Solutions for IPv6-based mobility in the EU project Moby Dick

M. Liebsch, X. Pérez, R. Schmitz, A. Sarma
NEC Europe Ltd.
Adenauerplatz 6
69115 Heidelberg
Germany
+49 6221 13708-19
+49 6221 90511-55
mobile@ccrle.nec.de

J. Jähnert
University Stuttgart
National Super-computing Center
Germany
+49 711 685 4273
+49 711 678 8363
jaehnert@rus.uni-stuttgart.de

S. Tessier
T-Systems Nova
Goslarer Ufer 35
10589 Berlin
Germany
+49 30 3497-3114
+49 30 3497-3199
tessier@t-systems.com

M. Wetterwald
Institut Eurecom
BP 193, 06904
Sophia Antipolis
Cedex, France
+33 4 9300-2631
+33 4 9300-2627
wetterwa@eurecom.fr

I. Soto
University Carlos III Madrid
Av. Universidad 30
28911 Leganés (Madrid) Spain
+34 916245974
+34 916248749
isoto@it.uc3m.es

Email for all authors: wtc2002_1246@ccrle.nec.de

Abstract: Mobile Internet technology is moving towards a packet-based or, more precisely, IPv6-based network. Current solutions on Mobile IPv6 and other related QoS and AAA matters do not offer the security and quality that users have come to take for granted. The EU IST project Moby Dick has taken on the challenge of providing a solution that integrates QoS, mobility and AAA in a heterogeneous access environment. This paper focuses on the mobility part of the project, describes and justifies the handover approach taken, shows how QoS-aware and secure handover is achieved, and introduces the project's paging concept. It shows that a transition to a fully integrated IP-RAN and IP-Backbone has become a distinct option for the future.

Keywords: Mobile IPv6, IP paging, handover latency, handover simulations, auto-configuration

1. Introduction

The availability of mobility on the Internet is often seen as an important enabler for the introduction of IPv6. Besides just being reachable anywhere in the network via a care-of-address, Mobile IPv6 together with additional techniques, such as fast handover, allows one to keep a connection without noticeable interruption while moving with the terminal (seamless handover). However, such a mobile scenario with heterogeneous wireless and wireline access poses a range of new problems, especially if authorised, chargeable access to the network with sustained quality via changing administrative domains is required.

The IST project Moby Dick [1] aims to implement such a full IPv6 network that is able to support heterogeneous access technologies across administrative domains. Though much work and a number of Internet Drafts deal with mobility, Quality of Service (QoS) as well as Authentication, Authorisation and Accounting (AAA), it is their combination towards secure, and QoS-enabled mobility towards fundamentally new application scenarios and business models that is required, and for which no solution exists today. This paper presents a snapshot of the mobility management view within the project Moby Dick and some of the solutions proposed to provide the above-mentioned integration. Other aspects not dealt with in detail here are the Moby Dick concepts of AAAC (AAA, auditing and charging), our solution for QoS matters, and the details of the planned integration of software modules towards a full implementation, which will be used for a field trial due in 2003.

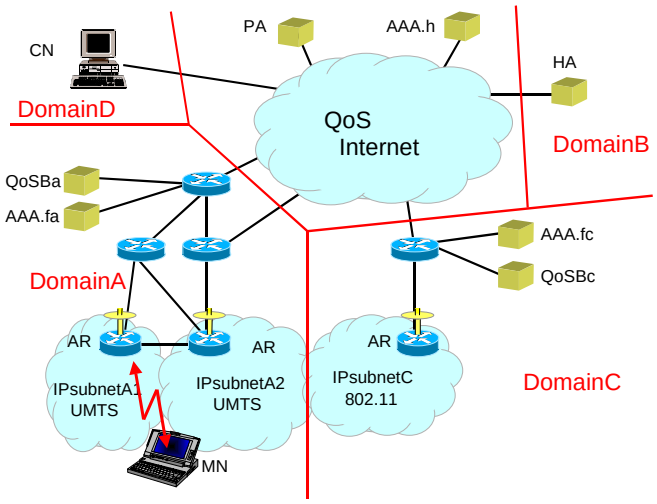
Section 2 in this paper introduces the Moby Dick architecture and outlines major goals of the project. The project's simulations and analytical work in Section 3 provide the basis of some of the decisions taken in the project, some of which deviated from the technically most ideal ones for pragmatic reasons. Section 4 shows the Moby Dick approach to use the fast handover technique to optimise the transfer of context information, such as the QoS part of the user profiles and AAA relevant information. This optimisation is essential to not lose all the benefits of fast handover in reducing latency and data loss. In Section 5, the project's paging approach is introduced. Conclusions and an outlook are contained in Section 6.

