A Proposed Mobile IP/NEMO Route Optimisation Scheme compatible with the Requirements for Aeronautical Use

Author: Tony Whyman
McCallum Whyman Associates Ltd

Email: tony.whyman@mccallumwhyman.com

Abstract

This paper has been produced in order to propose an outline solution to the requirements for Aeronautical Route Optimisation (RO) given in [1]. Possible architectures for an IP version of the Aeronautical Telecommunications Network (ATN-IP) have already been investigated by a Eurocontrol study, the results of which were published in [2] and presented to ICAO in early 2007. This study concluded that an approach based on the use of IPsec tunnels was the best available "industry standard" approach to meeting the mobility, security and performance requirements for the ATN-IP. This paper aims to develop on from the solution presented in [2] and to propose an approach that is fully integrated with Mobile IP, IPsec and NEMO, and developed as an RO strategy. Two appendices are provided: Appendix A demonstrates the use of the RO strategy by working through the known ATC and AOC Operational Scenarios; Appendix B reviews how the proposed RO approach meets the requirements given in [1].

Although the focus of the paper is on Route Optimisation for Aeronautical use, the wider implications are considered with the RO strategy for Aeronautical Communications being positioned as part of a family of IPsec based Mobility and RO strategies leveraging off the functionality of IKEv2 [8] and MOBIKE [9], and building on the ideas expressed in draft-ietf-mip6-cn-ipsec [13].

It should be emphasised that while this paper draws on the published Eurocontrol study, Eurocontrol endorsement of this paper has neither been sought nor received. Its status is that of a personal contribution.

1 Background

The ICAO ATN [3] was first standardised in the early 1990s using OSI protocols (ATN-OSI). It is now in operational use in the European Region and its use is rapidly increasing with over 200 commercial aircraft already equipped (mostly A320s, MD80s, B737s and B767s) as part of a continuing implementation programme, and making regular use of the service as part of normal flight operations [22]. The use of the ATN-OSI is now the subject of an Implementing Rule by the European Commission. As a result it is expected that all new aircraft in the B737/A320 class will be delivered with ATN-OSI as standard and the retrofit of the European Fleet will be complete by 2014. The system is also being progressively rolled out across European Air Traffic Control Centres.

Considerable experience has now been built up as regards implementation issues, the Safety, Security and Performance Requirements. Some of these requirements, but not necessarily all, are captured in [1]. In particular, Eurocae ED-120 [4] should be consulted for the Safety and Performance Requirements for ATC Data Link Services. The operational use of data link for ATC is also described in [2]. The application message set is described in [7].

This experience can be now be used to develop a next generation ATN based on IP protocols (ATN-IP) for deployment in the 2020+ timeframe, and for the support of new services and concepts. In this timeframe, ATC data link communications is expected to become the primary means of communication between controllers and pilots, and the specific impact of this will be on the availability target. At present [6], this is set at 99.99% for the Air/Ground Communications Service Provider (ACSP), and it should be assumed that this will increase by one or two orders of magnitude by the time the ATN-IP is deployed.

The very high availability requirement is a particular issue. There is a strong aversion in the aeronautical industry to single points of failure; Home Agent based approaches can be acceptable, but not if they give rise to single point of failure issues. In particular, the establishment and maintenance of communication

between an aircraft and a controlling Air Traffic Service Unit (ATSU) should avoid dependencies on the availability and correct operation of a Home Agent, or a function in a similar role. Route Optimisation is a way to achieve this goal.

There are also regulatory and institutional issues concerned with any special points in a network. A controlling ATSU and the air/ground network it uses to communicate with an aircraft can reasonably be in the domain of the same regulator, especially when terrestrial wireless networks are used. However, a Home Agent, for example, could be anywhere in the world, and under the control of a completely different regulator. Establishing a common standard for the operational approval of Home Agents, that is accepted and trusted by everyone, is a non-trivial technical and political problem. If possible, it is best avoided.

In the context of the availability target, security should be seen as equally important as, for example, successful Denial of Service attacks could have a severe impact on meeting the availability requirements. This is in addition to known application level vulnerabilities to masquerade, replay and modification.

When the ATN-OSI was developed, there was a strong underlying intent to follow industry standards. This was not achieved when the wider industry failed to follow predictions and adopt the ISO OSI protocols. The specification of the ATN-IP offers a chance to reset to industry standards, but it is equally important that those standards match the requirements of the aeronautical industry.

2 Current proposals for use of IPsec in RO

draft-ietf-mip6-cn-ipsec [13] has already proposed the use of IPsec for authorising a Mobile Node's use of its Home Address to a Correspondent Node, and correctly positions the RFC 3775 Return Routability Procedure [11] as a weak authorisation mechanism to be used only when stronger authorisation mechanisms are not available and when the known vulnerabilities of the Return Routability Procedure are acceptable.

However, it is not believed that [13] goes far enough in proposing an efficient scheme for aeronautical use. In particular, the proposal:

1. Is organised around the use of the Home Address as the mobile end point of the IKE SA, thus requiring an undesirable Home Agent dependency.

2. Proposes the use of transport mode SAs to protect the transfer of Binding Updates. This does not permit efficient change in the care-of-address with IKEv2/MOBIKE when using the care-of-address as the mobile end-point of the IKE SA.

3. Does not offer an integrated approach to creating the different types of communications path required: e.g.

    a. unprotected path with use of Home Address Option/Type 2 Routing Header

    b. protected (integrity and/or encryption) with Home Address Option/Type 2 Routing Header,

    c. unprotected IP-in-IP tunnels,

    d. ESP/AH protected tunnels.

The case that is potentially most interesting to Aeronautical Communications i.e. when the Home Address is not globally routable (avoiding a Home Agent dependency) and the care-of-address is thus the primary means of communications, is simply noted in a short appendix, without proposing a solution.

2.1.1 Comparison with the RFC 3775 Return Routability Procedure

There is a subtle difference between the proposed IPsec based approach in draft-ietf-mip6-cn-ipsec and use of the RFC 3775 Return Routability Procedure. In the latter case, the Correspondent Node (CN) does gain a reasonable degree of confidence that the Mobile Node (MN) is reachable via both the Home Address and

the care-of-address, and that packets can be exchanged via both addresses. However, in draft-ietf-mip6-cn-ipsec, this does not appear to be necessarily true.

