

NEMO Route Optimization Solution Space Analysis and Evaluation Criteria for Aviation

Serkan Ayaz, Christian Bauer, Wesley M. Eddy, Fabrice Arnal

Abstract—The aviation community is currently designing an IPv6-based aeronautical telecommunication network (ATN/IP), which aims to provide seamless communication services to the cockpit users. One of the challenging tasks in the ATN/IP is the scalable mobility management of aircraft as entire networks in motion. We have investigated possible IPv6-based network mobility (NEMO) route optimization (RO) solutions for safety related and non-safety related services. We have also presented realistic ATN/IP topology and a set of evaluation criteria for a better analysis of the possible solutions. Our investigations showed that MR-based RO solutions are more suited than MNN-based RO solutions to the aeronautical environment for the near future. We have also realized that multiple MR-based RO solutions could also be used together for a better end-to-end route optimization.

I. INTRODUCTION

In aeronautical communications, there are three different communications services that have different regulations and performance requirements. These services are Air Traffic Services (ATS), Airline Operational Services (AOS), and Aeronautical Passenger Communications Services (APC). ATS is classified as safety related services with certain requirements in terms of delay, availability, continuity and integrity [1]. The delay requirement is one of the most important considerations for a NEMO RO solution where some ATS messages require one-way end-to-end latency between 1.65 - 3 seconds [1]. The other two services are classified as non-safety related services with less stringent requirements. ATS and AOS are provided by the Aeronautical Telecommunications Network (ATN) which is an integral part of the air traffic management (ATM) system. The ATN is a global network interconnecting ground systems and flight systems used for air traffic control and airline operations. APC services are expected to be provided by some ISPs independent from the ATN and are beyond the scope of the paper.

The existing ATN technology and architecture is defined

Manuscript received September 01, 2008. This work is partially funded by the European Commission through the NEWSKY project under contract no. 37160.

Serkan Ayaz is with German Aerospace Center, Wessling, 82234 Germany (e-mail: serkan.ayaz@dlr.de).

Christian Bauer is with German Aerospace Center, Wessling, 82234, Germany (e-mail: christian.bauer@dlr.de).

Wesley M. Eddy is with Verizon, as an on-site contractor at NASA's Glenn Research Center (e-mail: weddy@grc.nasa.gov).

Fabrice Arnal, is with Thales Alenia Space 26, avenue Champollion BP 33787 31037 Toulouse Cedex 1, France (e-mail: fabrice.arnal@thalesaleniaspace.com).

by the SARPS [2] documents published by the International Civil Aviation Organization (ICAO) defining the ATN based on ISO protocols, using an adaptation of the inter-domain routing protocol (IDRP) to support mobility of aircraft. This version of the ATN is only partially deployed at the present time. The ICAO is currently producing a new set of SARPS that redefine the ATN as an IPv6-based network (ATN/IP), and stakeholders are beginning deployment of the ground portion. Definition of the mobility support for aircraft within this new ATN architecture is underway in the ICAO.

The rest of the paper is organized as follows; Section 2 provides information about ATN topology including possible ATS/AOS configurations and trust relationship among different components. Section 3 provides a general overview of NEMO RO solutions which will be used for ATN/IP. In Section 4, a set of evaluation criteria is provided in order to analyze possible NEMO RO solutions. Section 5 analyzes different MR-based NEMO RO solutions and Section 6 concludes the paper.

II. ATN TOPOLOGY

This section provides a general description of the ATN and its main components considering the existing structure.

A. ATN Related Definitions

1) *ACSP*: An Air/Ground Communications Service Provider (ACSP) operates an access network that includes air/ground data links. Global ACSPs (GACSP) utilize terrestrial and satellite link technologies to provide ATS/AOS services that have a world-wide network and they are comparable to the tier 1 service providers in the Internet. In the future it is foreseen that there will be local ACSPs (LACSP), in addition to GACSPs. Each GACSP operates VHF Data Link Mode 2 (VDL2) as the state of the art data link technology for terminal maneuvering area and en-route stages of flight. The VDL2 links provide a nominal throughput of 31.5 kbps for all aircraft within a single cell (typically up to 200 nautical mile radius and containing approximately 200 aircraft). The proposed future radio systems [12] will provide a throughput of approximately 300 to 400 kbps for the same radio cell. In addition GACSPs can also operate 802.16e link technology at the airport and satellite systems in oceanic/remote areas.