In all work, existing Internet Drafts and ongoing work in the IETF are taken into consideration, but some pragmatic deviations are used to achieve the goals of the project. At the same time, results and experiences from the project are and will increasingly be input into the IETF work.

2. Moby Dick Architecture and goals of project

The Moby Dick architecture follows three key design principles and goals: First, heterogeneous wireless access network should use standard IPv6-based protocols and technologies, thereby reusing as much of the capabilities of the underlying access technologies as possible. Second, the network should be able to provide real-time IP services with quality comparable to traditional cellular networks. And third, the architecture should consider

AAA elements enriched with Charging and Auditing to support the transition process from a free Internet to an economically sustainable Mobile Internet infrastructure. *Figure 1* depicts the Moby Dick network architecture, comprising QoS, mobility management and AAA related network components.



PA	Paging Agent	QoSB	QoS Broker
AAA.h	AAA Home	MN	Mobile Node
AAA.f	AAA Foreign	CN	Corresp. Node
HA	Home Agent	AR	Access Router

Figure 1: Conceptual view of the heterogeneous network

The overall network architecture of the Moby Dick approach includes two major elements:

- Mobile terminals running user processes (applications). Each terminal has interfaces using different technologies. In particular, W-CDMA, wireless LAN (802.11b), and Ethernet are used.
- Radio Gateways, providing an interface between a wireless and a wired network domain. It is assumed that these domains are different IP-subnets. These gateways are associated with the traditional concept of a Base Station, the actual access point of the wireless technology to a wired infrastructure

All data communication is based on IPv6, and QoS provisioning will follow the DiffServ model. Mobile IPv6 [2] will be used as IP mobility management protocol.

This network architecture [1], the core of the Moby Dick Project, is much simpler than traditional UMTS Terrestrial Radio Access Network (UTRAN) structures. The only radio-dependent elements are the W-CDMA interface and the radio link protocol. All other network elements, e.g. RNC, HLR, VLR, EIR, MSC, GMSC, SGSN and GGSN, as well as related interfaces and protocols are eliminated. Some functionality is replaced by a functional IP-based equivalent. Data transmission is pure IPv6 end-to-end, without permanent tunnelling protocols.

The project has completed the architectural work, most specifications and simulations, and is now in the implementation phase. The trial, running two sites in Madrid and Stuttgart, will follow in 2003.

3. Simulations and Analysis

We simulated Mobile IPv6 via ns-2 [3] for a scenario for up to three access routers (AR) and 30 mobile nodes using standard IEEE 802.11 wireless LAN [4] to compare basic MIPv6 with a fast handover procedure [7]. The study covered handover latency, packet loss, end-to-end delay, signalling load and channel utilization, and shows how various traffic types, such as UDP constant bit rate (CBR), Voice over IP (VoIP), and TCP, are affected by the handovers. We use stateless address auto-configuration and send the Mobile IPv6 *binding updates* (BU) with the newly formed care-of address via the old access router instead of via the new one. Redirection of the traffic to the mobile node (MN) will be processed directly at the receiving AR. The MN then switches to the new access router and waits for the redirected packets [5].

Figure 2 shows the studied scenario composed of a group of correspondent nodes, one for each mobile node, connected to one central router (CR) through the Internet, the access routers connected also to the CR, and ten mobile nodes per AR in the initial set-up. The distance between the access routers is 450 meters and the transmission range 250 meters. Thus, the coverage area of the access routers overlap and the mobile nodes always move randomly within the total coverage area. As mobility pattern we use the random waypoint mobility model [6].