In draft-ietf-mip6-cn-ipsec, the Home Address is used as the MN's IP Address for the IKE. All IKE and Child SA packets will thus be routed via the Home Agent until after the first successful Binding Update exchange. Only after that will packets be sent direct. There will thus be no direct exchange between MN and CN via the care-of-address until after the Binding Updates have been exchanged. While it is not clear whether this could result in any form of attack, there is certainly scope for error and some sort of return routability check would be desirable as part of the Route Optimisation procedure.

An alternative way to use IPsec that appears to give a Return Routability Check would be to base the use of IPsec on IKEv2 [8] and the MOBIKE [9] extensions. The proposed information exchange is illustrated below and starts with the MN using its Home Address as its IP source address for IKE exchanges (i.e. as its SA end-point address), and hence all exchanges with the CN are routed via the Home Agent.

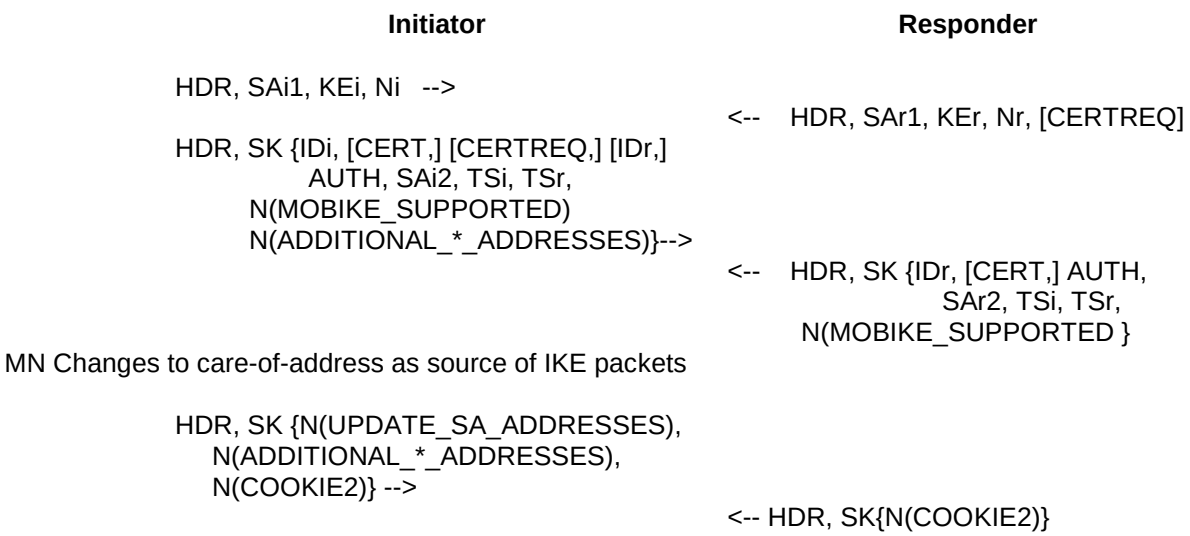

Figure 1 IPsec Initial Exchange for Route Optimisation

The exchange starts with a typical IKEv2 four message exchange (no use of NAT is assumed for simplicity). The first exchange is used to derive the keying material, and the second exchange authenticates both parties. The MN and CN may request and/or exchange certificates and the exchange includes the creation of a Child SA. However, this Child SA cannot be in transport mode if MOBIKE is to be used. Instead, in this proposal, the SA is a tunnel mode SA with a traffic selector that selects all mobility packets (protocol ID 135) exchanged between the MN's Home Address and the CN's IP Address. This traffic selector is given explicitly by the TSi and TSr payloads.

Use of MOBIKE is negotiated by the exchange of MOBIKE_SUPPORTED payloads, and the care-of-address is reported in the N(ADDITIONAL_*_ADDRESSES) payload.

Once the IKE SA and the Child SA have been established, the MN now switches to its care-of-address and sends an IKE Informational message to the CN. This contains an UPDATE_SA_ADDRESSES notify payload, which is effectively a "follow me" indication, and tells the CN that the MN has moved from using its Home Address as its SA end-point address, to using its care-of-address as its SA end-point address. This should also report the Home Address in an N(ADDITIONAL_*_ADDRESSES) payload to indicate that this is still usable in the event of an error affecting the care-of-address. The CN should then respond by returning an Informational message to the MN via its care-of-address, containing the Cookie sent to it by the MN.

The UPDATE_SA_ADDRESSES exchange is authenticated using the IKE SA key agreed when the IKE SA was established, and is sent from an additional IP Address reported in the IKE_AUTH exchange. The CN thus trusts the "follow me" request. Return Routeability is also demonstrated, and the Child SA is implicitly moved to the MN's care-of-address. However, its traffic selector is unchanged and still selects all mobility packets (protocol ID 135) exchanged between the MN's Home Address and the CN's IP Address.

If no response is received to the Information message then the care-of-address should be regarded as unusable and the route optimisation abandoned.

The CN should reject a "follow me" from any IP Address other than one reported in an ADDITIONAL_*_ADDRESSES payload. This is to prevent Denial of Service attacks from an attacker that is able to intercept the Informational message containing an UPDATE_SA_ADDRESSES payload and change its source IP Address to an unusable IP Address.

A Binding Update exchange can now take place. This will be passed over the Child SA between MN and CN and will be sent direct rather than via the Home Agent, given that the MN's SA end-point address is now its care-of-address. As the Binding Update is sent via a tunnel from the Home Address, the care-of-address should be reported using the Binding Update's "Alternative Care-of Address option".

2.1.2 Optimising the RO Optimisation

An interesting observation on the above is that if the MN to CN data exchange also has to be protected by encryption or an HMAC, then the Binding Update exchange is not really necessary. This is because when the IKE SA is established, as described above, the Child SA created on the initial exchange, could just as easily be a tunnel mode SA selecting all traffic between the MN's Home Address and the CN's IP Address – a host to host tunnel – with the tunnel using whatever level of protection is required.

Once the "follow me" exchange has taken place, there is now a protected tunnel between MN and CN for all traffic between the MN's Home Address and the CN's IP Address, with the MN's care-of-address and the CN's IP Address as its SA end-points. This provides optimised protected communication between MN and CN.

Should the MN change its care-of-address later, a similar "follow me" exchange can again move the IKE and Child SAs, but with no requirement for a Binding Update exchange as tunnel movement is sufficient.

However, this does raise two questions:

1. Why should a protected optimised communications path between MN and CN be simpler to set up and manage than an unprotected optimised communications path?

2. Why is it necessary in host to host (MN to CN) tunnels, where on the CN side the traffic selector IP Address and the SA end-point IP address are the same, to send the CN IP Address twice, i.e. in both an inner and outer header?