2) *ANSP*: An Air Navigation Service Provider (ANSP) manages the air traffic within a country or geographic region. Generally each ANSP has its own sub-network. An

ANSP might also be an LACSP within that geographical region by operating its own air/ground access network, which might be due to security or cost motivations. Although ICAO has an influence on ANSPs, these organizations also have their own (network) policies.

3) *AO*: Airline Operation (AO) is used for managing the business operations of the aircraft that belong to a certain airline. Generally each AO has its own sub-network.

B. ATN Network Elements

1) *Mobile Router (MR)*: An MR is a router onboard which is also called 'airborne router' in the aviation environment. It is reasonable to assume that in the future there is one IP-based MR on each aircraft that handles both ATS and AOS traffic, as the access technologies/access networks provide support for both services. Additional MRs may be on board for fault tolerance reasons.

2) *ATS/AOS Correspondent Nodes (CNs)*: ATS CNs are Air Traffic Service Units (ATSUs) that refer to the controllers managing a certain air space, along with some non-controlling CNs that may provide weather or air-traffic flow-control information. These nodes are located within the ANSP networks and generally dynamic; as the aircraft traverses different regions of the world, the responsible ATSU changes. Generally ATS CNs are geographically close to the aircraft, whereas AOS CNs are located in an AO network that might be distant from the aircraft. Within the AO network, AOS CNs could be in airline headquarters/operations center or an airport. These nodes are relatively static throughout a flight [4].

3) *Mobile Network Nodes (MNNs)*: An MNN is a node located within a mobile network, either permanently or temporarily. An MNN might be either a fixed node (LFN) or a mobile node (LMN) [11]. ATS and AOS domains have MNNs that are primarily LFNs, though potentially there could be some LMNs [4]. They are operated by and are under control of the airline, although ICAO regulations and standards affect the ATS systems.

4) *Home Agents (HAs)*: A router on a mobile node's home link with which the mobile node has registered its current Care-of Address (CoA) [5]. We assume HA(s) serve both ATS and AOS domains.

C. Possible ATS and AOS Configurations

In this section, we consider different network attachment possibilities and their affect to the routing paths between MR and CN for ATS and AOS services.

1) *ATS Configurations*: The routing paths in Figure 1 only depict ATS traffic, where the CNs are located inside the ANSP access network. Configuration 1 shows a deployment that already exists today. The ANSP is not operating the access network in its country but contracts an ACSP for providing connectivity to aircraft. The data traffic from the MR to CN uses the ACSP as an access network goes to the boundary router located at the ANSP where the packets are forwarded to the CN that resides inside this network.

Configuration 2 is another existing deployment where the ANSP is operating its own access network to which the aircraft can attach to. In this case the ANSP is also called an LACSP. Configuration 3 shows another potential deployment where the ACSP the aircraft is attached to is not directly connected to the ANSP. Routing between the MR and the CN is achieved by means of a transit provider such as GACSP-2.

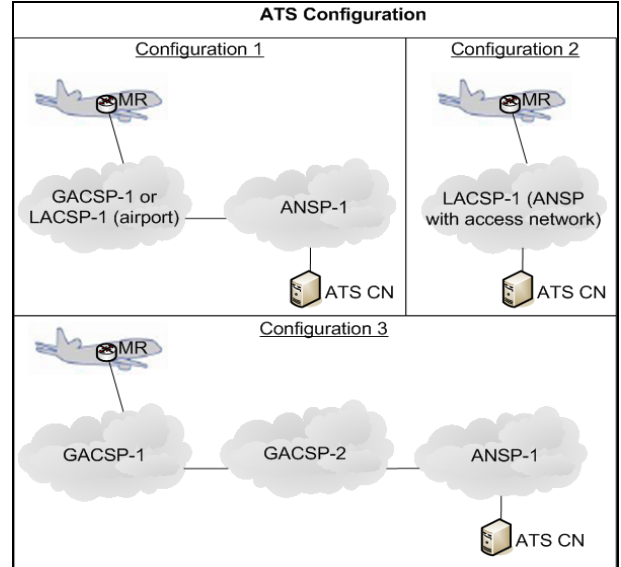


Fig. 1. Different ATS Configurations

2) *AOS Configurations*: The routing paths in Figure 2 depict AOS traffic only, where the CN is located at the airline network. In AOS configuration, the communication model is fundamentally different from ATS, such that the CNs are relatively static and may be geographically distant to the MR.

