IPv6 Moving Network Testbed with Micro-Mobility Support[1]

Miklós Aurél Rónai*, Kristóf Fodor*, Ralf Tönjes?

*Ericsson Research, Traffic Lab, P.O. Box 3, 1300 Budapest, Hungary
? Ericsson Eurolab Deutschland, Ericsson Allee 1, 52134 Herzogenrath, Germany
email: Miklos.Ronai@ericsson.com, Kristof.Fodor@eth.ericsson.se,
Ralf.Toenjes@ericsson.com

ABSTRACT

Mobile IP, in particular Mobile IPv6, has no native support for moving networks. A basic solution for network mobility is currently being standardised by the IETF Network Mobility (NEMO) working group. In the frame of the IST OverDRiVE project Ericsson Research Hungary Traffic Lab implemented a moving network testbed in which network mobility is based on the IETF NEMO basic solution. In addition, the testbed supports micro-mobility of user devices that move within large moving networks, such as trains. The moving network possesses multiple interfaces including access to WLAN, GPRS and UMTS.

This paper introduces the concepts developed in OverDRiVE, describes Ericsson's OverDRiVE moving network testbed, introduces some IP handover types, analyses measurements of IP handover delays for various mobility scenarios of moving networks and presents some 3G measurements. The results show that a radio unaware IP handover solution performs poorly with respect to handover outage time. Taking some information into account from the radio (e.g., triggers) can help making IP handovers faster. It can also be seen from the experiments that UMTS/WCDMA provides the necessary bandwidth for real time video applications.

I. INTRODUCTION

Users spend more and more time in vehicles and expect an infrastructure that fulfils their communication needs when travelling in cars, trains, etc. On the other hand, operators demand an efficient mobility management for user groups (and devices) having the same mobility pattern to avoid unnecessary signalling. Moving networks, which are network segments that can change their point of attachment to the Internet address these requirements. The nodes residing in a moving network are attached to a special gateway, a so-called mobile router (MR), through which they can reach the Internet.

Mobile IP, in particular Mobile IPv6 (MIPv6), has no native support for moving networks [1]. According to MIPv6 if a mobile node (MN) changes its location, then it registers its new care-of-address at its home agent (HA) with a binding update (BU). The mobile node remains reachable, because its home agent intercepts traffic directed to the mobile node and forwards the packets to the mobile node's care-of-address.

There are two possibilities what happens when MIPv6-enabled nodes are connected to a mobile router and it changes its location. Either the attached nodes recognize or they do not perceive anything from the movement. If the nodes recognize the movement they send binding updates at the same time causing a so-called binding update storm. If they do not perceive the movement, they cannot send binding updates to refresh their location information at their HAs, which results in losing reachability.

Solutions for moving networks and mobile routers face several challenges. The mobility of the moving network should be transparent to its residing nodes, thus the nodes inside the moving network should not perceive that the mobile router changed its point of attachment. This way the binding update storm can be avoided, as well. The mobile router should also support mobile nodes moving into and out of the moving network (roaming). The mobile router may provide connections to various access systems (multi-access/multi-homing), in this case the mobile router has to support handovers between different access systems (vertical handover).

The IETF Working Group on Network Mobility (NEMO) is currently standardizing a basic support for moving networks. The basic NEMO protocol [2] suggests a bi-directional tunnel between the mobile router and its home agent (Mobile Router – Home Agent tunnel, MRHA tunnel). The IST project OverDRiVE [3], coordinated by Ericsson Eurolab Deutschland, has developed a concept for moving networks [4][5] which is based on the NEMO basic solution. This concept was extended to support large vehicles, where the local mobility of nodes that move e.g., between different wagons of a train, need to be handled. This solution combines macro-mobility of the moving network and micro-mobility of devices within.

We implemented an IPv6 testbed based on this approach. In this solution the MRHA tunnel is used for network mobility, thus handling the movement of the entire moving network, and the BRAIN Candidate Mobility Management Protocol (BCMP) [6][7], which was earlier developed in the IST BRAIN [8] and MIND [9] projects is applied to solve local mobility.

[1] 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 Ericsson (co-ordinator), DaimlerChrysler, France Telecom, Motorola 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.

