



Mobility Options in the IP-based Aeronautical Telecommunication Network

Serkan AYAZ¹, Christian BAUER¹, Max EHAMMER², Thomas GRAUPL², Fabrice ARNAL³

¹German Aerospace Center (DLR), Wessling, Munich, 82234, Germany

Email: {serkan.ayaz, christian.bauer}@dlr.de

²University of Salzburg, Jakob Haringer Str. 2, 5020 Salzburg, Austria

Email: {mehammer, tgraeupl}@cosy.sbg.ac.at

³Thales Alenia Space, 26 avenue Champollion BP 33787 31037 Toulouse Cedex 1, France

Email: fabrice.arnal@thalesaleniaspace.com

Abstract: Currently aeronautical communications for cockpit users are based on analogue voice services and non-widely used networking solutions. A concept for IP-based aeronautical communications integrating different radio-link technologies and services is currently being discussed in aviation society. Providing seamless mobility to passengers and cockpit users travelling at high speeds and connected by a wide range of wireless networking technologies is a challenging task. Internet Engineering Task Force (IETF) is an organization developing IP standards. According to the recent IETF research on network layer mobility, two major fields of work can be identified: scope of mobility and management of mobility. The former notion introduces a hierarchical concept distinguishing between local and global mobility scope; the latter notion addresses the functional entity responsible for mobility signalling. This can either be the mobile node (MN) itself or the network performing signalling on behalf of the MN. The applicability of these concepts to the aeronautical environment is analyzed in detail. Mobile IPv6 (MIPv6), and IETFv2 Mobility and Multihoming (MOBIKE) are discussed as typical node-based global mobility management solutions, and Proxy Mobile IPv6 (PMIPv6) is analyzed as a typical network-based local mobility management solution.

Keywords: Aeronautics, Mobility, Mobile IPv6, MOBIKE

1. Introduction

The aeronautical environment categorizes three different communication services; all of them have different requirements and regulations. These services are Air Traffic Services (ATS), Aeronautical Operational Control Services (AOC), and Aeronautical Passenger Communications (APC). ATS and AOC are provided by the Aeronautical Telecommunication Network (ATN), which is considered an integral part of the Air Traffic Management (ATM) system. Although, currently most ATS/AOC communications are based on analogue voice it is predicted that by 2020 the primary means of communication will be data [1]. ATS data messages are classified as safety-of-life messages and have stringent requirements in terms of delay, availability, continuity, and integrity [1].

The current ATN standards are based on the International Organization for Standardization Open Systems Interconnection (ISO/OSI) reference model and its protocols (ATN/OSI) which deviate significantly from protocols of the more widely deployed IETF Internet protocol suite. Due to the marginal deployment of the ISO/OSI protocols, operation and maintenance costs are considerable. In 2005, the International Civil Aviation Organisation (ICAO) finalized a report on the feasibility of introducing the Internet Protocol (IP) into the ATN (ATN/IP) [15]. It was stated in this report that the

implementation of IP is considered feasible for ground-ground communication although further study would be required on the feasibility for air-ground communication. Eurocontrol has been working on the development and deployment of IP-based ground-ground communication and it is expected to be in service by July 2009 [16]. An ATN/IP solution that includes air-ground communication is expected to be operational in the 2015-2020 timeframe. One of the corner stones of the current ATN/IP development effort is the standardization activities conducted by ICAO [19]. These activities will be followed by the certification of the standards for aviation which is considered important for the ATN/IP realization process.

In [15], mobility was identified as a particular issue to be resolved and several studies concerning mobility solutions for air-ground communication were initiated. Ten different candidate mobility solutions for the ATN/IP were identified [2]. The identified candidate solutions belong to different layers such as, data link, network (e.g. MIPv6ⁱ or Border Gateway Protocol version 4 (BGPv4)), transport (e.g. Stream Control Transmission Protocol), and application layer.