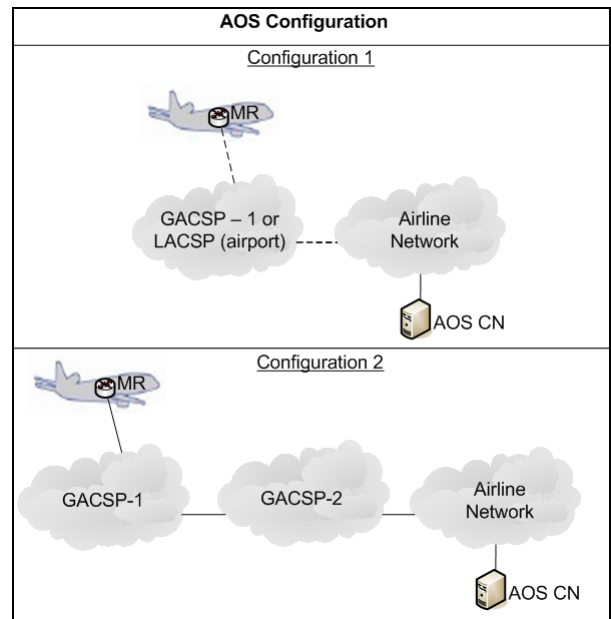


Fig. 2. Different AOS Configurations

D. Location of Home Agents

The topological location of the HAs determines the advertisement of the Mobile Network Prefixes (MNPs) that belong to aircraft. In the ATN, there are two possible options:

- 1) An airline has a HA which is serving the aircraft belonging to that airline.
- 2) One of the GACSPs provides HA(s) for the airline if they have an agreement

The second choice is more reasonable for two reasons. First, for airlines having a relatively small number of aircraft it will not be cost effective to deploy HA(s), in comparison to the GACSP that can act as a Mobility Service Provider for multiple airlines. Second if the HA(s) are deployed at the GACSP the aircraft will be at home as long as it is directly attached to that GACSP and hence there will be no tunneling overhead, assuming a local mobility management protocol like [6] is deployed. Based on this assumption, the MNP will be assigned to the aircraft by the contracted GACSP's address space. In this paper, we assume that a GACSP manages the HA(s) and controls the assignment of MNPs under contract with the airlines and/or ANSPs.

E. Trust Relationship among Network Elements

ANSPs and AOs have contracts with at least one GACSP (and often multiple GACSPs). Certificates can be assumed as possible to establish between an aircraft (belong to a certain airline) and GACSP (acting as a mobility service provider) bootstrapped by their pre-existing business relationships. The relationship between the aircraft and an ANSP (including ATS CNs within this network) is different, as these parties do not have contracts with each other. Although there is some form of trust (the aircraft trusts the instructions coming from an ATSU), it is difficult to extend it on having certificates between these entities for the near future.

Since it is difficult to estimate the time for the deployment of a world-wide Public Key Infrastructure (PKI) for aviation, assuming certificates between aircraft and all potential ATS CNs are not realistic for the near future. However, in the long-term, it is feasible to expect certificates to be available between aircraft and ATS CNs. It should be noted that ANSPs often have their own local network policies which might impose additional restrictions such as not accepting certificates rooted elsewhere. It is therefore important to consider such cases where even world-wide PKI is available.

The situation between an aircraft and its AOS CNs is different, as both are operated by the same entity. Certificates between these nodes could be expected, and are partially already available today (e.g. X.509 certificates in Secure ACARS).

III. GENERAL NEMO RO ANALYSIS

The base protocol of NEMO [10] provides a network

mobility solution without any RO capability. However, there is a strong demand for NEMO RO in aeronautical communications since without RO, the aircraft tunnels all traffic to the HA. The HA could be geographically distant from the aircraft due world-wide mobility of the aircraft and this tunneling causes increased delay and overhead in the network as it potentially crosses multiple continents. This section provides general non-nested NEMO RO analysis considering a correspondent entity (CE) that might be in either the ATS or AOS domain. The CE is an abstraction representing either a CN or a Correspondent Router (CR). Based on the discussion of trust above, in the near-term, it is expected that the CE will often be either a CR at the edge of an ACSP network. In the long-term, when a more widespread commonly-anchored PKI is possible for aeronautics, the CEs might usually be the end CNs themselves for both ATS and AOS flows. The distinction is not important for the analysis in this paper. The RO functions themselves can be performed either by the MR or by the MNNs themselves as described in [7]. The following subsections provide a general overview of RO possibilities.

