Architecture of an IP-based Aeronautical Network

Serkan Ayaz[1], Christian Bauer[1], Christian Kissling[1], Frank Schreckenbach[1],
Fabrice Arnal[2], Cedric Baudoin[2], Katia Leconte[2], Max Ehammer[3], Thomas Graeupl[3],
[1]German Aerospace Center (DLR), 82234 Wessling, Germany
[2] Thales Alenia Space, 31037 Toulouse Cedex 1, France
[3] University of Salzburg, Jakob Haringer Str.2, 5020, Salzburg, Austria

Abstract

The International Civil Aviation Organization (ICAO) has defined a mobile IPv6-based Aeronautical Telecommunications Network (ATN/IPS) as a next generation communication network for future Air Traffic Management (ATM). The ATN/IPS will be used with different terrestrial and satellite link technologies for supporting future ATM. In parallel, non-operational services will use different link technologies as well. In such an environment, the main challenge is to design a network architecture that integrates all link technologies in a way that mobile users (be it a cockpit user or a passenger) can make use of them in a seamless way. This paper presents the core functionalities developed within the NEWSKY project of such an integrated IP network architecture.

Introduction

In aeronautical communications, three main service types are defined and each service type has different requirements. These services are Air Traffic Services (ATS), used for controlling the aircraft within a certain airspace, Airline Operational and Administrative Services (AOC/AAC), used for business operations of the airline, and Airline Passenger Communications (APC), used by the passengers. While ATS and AOC will be carried over the Aeronautical Telecommunications Network (ATN), AAC and APC will be most probably segregated from the ATN in order to access the public Internet.

There are three main components of the ATN, namely Air/Ground Communications Service Provider (ACSP), Air Navigation Service Provider (ANSP), and Airline Operations (AO). An ACSP operates an access network with different link technologies and carries ATS and AOC traffic of an aircraft. An ANSP manages the air traffic within a country or geographic region and can have its own subnetwork where ATS correspondent nodes (CN) are located. Finally Airline Operations is used for managing the business operations of an airline and has its own subnetwork where AOC CNs are located.

Trends in Aeronautical Communications

Eurocontrol/FAA published operational requirements of the future ATM in the Communications Operating Concept and Requirements (COCR) document[1]. According to the COCR, the data communications services will be the primary means for air-ground communication after 2020 which will considerably increase the data traffic. In order to handle this, different link technologies should be used in a seamless way so that the services will not be affected due to a change of an attachment to a different link technology.

In the future ATM, an aircraft will have different link technologies available for information exchange, depending on the airspace type. As examples, IEEE802.16e will be used at the airport, L-band Digital Aeronautical Communication System (L-DACS) is foreseen to be mainly used in TMA and En-route airspaces, and satellite technologies can be used in all airspaces, including oceanic/remote/polar regions.

For APC/AAC, further link technologies are foreseen as provided by e.g. Aircell, Inmarsat, etc.

NEWSKY Vision of "Networking the Sky"

The NEWSKY project[10] addresses the challenge to develop an initial design of a global, seamless aeronautical communication network with focus on air-ground communications and IPv6 technologies.

NEWSKY pursues the vision of “Networking the Sky” by integrating different data link technologies (long range air-ground links, airport links, satellite links) and different services (ATS, AOC, APC) in a single, seamless network.

Whereas SWIM concepts provide a conceptual framework for global information sharing, NEWSKY is a technical enabler for the implementation of such an approach. NEWSKY does not develop new data links nor does it define a SWIM architecture offering various services. The NEWSKY project focuses on the design of a tailored IPv6 network including transport layer options and proposes an abstract signaling interface which may be utilized by data links.

Overall Network Architecture

The NEWSKY network architecture integrates four main functions in order to maintain seamless communication capabilities to the NEWSKY users. These functions are Mobility, Handover, Security, and Quality of Service (QoS).