In this document, two promising approaches, namely MIPv6 [7] and MOBIKE [11] are discussed in the ATM context, with special focus on overhead, delay, and security. These two solutions are selected since the former one appears to hold promise for a long term solution [7], and the latter one is proposed by the Eurocontrol IP study [18] as another potential solution. In addition to global mobility management (GMM) solutions analyses (i.e. MIPv6 and MOBIKE), we also discussed its integration with a local mobility management (LMM) solution (i.e. Proxy Mobile IPv6). GMM provides a mobile node to change the global, end-to-end routing of packets for the purpose of maintaining session continuity when movement causes a topology change, while LMM maintains session connectivity and reachability of a mobile node when the mobile node moves, and whose signalling is confined to an access network [20]. APC is not investigated in detail in this paper. However, it is assumed that the same considerations apply, in principle. The rest of the paper is organized as follows: Section 2 describes the properties of aeronautical communication. Section 3, 4, and 5 give a presentation and analysis of selected mobility solutions. Each mobility solution is discussed in terms of its signalling and delay overhead on the wireless link. Section 6 provides security considerations related to mobility. Finally, section 7 concludes the paper.

2. Aeronautical Communication Scenarios

Most aircraft communicate only with two different entities, the Air Traffic Services Unit (ATSU), which is responsible for the safety of flight, and the airline operating centre for the exchange of airline operations data. In case of ATS communication message exchanges commence between the aircraft and correspondent nodes located at the control facility. The correspondent nodes change as the aircraft moves across airspace sector borders where control is transferred between different ATSUs. In the case of AOC communication the data packets will be routed to correspondents geographically far more remote to the aircraft than to correspondent nodes involved in ATS. The AOC correspondents will also be most probably static for the lifetime of the flight, rather than dynamic like the ATS correspondents [14].

When evaluating mobility solutions in the context of aeronautical networking it is paramount to consider the performance requirements formally stated in [1]. It is important to note that for this investigation the overhead on the wireless channel, and its delay, and security aspects are the most relevant requirements, as they differ for each mobility approach. A fundamental problem of the aeronautical environment is the utilization of the (usually anaemic) bandwidth at the wireless link. This is a major performance restriction not present in other networking environments directly affecting the efficiency of the air-

ground connection. For instance VHF Data Link Mode 2 (VDL2) as the state of the art data link technology in aeronautical communication provides a nominal throughput of 31.5 kbps for all aircraft within a single cell (typically up to 200 nm radius and approximately 200 aircraft). The proposed future radio systems [3] will provide a throughput of approximately 300 to 400 kbps in the same area, which is still not comparable to short range technologies. Another characteristic problem of the aeronautical wireless links is their comparatively high transmission latency. Typical values are in the range of several 100 milliseconds. The limitations of the wireless link are a major motivation to investigate network-based LMM solutions in aeronautics. In addition, any supplemental node-based GMM solution should introduce as little overhead as possible on the wireless channel.

3. Proxy Mobile IPv6 (PMIPv6)

PMIPv6 is an LMM protocol introduced by the Network-based Localized Mobility Management (NETLMM) working group in the IETF [4]. The main benefit of this protocol is that an MN is not involved with the mobility signalling and that the network performs the required signalling on behalf of the MN attached to it. However, the protocol provides only local mobility such that in case of an access network change, all ongoing sessions are broken. In a PMIPv6 domain, two network elements are implemented; namely Local Mobility Anchor (LMA) that functions as a Home Agent (HA) for the MN in the PMIPv6 domain and Mobile Access Gateway (MAG) that performs signalling with a LMA for mobility management on behalf of the MN attached to the MAG. If the MN moves and changes its point of network attachment from MAG A1 to MAG A2 (see Figure 1), it can still use the same configured address. This is possible because the signalling between the MAGs and the LMA of the node is “tricking” the MN into believing that it is still on the same link. However, this approach works only within the same operational domain. If the aircraft leaves this domain a GMM protocol is required in order maintain the ongoing sessions.

3.1 Signalling Overhead on the Wireless Link

In PMIPv6 all mobility related signalling except MN identifier (MN-ID) provision to MAG, occurs on the ground so there is a negligible overhead on the wireless channel.

3.2 Delay Analysis

If the MN changes its point of attachment within the access network PMIPv6 requires the following procedures:

- Mobile Node Identifier (MN-ID) notification (unidirectional over the wireless link)
- MN-ID authentication (ground part of the access network)
- Proxy binding registration including a possible Internet Key Exchange (IKEv2) [10] exchange to secure the mobility signalling (ground part of the access network)
- IP address configuration assuming a successful router advertisement reception by the MN (unidirectional over the wireless link)

Under the assumption that the end-to-end latency of the ground access network is negligible when compared to the transmission latency of the wireless linkⁱⁱ, the signalling delay introduced by PMIPv6 is thus characterized by 1 wireless round-trip time (WRTT) after each mobility event.