Our analysis specifically considers the questions identified in RFC 4889 [7], but within the aeronautical context instead of the general setting of RFC 4889.

In order to compare the architectural differences between these two general RO approaches, we utilize standard DoDAF operational views in Operational Node Connectivity Description (OV-2), and Operational Activity Model (OV-5) diagrams [8]. The OV-2 diagrams show the "needlines" between operational nodes within the architecture. A needline is a requirement for transfer of information or services between nodes. We use the OV-2 diagrams primarily to compare the different requirements placed on the MNN and PKI between the two RO solution approaches. The OV-5 diagrams we use in this paper follow the "swimlanes" format where a column for each operational node contains the activities performed by the node and lines between the activities show the flow of information. We use these diagrams to further compare the scalability impact of the two different approaches to RO. Some of the information flows shown are one-time only to configure the MR at the time of its installation in an aircraft, and other flows shown are per-application session with a CN.

A. Route Optimization from MR to CE

Figure 3 illustrates the needed flows of information between nodes in order to perform RO from MR to CE, and Figure 4 expands on this by showing the allocation of functional activities between the acting nodes and the flow of information between those activities. Aside from the performance difference after cutover of data traffic onto an optimized path, RO occurs completely transparent to the MNN. This is an important property of the class of solutions where the MR performs the RO functions, as it allows the MNNs to remain simple IPv6 nodes without

requiring them to support MIPv6 or any extensions. This is evident in that the MNN does not appear on either diagram.

In Figure 3, the grey boxes and clouds are operational nodes, and the white rounded boxes label the information needed to move between them. These information flows can be found on Figure 4. A certificate from the PKI grants the MR ownership of an MNP from which the HoAs for onboard nodes are drawn.

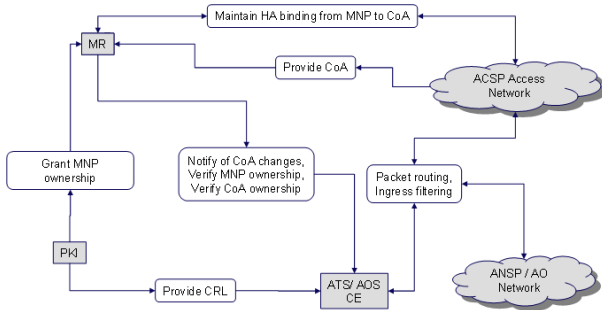


Fig. 3. Needline Diagram for MR to CE RO

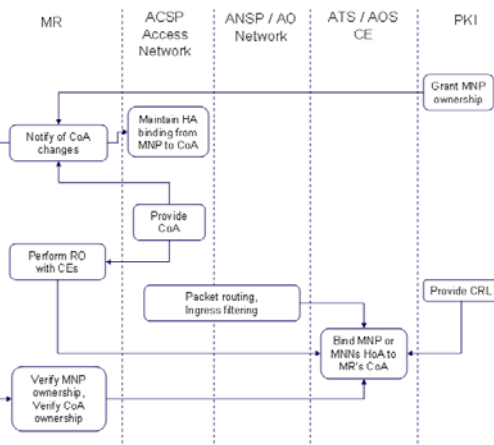


Fig. 4. Operational Activity Model for MR to CE RO

The PKI also publishes a certificate revocation list (CRL) needed to withdraw credentials previously granted to an MR. Interaction between the ACSP running the HA and the PKI in order to manage MNP assignment and ownership is not captured in this paper.

CoAs are provided to the MR by global or local ACSP access networks that it visits. The MR can then maintain the binding between the MNP and its current set of CoAs with an HA located in the GACSP's network. When the CoAs change, RO with an ATS or AOS CE depends on the MR signaling its CoA change somehow to the CE, along with some method of the MR verifying its ownership of both the MNP and the new CoA, analogous to the return routability test procedure in standard MIPv6, except for an entire MNP rather than a single HoA.

Figure 3 illustrates that the knowledge of packet filtering being performed by the ACSP and ANSP/AO can assist in this verification process. For instance, ubiquitous filtering can allow greater confidence that the source address of

received packets is unspoofed. Due to the more controlled and closed nature of the ATN in comparison to the public Internet, this may allow for some streamlining of the RO process away from the RTTs implied by typical MIPv6 RO.