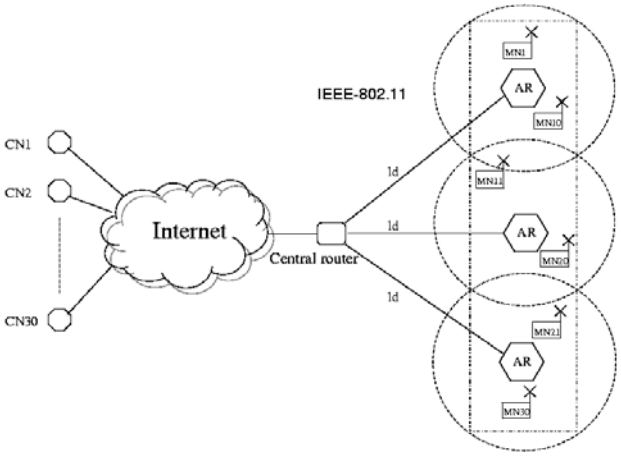


Figure 2: Simulation scenario

In *Figure 3* we can observe the variation of the latency, depending on the link delay between the AR and the CR for the fast handover procedure (MIPv6+FHO) and for basic MIPv6. The result clearly shows the advantage of using the fast handover procedure. In the extreme case of a one-second link delay, we save around two seconds of handover latency. Since packets are redirected when a BU sent by the MN reaches the MN's current AR, there is almost no time to lose a packet using the fast handover procedure. When the wired delay increases, the packet losses decrease because a data packet needs more time to arrive at the new access router, and the mobile node has

had more time to complete the handover process when the packets arrive.

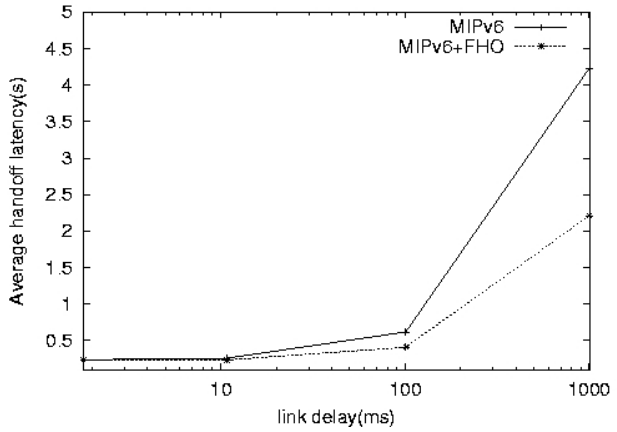


Figure 3: Handover latency enhancement

Based on these results [5], it was decided to implement the fast handover approach [7] in the Moby Dick test bed. Further likely improvements via HMIPv6 [8] are currently under study in the project. A first analytical study has shown an improvement in handover latency using a combination of FMIPv6 and HMIPv6 as compared to FMIPv6. Initial simulations seem to confirm this, and will be followed up in the project with further simulations studying the advantages of introducing HMIPv6.

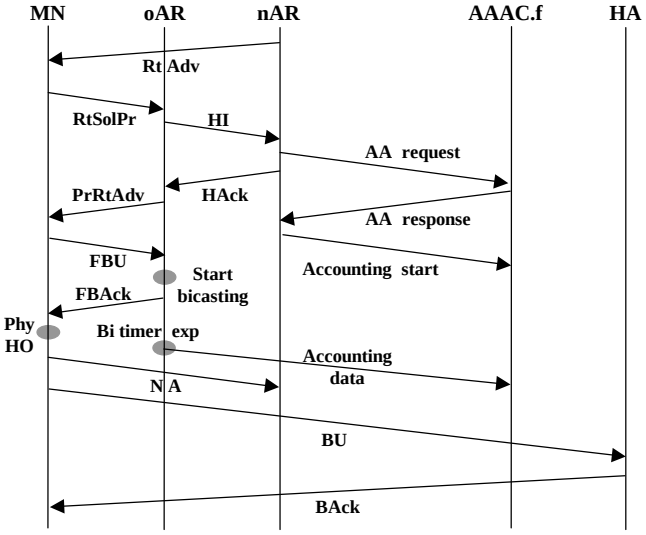
4. Handover integrating QoS and AAA elements

Within this project, we focus on fast and seamless intra-domain handover as the most likely scenario requiring uninterrupted services. Inter-domain handover requires additional, e.g. security message exchanges between administrative domains, and is not considered for this reason for this project. Furthermore, inter-domain handovers are estimated as being much less frequent. The fast handover approach [7] was selected for reasons discussed in the previous section on simulations. Further enhancements, especially with respect to the integration of AAAC (AAA plus Auditing and Charging) support, are presented here.