The answer to the first question is that IPsec only currently supports the creation of protected communications paths and hence an extra information exchange outside of IPsec is needed to establish an unprotected communications path.

The answer to the second question is similar, i.e. that IPsec only supports IP-in-IP tunnels and transport mode and (for IPv6) does not currently have any analogue to the Home Address Option/Type 2 Routing Header described in RFC 3775. IPsec tunnels (plus encryption) do allow the inner IP Address pair to be hidden from eavesdroppers. But, when there is no requirement to hide these addresses, IPsec lacks the means to avoid having to send an IP address twice, when it is both the traffic selector and the SA end-point. It would be desirable for the IKE itself to be able to negotiate the use of a Home Address Option/Type 2 Routing Header in support of Transport Mode or "No Protection" SAs. There is, of course, no value in using a Home Address Option/Type 2 Routing Header in support of tunnel mode SAs.

It can be observed that if IPsec did provide solutions to the above, then the entire RO procedure for all types of communications paths could be performed using IKEv2/MOBIKE and would not require a separate Binding Update exchange (e.g. for unprotected communications).

Although this seems to be counter-intuitive for the IPsec IKE to negotiate off security, the benefit is in having a single mechanism to manage unprotected mobile communications, when there is also a need for secure mobile communications.

2.1.3 Changing the care-of-address

Should the MN change its care-of-address again, a similar "follow me" exchange to that used when the SA was first established, can again move the IKE and Child SAs, and a new Binding Update exchange performed, if required. However, to prevent DoS attacks, this should usually be preceded by an MN initiated Informational exchange (from the current care-of-address) reporting the new care-of-address in an ADDITIONAL_*_ADDRESSES payload. If this has not been done, then the CN should use the IKEv2/MOBIKE Return Routability Check to ensure that the new IP Address is valid.

These two cases are illustrated below.

```
HDR, SK{
   N(ADDITIONAL_*_ADDRESSES),
   N(COOKIE2)} -->
                                        <-- HDR, SK{N(COOKIE2)}
MN Changes to new care-of-address as source of UDP packets

HDR, SK {N(UPDATE_SA_ADDRESSES),
   N(ADDITIONAL_*_ADDRESSES)
   N(COOKIE2)} -->
                                        <-- HDR, SK{N(COOKIE2)}
```

Figure 2 Pre-announced change of Care-of-address

MN Changes to new care-of-address as source of UDP packets

```
HDR, SK {N(UPDATE_SA_ADDRESSES),
   N(ADDITIONAL_*_ADDRESSES)
   N(COOKIE2)} -->
                                        <-- HDR, SK{N(COOKIE2)} //response
                                        <-- HDR, SK{N(COOKIE2)} //request
HDR, SK{N(COOKIE2)} -->
```

Figure 3 Unannounced change of Care-of-Address

2.1.4 Authentication Issues

Another issue is that draft-ietf-mip6-cn-ipsec does not seek to investigate the alternative authentication mechanisms that may be used. In practice, there could be several levels of authentication e.g.

1. No Authentication (perhaps trivially achieved by using a "well known" pre-shared key)
2. No Authentication of the MN, with PKI based authentication for the CN.
3. PKI Authentication of both the MN and CN
4. PKI Authentication of both the MN and CN including authorisation of the MN to use its Home Address.
5. PKI Authentication of the MN including authorisation of the MN to use its Home Address. No Authentication of the CN.

In the first three cases, the Home Agent must be involved in the exchange in order to notarise the use of the Home Address, i.e. using the Home Address as the Mobile Node's SA end-point IP Address for the initial exchange. However, in the latter two cases, there is no need to use the Home Address as the Mobile Node's SA end-point IP Address, as the care-of-address could be used instead for the initial IKE exchange. This is because there is no need to demonstrate routability to the Home Address prior to use of the care-of-address, as a means of proving authorisation to use the Home Address.

2.1.5 No Authentication SAs

The downside of the RFC 3775 Return Routability Procedure is that it is vulnerable to an attacker that can observe both parts of the communication path. However, its upside is that it does not require the existence of any trust framework between MN and CN. The CN simply trusts the Home Agent to have authenticated the MN and approved its use of the Home Address.

If IPsec is used to support Route Optimisation, as described above, and does not include authentication of the MN to CN, it appears to offer the same level of assurance but without the vulnerability. This is particularly useful when Route Optimisation is used opportunistically between a MN and a CN which otherwise have no need for authentication of the MN to the CN.

"No authentication" can be achieved trivially by using a widely known pre-shared key. It is also possible to consider extension of IKEv2 to include a "No Authentication" authentication type. That is, in addition to the existing RSA, Pre-shared Key and DSS signature authentication types specified by IKEv2. Even when there is no authentication, the IKE still agrees Diffie-Hellman keying material and can thus protect information exchanges using both encryption and HMAC based integrity checks. MOBIKE "follow me" exchanges can still be trusted.

With "No Authentication", the CN is able to achieve secure communications with the MN, can trust its use of the Home Address (notarised by the Home Agent) but has no means of validating the identity of the system using the Home Address, and hence cannot implement any access controls based on the MN's identity. This is no worse than non-optimised Mobile IP or Mobile IP optimised using the Return Routability Procedure.

"No Authentication" does not appear to expose the CN to any additional Denial of Service attacks, except that an attacker might be able to create many spurious Child SAs, and thus use up memory resources, if rate limiting, or regular weeding out of SAs is not performed. Otherwise, the risks are the same as any communications strategy that permits "guest access", and the CN's policies should strictly limit how any unauthenticated IKE SAs may be used. In particular, a Child SA's traffic selector should only select traffic between the CN and the initial MN's IKE SA end-point IP address.

2.1.6 Authenticated SAs

When a suitable PKI exists (or pre-shared keys are available and kept confidential) there is no reason why the MN should not also be authenticated to the CN. This could then be used for the implementation of Access Controls and accountability. However, there are two sub-cases to consider:

1. The authentication mechanism does not explicitly authorise the use of the MN's Home Address.

   In this case, the Home Agent is still required in its role as a notary for the MN's use of its Home Address. The RO procedure must start with the MN using its Home Address as the SA end-point address.

2. The authentication mechanism includes authorisation of the use of the MN's Home Address.

   In this mode, there is no requirement for the MN to use the Home Agent as a notary, as the authentication mechanism is sufficient to assure the CN that the MN has permission to use its Home Address. The IKE exchange can thus start with the MN using its care-of-address as its SA end-point address and the "follow me" exchange is not required as part of the initial establishment of the communications path.

