Demonstration of IPv6 Network Mobility in Aeronautical Communications Network

Eriza Hafid Fazli, Angels Via, Sébastien Duflot, Markus Werner, *TriaGnoSys GmbH*

Abstract **— This paper presents the development of a laboratory demonstrator within NEWSKY, a project co-funded by the European Commission within its 6th Research Framework Programme (FP6). Host and network mobility are some of the essential network functionalities required for efficient operation of a network-centric aeronautical communication system. This paper deals with the feasibility demonstration of Mobile IPv6 (MIPv6) and Network Mobility (NEMO) protocols to suitable provide mobility support for the future Air Traffic Management (ATM) network.**

Index Terms**—Air Traffic Management, Network Mobility, IPv6, Voice over IP**

I. Introduction

Several European research activities are being undertaken with the goal to develop improved communication technologies for aeronautical communication. These activities comprise ground-based, satellite-based, aircraft-to-aircraft and airport communication for all different application classes, like air-traffic services (ATS), airline operational and administrative communication (AOC, AAC), and aeronautical passenger communication (APC).

The project NEWSKY aims at developing a concept for a global, heterogeneous communication network for aeronautical communications, based on IPv6 protocol stack, focusing on Layer 3 (L3) or network design.

The networking concepts developed within NEWSKY project are validated by two means: extensive computer simulation, and laboratory demonstration. This paper presents the demonstration activity, where future Air Traffic Management (ATM) communication network is emulated in a laboratory environment. The main objective is to show mobility and handover of communications between satellite and terrestrial-based communication network segments. A real air interface is considered for the satellite link, using Broadband Global Area Network (BGAN) service from Inmarsat.

For the terrestrial communication link, an emulator of a potential future long-range air-ground communication technology, L-DACS-1 (L-band digital aeronautical communications system) will be used. The emulator will represent the characteristic of L-DACS-1 for both physical layer (in terms of Bit Error Rate, BER), and data link layer (in terms of delay and throughput). Details about the L-DACS-1 physical and data link layer, which is based on the B-AMC (Broadband Aeronautical Multi-carrier Communications) technology, can be found in [1], whereas performance characteristics are published in [2].

In addition to the L-DACS-1 emulator, a wireless link based on IEEE 802.16 WiMAX will also be integrated into the test-bed. The suitability of both technologies (L-DACS-1 and WiMAX) has been evaluated in NEWSKY and the results show their potentials to be used for future aeronautical communication networks.

As NEWSKY focuses on network layer (Layer 3 in TCP/IP protocol stack), the term “handover” is understood as network layer handover. To be more specific, layer 3 handover takes place when there is a need to change the IP address of a node, as when the node needs to change its default router. The similar term used in IETF world is IP mobility. Therefore the main idea of this paper is to demonstrate the feasibility, and to point out the limitations of IP-based mobility protocol, when used over real link technology, and real applications used in aeronautical communications.

The remainder of this paper is organized as follows. Section II discusses the architecture and the components needed to build the laboratory test-bed. Section III presents potential future ATM services which will be demonstrated, and finally Section IV presents some preliminary results from the tests performed with the test-bed.

II. Deployment of Network Mobility Protocol

A. *Mobile IPv6 and Network Mobility (NEMO)*

Several solutions have been proposed to handle the problem of host and network mobility for aeronautical communications. A Border Gateway Protocol (BGP) based solution similar to the one used in Connexion By Boeing (CBB) [3] system, IPSec-based solution [4], and Mobile IPv6 (MIPv6) [5] are to mention some. After intensive investigations the International Civil Aviation Organization (ICAO) Aeronautical Communications Panel Working Group I (ACP WG-I) as the main group developing aeronautical telecommunication networks (ATN) based on IP protocol stack has decided that MIPv6 and its extensions shall be used as a solution for global network mobility in future IPv6-based aeronautical telecommunication network (ATN).

Manuscript received September 17, 2008. This work was supported in part by the European Commission in the 6th Research Framework Programme (FP-6).

E. H. Fazli, A. Via, and M. Werner are with TriaGnoSys GmbH, 82234 Weßling, Germany (corresponding author: Eriza Hafid Fazli, phone:+49-8153-88678-209, e-mail: eriza.fazli@triagnosys.com)

S. Duflot is with the Institute Supérieur de l'Aéronautique et de l'Espace (ISAE), 31055 Toulouse, France. He is with TriaGnoSys GmbH for the whole duration of this work.