In this paper, after explaining the theoretical background of our mobility solution in section II, we describe the implemented testbed in section III. Section IV introduces an IP handover taxonomy and section V describes the measurement setup and discusses the results of the measurements. In section VI we conclude our work.

II. CONCEPT FOR LARGE MOVING NETWORKS

Figure 1 shows an overview of the Mobile Router – Home Agent bi-directional tunnelling mechanism. The tunnel connects the MR and its HA through the Internet and through different access systems (ACS). If the MR changes access systems, the tunnel is torn down at the old ACS and is built up through the new one. The tunnel keeps the moving network virtually in the home network of the mobile router and the residing nodes do not perceive the movement. This solution provides efficient mobility management, because the mobility of the entire user group residing inside the moving network is handled by the mobile router by sending only one update to the fixed network infrastructure. This solution fulfils all the above mentioned requirements, but raises route optimization concerns between the nodes inside the moving network and their correspondent nodes on the Internet.

In the figure we can see that BCMP is used for local mobility within the vehicle. In this example BCMP handles the movement of mobile nodes between access routers inside the train.

The presented solution supports local fixed nodes (LFN) and visiting mobile nodes (VMN) attached to the moving network. LFNs are unaware of any kind of mobility (either MIPv6 or BCMP). VMNs can move into and out of the moving network and can handle MIPv6 and BCMP signalling.

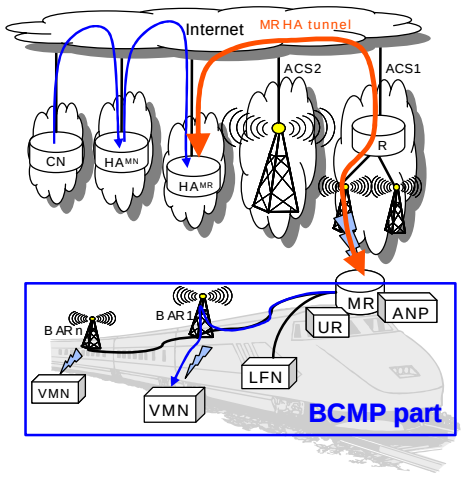

Figure 1: Theoretical overview of the Mobile Router Home Agent tunnel (MRHA) and BRAIN Candidate Mobility Management Protocol (BCMP) combined solution

In the case of VMNs the mobile nodes get their IP address from the BCMP User Registry (UR), when they connect to moving network's infrastructure. All IP addresses assigned to the visiting mobile nodes point to the BCMP ANchor Point (ANP), and are from the address space of the mobile router's home agent. Next, the VMN sends a binding update to its home agent using the IP address received from the user registry as a care-of-address. If a correspondent node (CN) from somewhere on the Internet sends packets to the mobile node that resides in the moving network, the home agent of the mobile node intercepts the packets according to Mobile IPv6. The home agent sends the packets to the mobile node's care-of-address, which in this case points to the mobile router's home agent. According to the NEMO solution after receiving the packets the mobile router's home agent injects them into the MRHA tunnel and at the other end of the tunnel according to our solution the mobile router forwards the packets to the BCMP anchor point, which in our case is co-located with the mobile router. From this point on, inside the moving network BCMP handles the delivery of the packets to the mobile nodes. Thus the anchor point tunnels the packets to that BRAIN Access Router (BAR), where the visiting mobile node is located. The BAR sends the packets, this time without tunnelling, through its radio interface to the destination mobile node.

In the case of LFNs the nodes get their IP addresses through IPv6 auto-configuration. All IP addresses assigned to local fixed nodes are also from the address space of the mobile router's home agent, but in this case the address points to the local fixed node itself. In the LFNs case everything is the same as described in the VMNs case until the MR receives the packets addressed to an LFN. However, if the mobile router receives a packet for a local fixed node, instead of giving it to the BCMP architecture the MR simply forwards the packet to the destination node through the moving network's fixed infrastructure.