   This mode supports scenarios where the Home Address is not globally routable, and/or where the Home Agent is not available, for whatever reason; it may not even exist. Note that the Home Address is only reported in an ADDITIONAL_*_ADDRESSES payload when it is routable.

The second case is of particular interest to Aeronautical Communications as a suitable PKI can be assumed and the Home Agent made optional for air-initiated communications (which is desirable given the availability requirement and regulatory issues). It also aligns with the strategy proposed in the Eurocontrol IP Study [2].

2.1.7 Implications for the Mobile Node to Home Agent Protocol

The Route Optimisation strategies described above do not require any changes to the MN to HA protocol. However, they do ask questions about whether the current protocol is the most efficient or consistent approach. Specifically, why is it necessary to have a separate Binding Update exchange outside of the scope of the IKE, when IPsec is already required between the MN and HA?

This question is particularly relevant when IPsec tunnels are used to protect both Mobile IP protocols and user packets. Manual keying can be used to establish such tunnels. However, in any large scale deployment, manual keying is impractical and the IKE should be used. When the IKE protocol is available, it is believed that there is potential for better integration between IPsec tunnel establishment and Mobile IP MN to HA Binding, by applying the strategies described above for Route Optimisation.

In the MN to HA protocol, an important function of the Binding Update is to establish a tunnel between the MN and HA. This tunnel is used to forward all outgoing packets from the MN to the HA when the packet has the MN's Home Address as its source address, and which are not selected by a more specific route to a CN (set up by Route Optimisation). It is also used for forwarding all outgoing packets at the HA with a destination address set to the Home Address of the MN.

If IPsec supported "No Protection" SAs, then such a tunnel could also be set up by the IKE as a "No Protection" SA in tunnel mode with a Traffic Selector that selects all traffic between the MN's Home Address and *any* IP Address. Alternatively, the same approach can be used to negotiate AH or ESP protected tunnels. This does appear to offer an integrated approach for both protected and unprotected MN to HA communication - but does require the addition of "No Protection" SAs to IPsec.

The Binding Update is also used to request Home Agent services (Home Registration). This functionality could also be provided under IKEv2, by defining a new "notify" payload message type value as "Home Registration" (and registering the message type value with IANA).

The IKE could then provide equivalent functionality to a Binding Update to a Home Agent, by proposing a "No Protection" (or protected) SA with a Traffic Selector between the MN's Home Address and the rest of the Internet and including a Home Registration notify payload with the proposal.

The advantages of this approach over the existing Binding Update would appear to be:

- Reduced number of messages exchanged
- Lower implementation complexity (fewer messages to process)
- Better integration with IPsec (AH and ESP protected tunnels between MN and HA are simple variations on the scheme)
- Use of the MOBIKE IKEv2 extensions permits a simple "follow me" approach to change of care-of-addresses, when the mobile node moves from one network to another.

The MN to HA dialogue would then also appear to align well with a particularly common use of IPsec. That is for Roadwarrior to corporate VPN communications.

2.1.8 Application to Basic NEMO Scenarios

One of the improvements of IKEv2 over IKEv1 is that it offers a much richer mechanism for the definition, negotiation and use of SA Traffic Selectors. While the traffic selector at the MN side could be as simple as selecting all traffic to or from the Home Address, if the MN was a Mobile Router, it could also select all traffic to or from all subnets supported by the Mobile Router on the mobile platform, thus meeting the basic requirement for mobility support for a mobile platform.

The main issue with Mobile Routers would appear to be over authorisation to offer routes to the IP Address Prefixes that it serves.

A Home Agent can authenticate a Mobile Router and use this authentication as the basis for the authorisation. However, when Route Optimisation is performed, a simple notarisation – as is the case with a single Home Address – is not so readily possible.

With a single Home Address, the fact that Return Routability with an MN on its Home Address works can be sufficient to declare that the Mobile Node has been authorised to use the Home Address – with confidence limited only by the degree of trust in the Internet Routing infrastructure. When the path is via the Home Agent, then it can be said that the Home Agent is acting as a notary for the Mobile Node's authorisation to use its Home Address.

However, a Home Address of a Mobile Router does not necessarily have to have a common prefix with any of the routes it offers, and even when such a common prefix exists, it does not necessarily imply that the Mobile Router is authorised to provide routes to it.

It would seem that unless a separate notarisation service is developed, Route Optimisation of a Mobile Router to Correspondent Node communications path is only possible when an authentication mechanism exists (e.g. a PKI) that allows the Correspondent Node to both authenticate the Mobile Router and authorise the routes that it offers via the Traffic Selectors proposed for Security Associations between the Correspondent Node and Mobile Router.

2.1.9 Multi-homing

IKEv2/MOBIKE does support multi-homing in the limited sense of being able to declare all other IP Addresses associated with the MN's public interfaces by including the ADDITIONAL_*_ADDRESSES notify payload in an informational exchange. However, this is only useful for error recovery. Genuine multi-homing in the sense of load balancing is outside of the scope of IKEv2/MOBIKE.

However, within the limitations of existing IPsec, it is possible to conceive of a multi-homing approach by a multi-homed MN establishing a distinct IKE SA with the CN from each of its active care-of-addresses. Simple load sharing could then be achieved by using different traffic selectors for the Child SAs established under each such IKE SA.

In the long term, a more integrated approach should be investigated.

2.1.10 NAT Traversal

IKEv2 supports NAT Traversal, as does MOBIKE with limitations. It should also be possible for IPsec based Route Optimisation to support Mobile Nodes that are permanently or temporarily positioned behind a NAT gateway.

However, NAT traversal uses UDP encapsulation, which is limited to the IKE and ESP tunnels. The same limitation will apply to IPsec based Route Optimisation. That is, IPsec based Route Optimisation for a Mobile Node that is behind a NAT gateway must always use ESP in tunnel mode to protect all traffic between the Mobile Node and the Correspondent Node.

A Mobile Node that supports NAT traversal should indicate this in the IKE_INIT. When the IKE_INIT exchange has completed, both Mobile and Correspondent Nodes should have detected the probable existence of a NAT Gateway and agreed to NAT traversal. When the Correspondent Node is behind a NAT Gateway, IPsec based Route Optimisation is not possible and should be abandoned.

When the Mobile Node is behind a NAT Gateway, the Mobile Node must propose an ESP tunnel mode SA to protect all traffic between the Mobile Node and the Correspondent Node. No other type of SA may be proposed.

