header (AH) [5]. The AH contains an Integrity Check Value field, which contains a value supplied by various algorithms including keyed Message Authentication Codes (MACs) based on symmetric encryption algorithms (e.g. DES) or on one-way hash functions (e.g. MD5 or SHA-1).

- Encryption: Because it is very easy to listen to the transmitted data, encryption is a must in tetherless communication. This is being done by encrypting the security payload (ESP) [6], encapsulating it into a pair of ESP-Headers/Trailers and adding the original IP header. Encryption algorithms are: DES in CBC mode, HMAC with MD5, HMAC with SHA-1, NULL (no encryption). If both authentication and

encryption is wanted, encryption is performed first. This enables the host to reject bogus packets rapidly without decrypting them first.

2.4 Protocol Integration

TCP connections are being slowed down at packet loss but on wireless links packets only have to be resent (The loss of a packet due to noise is much more likely than router congestion). One possible solution to this problem is to split the connection into multiple TCP connections. One disadvantage hereby is, that no end-to-end acknowledgement can be accomplished. Another is to use fast recovery algorithms as described in RFC 2001 [4]. However, some bandwidth will still be lost.

One problem that currently occurs due to tunnelling the packets is that resources on the air-interface are lost due to IP tunnelling that ends at the mobile node (no foreign agent in IPv6). Although the IP tunnel is only used between HA and MH, we can use header compression on that link. Encryption is not concerned since it is applied only to the inner packet. If the MH wants to communicate with a CH directly, it can notify of its current binding so that the CH can create or update entries in its Binding Cache. Before sending a packet to any destination address, the CH must check its Binding Cache for an existing binding for this address. If a binding was found, it will use IPv6 routing headers to send the packets from the correspondent node directly to the mobile node.

A problem caused by using tunnels occurs, if QoS services are needed. Tunnelling the IP packets from HA to MH hides the QoS information the original IP header contained. A solution for that would be copying the related field from the inner IP header to the outer one. In case of DiffServ, however, it is allowed to change the outer header during the node processing. When tunnel is not end-to-end, as is with Mobile IP, it should be copied back to the inner header upon decapsulating the packet.

QoS on a link from CH to MH established by a Binding Update will work fine since there are IPv6 routing headers used.

3. Comparison of Micro-Mobility proposals

The two major categories of Micro-Mobility protocols are [7]:

- Proxy-Agent Architectures (PAA)
- Localised Enhanced-Routing Schemes (LERS)

The PAA schemes extend the idea of Mobile IP into a hierarchy of Mobility Agents (which are extensions of MIP's Foreign Agents and/or Home Agents). A MH registers with its local Agent at the bottom level of the hierarchy, which in turn registers with its nearest Agent, and so on up the hierarchy toward the HA. This way, changes of the MH care-of-address travel up the hierarchy, while packets from a CH travel down, being tunnelled from one level to the next. As a representative protocol from this category, we will take a look at Mobile IP Regional Registration [8].

The LERS schemes include several distinctive approaches:

Per host forwarding schemes: Inside a domain, a specialised path set-up protocol is used to install soft-state host-specific forwarding entries for each MH. The domain, which appears as a subnet to routers outside the domain, is connected to the Internet via a special gateway, which must be pointed to by the default gateway of the routers inside the domain. For that category, we will examine the Handoff-Aware Wireless Access Internet Infrastructure (HAWAII) [9].

Multicast-based schemes: Multicast protocols are designed to support point-to-multipoint connections. So they share with IP mobility the same design goals of location independent addressing and routing and thus multicast-based mobility solutions have been proposed. A multicast-CoA is assigned to a single MH which can then be used to instruct neighbouring multicast-enabled routers to join the MH's virtual multicast group,

either prior to or during handovers. This can be visualised as a multicast cloud centred on the MH's current location but also covering where it may move to. An example is the Multicast for Mobility Protocol (MMP) [10].

MANET-based schemes: MANET protocols were originally designed for Mobile Adhoc NETworks, where both hosts and routers are mobile, i.e. there is no fixed infrastructure. The routing is multi-hop and adapts as the MHs move and connectivity in the network changes. MANET protocols can be modified for our scenario, where there is a fixed infrastructure and only hosts can be mobile. Currently there is only one proposal in this category: MER-TORA [11], where each node builds, and then maintains, a Directed Acyclic Graph after identifying its neighbours.

Table 2 summarises how our representative protocols tackle each Protocol Design Issue. This is followed by a discussion.

