Internet Draft
draft-lach-nemo-experiments-overdrive-01.txt
Expires: April 2003

Hong-Yon Lach
Christophe Janneteau
Alexis Olivereau
Alexandru Petrescu
Motorola
Tim Leinmueller
Michael M. Wolf
DaimlerChrysler
Markus Pilz
University of Bonn

October 2003

Laboratory and "Field" Experiments with IPv6 Mobile Networks in Vehicular Environments

<draft-lach-nemo-experiments-overdrive-01.txt>

Status of this Nemo

Abstract

This document gives a short high-level overview of experiments performed with IPv6 mobile networks using Mobile IPv6-based NEMO extensions in the context of the IST OverDRiVE project. Laboratory experiments include simple and nested mobile networks in a pure IPv6 environment while "field" experiments demonstrated continuous IPv6 vehicular connectivity over two publicly deployed IPv4 networks: 2.5G (GPRS) and Wireless LAN 802.11b deployed around and inside a metropolitan area. Lessons learned included the necessity for Route Optimization protocols for mobile networks, NAT traversal and IPv4-to-IPv6 transition protocols in public access wireless networks.

Table of Contents

Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC-2119 [1].

1. IST OverDRiVE Project

Work Package 3 of the European research project OverDRiVE [3] aims at developing IPv6 protocol mechanisms to support mobility of hosts, as well as of networks, that are deployed in vehicular environments. The scenarios envision that future vehicular environments in trains, ships or vehicles provide on-line information to the driver and passengers; provide even access to the vehicular communication components from the outside world (e.g. allow for software downloads be pushed to car computers). All electronic devices deployed in a vehicle (PCs, head screens, engine computers and sensors) are connected together with IPv6 protocols, and to the IPv6 Internet; the connection is realized either directly or through other IPv4 tunneling and gatewaying means.

The project has defined a set of scenarios which should be supported by a mobility (and security) solution [8]. The following two major characteristics are valid for all scenarios:

- Session continuity while changing the point of attachment to the Internet.

- Reachability of the mobile nodes regardless of the current point of attachment.

Thus, several functional scenarios become relevant:

- Moving of an Intra-Vehicular Area Network (IVAN): the IVAN moves homogeneously (network entities stay together) using a mobile router to provide the Internet connectivity for nodes within the IVAN.

- Moving into an IVAN with a mobile device. The mobile host moves into an IVAN and changes its WMAN connection to a WLAN connection, or its UMTS connection to a Bluetooth connection.

- Moving within an IVAN: in a larger IVAN (e.g. in a train) topological hierarchies might be used, involving more than one fixed (with respect to IVAN) or mobile router. Mobile nodes can move around inside the IVAN connecting to the appropriate access router inside the IVAN.

2. Laboratory Experiments

Several laboratory experiments in a pure IPv6 network were performed with mobile hosts and mobile networks. In some scenarios, more than one Local Fixed Node and one Correspondent Node were used; for example, in some scenarios there is an additional Mobile Host, or there are two mobile networks each hosting a Local Fixed Node. During all experiments, the mobility management messaging (between MR and HA, or between MH and HA) was not interrupting the end-to-end communication between these entities, even if several changes in Care-of Address were occuring. The end-to-end communications were happening between the LFN and the CN, or between two LFN's, or between one MH and one LFN, or between one MH and one CN. The CN's used were local video streaming servers and other servers connected on other parts of the worldwide IPv6 Internet.

A simple mobile network is composed of one Mobile Router and one Local Fixed Node, see Figure 1. The mobile network is initially attached at home and moves subsequently to Access Router AR1 and AR2.

```
                                                ----  CN link
                                             --| BR1|------
     ----                                   /   ----     |
    | HA |                                 /           ----
     ----                       ----------/           | CN |
       |            -------    |          |            ----
   ----------------| BR    |---| Network  |--------------
       | home link  -------    |          |              |
     ----    -----              ----------\              |
    | MR |  | LFN |                        \             |
     ----    -----                          \            |
       |       |                         ------        ------
       ---------                        | AR1  |      | AR2  |
     mobile net link                     ------        ------
                                            |             |
```

Figure 1: Simple Mobile Network

Figure 2 depicts another setting with one Mobile Router, one Mobile Host, same Home Agent. In a first scenario, the mobile network starts at home and then moves under AR1 and AR2. The Mobile Host stays at home.

Related to the same figure, another scenario is that the mobile network and the mobile hosts are first placed at home and then the mobile host moves under the mobile network. Subsequently the mobile network moves together with the mobile host under AR1 and AR2.