Mobility Architecture

Mobility management aims at maintaining transport level session continuity and global reachability for an aircraft when it is moving between different access networks. The NEWSKY mobility architecture is mainly based on Mobile IPv6 (MIPv6[2]) and its network mobility (NEMO) extension. This approach is in line with the decision for MIPv6 as basic mobility management protocol of the ATN/IPS[3] recently standardized by the ICAO.

Mobile IPv6 and the need for Network Mobility (NEMO)

MIPv6 is a mobility management protocol which allows nodes to remain reachable while moving between different IPv6 networks. Each mobile node is always identified by its home address (HoA), regardless of its current point of attachment to the Internet. While situated away from its home, a mobile node is also associated with a care-of address (CoA), which corresponds to the mobile node's current location. The protocol introduces an anchor point called “Home Agent” (HA) that stores the mobility information (i.e. mapping of HoA to CoA) for the mobile node. Since Mobile IPv6 is standardized as a host mobility protocol, it is not scalable in terms of mobility signaling overhead if we consider an aircraft with multiple numbers of hosts on board. To address such kind of problems, the Internet Engineering Task Force (IETF) has specified a Network Mobility (NEMO[4]) protocol that introduces a new network entity called Mobile Router (MR).

Deployment of HAs in the ATN

One important consideration is to place HAs in the ground part of the ATN. In the ATN, we suggest to locate HAs in Global Air/ground Communication Service Provider (GACSP) considering their global presence in the ATN.

An alternative would be to place the HAs in operation networks of the airlines. However, there are two main advantages of the first scenario, in particular for ATS communications: First, it will be more cost efficient for small airlines that might prefer not to deploy the HA in their networks and rely on GACPS as mobility service provider. Second, the aircraft will be attached to his home network as long as it is directly attached to that GACSP.

NEMO and the need for NEMO Route Optimization

NEMO enables the handling of an aircraft as a moving network rather than a number of moving hosts to dramatically reduce the signaling overhead over the aeronautical data links.

The main drawback of the NEMO protocol is that it does not support Route Optimization (RO), a feature which provides better end-to-end delay and overhead performance in the network. In NEMO, the packets exchanged between end nodes are routed via the HA. Due to this operation, delay requirements of some ATS services (Common Trajectory Coordination – COTRAC as example from COCR[1]) can not be met in the ATN in case the mobile node is far distant from the HA and communicating with a nearby correspondent node.

For example, we can assume an aircraft flying over Europe communicating with a nearby controlling ATSU and using a home agent in far Asia (e.g. in Japan). The following table provides a total delay value for a COTRAC service assuming Broadband-Aeronautical Multi-carrier Communications (B-AMC) link[5] (input technology for L-DACS-1) with High Density service volume. The number of messages exchanged with COTRAC service is taken from COCR[1]. For the wired part delay values, the round trip delay is taken as 300 ms[6]. As shown in the table, COTRAC delay requirement mentioned in COCR[1] can not be satisfied in this scenario. In order to decrease the RTT delay on the ground network, there is a need for a route optimization (RO) feature for the NEMO protocol. In this paper we have focused on one of the RO methods, namely, the Global Home Agent to Home Agent (Global HAHA) protocol.

Table 1. Delay values for COTRAC scenario without RO

Delay Wireless	FL One Way RL One Way	270msec. 550 msec.
Delay Ground Network (Europe-Japan-Europe)	Round Trip Delay	300 msec.

COTRAC Message Exchanges	FL= 3 Messages
	RL= 4 Messages
		3*(270+300) = 1.710 sec.
		4*(550+300) = 3.400 sec.

	Total Delay	5.110 sec.
COCR Requirement	Maximum Delay	5 sec.

Global HAHA

The idea of the Global HAHA[7] is to distribute the HA over distant sites in such a way that the MR can select a closer HA in order to reduce the total end-to-end communication delay. In the Global HAHA network, HAs are using the Inter-HAHA protocol[8] in order to share mobility information of MRs.

Figure 1 shows a sketch of two ATS configurations considering the Global HAHA protocol deployed in the GACSP network. In the first configuration (cf. Figure 1), after the aircraft attaches to the GACSP network, it finds the topologically closest HA and builds a mobility tunnel with the HA. Afterwards the MR starts data transmission with the ground entities (e.g. ATS CN) via the corresponding HA. In the second configuration (cf. Figure 1), the aircraft attaches to an ANSP access network and uses the HAs in the GACSP network and starts communication with the ATS CN.