It is evident that the more complex tasks are constrained to the MR and ACSP. The CE does not initiate activities, but relies on inputs from all of the other architecture in validating binding updates. The PKI is simply a producer of material used by others.

B. Route Optimization from MR to HA

Rather than removing the HA from the path between an MR and CN, some solutions introduce additional HAs topologically distributed throughout the network in order to allow selection of the HA that produces an optimal paths for a particular point in time. Under this class of RO techniques, each MR has a "primary" HA that synchronizes its binding cache entry for the MR's MNP with a group of other HAs. When the MR is at a place in the topology where it is advantageous to use another HA, some classes of solutions allow it to change the designation of its primary HA (e.g. global HAHA), and others allow it to utilize a "proxy" HA (e.g. Hierarchical Mobile IPv6) that is nearer to it [16].

The needlines and activities shown in Figures 3 and 4 for MR to CE RO all exist when using MR to HA RO techniques as well, but added complexity comes in two types of additional activities:

- 1) Inside the ACSP Access Network node, additional signaling is needed between the set of HAs.
- 2) Inside the MR node, additional procedures are needed to find topologically-close HAs that are usable.

The details of the first activity depend heavily on the specific RO technology, but operationally there is little difference between techniques. The second activity can be handled in several ways. One solution that has been used is to configure the MR with a list of HAs ahead of time and assign them priorities [15]. Other possibilities include use of Dynamic Home Agent Address Discovery (DHAAD). Some MR to HA RO techniques involve managing an increased number of addresses by the MR [16].

Operationally, the main difference between MR to CE and MR to HA techniques is primarily the possibility that the CE can be simplified to a CN (without the functions of a CR required).

C. Route Optimization from MNN to CE

The alternative to relying on the MR to initiate RO with CEs is that the MNNs might do this themselves with some assistance from the MR. Some desirable properties of this are that the MNNs may have deeper knowledge of their application flow needs for RO and be able to determine better for what flows RO should or should not be performed. Only MNNs that require RO would have to implement extensions, so certain avionics equipment that only sends non-latency-sensitive messaging flows would not need any

complications beyond normal IPv6 support. Involving MNNs in the RO process also allows for better support of nesting, however, nesting has not been considered a requirement for ATS/AOS NEMO [4]. A concept considered for future architecture has involved nesting in order to provide reachback to infrastructure for planes in oceanic flight through other planes in nearby flight paths. If supporting this concept becomes a requirement in the distant future, this could be a selling point for MNN-based RO rather than MR-based.

However, the introduction of the MNN into the operational model has significant implications. Each MNN requires extensions in order to be able to receive and react to mobility notifications from the MR, notify CEs, and assist in the verification of the CoA.

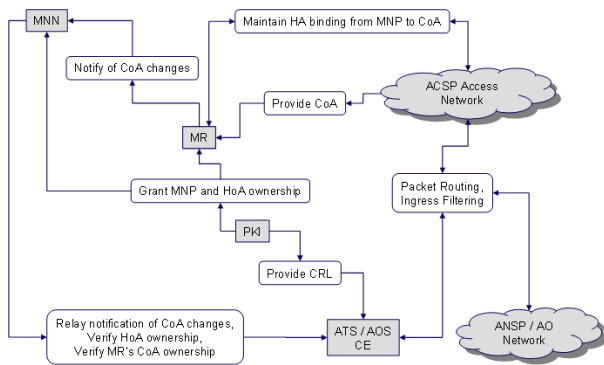


Fig. 5. Needline Diagram for MNN to CE RO

Many of the needlines identified in Figure 5 are similar to those in Figure 3. The notable differences are the addition of a needline between the MNN and PKI for granting ownership of an HoA. This seems to be needed to prevent some piece of “rogue” onboard equipment from claiming the HoA of another piece of avionics and either capturing, falsifying, or otherwise disrupting its traffic.