And still with the same figure, yet another scenario; every entity is at home, then MH moves under AR1, then the mobile network moves too under AR1; then MH moves towards the mobile network and, finally, the mobile network moves to AR2.

```
                                                ----  CN link
                                             --| BR1|------
     ----   ----                            /   ----     |
    | HA | | MH |                          /           ----
     ----   ----                ----------/           | CN |
       |      |     -------    |          |            ----
   ----------------| BR    |---| Network  |--------------
       | home link  -------    |          |              |
     ----    -----              ----------\              |
    | MR |  | LFN |                        \             |
     ----    -----                          \            |
       |       |                         ------        ------
       ---------                        | AR1  |      | AR2  |
     mobile net link                     ------        ------
                                            |             |
```

Figure 2: Mobile Router and Mobile Host at Home

Figure 3 shows a setting where the mobile router and the mobile host have different Home Agents. Various movements were performed.

```
                                              ----
                                           --| CN |
   ----                                   /   ----        ----   ----
  | HA1|                                 /               | HA2| | MH |
   ----                       ----------/                 ----   ----
     |            -------    |          |      -------      |      |
 ----------------| BR    |---| Network  |-----| BR    |--------------
     | home link  -------    |          |      -------
   ----    -----              ----------\
  | MR |  | LFN |                        \
   ----    -----                          \
     |       |                         ------
     ---------                        | AR1  |
   mobile net link                     ------
                                            |
```

Figure 3: Mobile Network and Mobile Host with Different Homes

In figure 4, the Mobile Host and the Mobile Router have two different Home Agents, both situated on the same home link. Various movements were performed.

```
                                                  ----  CN link
                                               --| BR1|------
   ----   ----   ----                         /   ----     |
  | HA1| | HA2| | MH |                       /           ----
   ----   ----   ----             ----------/           | CN |
    |      |      |   -------    |          |            ----
  -------------------| BR    |---| Network  |--------------
         | home link  -------    |          |              |
       ----    -----              ----------\              |
      | MR |  | LFN |                        \             |
       ----    -----                          \            |
         |       |                         ------        ------
         ---------                        | AR1  |      | AR2  |
       mobile net link                     ------        ------
                                              |             |
```

Figure 4: Home Agents on the Same Home Link

In figure 5, one Home Agent is placed in the mobile network.
Various movements were performed.

```
                                                ----  CN link
                                             --| BR1|------
     ----                                   /   ----     |
    | HA1|                                 /           ----
     ----                       ----------/           | CN |
       |            -------    |          |            ----
   ----------------| BR    |---| Network  |--------------
       | home link  -------    |          |              |
     ----    -----              ----------\              |
    | MR |  | LFN |                        \             |
     ----    -----                          \            |
       |       |                         ------        ------
       ---------                        | AR1  |      | AR2  |
       |       |                         ------        ------
      ----   ----                           |             |
     | HA2| | MH |
      ----   ----
```

Figure 5: Home Agent in the Mobile Network

An additional range of laboratory experiments were performed and
reported in section 2.4 of [8]. Examples include:

- a single Home Agent and two similar mobile networks, each composed of one Mobile Router and one Local Fixed Node.

- two Home Agents and two Mobile Routers (one Home Agent for one mobile network), but still one home link.

- two Home Agents and two Mobile Routers (one Home Agent for one mobile network), but on different home links.

- a Home Agent placed inside a mobile network serving another mobile network attached to the first.

The descriptions in section 2.4 of [8] include details of tunnel setup procedures and illustrations of MN-HA encapsulations, as well as packet paths between various entities. The laboratory experiments helped highlighting several areas for protocol improvement of the basic support of network mobility:

- Excessive tunnelling ("thick" tunnels): when MH attaches to the mobile network there are two MRHA encapsulating tunnels involved in the CN-MH path. Several levels of mobile networks induce excessive tunnelling that can lead to serious packet loss and worsen stack behaviour due to excessive fragmentation/reassembly. This is especially true in wireless environments.

- Crossover tunnels happen when the path between one tunnel's endpoints includes only one of the other tunnel's endpoints . A situation leading to crossover tunnels is depicted in Figure 16 of [8], where a HA is deployed inside a mobile network. The initial configuration is in diagram a and diagrams b, c and d represent snapshots of the movement scenario. The MR2HA2 tunnel setup procedure corresponding for the diagram d is practically impossible to perform.

- Externally influenced intra-aggregation communication (or disconnected operation problem): in the MH and MR with same HA case, depicted in diagram c of Figure 12 of [8], the LFN-MH communication (intra-aggregation) is influenced by the communication between MR and AR1 (external). If MR looses connection to AR1, then LFN looses connection to MH, a fact that, as paradoxical as it may seem, is a veritable side effect of tunnelling itself.