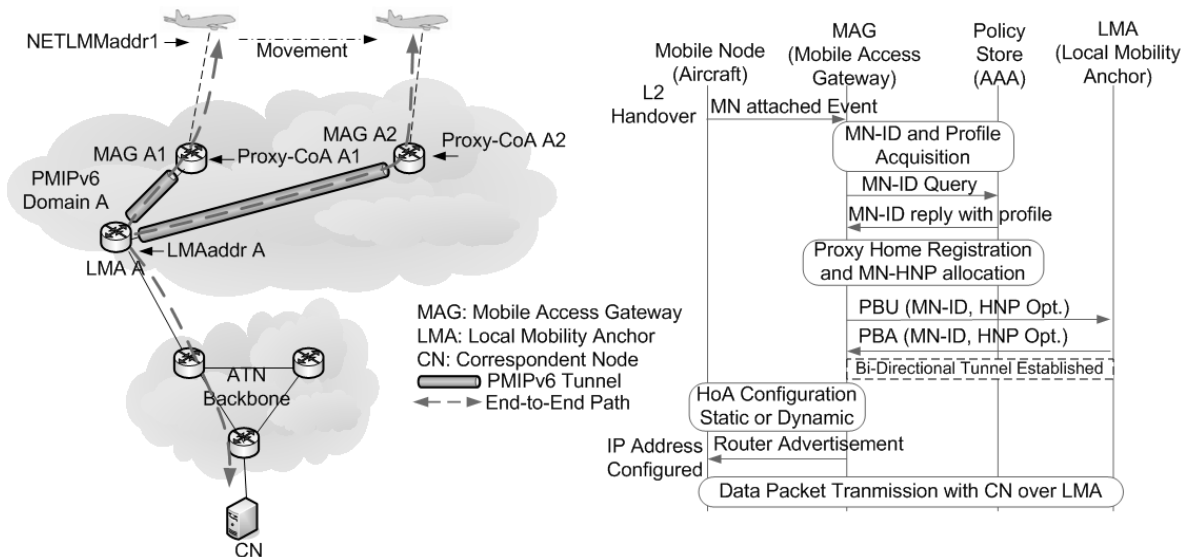


Figure 1: Local Mobility (PMIPv6)

4. Mobile IPv6 (MIPv6) with PMIPv6

Figure 2 illustrates a typical MIPv6 scenario. The aircraft has a home PMIPv6 domain providing LMA and HA functionality. The home domain acts as a proxy aggregating the aircraft's home address and advertising the aggregate prefix to the ATN backbone. As long as the aircraft is attached to its home domain, local mobility management (i.e. PMIPv6) handles the mobility and MIPv6 is not needed. Packets addressed to the aircraft's home address are routed in a standard fashion to the home domain network, where PMIPv6 routes the packet to the current location of the aircraft. If the aircraft visits a foreign domain, it dynamically configures a temporary address from that network and registers its Care-of Address (CoA) at the HA. Now the HA will intercept any incoming packets addressed to the aircraft and tunnel them (via IP-in-IP encapsulation or IP security (IPsec) tunnelling) to the aircraft's current CoA (*NETLMMaddr2*) as shown at the left side of Figure 2. Mobility signalling is secured by IPsec in transport or tunnel mode [5] [6]. Return routability (RR) procedure and correspondent node (CN) registration are performed for route optimization (RO) (right side of Figure 2) between the MN and the CN.