For this project, we assume the following:

- All Access Routers broadcast system information that is required by the Mobile Node to identify the new subnetwork prefix and configure its new care-of address.
- Static, pre-established security associations exist between:
  - the Mobile Node and the AAAC (home domain) server,
  - the AAAC (home domain) server and the Home Agent,
  - the Mobile Node and the Home Agent,
  - the AAAC (home domain) server and the AAAC (foreign domain) server, and
  - the AAAC (foreign domain) server and the Access Routers in the foreign domain
- Because this cannot pre-exist for all cases, a security association must be set up dynamically between:
  - the Mobile Node and the Access Router
- Pre-established security associations exist between *neighbour* ARs in an administrative domain.
- To keep fast handover extensions transparent to standard Mobile IP, we distinguish between *registration, fast intra-domain and inter-domain handover*, which require different handling.

4.1. Moby Dick signalling flow



RtAdv	Router Advertisement
RtSolPr	Router Solicitation for Proxy
HI	Handover Initiate
Hack	Handover Acknowledgement
PrRtAdv	Proxy Router Advertisement
NA	Neighbour Advertisement
FBU	Fast Binding Update
FBAck	Fast Binding Acknowledgement
Phy HO	Physical Handover
Bi timer exp	Bicasting timer expired
BU	Binding Update
BAck	Binding Acknowledgement

Figure 4: Moby Dick fast intra-domain handover message flow (including AAA)

In Moby Dick, the fast handover signalling flows are enhanced to carry vital QoS data and the authorisation key, as shown in *Figure 4*. The router advertisement from the new access router (nAR) carries the network prefix, which helps to identify the handover type (i.e. fast intra-domain or inter-domain). If the nAR is from the same domain, fast handover is initiated with the *router solicitation for proxy* message carrying the nAR address and the new care-of address (CoA, see next subsection) as parameters. The *HI* message from the old access router

(oAR) to the nAR then carries the new CoA, the key and the sub-profile with vital QoS information to the nAR, allowing the nAR to immediately grant authorised access to the Mobile Node including the required QoS. AAA and QoS message flows can take place in parallel, e.g. flows to and from AAAC.f (AAAC server, foreign domain) in *Figure 4*. The message flows in *Figure 4* are simplified and does not show the QoS flows. The *fast binding update* confirms the Mobile Node's willingness to handover and initiates bicasting from the oAR to both the Mobile Node and the nAR. *FBAck* then allows the Mobile Node to move to the nAR, connecting to the nAR with neighbour advertisement, and immediately can receive the (initially bicast) packets. In parallel, when the bicasting timer expires, final accounting data is sent to the AAAC.f.

4.2. Address auto-configuration for mobile terminal

In IPv6 and MIPv6, there are two mechanisms for a Mobile Node's CoA acquisition that affect handover performance, since they influence interruption time. These are stateless and stateful auto-configuration. The latter may either be DHCPv6 (Dynamic Host Configuration Protocol v6) or a new mechanism similar to DHCP focussing on mobility. The most time consuming factor is Duplicate Address Detection (DAD). According to the specification, DAD should be deployed for both approaches, but 'standard' DAD would make fast handover impossible. One solution would be to perform DAD in advance (i.e. during the preparation phase) of the handover. This implies that the new access router performs DAD on behalf of the mobile node, requiring large overlapping radio coverage areas to have time to prepare the handover. We decided in favour of stateless auto-configuration and to drop DAD, relying on the uniqueness of the layer-2 identifier or on the improbability of address duplication in case there is no layer-2 identifier, as argued in the next subsection.

The stateful approach increases network and administration complexity by adding components to the network. The advantage for operators is a full control of the IPv6 addresses, which are offered for lease to visiting mobile nodes. Further study is needed on security concerns for both approaches, e.g. for denial of service attacks.