Network Mobility (NEMO) protocol is introduced to extend MIPv6, where a router in the mobile network, the mobile router (MR), performs all mobility-related signalling for all nodes attached to the mobile network. Reference [6] explains the operation of NEMO basic support. In contrast to MIPv6, the NEMO standard does not define a route optimization mechanism. This issue was considered out of scope and shall be studied separately. Another notorious problem introduced by NEMO basic support is the routing inefficiencies in the case of mobile nodes and/or networks roaming inside a mobile network (nested mobility). This problem is also not studied in [6].

Although there are several proposals to further extend and improve NEMO basic support, as of today there seems to be no widely accepted standardized solution and stable protocol implementation, and therefore the basic support is considered as the baseline protocol for network mobility in the laboratory test-bed.

Having MIPv6 and NEMO in mind, the lab test-bed network architecture is built and presented in Figure 1.

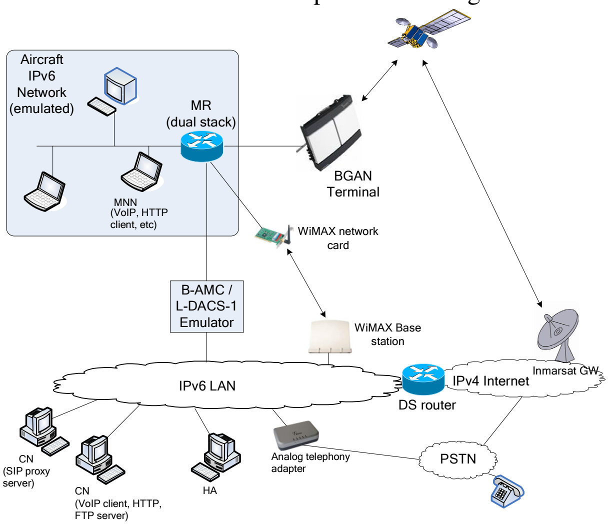

Figure 1: Laboratory test-bed network architecture

The figure includes the entities defined in MIPv6/NEMO, namely Home Agent (HA), Mobile Router (MR), Mobile Network Node (MNN), and Correspondent Node (CN). All MNNs are assumed to be fixed nodes in the mobile network. In developing the test-bed, an implementation of MIPv6 and NEMO protocol from Nautilus6 project has been used.

The MR creates a Care-of Address (CoA) using stateless auto-configuration mechanism, and registers the address to the HA using Binding Update (BU), and the HA replies using a Binding Acknowledgment (BA) message. All packets from and to the mobile network are routed through the HA.

For preliminary testing, all the links are emulated using Linux network emulator (netem) in a LAN, where propagation delay is emulated by adding a delay to an Ethernet interface, and the available transmission bandwidth is limited using a token bucket mechanism.

B. IPv4 Network Traversal

MIPv6 and NEMO are designed for host and network mobility for pure IPv6-based network. Furthermore, NEWSKY considers IPv6 as the baseline protocol stack for the future ATM network. As currently there is no widely deployed IPv6 network, it becomes necessary to define a mechanism for traversing IPv4 network segments. The issue becomes more pronounced when considering the use of BGAN for the satellite link, as all BGAN traffic are routed by Inmarsat ground earth station through the public IPv4 Internet.

For the laboratory test-bed implementation two potential solutions have been investigated, namely tunnelling and protocol translation. Both approaches assume the existence of a dual-stack (DS) IPv6/IPv4 router on the ground network which basically performs the function of an access router. This router is denoted "DS router" in Figure 1. The public IPv4 address of the DS router is assumed fixed and known to the MR.

1) Tunnelling

A tunnel interface is created between the MR and the DS router. The DS router is assigned an IPv6 prefix which it advertises on the tunnel interface. Once the tunnel interface is established, the intermediate IPv4 network will be transparent to the MIPv6 protocol.