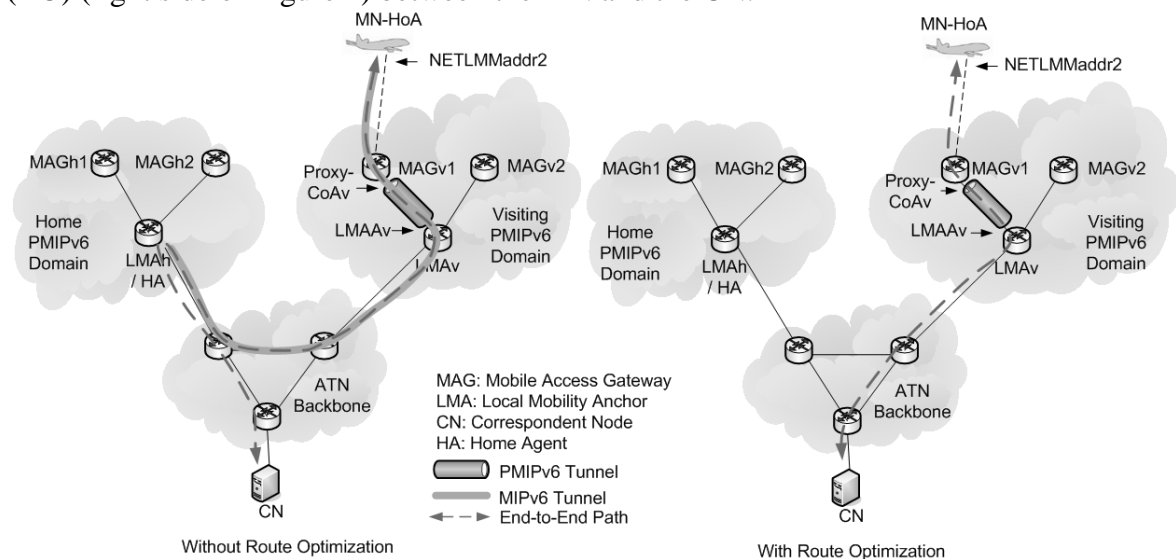


Figure 2: Local Mobility (PMIPv6) with Global Mobility (MIPv6)

4.1 Signalling Overhead on the Wireless Link

Figure 3 shows the MIPv6 specific mobility signalling and its overhead. HA registration is required when the MN visits a new network and acquires a new CoA. RR procedure and CN registration processes are needed for route optimization which is required to be sent by the mobile node every 7 minutes at the latest [7].

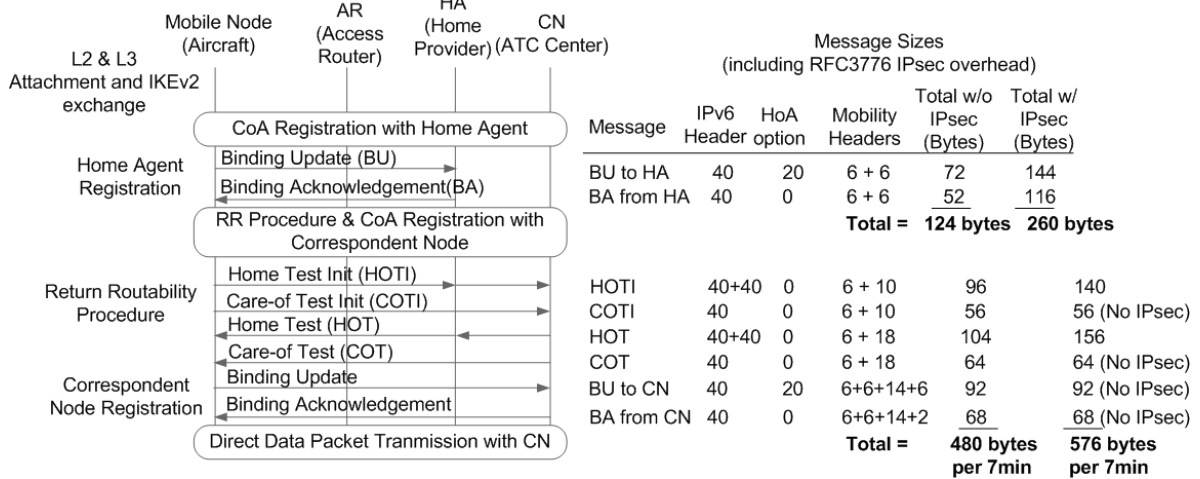


Figure 3: Mobile IPv6 Signalling

4.2 Delay Analysis

Mobility signalling takes place upon completion of the layer 2 and layer 3 attachments which may include a local PMIPv6 attachment. In the case of MIPv6 this involves the following procedures between the MN and the HA:

- CoA configuration assuming successful router advertisement reception by the MN (1 exchange over the wireless link; may be provided by PMIPv6)
- Establishment of a IPsec SA using IKEv2 (2 exchanges over the wireless link)
- CoA registration with the HA (1 exchange over the wireless link)

If route optimization is desired the following procedures have to be performed for every CN once in 7 minutes:

- RR Procedure (1 exchanges over the wireless link since Home Test Init (HOTI) and Care-of Test Init (COTI) messages are sent in parallel)
- Correspondent Node Registration (1 exchange over the wireless link)

Thus, under the same assumptions as above, it takes 4 WRTTs to establish basic MIPv6 functionality and additional 2 WRTTs with each CN for route optimization. If the MN has already established an initial SA with the HA and MOBIKE is supported, a CoA registration after a change of attachment takes only 3 WRTTs.