A Mobile Node may also move behind a NAT Gateway, when it changes its care-of-address. This is detected during the Informational Exchange initiated with an UPDATE_SA_ADDRESSES notify payload. If the SA used for the communications path between the Mobile Node and the Correspondent Node is not an ESP tunnel mode SA, then it must be replaced with an ESP tunnel mode SA.

The MOBIKE Return Routability Check must always be performed by the Correspondent Node, when a Mobile Node changes its care-of-address to a care-of-address behind a NAT Gateway. This is because the care-of-address and the source IP Address used for the Informational Exchange are unlikely to be same, and the source IP Address cannot be used to validate the "follow me".

2.1.11 Summary

It is not believed that draft-ietf-mip6-cn-ipsec is directly applicable to the Aeronautical Environment, for the reasons outlined above. However, it is possible to use it as the basis from which a suitable RO scheme can be developed.

draft-ietf-mip6-cn-ipsec appears to have limited itself by not considering what is possible with IKEv2 and MOBIKE. Use of MOBIKE allows for an integrated return routability check, but also exposes limitations in IPsec. By extending IPsec to include "No Protection" SAs and an SA mode that uses the RFC 3775 Home Address Option/Type 2 Routing Header, an efficient and fully integrated approach to mobility and security appears to be possible.

The approach also appears to scale naturally to when the MN is also a Mobile Router.

Authentication also needs to be considered and, in particular, the difference between:

- "No Authentication" or authentication which does not include authorisation to use the Home Address, and
- Authentication which does include authorisation to use the Home Address,

should be recognised. In the latter case, for MN initiated communications, the Home Agent can then be viewed as optional.

IPsec based RO, with authentication which includes authorisation to use the Home Address and optional use of a Home Agent is essentially the scenario described in the Eurocontrol IP Study [2]. The study confined itself to existing protocols and hence does not include a requirement for "No Protection" SAs or an SA mode that uses the RFC 3775 Home Address Option/Type 2 Routing Header. Protected tunnels were always used. However, it was also recognised that there were many situations where a Home Address Option/Type 2 Routing Header would be more efficient than tunnel mode and not all communication had to be protected.

Extending IPsec to include "No Protection" SAs and an SA mode that uses the RFC 3775 Type 2 Routing Header, while not essential, is desirable from the point of view of RO for Aeronautical use as well as for general use of Mobile IP. Such an extended IPsec should provide the basis of an efficient RO strategy for aeronautical use.

2.2 Extending IPsec

It is believed that there are three extensions necessary to IPsec, before it can be used as the basis for an efficient and consistent RO strategy:

1. The IKE [8] needs to be able to negotiate a "No Protection" Security Association.
2. The IKE similarly needs to be able to established unauthenticated SAs.
3. The use of the Home Agent Option (MN to CN) and Type 2 Routing Header (CN to MN) specified by [11] needs to be negotiable as an option for transport mode SAs, including "No Protection" SAs.

From the point of view of a Security Expert, the use of the IKE to negotiate a "No Protection" and/or unauthenticated security associations seems to be counter-intuitive. However, both have use in a Mobility Framework as described above. Although there is an argument for not developing a "No Protection" SA type on the grounds that once an IKE SA has been negotiated, there is no obvious cost/benefit in not using at least integrity protected SAs.

The specification of Home Agent Option/Type 2 Routing Header support is the real new work required, and is the subject of 3.3 below. Home Agent Option/Type 2 Routing Header support may be proposed by the IKE (IKEv2) in support of a transport mode SA by using an additional IKE notify payload.

3 Proposed IPsec Extensions

Draft specifications for the proposed extensions to IKV2 are given in this section.

3.1 No Protection SAs

The concept of "No Protection" SAs is introduced for completeness and to provide compatibility with existing Mobile IP. However, "No Protection" means what it says and these SAs are vulnerable to many different forms of attack. This is particularly true of a mobile environment where the trust in the network can vary greatly between different networks. For example, public WiFi networks rarely offer any form of protection from eavesdroppers. There is a good case for saying that "No Protection" SAs should never be used for either MN to HA communications or MN to CN communications. This mode is hence deprecated for use.

A "No Protection" SA is signalled by IKEv2 as an SA Proposal with a Protocol ID set to (to be allocated by IANA). No transforms are associated with this protocol and the number of transforms must be set to zero. An SPI size of four is specified. However, the SPI is only used to identify the SA in the context of the IKE (e.g. when used as the subject of a Delete payload).

Compression may not be used with "No Protection" SAs. More than one "No Protection" SA may be in place between the same pair of tunnel end-points, but only if they have different traffic selectors.

When a "No Protection" SA has been agreed in tunnel mode, packets are transferred using IP-in-IP encapsulation according to RFC 2003 [15] for IPv4 or RFC 2473 [16] for IPv6, with the outer IP header source and destination IP addresses set to the SA end-point IP Addresses.

No entry is made in the Security Policy Database (SPD) in support of "No Protection" SAs. The IKE needs only to arrange for IP-in-IP encapsulation to take place between the SA End Points and for traffic selected by the negotiated Traffic Selectors. This is typically a routing function rather than a security function.

A "No Protection" SA may also be negotiated for a Host to Subnet Transport Mode SA (see 3.3 below). However, it is not meaningful for transport mode. A transport mode "No Protection" SA proposal should be rejected.

3.2 The "No Authentication" Authentication Type

When the "No Authentication" authentication type (value to be assigned by IANA) is given in an authentication payload, it means that no authentication is offered by the sender of the payload, and its identity is unproven.

If the receiving system's local policy does not permit unauthenticated SAs then an Informational message is returned containing an error type notify payload UNAUTHENTICATED_SA_NOT_SUPPORTED (value to be assigned by IANA).

3.3 Negotiation of use of the Home Agent Option/Type 2 Routing Header (Host to subnet Transport Mode)

3.3.1 Definition

The Home Agent Option/Type 2 Routing Header applies to IPv6 only, and is specified in RFC 3775, where it is used following a successful Binding Update exchange between a Mobile Node and a Correspondent Node. This specification also allows the use of the Home Agent Option/Type 2 Routing Header to be negotiated by IKEv2.

When used in support of Transport Mode SAs, the Home Agent Option and Type 2 Routing Header can provide a more efficient implementation of host to subnet tunnels. It is particularly useful in support of Mobile IP Route Optimisation. However, It is also applicable to subnet to host Security Associations where there is no requirement to hide the subnet IP Addresses. For this reason, the name given to this function in IPsec is "Host to Subnet Transport Mode".