There are several possibilities of tunnel types that can be used. The simplest approach would be to use a simple IP-in-IP tunnel, as described in transition mechanisms for IPv6 [7]. However this interface is not supported by the Nautilus6 NEMO implementation. The proposed substitute is Layer 2 Tunnelling Protocol (L2TP) [8], which is designed to carry PPP (Point-to-Point Protocol) frames over an IP network. The two endpoints of an L2TP tunnel are the LAC (L2TP Access Concentrator) which is the tunnel initiator and the LNS (L2TP Network Server) which waits for tunnel requests. The necessary setup for tunnelling a PPP session with L2TP consists of two steps:

1. The LAC sends a request to the LNS in order to create the tunnel. Then, a Control Connection Establishment signalling is performed to set up the tunnel.
2. Once the tunnel is established, the network traffic between the two peers is bidirectional. In order to carry PPP frames through the tunnel, either the LAC or the LNS has to initiate a session, making a call through the tunnel. The traffic for each session is isolated by L2TP, so that multiple session establishments across a single tunnel are possible.

Because only the IPv4 address of the DS router is permanent, the LAC has to be in the MR, and the LNS in the DS router.

L2TP is actually a layer 5 protocol in OSI protocol stack. It adds additional PPP, L2TP, UDP, and IPv4 headers to the original IPv6 packet. This is shown in Figure 2.

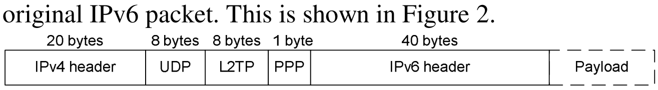

Figure 2: IPv6 packet encapsulation in L2TP tunnel

2) Network Crossing via Translation (NeXT)

Here we propose the use of NeXT, a new protocol to enable efficient transmission of IPv6 packets over IPv4 network. The protocol is based on modified mechanism of the standard NAPT-PT (Network Address and Port Translation – Protocol Translation), defined in RFC2766 [10]. The protocol presented here is an extension of the one in [9], mainly to support mobility-related signalling.

The main difference from the standard NAPT-PT is the fact that both ends are IPv6 hosts. Thus two translations between IPv6 and IPv4 and vice versa are required, i.e. one on the aircraft (MR) and one on the router on ground (TGS DS router), cf., Fig. 1.

Like in IPv4 NAT, the router has a table with the relation between the inner addresses (IPv6) and their correspondent external addresses (IPv4).

As all packets entering or exiting the A/C IPv6-network should be translated to version 4 and again to version 6, both translation routers must have the same translation tables. Otherwise some information about the source and the destination must be sent within the packet.

Header Translation

All the fields in IPv6 header must be transmitted to the other end of the link in order to translate the packet to IPv6 again. They suit to IPv4 fields except the addresses and ports, the *Flow Label* and the *Next Header*. The addresses and ports need to be sent only once per session, they will be stored in the table for further packets. The other two have 28 bits, so we suggest adding them as is shown in Figure 3. Four 0-bit padding has been added in order to have this extended header length multiple of 32 bits. All headers and payload coming after the IPv6 header is shown in Figure 3 as "Payload".

A UDP header has been added to have a more standardized IP packet structure so it can bypass all routers in Internet.

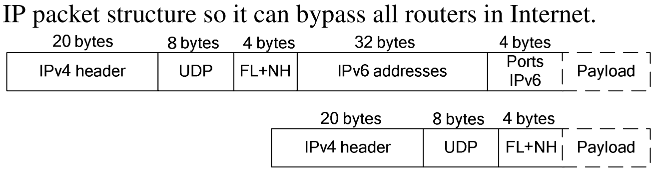

Figure 3: Header format for the first packet of the session (above) and for the following packets (bottom)

Protocol Operation

The protocol explained here assumes that most of the packets are generated from inside the mobile network (MR egress direction), thus, these packets are translated automatically whereas the packets generated outside need some signalling before.

The basic operation for the MR egress packets is explained here:

1. A node generates the first packet of a session, which is destined to the outside IPv6 world and therefore sent to the NAT router / MR.
2. When the router receives it, it looks for an entry in the translation table but it does not find any, as it is the first of a session. Then, it creates a new entry, assigning an address and port pair in this router and also in the router on-ground.
3. Afterwards the router translates and sends the packet with the IPv6 addresses and original ports, as shown in Figure 3
4. After going through the satellite link, the packet arrives at the DS-router who looks for an entry in the table, and, as it does not find any, it reads the IPv6 addresses and ports and creates a new one.
5. Afterwards, the packet is translated and sent to the IPv6-Internet.