III. ERICSSON TRAFFIC LAB'S OVERDRIVE MOVING NETWORK TESTBED

The overview of our testbed can be seen in Figure 2. The testbed comprises a fixed network and a moving network infrastructure. In the moving network infrastructure two BARs (BAR1 and BAR2) are connected to the mobile router (MR). To have BCMP mobility management inside the moving network the mobile router is co-located with a BCMP ANP and a user registry (UR). Two nodes are connected to the moving network, one is a visiting mobile node with BCMP and MIPv6 capabilities and the other one is a local fixed node only with IPv6 support. The VMN is connected to the BARs with its radio interface and the LFN is connected to the mobile router with a UTP cable.

The entire moving network is connected to the Internet through one of the mobile router's radio interfaces. Primarily the MR has an 802.11 WLAN radio card to be able to connect to a WLAN hotspot, but the MR also has a GPRS and a UMTS phone connected to it, so beside WLAN it can access the Internet also via GPRS and UMTS. The mobile router can switch between the different access systems without disconnecting the sessions of the applications running on the LFN or on the VMN.

The fixed infrastructure of the testbed consists of two access routers (AR1 and AR2), the home agent of the

mobile router (HA^{MR}), a correspondent node (CN) and a Virtual-GGSN (VGGSN). We call this entity VGGSN because from the home agent's point of view it can be regarded as a gateway to the GPRS network. However, it is only virtually a gateway. The access routers are connected to the mobile router's home agent and they represent two WLAN hotspots. The correspondent node and the VGGSN are also connected to the mobile router's home agent. Please note that the correspondent node and the access routers (AR1 and AR2) could be connected to somewhere else on the Internet and are connected directly to the mobile router's home agent just for the sake of testing simplicity.

To understand the necessity of VGGSN let us shortly explain how the GPRS and UMTS connections of the mobile router are configured. To reach the mobile router from the Internet the MR must have a publicly available and routable IP address. When the mobile router is connected through the GPRS or UMTS access networks it gets the IP address from the service provider of the access system. In most cases the operators provide addresses of their private domains (e.g., 10.x.y.z) only, which are not available from outside their domain. To allow users to reach the Internet these providers use a Native Address Translator (NAT). However, NAT provides only one-way reachability, which means that it does not allow reaching the node from the Internet for everyone. To make a node inside a private domain available from outside the domain a tunnel has to be built up through the NAT between the node inside the private domain and another node somewhere in the Internet, which has a publicly available and routable IP address. Because of this NAT issue our testbed employs an entity, which is called Virtual GGSN, since it could be regarded as a gateway to the GPRS and the UMTS network. However the functionality of this entity could be integrated in the mobile router's home agent as well, we decided to keep it separately, so we can point out that this functionality is not necessary to be run on the home agent of the mobile router. To solve the tunnelling through the GPRS and UMTS access systems we use VTun [10], but IPsec could be used as well.

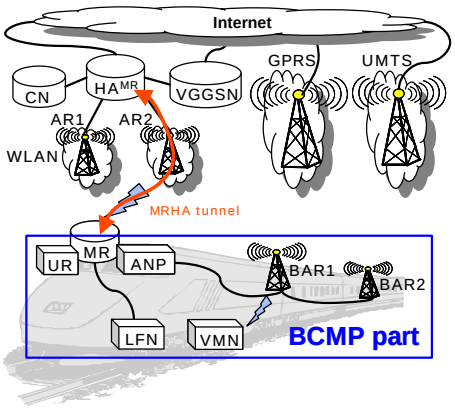

Figure 2: Moving network testbed overview

In the testbed the mobile router has permanently established connections with VTun through the GPRS and the UMTS network to the VGGSN. Hence the mobile router is multi-homed, but in the current implementation it listens always only on one of its connections, either on WLAN or GPRS or UMTS.

We implemented several types of IP handovers. The mobile router can perform handovers between the WLAN hotspots (AR1 and AR2). The MR can perform a radio-unaware or a make-before-break IP handover (see Section IV for the handover descriptions). In case of the radio unaware handover the access router's radio interface, which the MR is connected to, is pulled down, thus the MR is forced to perform a handover between the two ARs. So after the MR detects that the AR has disappeared it switches to the other one. In case of the make-before-break IP handover the MR is told to immediately switch between the two ARs. The MR can perform vertical handovers between the WLAN, GPRS and UMTS access systems as well. In real life the above mentioned handovers would be performed during the movement of the vehicle.