Use of the Host to Subnet Transport Mode is proposed and accepted during the negotiation of an SA by the IKEv2. As the mode is asymmetric, it is necessary to introduce terminology to distinguish the two sides of the SA. The terms "left" and "right" side are used here for that purpose.

On one side of the SA (the "right" side), the IP Address of the SA end-point and the IP Address given by the traffic selector for the SA must be the same.

On the other side of the SA (the "left" side), the IP Address of the SA end-point and the IP Address given by the Traffic Selector for the SA are different. In addition, the IP Address given by the Traffic Selector, need not be aggregatable by either the "right" side of the SA nor by any router directly reachable from the "left" side. Only a single IP Address can be given as the "right" side IP Address by the Traffic Selector for the SA. However, the "left" side can be one or more IP Address ranges, when the "left" side is a Mobile Router.

3.3.2 Negotiation using IKEv2

Use of Host to Subnet Transport Mode is proposed when either a HOST2SUBNET_MODE_LEFT_SIDE (value to be assigned by IANA), or a HOST2SUBNET_MODE_RIGHT_SIDE (value to be assigned by IANA) is included as a notify payload in an IKE request message and in support of a CHILD_SA proposal. A USE_TRANSPORT_MODE notify payload must not be included in the proposal.

Use of Host to Subnet Transport Mode is accepted when either a HOST2SUBNET_MODE_LEFT_SIDE, or a HOST2SUBNET_MODE_RIGHT_SIDE notify payload is included in an IKE response message accepting a Child SA proposal and HOST2SUBNET_MODE_RIGHT_SIDE or HOST2SUBNET_MODE_LEFT_SIDE, respectively, had been included with the corresponding Child SA proposal.

When an SA Initiator or Responder includes a HOST2SUBNET_MODE_LEFT_SIDE notify payload, it become the left side of the SA. When an SA Initiator or Responder uses a HOST2SUBNET_MODE_RIGHT_SIDE notify payload, it become the right side of the SA.

When use of Host to Subnet Transport Mode is accepted, the SA Traffic Selectors agreed must be compliant with the definition given above. The right side traffic selector's IP Address must be a single unicast IP Address and the same as the right side SA end-point IP Address.

Use of Host to Subnet Transport Mode is compatible with "No Protection" and AH and ESP protected SAs. It is also possible for the "left" side to request and use an IP Address that is assigned for it by the "right" side (see section 2.19 of RFC 4306 [8]).

If Host to Subnet Transport Mode is proposed but is not acceptable by the responder, the SA proposal must be rejected. A new notify error status payload HOST2SUBNET_MODE_REJECTED (value to be defined by IANA) is provided so that a meaningful error response can be given when no alternative and acceptable SA proposal has been made.

3.3.3 "Left" Side Procedures for Packet Transfer

Once use of Host to Subnet Transport Mode has been successfully negotiated:

1. The SPD must be updated to include the negotiated SA. As far as the SPD is concerned, this is a transport mode SA. The traffic selector for this SA will be for traffic between the left side's SA end-point IP Address and the right side SA end-point IP Address (which is anyway identical to its traffic selector).

2. The local routing function must be updated such that IP packets with a source IP Address set to an IP Address selected by the left side's Traffic Selector and a destination IP Address set to the right

side IP Address, will be processed such that the source IP Address is replaced by the left side SA end-point address, and an RFC 3775 Home Address Option is inserted into the IP packet header, with the "Home Address" set to the replaced source IP Address.

3. Similarly, the local routing function must also be updated to permit the receipt and processing of an incoming packet with an RFC 3775 Type 2 Routing Header with a source IP Address set to the right side SA end-point address, a destination IP Address set to the left side SA end-point address, and the "Home Address" in the Type 2 Routing Header set to an IP Address compatible with the left side SA Traffic Selector.

An outgoing packet with a source address set to an IP Address selected by the left side Traffic Selector and a destination IP Address set to the right side SA end-point address will first be selected by the routing function. The Home Address Option will be added and the source IP Address replaced with the left side SA end-point IP Address. It will then be selected by the SPD and processed according to the requirements of the transport mode SA.

An incoming packet with a source IP Address set to the right side SA end-point address, a destination IP address set to the left side SA end-point address, and an acceptable Type 2 Routing Header, will first be selected by the SPD and processed according to the requirements of the transport mode SA. It will then be processed by the routing function, the Type 2 Routing Header removed, and the Home Address it contains replacing the destination IP Address. It will then be forwarded to its destination.

3.3.4 "Right" side Procedures for Packet Transfer

Once use of Host to Subnet Transport Mode has been successfully negotiated:

1. As for the left side, the SPD must be updated to include the negotiated SA. As far as the SPD is concerned, this is a transport mode SA. The traffic selector for this SA will be for traffic between the left side's SA end-point IP Address and the right side SA end-point IP Address (which is anyway identical to its traffic selector).

2. The local routing function must be updated such that IP packets with a source IP Address set to the right side IP Address and with a destination IP Address set to an IP Address selected by the left side's Traffic Selector, will be processed such that the destination IP Address is replaced by the left side SA end-point address, and an RFC 3775 Type 2 Routing Header is inserted into the IP packet header, with the "Home Address" set to the replaced destination IP Address.

3. Similarly, the local routing function must also be updated to permit the receipt and processing of an incoming packet with an RFC 3775 Home Address Option with a source IP Address set to the left side SA end-point address, a destination IP Address set to the right side SA end-point address, and the "Home Address" in the Home Address Option set to an IP Address compatible with the left side SA Traffic Selector.

An outgoing packet with a source address set to the right side SA end-point address and a destination IP Address set to an IP Address selected by the left side Traffic Selector will first be selected by the routing function, the Type 2 Routing Header added and the destination IP Address replaced with the left side SA end-point IP Address. It will then be selected by the SPD and processed according to the requirements of the transport mode SA.

An incoming packet with a source IP Address set to the right side SA end-point address, a destination IP address set to the left side SA end-point address, and an acceptable Home Address Option, will first be selected by the SPD and processed according to the requirements of the transport mode SA. It will then be processed by the routing function, the Home Address Option removed, and the Home Address it contains replacing the destination IP Address. It will then be forwarded to its destination.

3.3.5 Host to subnet Transport Mode and MOBIKE

The MOBIKE extensions to IKEv2 may be used with Host to subnet Transport Mode. However, the IKE initiator (mobile node) must always be the left side in any Host to subnet Transport Mode SAs. The right side is not permitted to change its SA end-point address or to be multi-homed.

Note: this restriction only needs to be in place whilst a Host to subnet Transport Mode SA exists.