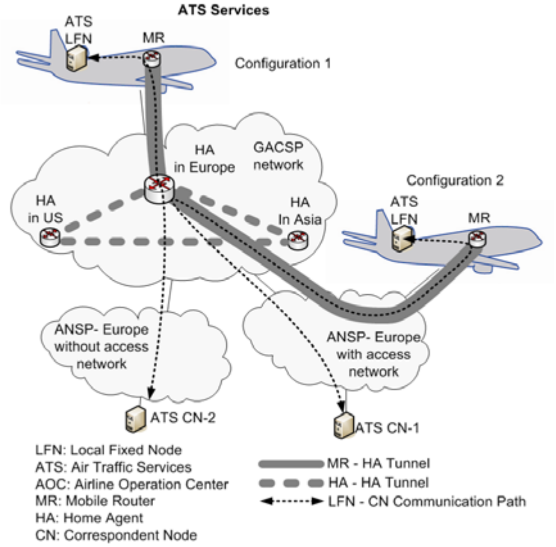

Figure 1: Global HAHA usage for ATS Services

In case of AOC communication, the same configurations hold but the location of the CN is changed from an ANSP network to an airline operations network.

Handover Architecture

The NEWSKY handover architecture is mainly based on the IEEE 802.21 standard[9] whose aim is to provide link layer intelligence and network information to upper layers (layer 3+) in order to facilitate handovers between different access networks, especially between those that are based on different link technologies.

Handover Types

The future ATN will be a heterogeneous network since it is composed of diverse terrestrial and satellite technologies. In such an environment, two main handover types are identified: *intra*-access network (Intra-AN) handovers and *inter*-access network (Inter-AN) handovers. Furthermore, we have to differentiate between *intra*-technology and *inter*-technology handovers.

Intra-AN/intra-technology handover usually have their well proven handover mechanisms. IEEE 802.21 addresses the other scenarios and enables optimized handover decisions and executions by providing abstract link layer intelligence and network information to upper layers.

IEEE802.21 Service Categories

IEEE 802.21 (i.e. Media Independent Handover Functionality) consists of three services as shown in Figure 2.

Media Independent Event Service (MIES)

Events originate from the MIHF or any lower layer from either the local or a remote protocol stack in a node. An event itself can indicate a management action, a command status, a change in the state or transmission behavior of the lower layers. Events are consumed by the MIHF or an upper layer entity either in the node that originated the event or in a remote node, which has subscribed to the respective event type. The events originate from the lower layers and are propagated via the MIHF to the upper layers, which reside either in the local or a remote peer.

Media Independent Command Service (MICS)

Commands allow the upper layers to control the lower layers to perform tasks such as reconfiguration and selection of an appropriate link. Commands originate at the MIH users or the MIHF itself and are destined to the MIHF or any lower layer, where the location can be either the local or a remote protocol stack.

Media Independent Information Service (MIIS)

Discovery of and obtaining information from different networks within a certain geographical area is the functionality provided by the Information Service. The MIIS provides information elements in a certain structure and representation along with a query/response mechanism to exchange information in a media independent way, usually between the mobile node and an information server.

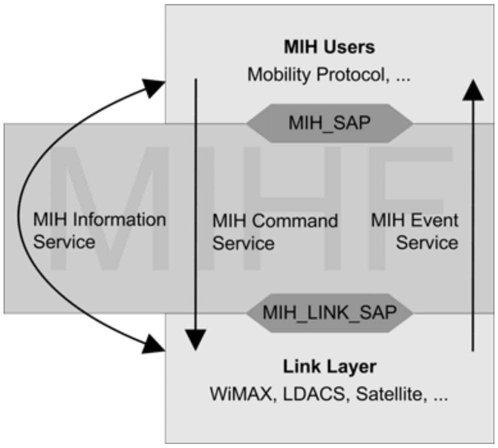

Figure 2: IEEE 802.21 Handover Framework

Handover Decision Making

Handover decision making involves information from both the mobile node and the network infrastructure and should take into account a variety of aspects:

- Handovers between different access networks should not be perceivable by the end user, e.g. by a change in service quality. The QoS of a new access network may not be acceptable and an upper layer entity may decide against performing a handover to this network.
- Application aware handover decisions: Interruptions or idle phases during transmissions could be used to perform a handover at this time so that service interruption is minimized.
- Fulfilling QoS requirements by minimizing packet loss during a handover and proper assessment of the network conditions to optimize the handover decision itself.
- Discovery of potential access networks, including information about link technologies, availability, link quality, etc.
- Network selection based on required QoS, cost, preferences, policies etc.

Security Architecture

Security and regulatory investigations have resulted in a constrained onboard architecture as baseline, where operational and non-operational traffic are physically segregated. Nevertheless, the integration of ATS/AOC services on one side and AAC/APC services on the other side is intended.

An unconstrained, fully integrated architecture has been considered as a long term concept. The different services are separated through security tunnels managed by the airborne router(s).

The aircraft has a routing function that routes the traffic via security tunnels (most likely IPsec tunnels) which are established between security access gateways (SAGs). At the tunnel termination point the traffic is decapsulated and is forwarded to the appropriate system or device.

The SAG performs security tunneling of the traffic based on different policy requirements. Each application (or set of applications) should have its own policy entry when traversing the SAG which takes proper action to secure the data traffic (i.e. protect, bypass, or discard packet).

QoS Architecture

The NEWSKY QoS architecture is compliant with the DiffServ Architecture. The main rationales for using the DiffServ model are the following:

- DiffServ allows a relevant separation among different service and priority categories,
- DiffServ does not depend on any in-band signaling,
- The DiffServ architecture avoids the signaling overhead of resource reservation techniques such as e.g. IntServ,
- The mobility architecture does not have any impact on the QoS provision (in contrast to using resource reservation techniques based on e.g. RSVP)
- It is assumed that the system dimensioning is done in a way to always provide enough resources for the traffic belonging to different QoS classes.

The aircraft ATS/AOC IP router includes a strict priority scheduler to ensure compliance with the hard QoS priority management (between ATS and AOC and among different priority classes within ATS and within AOC). The aircraft APC/AAC IP router includes a COTS scheduler to guarantee a fair sharing of resources among passengers. The scheduling algorithm can depend on the company policy and on the complexity. The ground access routers include a Weighted Fair Queuing (WFQ) scheduler to fairly share the resource among the set of aircraft connected to the access point while respecting service priority.

The identification of traffic classes for ATS/AOC services is based on the DSCP tagging (in the IPv6 header) performed by the application. The identification of traffic classes for AAC/APC services is based on the DSCP tagging (in the IPv6 header) performed by the on-board firewall and by the border routers on the ground.

The overall QoS architecture is presented in Figure 3. It takes into account the constraint from the constrained security architecture to separate the safety and non-safety communications with two different on-board routers. We thus have two separate Diffserv domains (blue and green clouds). The end-to-end QoS (end of Diffserv domain) is ensured between the on-board local fixed node (LFN) (ATS, AOC, AAC and APC) and the edge router (last router before core network) on the other side.