4.3 Enhanced Route Optimization

The maximum lifetime of a binding between the MN and the CN is restricted to 7 minutes [7] and therefore requires frequent Route Optimization (RO) signalling. Due to this increased signalling the associated overhead can become an issue even for rarely moving nodes. The Enhanced RO [8] has been proposed to reduce this signalling overhead while providing even higher security. This optimization is possible due to a Cryptographically Generated Address (CGA) as specified in [12] which provides a strong cryptographic binding between the MNs (generated) interface identifier and the MNs public key. In the case of Enhanced RO, the lightweight procedure limits the signalling to a single complete RR procedure and BU exchange between the MN and the CN. If the CoA changes after the initial network attachment no further HoTI/HoT exchange is needed. In addition the binding lifetime at the CN has been increased to 24 hours.

5. MOBIKE with PMIPv6 Scenario

The MOBIKE based mobility approach is discussed in [9]. This approach implicitly provides network layer mobility and security features to the aircraft. As shown on the right side of Figure 4, all traffic between the MN and the CN follows an optimal path. When the MN is at home it acquires a home address (i.e. MN-HoA) and performs IKEv2 exchanges as specified in [10]. After IKEv2 messages are exchanged, a tunnel is established between the MN and the CN. When the aircraft moves to another domain (i.e. access network) a MOBIKE Address Update notification is sent by IKEv2 to update the Security Association (SA) addresses at the CN (i.e. *NETLMMaddr2*). Only the outer tunnel source address of the MN packets is affected by this address update. End-to-end communications are unaffected by the change in the aircraft's dynamic address, thus providing session continuity. MOBIKE [11] provides signalling optimization with only one message exchange (request and response) in case of attaching a new network as shown on the right side of Figure 4.

This scenario is only applicable to a communication scenario where the MN needs not to be reached from outside. A typical case is AOC communication, where the aircraft has the responsibility to register with its airline operations center.

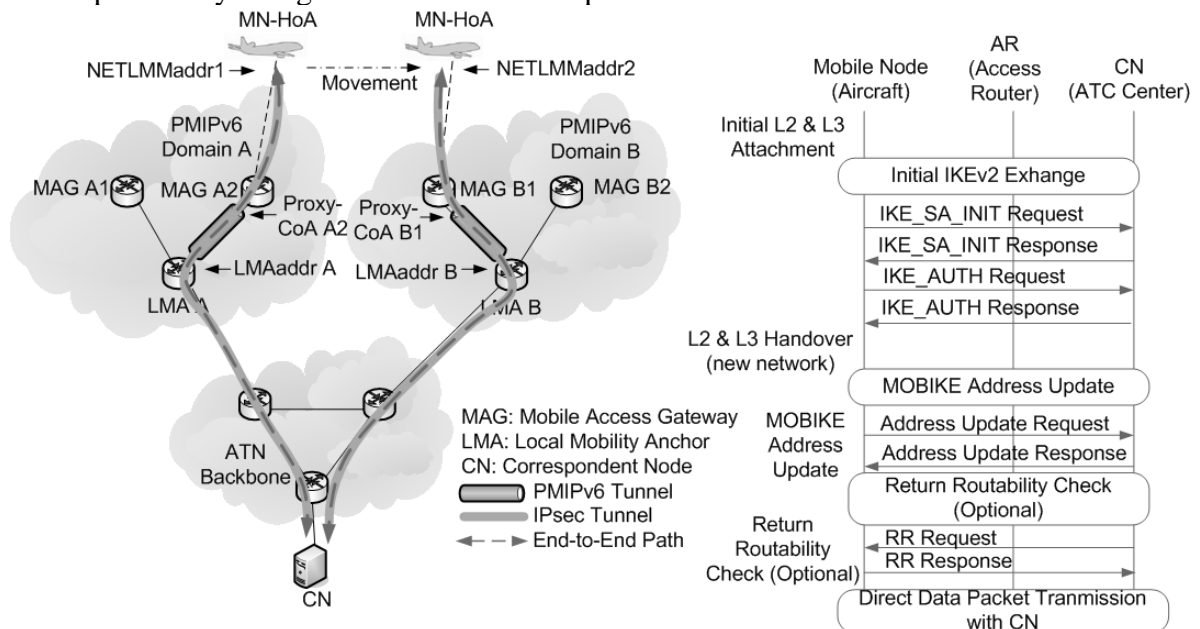


Figure 4: Local Mobility (PMIPv6) with Global Mobility (MOBIKE)