- Under-optimal paths: when comparing the length of the CN-MH communication path depicted in top-left diagram of Figure 13 of [8] to the CN-MH communication in Figure 15 of [8], it is clear that the path taken by packets is much longer than the optimal. The first diagram can be considered as an ideal to be attained, and the only optimal path that can be achieved is CN-AR-MR-MH (eliminating the BR-HA-BR additional segment). This is not the ideal path (since MH is not physically home) but represents an achievable goal, if employing Route Optimization techniques.

- Asymmetric communication paths: outgoing communication paths have different lengths than incoming communication paths, between the same two entities. See example in Figure 14 of [8].

3. "Field" Experiments

"Field" experiments were performed in a typical deployment of wireless networks. An overall picture of the experiments is described in Figure xx. Three wireless access networks are depicted: the home network (hosting the Home Agent), the Orange network (an European Telecom operator for mobile phones) and the Wixos network (a WiFi HotSpot network deployed in a large city).

The three networks are inter-connected at Internet level. The Mobile Network, pictured at the bottom, was obtaining Internet access via one of the three Wireless Access Networks.

```
                    ------------             -----------
                   |  Internet  |-----------| Web Server|
                   /------------\            -----------
                  /       |      \
                 /        |       \
                /         |        \
          --------     --------   -------
         |Home Net|   | Orange | | Wixos |
          --------     --------   -------
             |            |           |
                  Wireless Access


         WLAN    GPRS
           |      |
          ----------
         |Mobile Net|  ---------->
          ----------
```

Figure xx: Overall Picture of Field Experiments

3.2 Mobile Network

The mobile network used in the field experiments is a very simple wireless segment (802.11b in ad-hoc mode) linking together an IPv6 Mobile Router and a Local Fixed Node running user applications (notably an http client). In addition, the mobile network contained two boxes helping interconnect the MR to the wireless access networks (FrontBoxes). Inside the mobile network, IPv6 protocols are used exclusively; the Mobile Router runs an implementation of Mobile IPv6 Mobile Router in implicit mode [2]. However, both Orange and Wixos offer IPv4 access exclusively. FrontBoxes help solve this problem.

Front boxes are entities connected to the Mobile Router that help differentiate between mobility management tasks and particular link layer/tunnelling functionalities. The GPRS Front Box establishes a GPRS connection (i.e. establishes a PPPv4 connection, through a PDP Context to the GPRS SGSN), configures an IPv4 interface and establishes a UDP tunnel through a NAT box to the home IPv6 network, all over its egress interface. The ingress interface of the FrontBox is assigned an IPv6 address and prefix (deduced from the IPv6 prefixes of the home network); the FrontBox sends IPv6 Router Advertisements over its ingress interface towards the Mobile Router. Tunnelling IPv4 packets into UDP IPv4 streams in order to traverse

NAT is proposed in [12]. In these experiments, IPv6 packets were tunneled instead.

Similarly, the Wireless LAN Front Box offers native IPv6 connectivity towards the Mobile Router, when the mobile network attaches to the Wixos WiFi HotSpot network.

3.3 Home Network

The home network is connected to both IPv4 and IPv6 Internets. It hosts an IPv6 Home Agent, a 6to4 Gateway and a Udptun Gateway. The Home Agent runs Mobile IPv6 with NEMO implicit mode [2]. The Udptun Gateway constitutes the UDPv4 tunnel endpoint for both the GPRS and WLAN FrontBoxes.

In addition, the home network offers two WLAN access points towards the mobile network. One of the AP's is connected to the home link (where HA resides); the other AP is attached to another link of the home network. Both AP's offer native IPv6 connectivity towards the Mobile Router; when the MR connects to the home network AP's, it does by bypassing the FrontBoxes.

3.4 Orange Wireless Access (GPRS)

The GPRS access system offer IPv4 access with a private addressing scheme. It distributes private non-routable addresses (10.x.y.z) over a PPP connection, addresses being assigned by DHCP servers. This network is connected to the Internet with NAT boxes.

3.5 Wixos Wireless Access (WLAN)

Wixos is an 802.11b Metropolitan Area Network. During June 2003, the Wixos network was available for public experimentation. For more information about the Wixos network see [6]. Disclaimer: none of the participants in the IST OverDRiVE project are affiliated, or represent, in any legal or other way the Wixos Network. The Wixos network was used as a public access network.