Table 2: Summary of how exemplar protocols tackle each Protocol Design Issue

	Regional Registration	HAWAII	Multicast for Mobility Protocol	MER-TORA
Packet forwarding (downstream)	sequential tunnels	host routes for end-to-end encapsulated packets	multicast forwarding (multicast encapsulation)	prefix-based route to cross-over router; host-specific route below
Path updates	MIP + regional registration extensions (UDP)	UDP Path Updates	CBT Join/Ack + ICMP (Instruct)	UNICAST-UPDATE message from old-AR to new-AR for installing hard state, host-specific routes
Handover management	MIP, Route Optimisation	Forwarding/Non-Forwarding schemes	multicast join, advance registration, simultaneous bindings	localised at the edge of the network; inter-Access Router (AR) tunnelling
Support for idle MHs	No	paging using IP multicast	reduced signalling in wired network	No
Requirements for MHs (in addition to basic MIP support)	I flag, registration keys as in MIP Route Optim., multiple level registrations	FA-NAI, MN-NAI, Challenge/Response, Route Optimisation	MIP Route Optim., multicast CoA	TORA, address acquisition, tunnel initiation, address return
Requirements for core network interface	HA must be able to handle the GFA IP Address extension	HA must accept registrations generated without an MN-HA authentication extension	HA must accept registrations generated without an MN-HA authentication extension	no distinction between 'macro' and 'micro' mobility
Address management	Co-located CoA (bypasses the domain hierarchy), or FA-CoA	static Co-located CoA in foreign domain**,** Home Address in home domain	MH retains a multicast IP address within the domain. Ingress router seen as FA.	AR allocates an IP address from set it 'owns'. De-allocated at session end.
Routing topology	static configuration of enhanced MIP FAs in a tree structure	all nodes must be HAWAII-aware; standard routing protocols keep the default route up to date	all nodes must support CBT IP multicast (sparse mode)	all routers in a tree or in a mesh implement TORA (proactive prefix-routing + reactive host-routing)
Security	MIP + key distribution and authentication according to MIP-RO (FA-Key Reply extension) / DIAMETER		assumes Security Association between FA and HA	use of existing mechanisms (RADIUS / shared keys / MIP+AAA)

We now give a qualitative discussion of each Protocol Design Issue in turn, comparing our four exemplar protocols and drawing out points of interest.

3.1. Packet Forwarding

The main contrast here is between, on the one hand, Regional Registration and MMP which extensively use tunnels, and on the other hand HAWAII and MER-TORA which do not. Regional Registration forwards downstream data within the domain using sequential tunnels between FAs. This may be *inefficient*, although packet de-capsulation and encapsulation can be avoided by changing the IP addresses in the encapsulating header. With MMP packets are encapsulated by the ingress router into multicast packets and are forwarded

using CBT interface-based routing. However, the major concern with tunnelling is that it obscures the original header, so making *applicability* of capabilities that depend on header fields more difficult (e.g. QoS). For Regional Registration, HAWAII and MMP, upstream packets can be forwarded with the same mechanisms that are defined for basic Mobile IP (e.g. using reverse tunnelling). On the other hand, MER-TORA uses the MER-TORA protocol for up and down-stream packets. In MMP packets destined for another MH within the domain are sent up to the ingress router, which reverses them back to the target MH.

3.2. Path Updates

There are some interesting contrasts here. HAWAII and MMP both use soft-state path updates that are aggregated / merged as they travel up the tree, whilst MER-TORA uses hard state path updates[2]. Both methods aim to improve *scalability*. A quantitative comparison between them will be carried out later. Next, compare what happens as a MH changes its point of attachment: in MER-TORA it results in more host-specific state being installed (which 'over-rides' the prefix-based routes); whilst this is not so for the other schemes, essentially because their routing is entirely host-specific. Again, this will impact on the *scalability*, and the comparison may depend on how frequently the MH moves to another BS (for example). For both Regional Registration and HAWAII, a raceless (*robust*) and yet simple path management scheme is difficult to achieve if handoffs occur quickly [8, 12]. Because Regional Registration reuses the existing Mobile IP protocol messages, it can leverage on the recent enhancements to Mobile IP (e.g., for authenticating path updates), making its *deployment* easier. On the other hand, the scheme does not directly fit into the IPv6 mobility framework.