5.1 Signalling Overhead on the Wireless Link

As shown on the right side of Figure 4, the IKE initialization phase including SA establishment and authentication is mandatory (see section 6). This results in (at least) 2 message exchanges (request and response). The additional overhead caused through MOBIKE is 8 bytes within the *IKE_AUTH* message, where the support of this method is signalled. The address change is signalled to the communication peer through an IKE informational exchange, which is the “update SA addresses” notification message. Additional options can be transferred within this notification, hence the size is variable. Transmitting the message with the address update only results in a message size of 132 bytes (assuming the IPsec configuration of section 6). Upon receipt of the address update an informational reply message is sent by the peer, which is approximately the same size. If a return routability check is required (dependent on the implemented policy) an informational exchange message (optionally) including a cookie is used. The size of the cookie is variable between 8 and 64 bytes. Again, considering the assumptions of section 6 and a cookie size of 32 bytes the return routability message is 108 bytes long. The findings of the overhead

analysis are summarized in Table 1 (assuming the IPsec configuration of section 6). The overhead for the configuration of the local IP address is not included.

Table 1: Overhead Introduced by the Investigated Mobility Approach on the Wireless Link Under the Assumptions of Section 6 (AES-CBC 256) in Byte

Mobility Protocol		PMIPv6	MIPv6	MIPv6 with enhanced RO	IPsec tunnel movement
Initial network attachment		0 B	IKEv2: 3672 B MIPv6: 260 B	IKEv2: 3672 B MIPv6: 260 B	IKEv2: 3672 B per CN
Move of network attachment		0 B	MOBIKE: 264 B MIPv6: 260 B	MOBIKE: 264 B MIPv6: 260 B	MOBIKE: 264 B per CN RR check: 216 B per CN
Route optimization	Initial	N/A	576 B per CN Every 7 min	2460 B per CN ⁱⁱⁱ Every 24 h	(implicitly established)
	Consecutive	N/A	576 B per CN every 7 min	280 B per CN Every 24 h	(implicitly established)

5.2 Delay Analysis

The establishment of a MOBIKE tunnel with a CN requires the following procedures. For the first establishment of the tunnel:

- Establishment of a IPsec SA using IKEv2 Exchange (2 WRTT)
After each consecutive mobility event only a MOBIKE address update is needed:
- MOBIKE Address update (1 WRTT)

Thus, under the same assumptions as above, the initial establishment of the IPsec tunnel takes 2 WRTTs per CN and 1 WRTT per CN after each mobility event. The findings of the delay analysis are summarized in Table 2.

Table 2: Delay Introduced by the Investigated Mobility Approaches on the Wireless Link in WRTT

Mobility Protocol	PMIPv6	MIPv6	MIPv6 with enhanced RO	IPsec tunnel movement
Initial network attachment	1 WRTT	1 WRTTs	1 WRTTs	2 WRTTs per CN
Move of network attachment	1 WRTT	1 WRTTs	1 WRTTs	1 WRTTs per CN
Route optimization (initial and consecutive)	N/A	2 WRTTs per CN Every 7 min	2 WRTTs per CN Every 24 h	(implicitly established)

6. Security Considerations related to Mobility

In order to secure mobility signalling between MN and HA, IPsec is mandated in [5] [6]. IPsec provides numerous possibilities for confidentiality, data integrity, access control, and data source authentication. These services are provided by maintaining a shared state between the source and the sink of IP datagrams. Establishing such a state manually is not only error prone and tedious, but also not scalable. Internet Key Exchange (IKEv2) [10] is used to create this state dynamically which performs mutual authentication and establishes an SA. An SA offers security services to the traffic passed through the SA and needs at least two message exchanges for a successful establishment. On the right side of Figure 4, the initial exchanges are shown. The first exchange, IKE_SA_INIT, is responsible for the initialization and negotiates cryptographic algorithms, exchanges nonces and does a Diffie-Hellman (D-H) exchange. With the D-H exchange a secret key between the source and the sink is established. Based on this secret the keys for encryption and integrity algorithms are derived. From now on all messages that follow are encrypted and integrity protected (except the outer header). In the following the second message exchange, IKE_AUTH, is performed. This message authenticates the previous communication, exchanges identities and possibly certificates, and may establish the first SA. This is dependent whether both communicating partners agree on the proposed methods or not.