The network offers IPv4 access in several "hotspot" areas. Most of the hotspots are not overlapping (in terms of wireless coverage). The IPv4 network offers private non-routable IPv4 addresses. The network was not using, at the time of testing, any form of Mobile IPv4; an address acquired in one WiFi hotspot is not valid under another WiFi hotspot of the same Wixos network.

3.6 Scenarios and Results

In one scenario, the mobile network was first connected to the home network outside the metropolitan area, then moved onto the highway, then entered a metropolitan area hotspot, then went out of the hotspot and entered again another hotspot. During all this trajectory, a continuous IPv6 connection was maintained between the Local Fixed Node and a Correspondent Node (web server kame.net, placed in Japan) connected on the IPv6 Internet.

In another scenario, the Local Fixed Node running exclusively IPv6 protocols, browsed an IPv4 web server. This could be accomplished by configuring a "proxy" server on the LFN client. The proxy server is connected to both the IPv6 and IPv4 Internets; it is physically placed at University of Bonn. The proxy server converts http IPv6 requests into IPv4 requests, forwards the request to the IPv4 Internet, and forwards the received IPv4 reply back to the IPv6 client of the LFN.

The first mobility scenario (mentioned above) involved a dynamic change of IP addresses (both v4 and v6) to the Mobile Router. However, the IPv6 address of the LFN was not changing and, as such, the applications running on the LFN were not interrupted. Hiding the change of IP address was performed at two levels of different granularity. The dynamics of address assignment to the Mobile Router and FrontBoxes is depicted in figure xx.

```
   AP1     AP2     BS1     BS2    shadow    BS3     AP3     BS4     AP4

    \______/        \_______|_______/        |       |       |       |
     No ad                 ad1              ad2     ad3     ad4     ad5

    |       |       \_______|_______________/        |       |       |
   AD1     AD2                    AD3               AD4     AD3     AD4
```

Figure xx: Dynamics of IPv4 and IPv6 Address Assignment

The first line in figure xx depicts the sequence of WLAN Access Points and GPRS Base Stations to which the Mobile Router and FrontBoxes attach. AP1 and AP2 are both in the home network (AP1 connects HA). BS1 and BS2 are deployed along the highway segment, and the "shadow" area depicts an uncovered segment along the highway (a tunnel). BS3 is deployed at junction zone between highway and city. AP3 and AP4 are the hotspot areas, separated by BS4.

Dynamics of IPv4 address change show a high level of granularity (fine-grained). The IPv4 addresses distributed either by GPRS or by WLAN are pictured on the second line, lower case. When the mobile network connects to the home network, no IPv4 address is assigned. Under BS1 and BS2, the mobile network is assigned IPv4 address ad1. Switching between these two BS's does not incur a change in the IPv4 address, ad1 is kept. Due to the presence of the shadow area (the uncovered tunnel), the mobile network will be assigned a new IPv4 address (ad2) under BS3. Even though GPRS ensures the same IPv4 address assigned to a mobile, there exists no mechanism to assign the same IPv4 address to the same mobile following a short disconnection.

Dynamics of IPv6 address change show a lower level of granularity (coarse-grained). Assignment of IPv6 addresses to the Mobile Router (the Care-of Addresses) is pictured on the bottom line. At home, IPv6 addresses AD1 and and AD2 are assigned to the Mobile Router, AD1 being the Home Address. Whenever the GPRS FrontBox is conneted to a BS, AD3 is assigned to the Mobile Router (BS1-4). Whenever the WLAN FrontBox is connected to an AP (AP3-4), AD4 is assigned to MR.

Less change in the IPv6 address of the MR reduces the number of binding information exchanges with the Home Agent. For example, when there is a change ad1-ad2, the corresponding address AD3 Care-of Address is stable, no need to inform the Home Agent.

During the experimentation, the dynamics of encapsulation (v6-in-v6 and v6-in-v4) was also observed. For further information and lessons learned, see [10].

4. Conclusions and Future Work

This report described laboratory and field experiments with an IPv6 mobile network. A wide range of laboratory experiments showed the viability of NEMO-based network mobility protocols to support scenarios with simple mobile networks, nested mobile networks, and mobile HA's. At the same time, the experiments helped proving the analytical expectations (such as excessive encapsulations) and also raised new problems (such as crossover tunneling). Solving these problems involves developping new protocols for Route Optimization for mobile networks.

Field experiments involved accessing two publicly-deployed wireless access systems (GPRS and WLAN) and showed the need for NAT traversal and IPv6 transition mechanisms. These mechanisms were separated from Mobile IPv6 mobility management by means of FrontBoxes.

Delivering multicast traffic to hosts inside the mobile network is an important work item identified within the project. Several schemes are currently being considered (home and remote subscriptions).