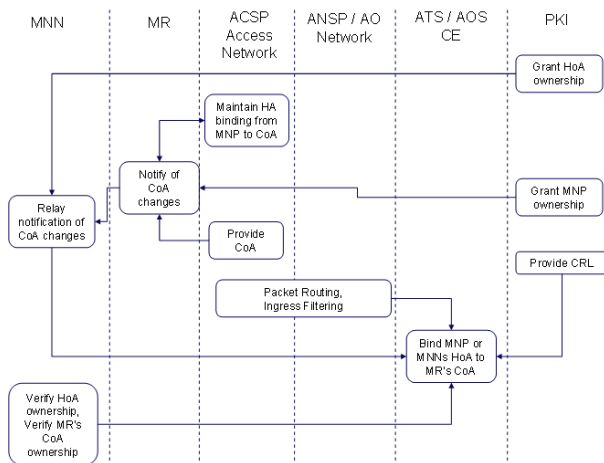


Fig. 6. Operational Activity Model for MNN to CE RO

The needline for notifying the CE of CoA changes moves from going from being based at the MR in Figure 3 to being based at the MNN in Figure 4. This is triggered by the

MNN’s receipt of notifications from the MR when CoAs change. The MR’s assistance in this is required because the MNNs themselves are only connected to the onboard avionics busses/networks, and not to the dynamic air-ground links that the MR manages access to. Also notable is the expectation that the MNN assist in verifying the MR’s CoA ownership to the CE. This is accomplished in different ways, depending on the particular RO technology, though the variation is not significant to the level of architectural analysis pursued in this paper.

In Figure 6, the activity model now shows a swimlane for the MNN, and the allocation of functions to the MR is reduced due to the MNN taking over responsibility for performing RO with the CE. The activities of the ACSP Access Network, ANSP/AO Network, and ATS/AOS CE are unchanged by this re-allocation of responsibility. However, the PKI is affected in that now in addition to granting MNP ownership to MRs, it is also required to grant HoA ownership to individual MNNs within the MNP. Perhaps this can be delegated away from the root to some level, but it cannot go as far as the MR owning the MNP itself, because this device is in the air and cannot be expected to be query-able, provide CRLs, or otherwise actively manage credentials used by other nodes.

Additionally, the use of the PKI on a per-MNN/HoA basis rather than strictly aggregated at the MNP level leads to PKI maintenance and operations scaling less well with growth in the number of planes and onboard avionics devices. The MR-based RO alternative only has a scaling dependence on the number of MRs, and not the size of the onboard networks behind them.

Perhaps the largest concern with Figure 6 is due to signaling traffic. This is similar to the PKI scaling dependence on the number of MNNs, in that the swimlane for the MNN must be replicated for every piece of RO-capable avionics in the onboard network. Each MNN performing its own RO can lead to greater utilization of the air-ground links following CoA changes. Since these links are already tight, this is highly undesirable. A clever RO solution might utilize the fact that ATS CNs are often “topologically close” and flows to them might share a CE’s binding if made on the MNP-granularity rather than the per-HoA basis. This could involve some mechanism in the onboard network to filter out multiple temporally-close RO signaling attempts to the same CE. However, this does not seem to be part of any proposed RO solution, to-date.

IV. EVALUATION CRITERIA

In order to assess the performance of each NEMO RO solution, there is a need for evaluation criteria. The purpose of this section is to identify simple and low-level criteria that could help designers of the ATN/IP network to select among the different solutions what could be the one(s) that really fit their needs. The ratings are Good/Neutral/Bad for all criteria.

A. Routing Related Performance

The direct path created by end-to-end RO from the MR to the CN is obviously most preferred, but this could be relaxed by considering the CR which is a router enhanced with Mobile IP/NEMO features topologically-close to the CN, or close to the transit exchange point of the CN networks, for example within the ATN backbone. Any path that involves unnecessary traversal of multiple continents is undesirable.

B. RO Signaling Overhead and Handover Delay

In most solutions, the RO signaling consists of data sent along or just after the Binding Update / Binding Acknowledgments exchanges during a handover, but the most important amount of overhead usually comes from in-band signaling transported for every data packets sent from and to the MR, such as routing headers and security mechanisms. It is also important to keep in mind the low speed wireless links in the ATN context in this criterion.

Furthermore, handover delays at the user level may be considered as a special QoS metric particularly when thinking about critical ATS services. Though the delay should mostly comes from the performance and the coordination of lower layers to open, transfer, and close communications, the NEMO RO solution will probably add additional penalty to L2 handover that should be minimized.

C. Scalability

As mentioned in section 3, in case the NEMO RO is managed by MR instead of MNNs will provide better scalability performance which should be considered during the design of NEMO RO. Scalability also deals with the prevention of network congestion that could occur near important convergence point (e.g. HAs).