4.3. Care-of address acquisition for technologies with missing layer-2 identifier

In absence of unique layer-2 identifier, as for W-CDMA, Moby Dick considers the following proposals to provide unique IPv6 care-of addresses.

The first approach uses *random numbers* to generate the interface identifier field of the IPv6 addresses. In [9], the probability of address duplication using this mechanism is estimated. This probability is so low that IPv6 addresses created in this way without DAD may safely considered to be unique. [9] also contains information on generating such random numbers. More information is available in RFC 1750 or in [10]. To give an idea of the risk involved in using this method of stateless auto-configuration and dropping DAD for Moby Dick networks, we cite some results from [9]:

- It is more likely for a Moby Dick user to be unable to communicate due to a problem with the network equipment (probability = $3{,}3 * 10^{-7}$) than to have a duplicate address ($5{,}4 * 10^{-12}$ when entering a network with 5000 interfaces).
- If users cause 140 handovers per day in networks containing 500 interfaces, there would be 6 users out of 1,000,000,000 that would have a problem with a communication during a year.

The second approach uses *IMEI and modified EUI-64 identifiers*. We propose a possible, yet simple solution for the project and beyond. Each GSM or UMTS Mobile Station Equipment is assigned a unique International Mobile Equipment Identity (IMEI), closely related to the terminal hardware. The IMEI is composed of a Type Approval Code (TAC, 6 digits), a Final Assembly Code (FAC, 2 digits), identifying the place of manufacture/final assembly, and an individual Serial Number (SNR), 6 digits, identifying each equipment within each TAC and FAC. A Check Digit may complement the IMEI (14 digits) and is communicated verbally.

If we encode each of the 14 significant digits using 4 bits, we obtain a 56-bit long number, to which we can add the '03' octet, setting the u and g bits defined in the IPv6 addressing architecture draft [11]. We then get a new type of modified EUI-64 identifier representing the W-CDMA interface with the same unique properties as for 48-bit MAC addresses in the IEEE environment. We will not use the IMEI for the Access Point interface, so it will not be part of any Router Advertisement message. It will be used for the Mobile Node only. This identifier must be provided when verbally reporting stolen terminals to network operators. Usually, operators verify the owner's identity before accepting such a report. Somebody capable of intercepting the IMEI of a terminal from its IPv6 address cannot easily report it as stolen. In addition, he would need some additional computing capability to retrieve the Check Digit that we did not include in the address. Otherwise, the risk is identical to that of using the MAC address for a LAN terminal. Referring to related 3GPP specifications, it is sometimes required to transmit the IMEI from the mobile terminal to the system on request. This is for reasons other than to have additional security checks, which is why [12] proposes to transmit the IMEI without protection. Since no major security problems have been found when sending the IMEI unencrypted over the air interface, the Moby Dick project uses an individual mobile terminal's IMEI for the described auto-address configuration.

5. Paging

Mobile terminals that could enter an idle state when no communication is open and when the probability of incoming traffic is low would save sending frequent location updates to the network. For incoming traffic, a mechanism called paging is used to re-activate a mobile

terminal and to find its exact location. Paging allows mobile terminals to roam in an area comprising one or more IP subnets without requiring to update routing information on the network side. The idle mode thus reduces battery drainage and saves on scarce radio bandwidth by cutting signalling overhead. When incoming traffic is directed to an idle mobile terminal, the paging mechanism wakes up the idle terminal and initiates re-establishment of the required routing information.

We propose an architecture and a protocol for IP based paging, which can easily be integrated into a Mobile IPv6 platform. A generic version of the concept has been submitted as an Internet draft to the IETF Seamoby Working Group as a proposal for generic IP paging protocol development [13], and is based on IETF requirements on IP paging [14].