A DVB-T FrontBox would allow the Mobile Router to receive high-speed (broadband) Internet flows (larger bandwidths than with GPRS or WLAN). Developing a DVB-T FrontBox is one of the potential future work items.

Acknowledgements

This work has been performed in the framework of the IST project IST-2001-35125 OverDRiVE (Spectrum Efficient Uni- and Multicast Over Dynamic Radio Networks in Vehicular Environments), which is partly funded by the European Union. The OverDRiVE consortium consists of Motorola, DaimlerChrysler, France Telecom, Ericsson and Radiotelevisione Italiana as well as Rheinisch-Westfälische Technische Hochschule RWTH Aachen, Universität Bonn and the University of Surrey. The authors acknowledge the contributions of their colleagues in the OverDRiVE consortium.

o

References

[1] S. Bradner. Key Words for Use in RFCs to Indicate Requirement Levels. RFC 2119, BCP 0014, IETF. March 1997.

[2] V. Devarapalli, R. Wakikawa, A. Petrescu and P. Thubert. Nemo Basic Support Protocol (work in progress). Internet Draft, IETF. draft-ietf-nemo-basic-support-00.txt. June 2003.

[3] IST OverDRiVE project on the World Wide Web: http://www.ist-overdrive.org, accessed June 23rd 2003.

[4] T. Ernst and H.-Y. Lach. Network Mobility Support Terminology (work in progress). Internet Draft, IETF. draft-ietf-nemo-terminology-00.txt. May 2003.

[5] D. Johnson, C. Perkins and J. Arkko. Mobility Support in IPv6 (work in progress). Internet Draft, IETF. draft-ietf-mobileip-ipv6-22.txt. May 2003.

[6] Wixos Wireless LAN Network on the World Wide Web: http://www.wixos.net, Accessed June 22nd 2003.

[7] C. Janneteau, ed., "Scenarios, Services and Requirements", OverDRiVE Deliverable D03, September 2002.

[8] M. Ronai, ed., "Concept of Mobile Router and Dynamic IVAN Management", OverDRiVE Deliverable D07, March 2003.

[9] A. Petrescu, ed., "Issues in Designing Mobile IPv6 Network Mobility with the MR-HA Bi-directional Tunnel (MRHA), draft-petrescu-nemo-mrha-03.txt, (Work in Progress), October 2003.

[10] A. Petrescu and H.-Y. Lach, "MR-HA Bidirectional Tunnelling for Network Mobility", Motorola Labs internal tech report, October 2003.

[11] H.-Y. Lach, C. Janneteau and A. Petrescu, "Network Mobility in Beyond-3G Systems", IEEE Communications Magazine, July 2003.

[12] H. Levkowetz, S. Vaarala, "Mobile IP Traversal of Network Address Translation (NAT) Devices", RFC 3519, Proposed Standard, IETF. May 2003.

Authors' Addresses

Hong-Yon Lach
Motorola Labs
Parc les Algorithmes St Aubin
Gif-sur-Yvette 91193
France
Phone: +33 1 69352536
Hong-Yon.Lach@motorola.com

Christophe Janneteau
Motorola Labs
Parc les Algorithmes St Aubin
Gif-sur-Yvette 91193
France
Phone: +33 1 69352548
Christophe.Janneteau@motorola.com

Alexis Olivereau
Motorola Labs
Parc les Algorithmes St Aubin
Gif-sur-Yvette 91193
France
Phone: +33 1 69352516
Alexis@motorola.com

Alexandru Petrescu
Motorola Labs
Parc les Algorithmes St Aubin
Gif-sur-Yvette 91193
France
Phone: +33 1 69354827
Alexandru.Petrescu@motorola.com

Tim Leinmueller
DaimlerChrysler AG
Research Telematics and E-Business
Communication Systems (RIC/TC)
HPC: U800
P.O. Box 2360
89013 Ulm / Germany
Phone: +49 731 505 2379
Tim.Leinmueller@daimlerchrysler.com

Michael M. Wolf
DaimlerChrysler AG
Research Telematics and E-Business
Communication Systems (RIC/TC)
HPC: U800
P.O. Box 2360
89013 Ulm / Germany
Phone: +49 731 505 2379
Michael.M.Wolf@daimlerchrysler.com

Markus Pilz
University of Bonn
pilz@cs.uni-bonn.de

Changes

From version 00 to 01:
-improved presentation.
-added conclusive remarks of laboratory experiments.
-enhanced the section of field experiments.
-improved the conclusions section.
-changed addresses and affiliations of some authors.

Funding for the RFC editor function is currently provided by the Internet Society.