The visiting mobile node inside the moving network is also able to perform handovers between the two BARs that are connected to the mobile router. In real life this type of handover would be performed, when the user changes its location inside the vehicle.

To create an implementation based on the MRHA proposal we used the Mobile IPv6 for Linux (MIPL) [11] stack from Helsinki University of Technology (HUT). You can learn more about our moving network testbed implementation in [12].

IV. IP HANDOVER TAXONOMY

In our previously described testbed we performed some handover measurements. To understand the results we introduce a taxonomy about mobile node initiated IP handovers.

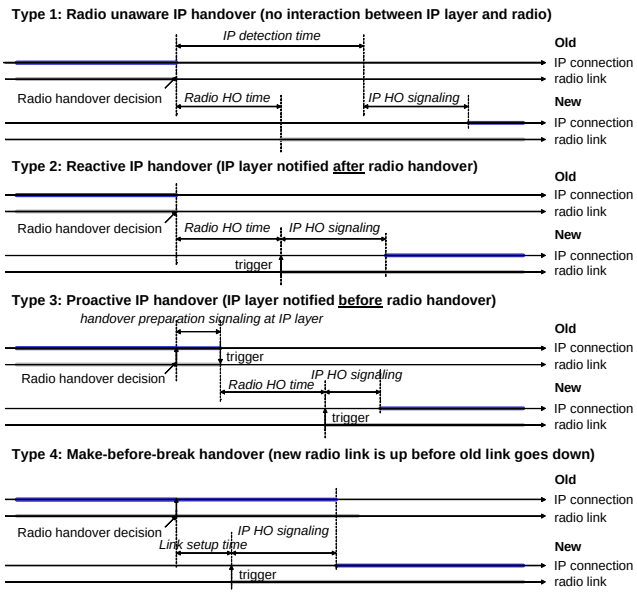

Figure 3: IP handover types

In case of radio unaware IP handover (type 1) no interaction takes place between the radio and the IP layer.

Performing this handover needs a lot of time, because the IP layer has to detect that the old connection is lost and the new one is up without any help from the radio. The radio unaware IP handover can be regarded as a handover with the original layer 3 movement detection, it has a very poor performance and it can be used for device portability only.

In case of reactive IP handover (type 2) the IP layer is notified with a trigger after the radio handover. Due of this trigger the IP layer can perform the handover instantly after the new radio link is up. Such handovers are much faster than radio unaware handovers. This type of handover is called "unplanned handover" in BCMP.

In case of proactive IP handover (type 3) the IP layer is notified about the radio handover beforehand and can perform preparations before the radio link goes down. After the IP layer is ready with the preparations it triggers the radio that the handover can be performed. After the new radio link is up the radio triggers the IP layer telling that it can continue the IP handover through the new radio link. This type of handover could be performed with less disruption in user sessions than the previous one. Type 3 handover is called "planned handover" in BCMP. At the IETF the reactive IP handover is the typical assumption for basic IP mobility protocols and the proactive IP handover for "fast handover protocols".

The make-before-break IP handover (type 4) needs special requirements from the radio technology. It is necessary that the node that wants to perform a handover between two access points hears both access points at the same time. In this case IP layer handover is performed parallel with the radio handover thus resulting in a very fast switch between the old and the new link. The make-before-break IP handover has very good performance, but puts special requirements on radio.

V. MEASUREMENTS

In this section we will present type 1 and type 4 IP handover and 3G measurements we performed in our moving network testbed. In the experiments the moving network did not move. We will show that the radio unaware IP handover (type 1) performs really poor and the make-before-break IP handover (type 4) performs very well with respect on handover outage time. Our experiments also showed that 3G provides the necessary bandwidth for real time video applications

A. Specification of the testbed

The testbed consists of the following equipment: the correspondent node, the local fixed node and the visiting mobile node are Pentium P4 1.8 GHz laptops, the VGGSN is a Pentium P1 133 MHz PC and all other network elements (HA, AR1, AR2, BAR1, BAR2 and MR) are AMD Athlon XP 1800+ PCs. The network cards in the PCs are Intel EtherExpress Pro 10/100 Ethernet cards and the wireless cards are AVAYA Orinoco Silver 802.11b PCMCIA WLAN cards. All of the computers were equipped with the same Linux distribution (Debian Sarge) and kernel (2.4.20). For the implementation of our mobile router prototype we took version 0.9.5 of the MIPL stack.