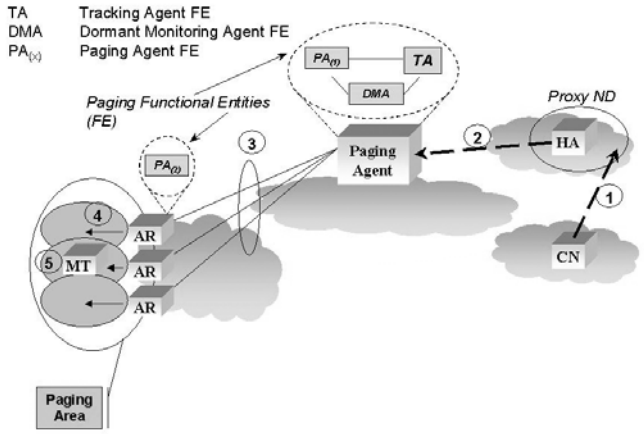


Figure 5: Integration of an IP paging architecture into a Mobile IPv6 managed platform

A mobile terminal moves within a registered *paging area* without sending location updates to the network. A paging area can be confined to one or more IP subnets, supported by access routers providing the respective access technology. When registered as idle, a mobile terminal's location is known to the system with the granularity of the registered paging area. The concept introduces a new function, a *Paging Agent* (PA), which is responsible for polling a paging area to find the exact location of an idle mobile terminal. Different paging strategies may be used to optimise the paging process. *Figure 5* depicts the architecture of a Paging Agent, including the functional elements (FE) described in [14]. The functional architecture of [14] comprises a *DMA-FE* to handle user data packets, a *TA-FE* to track a host's location and a *PA-FE*, which is responsible for the paging process. The concept described in [13] specifies a composite Paging Agent implementing the *DMA-FE*, the *TA-FE* and the generic IP part of the *PA-FE* (*PA$_{(1)}$-FE*). The attendant function in ARs is indicated as *PA$_{(2)}$-FE* in *Figure 5*. Our intention is to keep paging and a specific idle mode transparent to the Home Agent (HA) and the Correspondent Nodes (CN) communicating with a mobile terminal.

The IP paging protocol is independent of access technologies, but related attendant functions on access routers (*PA$_{(2)}$-FE*) are able to map generic IP paging requests to the specific access technology if the lower layers support paging or dormant mode (e.g. W-CDMA or IEEE 802.11). This maintains a consistent architecture and protocol at the IP layer despite the heterogeneous infrastructure. A mobile terminal enters the idle state e.g. when timers and binding caches for mobility management expire and it is no longer involved in an ongoing communication. A mobile terminal registers as idle with a PA and keeps the PA informed of its current paging area. The PA is then registered with the MN's HA using e.g. the *alternate CoA* sub-option of MIPv6 for *binding updates*. This allows user data packets to be forwarded to the DMA in the PA rather than to compel the DMA to capture all arriving packets to check whether or not they address a mobile terminal that is registered as idle with the PA. When a HA intercepts packets (1) for an idle mobile terminal, packets are forwarded to the PA by IP-IP encapsulation (2). The PA receives the tunnelled packet, decapsulates it and looks up the paging area registered for the respective mobile terminal. The user data packet (*paging trigger packet*) is buffered while the mobile terminal is paged. The PA polls all the paging related attendants in ARs assigned to the registered paging area by sending IP *paging request* messages (3). Individual attendant functions map the generic IP paging request to the local access link, possibly utilising L2 support (4). The mobile terminal, on receiving the paging request, re-establishes full access link capabilities, acquires a valid CoA and notifies the HA as well as the PA of its current location (5). This allows further packets intercepted at the HA as well as paging trigger packets to be forwarded to the mobile terminal by means of IP-IP encapsulation.

6. Outlook and Conclusions

The major outcome of the Moby Dick project so far is the proof that the integration of AAA, mobility and QoS issues into one common platform leads to new requirements not yet sufficiently considered within existing approaches. In addition, Moby Dick has shown that some new mechanisms required for this integration would have a negative impact on handover performance. This paper has proposed a solution with major focus on mobility aspects. Simulations have shown that the *fast* handover approach is the best compromise between complexity and efficiency to enhance handover performance in a heterogeneous environment. The project integrates an IP based paging concept into the overall architecture to reduce power and bandwidth consumption for future multimedia devices. The described mechanisms are under development and will be validated in a field trial in 2003.

7. References

[1] The EU IST project Moby Dick: "*Mobility and Differentiated Services in a Future IP Network*", IST-2000-25394, 2000, http://www.ist-moby_dick .org.