In order to approximate the overhead caused by IPsec, we assumed an example configuration, including the IKE (28 Bytes), UDP (16 Bytes), and IPv6 (40 bytes) headers. For the IKE_SA_INIT we assumed the Diffie-Hellman group 2 (16+128 bytes), a nonce length of 136 bytes, a proposal of three encryption variants (56 bytes), a single proposal for the pseudo random function (20 bytes), and a single proposal for the integrity check (20 bytes). For the IKE_AUTH we assumed a fully qualified domain name string for

identification (30 bytes), proposals for encryption and integrity (68 bytes), three proposals for a traffic selector initiator range (272 bytes), three proposals for a traffic selector responder range (272 bytes), and an authentication signature of 100 bytes. Further we assumed that AES-CBC 256 (cyclic block cipher, which has a 16 byte initialization vector and a 16 byte aligned payload length) and HMAC_SHA_96 (12 byte integrity check) was selected from the proposal. Hence we come up with the overhead shown in the left side of Table 3 for the IKE initialization phase [10].

Table 3: IKEv2 Overhead Assuming the IPsec Configuration of Section 6

Initial IKEv2 Exchange		Binding Update (BU) / Binding Acknowledgement (BA) → MIPv6 case		
Message	Size (Bytes)	Message	Size (Bytes)	Exchange (Bytes)
IKE_SA_INIT Request	460	BU (MN not at home) incl. alternate CoA – ESP Transport	144	260
IKE_SA_INIT Response	436	BA (MN not at home) – ESP Transport	116	
IKE_AUTH Request	1412			
IKE_AUTH Response	1364			
Total IKEv2 Exchanges	3672			

Considering the security overhead regarding MIPv6 mobility solution, an SA needs to be established between a MN and a HA. Therefore, the procedure described above has to be used. For the route optimization procedure used in MIPv6 a different approach is utilized though. Here the tokens carried in the Home Test (HoT) and Care-of Test (CoT) messages are used to create a Binding Management Key (Kbm), which is used to encrypt subsequent Binding Updates toward and Binding Acknowledgements from the Correspondent Node, respectively. Kbm has a maximum lifetime of 4 minutes, which is relatively short. But, enhanced RO [8] provides 24 hour binding lifetime and a permanent home keygen token.

7. Conclusion

In this paper, we investigated MIPv6 and MOBIKE as a global mobility solution and PMIPv6 as a local mobility optimization in the ATN/IP. The analyses covered mobility signalling overhead, delay and security issues in the context of ATM.

As a first task, we have investigated PMIPv6 which is a promising solution for ATN/IP since it significantly reduces the overhead on the wireless link for mobility signalling. This is very attractive as the bandwidth for aeronautical links is scarce and expensive. Another benefit of PMIPv6 is due to its excellent delay performance since all the mobility signalling is done in the wired links which is faster and more reliable compared to wireless links.

We have investigated two GMM solutions as a second task considering some security aspects. The findings indicate clearly that the overhead of these two solutions is significant on the wireless link; both in terms of data volumes and latency. Thus the use of PMIPv6 is highly desirable to decrease the mobility signalling over the wireless link wherever possible. It is important to note that the overhead of the MOBIKE as well as the impact of MIPv6 route optimization depends strongly on the number of CNs and thus on the use-case (ATS vs. AOC). Route optimization and IPsec tunnel movement should be avoided if minimum latency is not absolutely required like this is the case in AOC. MOBIKE has been identified as an appropriate mobility solution for AOC offering VPN-like network access for flight crews to the company intranet. Comparable VPN solutions are widely deployed and used in the Internet today, making MOBIKE an acceptable solution for airlines.