The following packets of the same session are translated using the table and sent to the other end of the satellite link using the format described in Figure 3.

On the other hand, for the packets generated outside, the protocol is the following:

1. A node outside the A/C (i.e., a CN) sends a packet to a node inside. The packet is routed to the HA, which will then forward it to the DS router.
2. The DS router looks up in its address translation table and, as it does not find anything, it looks up the destination address in a table where there are all the addresses that each router has.
3. When it finds the correspondent router, the DS router sends a signalling packet to the MR with the addresses and ports in IPv6 and asking for the IPv4 corresponding addresses.
4. MR assigns IPv4 addresses and ports and creates a new entry in the table.
5. MR sends them back to the DS router.
6. After receiving the information, the DS router creates a new entry in the translation table and translates the header. Note that, unlike in the other direction, this first packet does not contain the IPv6 addresses.
7. The DS router sends the packet.
8. The MR receives the packet and translates it to IPv6.
9. The MR sends the packet to the node inside the A/C.

Table 1 lists the advantages and drawbacks of the two approaches.

	Advantage	Drawback
Tunnel (L2TP)	• Independent of upper layer protocol • Stable implementation	Inefficient due to large overhead
NeXT	Small overhead	• Extra processing • Needs additional signalling • Requires reassembly when packets are fragmented • Does not support multicast

Table 1: Comparison of IPv4 traversal methods

The most important advantage of NeXT compared to L2TP is the fact that no extra headers must be added, which makes the transmission through the satellite link cheaper.

However, it leads to a more complex packet processing at each end of the IPv4 link, which is expensive in terms of delay and complexity of the routers. Also add that L2TP has some publicly available implementations whereas NeXT doesn't.

NeXT modifies packets within the path and may raise security concern. This issue still needs to be looked at more carefully. Additionally, support of multicast still needs to be added. On the other hand, L2TP does not have such limitation. A more detailed comparison of both solutions can be found in [17].

III. Representative Services /Applications

Future ATM communications will rely more on data services, and the usage of voice as in the current VHF-based radio system will be greatly reduced. In the design of the NEWSKY network it is assumed that future voice service will be provided via Voice over IP (VoIP). Both VoIP and data transfer applications are considered in the demonstration.

A. *Voice over IP (VoIP)*

The provision of VoIP service relies on the Session Initiation Protocol (SIP) [12]. The entities of VoIP systems are SIP User Agents (UA), SIP server, which can be Redirect or Proxy server, and SIP Registrar server. Depending on the implementation, these entities can be also co-located. For instance a SIP proxy server may also act as a Registrar server. Within the test-bed architecture at least one VoIP UA/client is located at the mobile network. Asterisk open source PBX server [13] is chosen as the SIP proxy server. One major motivation to choose Asterisk is that it supports both IPv6 and IPv4, and it is capable of translating addresses transparently between the two address types.

A realistic VoIP environment is realised through the interface to ordinary Public Switched Telephone Network (PSTN). To have this feature the options are either to use paid interconnection service in the Internet or to use a dedicated adapter to perform the interconnection. We decided to take the second option as it provides more control over voice and connection quality.

B. *Data / File Transfer*

Future ATS/AOC data applications have been investigated considering the communication needs and subject-matter experts' opinion, and are presented in [14]. The messages defined there are, however, quite bursty with relatively low arrival rates and short call durations, and hence will not produce significant demand to properly evaluate performance of network handover. The need for intensive data transfer applications may appear for instance in flight-plan file transfer from Electronic Flight Bag (EFB), and distribution of graphical weather maps. In APC domain, web browsing, FTP data download, and email access are the main services considered.

IV. Demonstration Results and Discussions

All the above mentioned components, namely MIPv6/NEMO protocol implementations and service components, are installed and configured in the laboratory test-bed. Handovers are triggered using basic L3 mechanism namely by Neighbour Unreachability Detection and by indication from Router Advertisements.

Some preliminary tests results and measured parameters from the test-bed are presented in the following subsections. All the tests are so far made using emulated links, where the terrestrial link is emulated with 27 ms of propagation delay and 1 Mbps available bandwidth, and the satellite link with 270 ms of propagation delay and 512 kbps available bandwidth.