During our experiment we used TCPdump and an own test environment. The environment consists of a packet sender and a packet receiver program. The packet sender, which is placed on the correspondent node, emits 65-byte-long UDP packets at a pre-defined rate. We chose the UDP transport protocol instead of TCP so that we can avoid the effect of TCP's traffic control mechanisms. The receiver, which is running on the local fixed node behind the mobile router, logs the packet loss and whether the sequence of the packets swapped. With TCPdump we logged at the LFN the inter-arrival times of the incoming UDP packets. In the experiments we tuned the radio interfaces of the access routers and the mobile router to the same channel.

B. IP handover measurements

The mobile router performed handovers between the two WLAN access routers (AR1 and AR2). First we measured the outage time of the mobile router's handover, when the access router, which the mobile router was attached to, suddenly disappeared. We sent UDP packets in every 10 milliseconds and by pulling down the air interface of the access router, which the MR was connected to, in every 25 seconds we forced the MR to perform a handover. The histogram of the handover outage times can be seen in Figure 4. In the figure on the X axis we can see the intervals of the handover outage times in milliseconds and on the Y axis we can see how many handovers were performed in the given outage time interval during the experiment. The mean value of these measurements was 4080 ms, which means that after the old access router disappeared the mobile router needed 4.08 seconds in average to find and connect to the other WLAN access router. The histogram shows that 77% of the handover outage times were between 3100 and 5500 ms and 57% were between 4000 and 5500 ms. The smallest value we measured for the handover outage time was above 1.1 second, which is also a quite long delay. We can observe that performing handovers without any radio information (trigger) leads to very poor handover performance and causes a long disruption in user sessions.

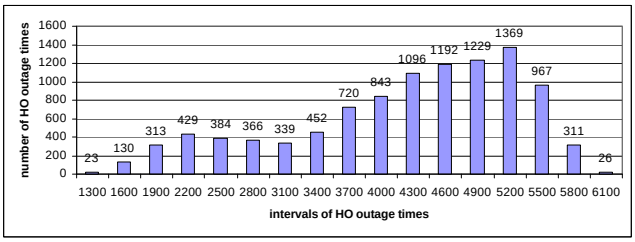

Figure 4: Histogram of handover outage time when AR disappears (radio unaware - type 1 - IP handover)

In the next experiment we turned on the radio interfaces of both access routers. This way the mobile router could hear both access routers at the same time, thus it could perform a make-before-break (type 4) handover. This time we measured the packet loss during handovers, because the inaccuracy of the previous measuring method did not allow to measure handover outage times in the range of 1-2 ms. We sent UDP packets in every 2

milliseconds and we performed a handover with the MR in every 2 seconds. We measured 0.7% packet loss in average, thus we could say that the outage time was about 1.4 ms (in every 2 seconds 0.7% of the time is spent with the handover). In this experiment packet loss can occur if a packet arrives at the same time when the routing tables are being updated and because of this the packet cannot reach the mobile router. As we can see this type of handover can be performed very fast. During this handover users cannot perceive any kind of disturbance, for example, in their streaming video application.

The comparison of the different IP handover types can be seen in Figure 5. The measurements of the reactive (type 2) and the proactive (type 3) IP handover outage times were taken from [13], where the measurements included the handover preparation as well (this is why the proactive handover needs more time).

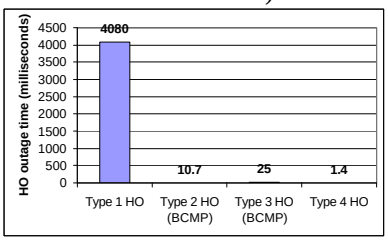

Figure 5: Comparison of IP handover outage times (mean values)

C. *UMTS/WCDMA measurements*

We performed some measurements through a publicly available UMTS/WCDMA network. We investigated the delay by sending ping packets from a local fixed node located inside the moving network to the home agent of the mobile router and the throughput by downloading a file from the Internet to a local fixed node. According to our measurement the average delay through the UMTS/WCDMA network was 220 ms and the average bandwidth was 310.31 kbit/s, which could be regarded as very good.