In the case of ATS communications, it is necessary for the aircraft to be reachable while moving (i.e. by a network entity on the ground such as a non-controlling ATSU). This requires a location management entity aware of the current point of network attachment of the aircraft. MIPv6 is a well known solution to this problem. If RO is required in the ATS case it is desirable to have Enhanced RO [8] to decrease the overhead in the wireless link.

Considering security, one important consideration is the MN authentication which may be provided by Public Key Infrastructure (PKI). In case MIPv6, MN and HA use

certificates for authentication, whereas in MOBIKE certificates will have to be used between MN and CN. From this perspective, MOBIKE scenario requires a global end-to-end PKI deployment which is not feasible for the near future. Another drawback of MOBIKE is that it provides IPsec protection for all packets. However, some packets may not require any kind of security protection. In this case MIPv6 provides IPsec as an option.

Our future work will focus on the extensions of MIPv6 like network mobility (NEMO), multihoming support, and fast handover aspects. The provision for resilience against HA failure is an important aspect of this work.

Acknowledgement

This work is partially funded by the European Commission through the NEWSKY project [13] under contract no. 37160. The authors would like to thank Daniel Medina and Frank Schreckenbach for the discussions.

References

- [1] Communications Operating Concept and Requirements for the Future Radio System, version 2.0, Eurocontrol/FAA
- [2] ICAO ACP WG I-01/WP-06, Analysis of candidate ATN IPS mobility solutions, June 2007
- [3] N. Fistas, B. Philips "Future Communication Study – Action Plan 17, Final Conclusions and Recommendations", Proc. DASC'07, 2007
- [4] S. Gundavelli, V. Devarapalli, K. Chowdhury, B. Patil, draft-ietf-netlmm-proxymip6-08, Proxy Mobile IPv6, December 25, 2007
- [5] J. Arkko, V. Devarapalli, F. Dupont, RFC 3776, Using IPsec to Protect Mobile IPv6 Signalling Between Mobile Nodes and Home Agents, June 2004
- [6] V. Devarapalli, F. Dupont, RFC 4877, Mobile IPv6 Operation with IKEv2 and the Revised IPsec Architecture, April 2007
- [7] D. Johnson, C. Perkins, J. Arkko, RFC 3775, Mobility Support in IPv6, June 2004
- [8] J. Arkko, C. Vogt, W. Haddad, RFC 4866, Enhanced Route Optimization for Mobile IPv6, May 2007
- [9] Eurocontrol "A/G IP Study", Helios Technology Ltd.
- [10] C. Kaufman, RFC 4306, Internet Key Exchange (IKEv2) Protocol, December 2005
- [11] P. Eronen, RFC 4555, IKEv2 Mobility and Multihoming Protocol (MOBIKE), June 2006
- [12] T. Aura, RFC 3972, Cryptographically Generated Addresses (CGA), March 2005
- [13] <http://www.newsky-fp6.eu/>
- [14] W. Eddy, W. Ivancic, T. Davis, draft-ietf-mext-aero-reqs, NEMO Route Optimization Requirements for Operational Use in Aeronautics and Space Exploration Mobile Networks, December 12, 2007
- [15] Use of Internet Protocols Suite (IPS) As a Provision for Aeronautical Internetworking, ICAO ACP WGN Report on TCP/IP, May 2005
- [16] ICAO ACP WG I-06, Information Paper, European Air Traffic Management, Pan-European Network Services (PENS), March 2008
- [17] ICAO ACP WG I-06/WP-08, Updated Mobility Management Requirements for the "Manual for the ATN using IPS Standards and Protocols", March 2008
- [18] Eurocontrol A/G IP Study, EATM-DAP/CSP, January 2007
- [19] ICAO ACP WG I-06/WP-08, Draft "Manual for the ATN using IPS Standards and Protocols (Doc 9896)", version 13f, February 2008
- [20] J. Kempf, RFC 4830, Problem Statement for Network-Based Localized Mobility Management (NETLMM), April 2007

ⁱ ICAO adopted Mobile IPv6 as a global mobility management protocol for the ATN/IP in the 6th meeting[17]

ⁱⁱ This assumption is justified by the fact that the *minimum* required 95-percent quantile of the 1-way latency of the wireless link is as high as 740 ms [1].

ⁱⁱⁱ Assumptions: RSASSA-PKCS1-v1_5 with SHA-1 and a 1024 bit RSA key for the signature option and 1024 bit RSA key for the public key for the CGA parameters option [12]