D. Deployment

Certification is known to be long and complex process in the field of aeronautical domain. It can be expected that maintaining and managing a small number of different entities within the whole network is preferable.

E. Security

The selected NEMO RO solution should provide authentication, and integrity features. For example vulnerability of any part of transmission path between MR and CN should be considered.

F. Fault Recovery

Any NEMO RO solution should be robust against system failures in case any network entity fails. From NEMO perspective, HA and MR should not be single point of failure. However, in case there is a single MR on board, the system should recover as soon as possible.

V. ANALYSES OF POSSIBLE SOLUTIONS

As mentioned in Section 3, the NEMO RO can be either

performed by MR or MNN. In this section, we will consider different MR-based RO options since they are more scalable compared to MNN based solutions and do not require modifications to the end nodes. The proposed solutions are evaluated considering the evaluation criteria in section 4 as shown in Table I.

A. MIRON Approach

Mobile IPv6 Route Optimization for NEMO (MIRON) protocol provides NEMO RO solution between MN and CN which is explained in [13]. MR performs all mobility signaling (i.e. Return Routability procedure and CN binding registration) on behalf of the MNs, so that there is not any modification needed for the end hosts (i.e. LFNs). However the RR signaling should be repeated every 7 minutes like MIPv6 base protocol. Moreover, the protocol limits the usage of IPsec such that only ESP option can be used. In case IPsec AH option the RO path can not be used since MIRON changes the source address for outbound traffic, and destination address for inbound traffic address which is affecting the AH integrity check. Considering fault recovery aspects after MR reboots, it should establish flows for every MNN which might take some time.

B. Global HAHA Approach

Global HAHA protocol [3] is an infrastructure based solution to Network Mobility (NEMO) route optimization (RO) problem. The main idea behind Global HAHA is to distribute multiple HAs in different parts of the network and let them exchange the binding information of MRs with each other. MRs select the topologically closest HA by using dynamic home agent address discovery (DHAAD) mechanism. Since packets exchanged between MR and CN via HA, the protocol does not provide complete optimization. The level of optimization depends on the topological closeness of HA to MR and CN. Considering the global coverage of GACSPs in the ATN/IP, it is reasonable to consider Global HAHA protocol running within GACSPs network. Considering security aspects, the protocol does not introduce any new security issue in addition to the basic NEMO support [10]. Considering fault recovery aspects, after MR reboots, it only sends a binding with the HA.

C. Optimized Route Cache Approach

Optimized Route Cache protocol is another infrastructure based solution which defines a new anchor router called "Correspondent Router" in the ground network and MR performs route optimization with CR [14]. Like Global HAHA, the level of route optimization depends on topological closeness of CR to MR and CN. The protocol has CR discovery and CR registration procedures which are similar to Global HAHA protocol. Considering security aspect, the protocol uses Mobile IPv6 security mechanisms like return routability procedure. One precondition for the CR discovery, it should be on the path between MR and CN. Considering fault recovery aspects, the CR approach is

TABLE I
ANALYSES OF MR-BASED NEMO RO SOLUTIONS

Evaluation Criteria	MIRON	Global HAHA	Correspondent Router
Routing Related Perform	Good: Direct communication path.	Neutral: Communication path between MR and CN is via closest HA.	Neutral: Communication path between MR and CN is via CR.
RO Signaling Overhead and Handover Delay	Bad: HA Registration, RR procedure (every 7 min.)	Good: Only HA Registration	Bad: CR Registration, RR procedure (every 7 min.)
Scalability	Good: MR-based RO	Good: MR-based RO. Distributed HAs in the network	Good: MR-based RO. Distributed CRs in the network
Deployment	Neutral: MR and CN needs modification	Neutral: MR and HA needs modification	Neutral: MR needs modification. CR new entity
Security	Neutral: IPsec AH problem. Vulnerability to on-path attackers due to RR procedure	Good: IPsec supported with full functionality. IKEv2 based authentication	Neutral: CR is not known to MR in advance. Vulnerability to on-path attackers due to RR procedure
Fault Recovery	Neutral: In case MR reboot MR should establish flows for each MNN	Good: In case MR reboot, it should send only binding registration to HA	Neutral: In case MR reboots, it has to wait a new packet from CN to trigger CR discovery.

comparable with the Global HAHA. However, in case MR fails, it has to wait a new packet from CN to trigger CR discovery.