When the Mobile Node changes its care-of-address, this will be signalled by an IKE Informational message exchange that includes an UPDATE_SA_ADDRESSES notify payload. Once the change of care-of-address has been agreed, both left and right sides must update both the SPD transport mode entry and the routing function with the new left side SA end-point IP Address.

When MOBIKE is used, there may also be periods when the left side SA end-point IP Address is included in the scope of the left side Traffic Selector. For example, this will occur in Mobile IP when the Mobile Node is using its Home Address as the left-side SA end-point IP Address.

Both left and right sides should treat this as a special case. It is not an error.

Left side outgoing IP packets with a source IP Address set to the left side SA end-point IP Address must not have a Home Address Option added. Right side outgoing IP packets with a destination IP Address set to the left side SA end-point IP Address must not have a Type 2 Routing Header added.

4 Application to Mobile IP Route Optimisation

IPsec, with the extensions specified above, may now be applied to provide an efficient and unified approach to Mobile IP Route Optimisation. The procedures for the Mobile and Correspondent Nodes are described below.

4.1 Mobile Node Procedures

4.1.1 RO Initiation

A Mobile Node (MN) may decide to create an optimised path to a Correspondent Node (CN) using IKEv2 either after communication with the CN via the Home Agent (HA) has started, or when it otherwise determines a need for such a path in advance of any communication. If the MN is able to offer credentials to the CN that include authorisation of its use of its Home Address, then there is no requirement for the MN to have previously bound to or otherwise be in contact with an HA.

NAT Traversal may be supported. However, only the Mobile Node may be behind a NAT Gateway, and IPsec based Route Optimisation should be abandoned if the Correspondent Node is found to be behind a NAT Gateway.

The MN uses IKEv2 to establish an SA with the CN. Authentication may be performed using a pre-shared key or may be certificate based. The MN's identity will normally be given by its Home Address, but another means of identifying the MN may be specified by the local policy. Use of MOBIKE should always be proposed.

The SA end-point at the MN is normally its Home Address, unless the MN is able to offer credentials to the CN that include authorisation of its use of its Home Address, when the care-of-address may be used instead. When the Home Address is used as the SA end-point for the initial IKE exchange, the care-of-address must be provided in a ADDITIONAL_*_ADDRESSES payload.

When determining the type of SA to propose:

1. if the local Security Policy requires that the MN's Home Address(es) are hidden in packets exchanged by the MN and the CN then an encrypted tunnel mode SA using ESP must be proposed.

2. If NAT Traversal is supported and the Mobile Node is behind a NAT Gateway then an ESP tunnel mode SA must be proposed.

3. Otherwise, a Host to subnet Transport Mode SA should be proposed, with the MN as the "left" side and the CN as the "right" side. "No Protection", AH and/or ESP may be proposed for the SA.

For a single host MN, the SA Traffic Selector should select all traffic between the host's Home Address and the CN's IP Address. For a Mobile Router, the SA Traffic Selector should select all traffic between the local IP network(s) served by the router and the CN's IP Address.

If the Home Address has been used as the MN's SA end-point then, after the IKE and Child SA have been established, the MN should change its SA end-point address to its care-of-address and send the CN an Informational IKE message containing an UPDATE_SA_ADDRESSES notify payload, in order to report this change to the CN. If the Home Address continues to be routable, then it should be included in an ADDITIONAL_*_ADDRESSES payload sent with the UPDATE_SA_ADDRESSES notify payload.

Once a positive response has been received to this informational message, the MN may use the care-of-address as the SA end-point address for the IKE SA and its Child SAs.

If a negative response is received or no response is received, then Route Optimisation has failed and the communications path via the Home Agent must continue to be used, if available.

4.1.2 Changing the Care-of-address

The MOBIKE extensions to the IKEv2 should be used when an MN changes its care-of-address, at any time after the completion of the initial exchange described above. It does this by using the IKEv2 to send an informational message containing an UPDATE_SA_ADDRESSES notify payload from the new care-of-address (a "follow me" strategy). Once a corresponding response message has been received from the CN, the new care-of-address becomes the local SA end-point address for the IKE SA and Child SAs between the Mobile and Correspondent Nodes.

If NAT Traversal is supported and the Mobile Node has moved behind a NAT Gateway, then the SA must be replaced with an ESP tunnel mode SA, if it is not already an ESP tunnel mode SA. The Mobile Node is responsible for replacing the SA.

4.2 Correspondent Node Procedures

A CN that supports IKEv2 may receive and process a request for an IKE SA from an MN at any time. If no authentication is offered then the SA is accepted if and only if the local security policy permits the acceptance of unauthenticated SAs.

When an SA is unauthenticated, the CN should not accept any Child SA unless the remote Traffic Selector selects only traffic to or from the IP Address used as the SA end-point address for a IKE packet that includes the INITIAL_CONTACT notify payload. This is assumed to be the MN's Home Address.

Otherwise, and depending on local policy, the CN may authenticate the MN using a pre-shared key or a certificate based authentication mechanism. Acceptance of a CHILD SA proposal from the MN in support of Route Optimisation is subject to the local Security Policy. For example, access may only be granted to an MN when its certificate has been signed by a trusted Certification Authority.

If the credentials offered by the MN implicitly or explicitly authorise the use of a given Home Address or IP Address Prefix(es) then these may be proposed by the MN as the remote Traffic Selector and accepted by the CN. Otherwise, and as above, only the SA end-point address for an IKE packet that includes the INITIAL_CONTACT notify payload may be offered as the remote Traffic Selector.

At any time during the lifetime of an IKE SA with the MN, the CN may receive an informational request message from the MN containing an UPDATE_SA_ADDRESSES payload, but should only use the source IP address of this packet as the remote SA end-point address for the IKE and Child SAs, if either:

- The source IP address was listed in the most recent ADDITIONAL_*_ADDRESSES payload received from the MN, or

- Use of the IKEv2/MOBIKE Return Routability procedure confirms that the source IP Address is routable.

4.3 Security Considerations

In general, the CN cannot identify or approve an MN from the source address of an IKE_INIT (which may be its current care-of-address). This leaves the CN open to potential Denial of Service attacks as there is significant computational effort involved in computing the Diffie-Hellman keying material required prior to authentication; this only takes place on the next message exchange. This is a common issue with IPsec, and, in order to mitigate this risk, the CN may implement some or all of the following strategies:

1. Using the "cookie" procedure specified in section 2.6 of RFC4306 [8] to ensure that the sender of an IKE_INIT is also able to receive packets sent from its source IP Address.