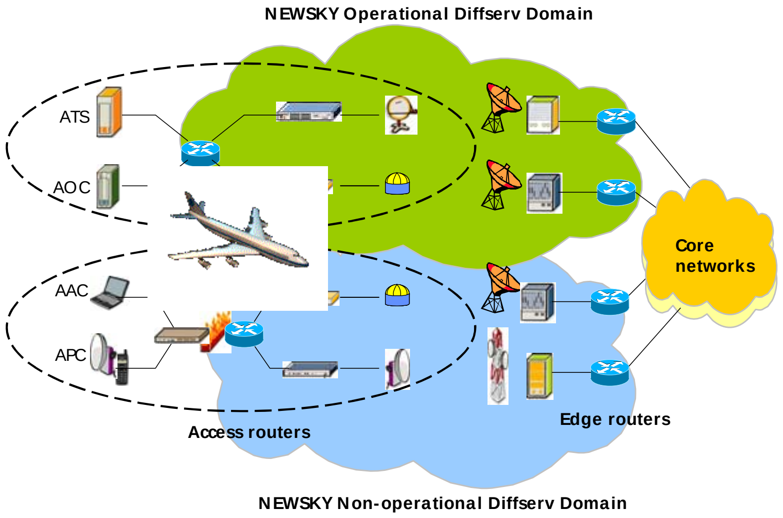
NEWSKY Operational Diffserv Domain
ATS
AOC
AAC
APC
Core networks
Edge routers
Access routers
NEWSKY Non-operational Diffserv Domain

Figure 3: NEWSKY QoS architecture (Diffserv)

Integrated Network Architecture

The security architecture introduces an entity on the ground and one on the on-board network which is called security access gateway (SAG). On the ground network, these entities are located in the sub-networks where correspondent nodes are located. Based on existing network configurations we assume there is a centralized topology in the ANSP and AO networks (all incoming and outgoing streams going through the same entity). Also the SAG should be placed at the borders of these networks.

The mobility architecture introduces a new functional entity in the ground network, namely a home agent (HA) described in the previous section. Home agents are special types of routers and are located in the GACSP networks.

Mobility and Security Integration

Mobility and security tunnels are not directly related to each other. The security tunnel endpoints shall never be too far away from the boundary of the hosts sub-network. That is, the SAG shall always be within the sub-network of the correspondent node. Mobility tunnels can thus not be re-used as security tunnels as the security endpoint for MIPv6 signaling is the HA that is located in the GACSP network.

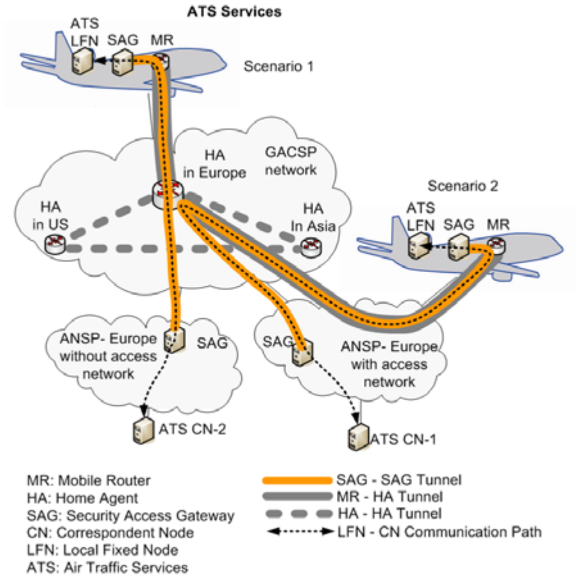

Figure 4: Global HAHA with SAG for ATS

Figure 4 shows the Global HAHA and security architecture integration (SAG and security tunnels) where the packets sent by on-board LFN are first tunneled by SAG (i.e. security tunneling) and then MR performs mobility tunneling to the packets received from SAG. On the ground side, the topologically closest HA receives the packets and decapsulates the packets and forwards them to the SAG. After the SAG receives the packets, it performs decapsulation and forwards the traffic to the CN. On the reverse path (i.e. from CN to on-board LFN) the CN sends the packets directly to the

HA, but since all the packets are forwarded via the SAG, the SAG performs additional security tunneling to those packets and forwards them to the HA. The HA performs mobility tunneling and sends the packets to the MR.

Mobility, Security and QoS Integration

The QoS architecture as presented before defines the two DiffServ domains where QoS is applied (separation of operational and non-operational services). The entities to be considered from the QoS point of view are the on-board LFN (ATS, AOC, AAC or APC) and the border router on the ground (last router before the correspondent node or the core router). Placement of these entities with respect to mobility and security entities and tunnels is investigated hereafter.