A VoIP call and an FTP file transfer session are created, first on the emulated terrestrial link, and then in the middle of the connection the link is switched to satellite, and some while later back to terrestrial before the session ends.

A. *Performance Parameters Definition*

Handover delay and packet loss are used to assess the handover performance. Handover delay is defined as the elapsed time between mobile node/router is no longer able to transmit IP packets due to handover and the instant it is again able to transmit packets. Whereas packet loss is defined as the percentage of IP packets which are created but are not received correctly. Qualitatively, both parameters will have impacts on the perceived QoS by the user.

B. *VoIP Calls*

Figure 4 displays the one-way bit rate at the MNN during a voice call with a CN. Both nodes use a 64kbps G.711 μ-Law codec.

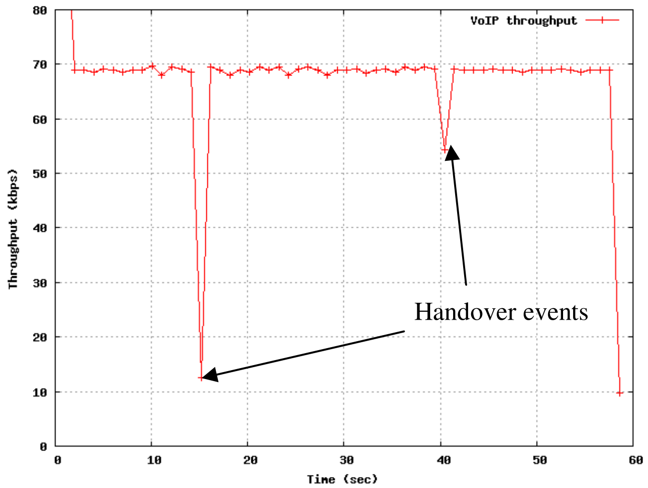

Figure 4: One-way VoIP bit rate

The trace shows effective rate slightly larger than 64kbps due to additional RTP-UDP-IP header added to the data stream. Since VoIP uses connectionless User Datagram Protocol (UDP) as transport layer protocol, packet loss during handover can not be avoided. Within our experiments, packet loss ratio in the range of 1% is observed, with handover delay in the order of 1 second. The amount of packet loss is related to the handover delay; therefore minimizing packet loss can be achieved by minimizing handover delay. This can be achieved for instance by using indication from Layer 2 (L2) to detect movement and trigger the MR to send Router Solicitation (RS) message instead of waiting for Router Advertisement (RA) from the access router.

Another contribution to the handover delay comes from the Duplicate Address Detection (DAD) process to ensure that the newly created CoA is unique. The delay due to DAD can be reduced by using Optimistic DAD option as in [15].

Finally packet loss can be greatly reduced if a make-before-break scheme is used [16]. However it may lead to packet reordering, especially when the links have significantly different propagation delays, and thus this option needs to be taken into account carefully.

C. *File Transfer Throughput*

With an FTP server installed at a CN, an FTP download session is established at the MNN, and handovers are triggered in the middle of the session. Figure 5 shows the average throughput of a download of a 5 MByte bitmap image. The tests are performed using TCP CUBIC, which is the default TCP version used in Linux kernel from version 2.6.19 onwards.

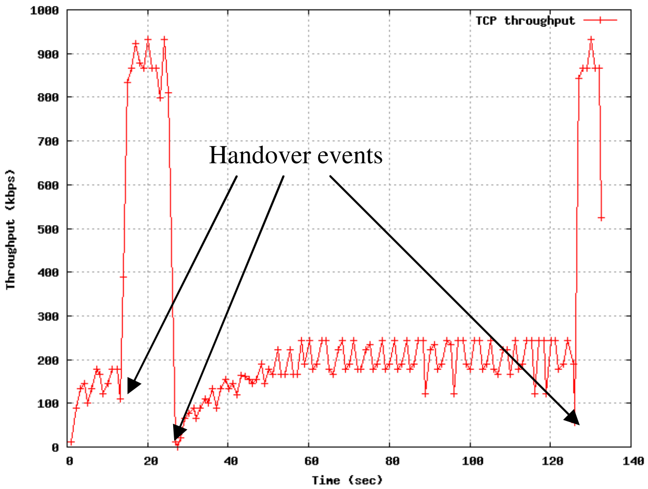

Figure 5: Average throughput of an FTP download session

Several remarks are as follows. First, the effective network throughput drops to zero for 2-4 seconds during handover signalling (movement detection, DAD, and BU-BA signalling exchange), as the TCP sender waits for ACK from the receiver, which do not arrive eventually, until the timeout of the retransmission timer. Due to reliable nature of TCP, however, there is no packet loss encountered within this period.