3.3. Handover Management

All the protocols suggest conceptually very similar mechanisms for supporting fast and smooth handovers. Essentially, packets are forwarded from the old to the new base station after a handover and/or a route is set up to the new BS before the connection via the old one is lost. There is no obvious reason why one class of protocol should inherently perform better than another class. MMP has inherent support for simultaneous bindings through its advance registration feature, which may prevent packet loss during handovers; whilst HAWAII can optionally use dual-casting from the cross-over router, and it appears that this capability could also be added to MER-TORA if required. Regional Registration uses standard MIP move detection mechanisms, extended if necessary with fast handover support [13, 14, 15], and smooth handovers as specified in MIP Route Optimisation [16]. Similarly, both HAWAII and MER-TORA can optionally deliver, from the old to the new BS, packets that would otherwise be lost during handover. There are differences, however: in the Single Stream Forwarding sub-scheme HAWAII uses what it calls 'interface-based forwarding' which means that the outgoing interface (on which to forward the packet) is determined by both the IP address and the incoming interface, whilst MER-TORA uses a temporary tunnel. However, in MER-TORA if there is no tunnel when the link to the MH is lost (e.g. because handover is not predicted), then a virtual link is constructed to the MH from the old BS. It retains this for some time in the hope that it will be notified of the MH's new location. This virtual link should improve *robustness*, compared to the routing loops that can transiently appear in some HAWAII sub-schemes. There has been some work to try and quantify the *efficiency* of handover schemes, e.g. [12] compared HAWAII to basic and route optimised MIP. However, there are no similar papers comparing all four of our protocol classes.

3.5. Support for Idle Mobile Hosts

Apart from HAWAII, paging seems to have received relatively little attention. Its proposal uses administratively scoped IP multicast [17] to distribute paging requests to BSs. This should push paging to the edge of the access network, which assists in *scalability* and *robustness*. A similar scheme is probably widely applicable to other IP mobility protocols. MMP naturally tracks MHs as they move, through the standard messages to join to / prune from the multicast tree. It is suggested that the location management overhead may be able to be reduced for idle hosts by reducing the refresh frequency of the CBT "soft state" mechanism. A paging protocol has also been proposed for Regional Registration [18]. The protocol aims at independence of link layer technologies; the MH agrees a 'sleep pattern' with the network, which requires synchronised sending of Paging Agent Advertisements from FAs belonging to the same Paging Area.

[2] more accurately, hard state updates for the mobility related changes in topology, and both hard and soft state updates for non-mobility related changes.

3.6. Requirements for Mobile Hosts

HAWAII and MMP appear to have the *simplest* requirements on MHs, i.e. only MIP capability with extensions. However, a dumb MH might not be able to accept a multicast IP address as a CoA. In HAWAII the MH must be able to acquire a co-located CoA in a foreign network; in MER-TORA, [11] suggests that a FA-CoA must be acquired. In Regional Registration the leaf FAs support basic MIP which guarantees the *compatibility* with dumb MHs.

3.7. Address Management

Address management is a key issue and a significant contrast between the protocols. With HAWAII, MMP and MER-TORA a MH keeps its IP address throughout the lifetime of the session (or longer), at least while it is in the same domain. This would (for example) ease the *applicability* of RSVP-based QoS support. By contrast, in Regional Registration the CoA changes at each handover. HAWAII requires that in a foreign network a MH acquires a publicly routable co-located CoA. Given the scarcity of public IPv4 addresses, this is a major drawback from the point of view of *scalability*. Also, because the CoA must be unique within a domain, a co-ordinated address allocation mechanism must be available. Regional Registration can also use a co-located CoA, and then similar comments would apply. But it can also use a FA-CoA and then IPv4 address exhaustion is not a problem. Within the domain, private CoAs can be used since they are not visible outside the domain. In MER-TORA, a MH is allocated an IP address by the BS (more accurately, the Access Router) where it starts a 'session', from the IP address block that the BS 'owns'. The pros are: fully prefix-based routing until the MH moves so minimising host-specific routing, and consistent address allocation across domain is *simple* since each AR owns its own address block. The cons are: more addresses are probably needed than for a IP mobility scheme with flat addressing across the domain, and more frequent address de-allocation is required (for *scalability* the IP address should be returned as soon as possible, e.g. at the end of an active session and not just when the MH powers down). If the number of MHs is large and their sessions short, then clearly a good, scalable DHCP implementation is needed. In MMP, the MH acquires a multicast CoA, so the shortage of IPv4 multicast addresses appears to be a major *deployment* problem. This should be less so in IPv6.

3.8. Routing Topology

Clearly, the relevant routing protocol capability needs to be *deployed* in the nodes in the network. The effort is probably greatest for MER-TORA, because standard unicast routing (e.g. OSPF) is replaced by TORA. However, [19] argues that it will give *scalability* advantages. *Robustness* is probably best for MER-TORA, since TORA was originally designed for mobile ad hoc networks (MANETs) so it will react immediately to any failure of links or routers. HAWAII relies on standard routing protocols for detecting failures; by integrating HAWAII with a routing daemon, a change in default route can trigger soft-state refreshes to HAWAII paths. Regional Registration and MMP would also rely on standard protocol recovery mechanisms to adopt to changes and failures. Regional Registration uses a central routing tree, whilst the others can have a tree or mesh topology.