For integration of the QoS support, we define the following additional entities:

- Edge router (last router before the CN): the end-to-end QoS is ensured between the last router before the ground ES and the LFN on-board, which both have access to the QoS information. These two points correspond to the boundaries of the DiffServ domain in the QoS architecture.
- Border routers between the different autonomous networks (corresponding to separate DiffServ domains applied to different networks or sub-networks) in order to ensure QoS re-negotiation and continuity.

The end-to-end QoS must be ensured between the LFN and the edge router. The DSCP tag is set and removed by these nodes and determines priority class for which the corresponding Quality of Service should be assured by the network.

We need to ensure that this information on the level of QoS required (determined by the DSCP mark) propagates along the network path. For this, we need to take into account the tunneling performed by security and mobility functions:

- Due to the security tunnel, there is a need for DSCP re-tagging (or DSCP tagging propagation) in on-board and ground SAG in order to ensure SAG to SAG QoS (as the inner header information is not available anymore at SAG level). For re-tagging of the packets in the tunnel, the DSCP field of the original packet is checked to determine the level of required QoS. Afterwards, this information is set in the new (outer) header of the tunnel-packet, where the equivalent DSCP field is set accordingly.
- Due to the mobility tunnel, there is also a need for DSCP re-tagging (or DSCP tagging propagation) between the MR and the HA for the same reason as for the security tunnel. It is done in the same way as for the security tunnel but using this time the DSCP mark set by the SAG. Thanks to this re-tagging of packets in the mobility tunnel, the MR and all potential routers on the path to the HA, have access to the QoS information in order to implement QoS mechanisms (queuing, scheduling, etc.).

Figure 5 shows an example of integration of QoS entities with security and mobility entities. In case of ATS services, with the Global HAHA approach, the two possible configurations for access networks, and the constraining security architecture (tunnels for all ATS and AOC services) are shown in the figure.