Second, although not immediately related to the handover events, the middle part of the graph shows the known problem of TCP congestion-control mechanism when applied over large bandwidth-delay-product (BDP) links such as satellite, namely the long time it takes to reach optimum throughput and the underutilisation of the link. Optimizing TCP can be achieved either by tuning TCP parameters, e.g., setting the maximum or the initial window size, or by using Performance Enhancement Proxy (PEP). Tuning TCP only to one link may lead to sub optimum performance in other links, whereas PEP breaks TCP end-to-end connection and does not work if the packets are encrypted. TCP optimization over heterogeneous links is considered out of scope for the current study and would subject to further investigation.

Future work with the test-bed will focus on the integration of the real BGAN satellite link, the WiMAX base station, and the L-DACS-1 emulator. Some optimisation issues, such as the minimization of handover delay, and the packet overhead due to IPv4 network traversal will also be addressed.

References

[1] B-AMC Project, "System Specification Including Standardisation and Certification Considerations," report D-3, Issue 1.0, August 2007. Available: http://www.eurocontrol.int/communications/gallery/content/public/documents/B_AMC%20Project%20Deliverable_D3_V10.pdf

[2] B-AMC Project, "Expected B-AMC System Performance," report D-5, Issue 1.1, September 2007. Available: http://www.eurocontrol.int/communications/gallery/content/public/documents/B_AMC%20Project%20Deliverable_D5_V11.pdf

[3] B. Skeen, "Global IP Network Mobility," Presentation 19th APNIC Open Policy Meeting, February 2005. Available: http://www.apnic.net/meetings/19/docs/sigs/routing/routing-pres-skeen-global-ip-netmob.pdf

[4] Eurocontrol EATM-DAP/CSP CSP Business Division, "A/G IP Study: Deliverable D5/D6 – The Future Communication Infrastructure – Concept and Transition," January 2007. Available: http://www.icao.int/anb/panels/acp/WG/n/swgn1-12/P684D013-1_0%20D5-D6%20The%20FCI%20Concept%20and%20Transition.pdf

[5] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," RFC 3775, June 2004.

[6] V. Devarapalli et al., "Network Mobility (NEMO) Basic Support Protocol," RFC 3963, January 2005.

[7] R. Gilligan and E. Nordmark, "Transition Mechanisms for IPv6 Hosts and Routers," RFC 1933, April 1996

[8] W. Townsley, et al., "Layer Two Tunneling Protocol 'L2TP'," RFC 2661, August 1999.

[9] A. Via and A. Jahn, "IPv6 Networking Over Satellite For Mobile User Groups", International Workshop on IP Networking over Next-generation Satellite Systems (INNSS'07), Budapest

[10] G. Tsirtsis, and P. Srisuresh, "Network Address Translation - Protocol Translation (NAT-PT)," RFC2766, February 2000.

[11] T. Narten, E. Nordmark, and W. Simpson, "Neighbor Discovery for IP Version 6 (IPv6)," RFC 2461, December 1998.

[12] J. Rosenberg, "SIP: Session Initiation Protocol," RFC 3261, June 2002.

[13] WWW Page: www.asteriskv6.org. Last visited: September 16, 2008.

[14] Eurocontrol/FAA Future Communication Study, "Communications Operating Concept and Requirements for the Future Radio System," COCR version 2.0, May 2007.

[15] N. Moore, "Optimistic Duplicate Address Detection (DAD) for IPv6," RFC 4429, April 2006.

[16] H. Petander and E. Perera, "Improved Binding Management for Make Before Break Handoffs in Mobile IPv6," draft-petander-mip6-mbb-00, October 2005.

[17] À. Via, E. H. Fazli, et al.,"IP Overhead Comparison in a Test-bed for Air Traffic Management Services", in *Proc. IEEE 69th Vehicular Technology Conference*, Barcelona, 2009