VI. CONCLUSION

IPv6-based ATN is currently under development by the ICAO where MIPv6 is a strong candidate as a global mobility management protocol [9]. However, MIPv6 only provides host mobility which is not enough considering large number of hosts within an aircraft. In this case, there is a need for network mobility which provides mobility functionality for all hosts for different types of services.

With this study, we realized that the ATN topology leads to a situation where local mobility [6] and infrastructure-based techniques [3] are possible candidates to investigate more in detail. We also mentioned that the security scheme

can not assume full trust relationships between the MR and ATS CNs for the near future. In section 3, we provided an explanation of two possible RO approaches that are triggered either by MR or MNN. Although both approaches have Pros and Cons, MR-based RO is more desirable than MNN-based RO since PKI requires less work and end nodes do not require any modifications. Finally, we investigated three MR-based NEMO RO solutions and realized that Global HAHA approach is well suited for aeronautical environment considering GACSPs. In addition, we believe CR approach is a kind of add on solution to Global HAHA (ANSP and AOs may or may not implement it) which might be used in case HA failures and to provide a better route from MR to CN. MIRON solution look promising for the far future since it requires modifications to the CNs. In addition, usage of Cryptographically Generated Addresses (CGAs) [17] for a more secure solution instead of RR procedure could be a better solution for MIRON and CR approaches. As a next step, we will perform simulations in order to assess the performance of each solution.

REFERENCES

- [1] Communications Operating Concept and Requirements for the Future Radio System v 2.0, Eurocontrol/FAA.
- [2] Manual of Technical Provisions for the Aeronautical Telecommunication Network (ATN) – ICAO Doc. 9705.
- [3] P. Thubert, R. Wakikawa, V. Devarapalli, “Global HA to HA protocol”, IETF Draft, draft-thubert-mext-global-haha-00, March 18, 2008
- [4] W. Eddy, W. Ivancic, and T. Davis, “NEMO Route Optimization Requirements for Operational Use in Aeronautics and Space Exploration Mobile Networks”, IETF Internet-Draft (draft-ietf-mext-aero-reqs-02), May 13, 2008.
- [5] D. Johnson, C. Perkins, and J. Arkko, “Mobility Support in IPv6”, RFC 3775, June 2004.
- [6] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, and B. Patil, “Proxy Mobile IPv6”, RFC 5213, August 2008.
- [7] C. Ng, F. Zhao, M. Watari, and P. Thubert, “Network Mobility Route Optimization Solution Space Analysis”, RFC4889, July 2007.
- [8] US Department of Defense, “DoD Architecture Framework Version 1.5, Volume I: Definitions and Guidelines”, April 23, 2007.
- [9] ACP-WG I-06/WP-08, “Updated Mobility Management Requirements for the Manual for the ATN using IPS Standards and Protocols”, Vic Patel and Tom McParland, 17-20 March 2008.
- [10] V. Devarapalli, R. Wakikawa, A. Petrescu, P. Thubert, “Network Mobility (NEMO) Basic Support Protocol”, RFC 3963, January 2005
- [11] T. Ernst, H-Y. Lach, “Network Mobility Support Terminology”, RFC 4885, July 2007
- [12] N. Fistas, B. Philips, “Future Communication Study – Action Plan 17, Final Conclusions and Recommendations”, Proc. DASC’07, 2007
- [13] C. Bernardos, M. Bagnulo, M. Calderon, “Mobile IPv6 Route Optimization for Network Mobility (MIRON)”, draft-bernardos-nemo-miron-01, July 9, 2007
- [14] R. Wakikawa, M. Watari, Optimized Route Cache Protocol (ORC), draft-wakikawa-nemo-orc-01, 24 Oct 2004
- [15] W. Ivancic, D. Stewart, T. Bell, P. Paulsen, and D. Shell, “Use of Mobile-IP Priority Home Agents for Aeronautics, Space Operations, and Military Applications”, Proceedings of the IEEE Aerospace Conference 2004, March 2004.
- [16] H. Soliman, C. Castelluccia, K. El Malki, L. Bellier, “Hierarchical Mobile IPv6 Mobility Management (HMIPv6)”, RFC 4140, August 2005.
- [17] J. Arkko, C. Vogt, W. Haddad, “Enhanced Route Optimization for Mobile IPv6”, RFC 4866, May 2007.