[2] D. B. Johnson et al., "*Mobility Support in IPv6*", draft-ietf-mobilip-ipv6-13.txt, work in progress, November 2000.

[3] Misc: *Network Simulator (ns)*, version 2, available at: http://www.isi.edu/nsnam/ns.

[4] IEEE: "*IEEE Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*", June 1999.

[5] X. Pérez, H. Hartenstein, "*A Simulation Study on the Performance of mobile IPv6 in a WLAN-Based cellular Network*", The International Journal of Computer and Telecommunications Networking special issue on "*The new Internet Architecture*", 2002.

[6] J. Broch and D. A. Maltz and D. B. Johnson and Y-C.Hu and J. Jetcheva: "*A performance comparison of multi-hop wireless ad-hoc network routing protocols*", MOBICOM, 1998.

[7] G. Dommety, A. Yegin, C. Perkins, G. Tsirtsis, K. El-Malki, M. Khalil, "*Fast Handovers for Mobile IPv6*", draft-ietf-mobileip-fast-mipv6-03.txt, work in progress, July 2001.

[8] H. Soliman and C. Castelluccia and K. El-Malki and L. Bellier: "*Hierarchical MIPv6 mobility management (HMIPv6)*", draft-ietf-mobileip-hmipv6-05.txt, work in progress, July 2001.

[9] M. Bagnulo, I. Soto, A. García, A. Azcorra, "*Random generation of interface identifiers*", draft-soto-mobileip-random-iids-00.txt, work in progress, January 2002.

[10] G. Montenegro, C. Castelluccia, "*SUCV Identifiers and Addresses*", draft-montenegro-sucv-02.txt, work in progress, November 2001.

[11] R. Hinden, S. Deering, "*IP Version 6 Addressing Architecture*", draft-ietf-ipngwg-addr-arch-v3-07 .txt, work in progress, November 2001.

[12] 3GPP TS 33.102 v3.11.0, "*Technical Specification Group Services and System Aspects; 3G Security; Security Architecture (Release 1999)*":

[13] M. Liebsch, G. Renker, R. Schmitz, "*Paging Concept for IP based Networks*", draft-renker-paging-ipv6-01.txt, a work in progress, September 2001.

[14] J. Kempf, et. al., "*Requirements and Functional Architecture for an IP Host Alerting Protocol*", RFC 3154, August 2001.

8. Glossary

3GPP: 3rd Generation Partnership Project
AAA: Authentication, Authorisation and Accounting
AAAC: AAA, Auditing and Charging
AR: Access Router
BU: Binding Update
CBR: Constant Bit Rate
CDMA: Code Division Multiple Access
CN: Correspondent Node
DAD: Duplicate Address Detection
DHCPv6: Dynamic Host Configuration Protocol version 6
DMA: Dormant Monitoring Agent
EIR: Equipment ID Register
EUI-64: The IEEE defined 64-bit extended unique identifier
FE: Functional Entity
FHO: Fast Handover
FMIPv6: Fast MIPv6
GGSN: Gateway GPRS Support Node
GMSC: Gateway MSC
HA: Home Agent
HLR: Home Location Register
HMIPv6: Hierarchical MIPv6
IEEE: Institution of Electrical and Electronic Engineers
IETF: Internet Engineering Task Force
IMS: IP Multimedia Subsystem
IST: Information Society Technologies
IMEI: International Mobile Equipment Identity
IP: Internet Protocol
IP-RAN: IP Radio Access Network
IPv6: IP version 6
LAN: Local Area Network
MAC: Media Access Control
MIPv6: Mobile IPv6
MN: Mobile Node
MSC: Mobile Service Switching Centre
MT: Mobile Terminal
ND: Neighbour Discovery
PA: Paging Agent
QoS: Quality of Service
RAN: Radio Access Network
RFC: Request for Comments
RNC: Radio Network Controller
SGSN: Serving GPRS Support Node
TA: Tracking Agent
TAC: Type Approval Code
TCP: Transmission Control Protocol
UDP: User Datagram Protocol
UMTS: Universal Mobile Telecommunications System
UTRAN: Universal Terrestrial Radio Access Network
VoIP: Voice over IP
VLR: Visited Location Register
W-CDMA: Wideband CDMA