We also tested the UMTS/WCDMA network with a video application. We sent real time streaming video through the 3G network from the correspondent node to the mobile node behind the mobile router and we could see that there was no (or only rarely and negligible) disturbance in the picture of the video at the receiver mobile node.

VI. CONCLUSION

A prototypical IPv6 testbed was implemented that supports mobility of entire networks and mobility within (large) moving networks. The testbed supports horizontal and vertical handover between different access systems (WLAN, GPRS and UMTS/WCDMA). The testbed was demonstrated at the IST Mobile and Wireless Communications Summit in June 2003 [14] and with LFN support, UMTS and GPRS access and make-before-break handover extensions at the PCC Wireless Communications Research Days in November 2003 [15]. With our testbed we showed the first time how a network mobility solution, which is based on a macro-mobility protocol (Mobile IPv6) can interwork with a micro-mobility approach (BCMP) to provide continuous IPv6 Internet access to users residing in vehicles. In the testbed we used an IPv6 Mobile Router prototype implementation based on the Mobile IPv6 for Linux (MIPL) stack.

The measurements showed that to perform a switch between two access routers the radio unaware (type 1) IP handover needs much more time (4080 milliseconds) than all other IP handover types (reactive, proactive and make-before-break) that are someway aware of the radio handover. The make-before-break IP handover caused only a short break in the user session (1.4 milliseconds). According to the measurements with BCMP reactive (type 2) and proactive (type 3) handovers perform around 10.7 ms and 25 ms respectively [13]. This shows that it is crucial to take some information from the radio (e.g., triggers) into account, because it helps making IP handovers much faster. The 3G measurement results showed that UMTS/WCDMA provides enough bandwidth for real-time user applications (e.g., streaming video).

REFERENCES

[1] T. Ernst et al.: Mobile Networks in Mobile Ipv6, darft-ernst-mobileip-v6-network-03.txt, “work in progress”, March 2002.

[2] Vijay Devarapalli, Ryuji Wakikawa, Alexandru Petrescu, Pascal Thubert: “Network Mobility (NEMO) Basic Support Protocol”, Internet draft, December 2003, http://www.ietf.org/internet-drafts/draft-ietf-nemo-basic-support-02.txt

[3] OverDRiVE web page: http://www.ist-overdrive.org

[4] M. A. Rónai, R. Tönjes, M. Wolf, A. Petrescu, “Mobility Issues in OverDRiVE Mobile Networks”, in proceedings of the Mobile and Wireless Communications Summit 2003, pp. 287-291.

[5] Miklós Aurél Rónai (ed.), “Concept of Mobile Router and Dynamic IVAN Management”, OverDRiVE deliverable D07, March 2003

[6] C. Keszei, N. Georganopoulos, Z. Turanyi, A. Valko, ”Evaluation of the BRAIN Candidate Mobility Management Protocol“, IST Global Summit, Barcelona, September 2001

[7] Pedro M. Ruiz et al, “MIND protocols and mechanisms specification, simulation and validation”, MIND Deliverable D2.2, http://www.dit.upm.es/~ist-mind/deliverables/MIND_D22_annex.pdf

[8] BRAIN: http://www.ist-brain.org

[9] MIND: http://www.ist-mind.org

[10] VTun homepage: http://vtun.sourceforge.net

[11] MIPL homepage: http://www.mipl.mediapoli.com

[12] Markus Pilz (ed.), “Functional Description and Validation of Mobile Router and Dynamic IVAN Management”, OverDRiVE deliverable D17, March 2004

[13] Gergely Biczók, Kristóf Fodor, Balázs Kovács, “Handover Latencies in BCMP Networks”, Komunikácie/Communications journal, Zilina, Slovakia

[14] Tim Leinmüller (ed.), “Description of Demonstrator for Mobile Multicast and the Vehicular Router“, OverDRiVE Deliverable D14, March 2004

[15] PCC Wireless Communications Research Days, November 2003, http://www.pcc.lth.se