4. Conclusion

In this paper we have both presented the Mobile-IP protocol, together with its known problems. Some of these problems can be solved (our reduced), by implementing a micro-mobility solution. Although evaluation criteria have been identified [10], a decision, which proposal should be favoured, is not finally clear yet. We plan to deal with this later in our work.

From the discussion of the Protocol Design Issues it can be deduced that some bear more importance and complexity than others. Handover mechanisms and the interface between the mobile host and the access network entities appear surprisingly similar, whilst address management is a key differentiator.

Our goal is to produce a clear perspective of the functionalities that need to be achieved by a new (or evolved) IP-mobility protocol, which we plan to propose at the final stage of our project. Another possible future direction could be designing a standard interface, or a standard architectural approach to IP micro-

mobility. Already there is some effort in this direction: the Edge Mobility Architecture (EMA) [19] and Open Base Station Architecture (OBAST) [20], both of which aim to create a common approach to IP mobility whatever the wireless link technology.

5. Acknowledgement

This work has been performed in the framework of the IST project IST-1999-10050 BRAIN, which is partly funded by the European Union. The authors would like to acknowledge the contributions of their colleagues from Siemens AG, British Telecommunications PLC, Agora Systems S.A., Ericsson Radio Systems AB, France Télécom - R&D, INRIA, King's College London, Nokia Corporation, NTT DoCoMo, Sony International (Europe) GmbH, and T-Nova Deutsche Telekom Innovationsgesellschaft mbH.

6. References

[1] C. Perkins, Mobile IP - Design Principles and Practices, January 1998
[2] C. Perkins, ed., IP Mobility Support, RFC 2002, October 1996
[3] C. Perkins, D. Johnson, Mobility Support in IPv6, Internet draft draft-ietf-mobileip-ipv6-12, April 2000
[4] W. Stevens, TCP Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery Algorithms, RFC 2001, January 1997
[5] S. Kent, R. Atkinson, IP Authentication Header, RFC 2402, November 1998
[6] S. Kent, R. Atkinson, IP Encapsulating Security Payload (ESP), RFC 2406, November 1998
[7] P. Eardley, A. Mihailovic, T. Suihko, A Framework for the Evaluation of IP Mobility Protocols, June 2000
[8] E. Gustafsson, A. Jonsson, and C. Perkins, Mobile IP Regional Registration, Internet Draft, draft-ietf-mobileip-reg-tunnel-02, March 2000
[9] R. Ramjee, T. La Porta, S. Thuel and K. Varadhan, IP micro-mobility support using HAWAII, Internet Draft, draft-ietf-mobileip-hawaii-00, June 1999
[10] A. Mihailovic, M.Shabeer, A.H. Aghvami, Multicast for Mobility Protocol (MMP) for emerging internet networks, To appear in Proceedings of PIMRC2000, London, UK, September 2000
[11] A. O'Neill, G. Tsirtsis, and S. Corson, Edge Mobility Architecture, Internet Draft, draft-oneill-ema-01.txt, March 2000
[12] R. Ramjee et al., HAWAII: A Domain-based Approach for Supporting Mobility in Wide-area Wireless networks, 1999
[13] P. Calhoun, H. Akhtar, E. Qaddoura, and N. Asokan, Foreign Agent Keys Encoded as Opaque Tokens for use in Hand-off Process, Internet Draft, draft-calhoun-mobileip-fa-tokens-00.txt, March 2000.
[14] J. Kempf and P. Calhoun, "Foreign Agent Assisted Hand-off, Internet Draft, draft-calhoun-mobileip-proactive-fa-01.txt, June '2000
[15] K. El Malki and H. Soliman, Hierarchical Mobile IPv4/v6 and Fast Handoffs, Internet Draft, draft-elmalki-soliman-hmipv4v6-00.txt, March '2000
[16] C. Perkins, D. Johnson, Route Optimization in Mobile IP, Internet Draft, draft-ietf-mobileip-optim-08.txt, February '1999
[17] R. Ramjee, T. La Porta, and L. Li, Paging support for IP mobility using HAWAII, Internet Draft, draft-ietf-mobileip-paging-hawaii-00.txt, June 1999
[18] H. Haverinen and J. Malinen, Mobile IP Regional Paging, Internet Draft, draft-haverinen-mobileip-reg-paging-00.txt, June '00
[19] A. O'Neill, G. Tsirtsis, and S. Corson, Edge Mobility Architecture, Internet Draft, draft-oneill-ema-01.txt, March '2000
[20] Discussion on OBAST in 'cellular' IETF mailing list. cellular@cdma-2000.org