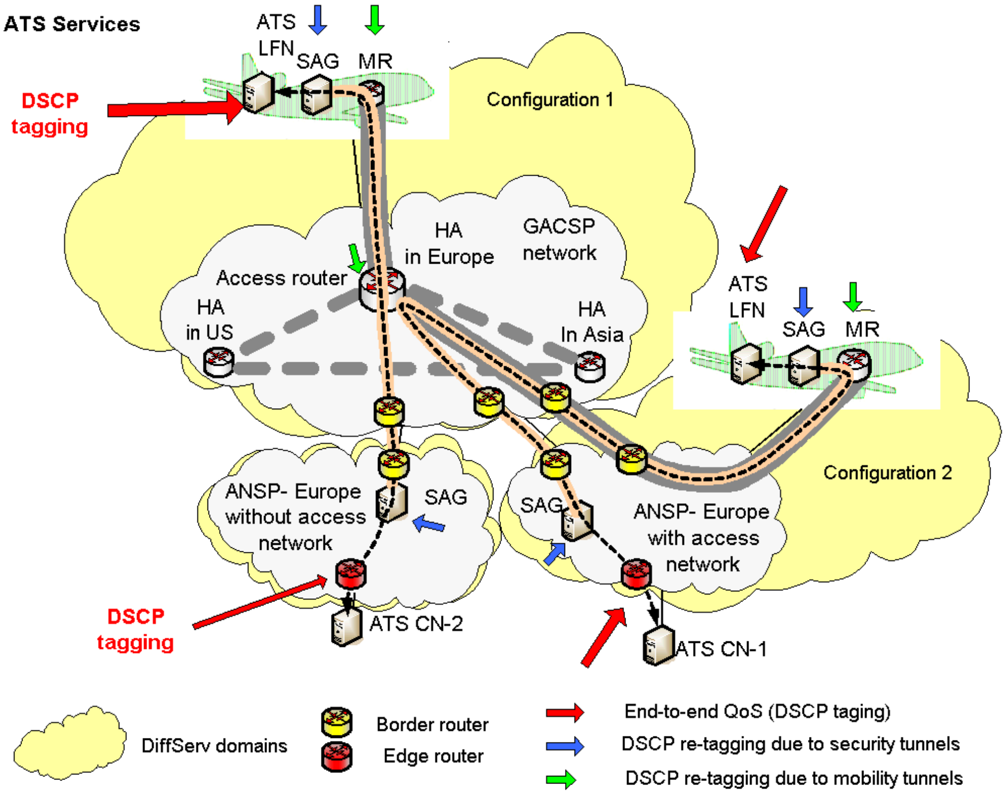

Figure 5: Example of integration of QoS entities with security and mobility

This principle and additional entities would be the same for the different scenarios (i.e. AOC, AAC, APC), the important point is that the end points for QoS are always outside the security and mobility tunnels and that QoS retagging will be necessary at any tunnel entrance where the QoS information contained in the header is not accessible anymore.

Conclusion

Our security investigations have resulted in a constrained architecture as a baseline, where operational and non-operational traffic are physically segregated (i.e. separated mobile routers). Nevertheless, an unconstrained fully integrated architecture can be thought as long term concept, depending on the evolution of the regulations and available security mechanisms. In such a network, the services would be separated through security tunnels managed by a single airborne router.

The NEWSKY mobility solution is based on Mobile IPv6 and its extensions. Network mobility (NEMO) enables the handling of an aircraft as a moving network rather than as a number of moving hosts to dramatically reduce the signaling overhead over the aeronautical data links. The Global HAHA has been selected as one important candidate for NEMO Route Optimization (RO) solution for all services.

The security architecture is based on security tunnels between on-board and ground Security Access Gateways. These tunnels have to be established in addition to the Mobile IPv6 tunnels between the mobile router and the Home Agent on the ground. Home Agents should be placed in the ACSP networks that should provide the mobility service to the aircraft, whereas the Security Access Gateways are more likely placed in the ANSP or AO networks. This means the security tunnel is inside the mobility tunnel.

The QoS solution is based on DiffServ with DSCP tagging in the end nodes or the first router. Again we have to distinguish between the operational services and the non-operational services, for which we cannot access the end system protocol stack. Also, in order to ensure the end-to-end QoS, some retagging is necessary at the entry point of tunnels for the information to be available in all nodes of the networks. There is also a QoS renegotiation required between the border routers of different DiffServ domains in order to handle the packets traverses these domains.

Acknowledgement

This work is co- funded by the European Commission through the NEWSKY project[10] under contract no. 37160.

References

[1] Eurocontrol/FAA, "Communications Operating Concept and Requirements for the Future Radio System", v2.0.

[2] Johnson, D. ,C.Perkins, J. Arkko, "Mobile IPv6", RFC 3775, June 2004.

[3] ICAO, Manual for the ATN using IPS Standards and Protocols, Doc 9896-AN/469, 1st Edition (Unedited).

[4] Deverapalli, V., R. Wakikawa, A. Petrescu, P. Thubert, "Network Mobility (NEMO) Basic Support Protocol", RFC 3963, January 2005.

[5] DLR, "Expected B-AMC System Performance", Report D5, September 2007.

[6] NTT Communications Europe Website, Performance Statistics, http://www.ntt.eu/products_and_services/global_ip_network/sla.aspx.

[7] Thubert, P., R. Wakikawa, V. Devarapalli, "Global HA to HA Protocol", March 2008.

[8] Wakikawa, R., V. Devarapalli, P. Thubert, "Inter Home Agents Protocol", February 2005

[9] IEEE P802.21, "IEEE Standard for Local and Metropolitan Area Networks: Media Independent Handover Services", January 2009

Email Adresses

serkan.ayaz@dlr.de

christian.bauer@dlr.de

christian.kissling@dlr.de

frank.schreckenbach@dlr.de

fabrice.arnal@thalesaleniaspace.com

cedric.baudoin@thalesaleniaspace.com

katia.leconte@thalesaleniaspace.com

mehammer@cosy.sbg.ac.at

tgraeupl@cosy.sbg.ac.at

2009 ICNS Conference
13-15 May 2009

[10] NEWSKY project website: www.newsky-fp6.eu