2. Responding to IKE_INIT requests from only a "white list" of possible care-of-addresses.

3. Ignoring a "black list" of known attackers or otherwise untrusted systems.

4. Limiting the rate at which IKE_INIT requests are processed either from all sources, or a "grey list" of unknown sources.

The "No Protection" SA type defined above in 3.1, does what it say on the box, and does not offer any protection. It is thus vulnerable to many types of attack. In general, its use is deprecated in favour of the use of AH or ESP protected SAs. The purpose of "No Protection" SAs is to provide a full range of tunnelling options for the IKE. The fact that a protected SA is no more than a configuration option should persuade most network managers to select it by default, thus improving the overall security of the internet compared with a situation where there was a lack of integration between Mobile IP and IPsec.

The Host to subnet Transport Mode SA defined above in 3.2 does not hide the left side Home Address(es). This may not always be desirable. In such situations, tunnel mode should always be used.

"No Authentication" IKE SAs also permit an unauthorised attacker to cause the responder to commit state and CPU and thus could be used for a Denial of Service attack. However, the attacker must use a valid IP Address and also commit similar levels of state and CPU to the attack. The scope of such an attack is thus limited and can be mitigated by weeding out otherwise unused SAs and black listing initiators that persist in creating such SAs.

5 Conclusion

In Mobile IP, the Home Agent acts as a rendezvous point, authenticates a Mobile Node and authorises use of its Home Address. IPsec already plays an essential role in authenticating a Mobile Node to its Home Agent and protecting the communication between them.

The Return Routability Procedure is a Mobile IP mechanism that allows a Home Agent to act as a notary and to give assurance to a Correspondent Node that the Mobile Node has been authorised to use its Home Address, when there is otherwise no trust relationship between the Correspondent Node and the Mobile Node. Proof of Authorisation of the use of the Home Address is an essential pre-requisite for any Route Optimisation that tries to avoid routing via a Home Agent. However, this procedure is inherently vulnerable to an attacker that is able to observe both communications paths involved in the procedure.

IPsec support is already mandatory in the Mobile Node. When IPsec is also supported in the Correspondent Node, it seems a natural extension to its existing role in Mobile IP, for IPsec to be used as the basis of a Route Optimisation strategy that avoids the known weakness in the Return Routability Procedure. As has been discussed above, even when there is no trust relationship between Mobile Node and Correspondent Node that IPsec can use to authenticate the MN to CN, it is still possible to have an IPsec based Route

Optimisation strategy that avoids the weakness in the Return Routability Procedure. In this mode of use, the Home Agent continues to act as a notary for the Mobile Node's authorisation to use its Home Address.

When IKEv2 and MOBIKE are used to manage IPsec communications between Mobile Node and Correspondent Node, the result is an efficient and secure protocol that also includes a Return Routablity check between Mobile and Correspondent Node via the mobile's care-of-address, as part of the basic procedure.

If an authentication mechanism (e.g. X.509 certificates and supporting PKI) exists that additionally allows the Correspondent Node to verify that the Mobile Node is authorised to use its Home Address, then the Home Agent does not even need to take part in the Route Optimisation process. It is only required in its role as a rendezvous point and hence does not need to be active when a communications path is initiated by the Mobile Node.

This situation is particularly interesting to Aeronautical Communications, where the high availability requirements and the consequential regulatory issues can give problems when a Home Agent is an essential part of the communications infrastructure.

Aeronautical communications is a controlled environment using systems that have been either certified or approved for operational use. It is therefore feasible to assume that, if required to do so, all systems support IPsec, use a common PKI and that PKI provides implicit or explicit authorisation of a Mobile Node's use of its Home Address.

There are already existing registration databases for aircraft, allocating Tail Numbers and ICAO 24-bit aircraft addresses. Air Traffic Control Centres are similarly registered and assigned a four character ICAO Ground Facility Designation, and Airlines have unique IATA registered codes. The basic registration structures are thus in place for the implementation of such a PKI.

An IPsec based Route Optimisation Strategy that assumes existence of a PKI that allows a Correspondent Node to authenticate a Mobile Node and authorise its use of its Home Address, appears to be the correct basis of a Route Optimisation strategy suitable for Aeronautical use.

Appendix A explores in more detail how such a Route Optimisation strategy can be used in ATC and AOC operations. Appendix B examines how the requirements for aeronautical Route Optimisation [1] are met by the proposed RO strategy.

This paper has also raised questions as to why Mobile IP and IPsec are provided as different protocols. With an IPsec based Route Optimisation strategy, a Binding Update can be used to establish an unprotected path between MN and CN, but has no role to play in establishing a protected path – even though an IKE SA is established in both cases. On the other hand, when a protected path is required, an IP-in-IP tunnel is always required. There is no option in IPsec to use something similar to the Mobile IPv6 Home Address Option/Type 2 Routing Header.

This paper answers such questions by proposing the addition of a new SA mode (Host to subnet transport mode) to IPsec that provides the same functionality as the Mobile IPv6 Home Address Option/Type 2 Routing Header. Together with the counter-intuitive concept of "No Protection" SAs, this allows the functionality of the Binding Update to be integrated into IPsec for both Mobile Node to Home Agent dialogues as well as Mobile Node to Correspondent Node dialogues. When IKEv2/MOBIKE is also used, this appears to result in an efficient, secure and consistent framework for mobile communications supporting several grades of end-to-end security. Other functionalities, such as Mobile Routers, appear to be a straightforward part of such a framework, as does NAT Traversal.

6 References

[1] NEMO Route Optimization Requirements for Operational Use in Aeronautics and Space Exploration Mobile Networks, draft-ietf-mext-aero-reqs-01, February 25, 2008

[2] EATM - DAP/CSP CSP Business Division - A/G IP Study: Deliverable D5/D6 – The Future

Communications Infrastructure - Concept and Transition.

http://www.icao.int/anb/panels/acp/WG/n/swgn1-12/P684D013-1_0%20D5-D6%20The%20FCI%20Concept%20and%20Transition.pdf

[3] ICAO Doc. 9705 “Manual of technical provisions for the ATN” – Third Edition.

[4] Eurocae ED-120 Safety and Performance Requirements Standard for Air Traffic Data Link Services in Continental Airspace (Continental SPR Standard).

[5] Eurocae ED-78A Guidelines for Approval of the Provision and Use of Air Traffic Services Supported by Data Communications

[6] EATM – DAP/SPR - LINK 2000+ PROGRAMME - Generic Requirements for a LINK 2000+ Air/Ground Communications Service Provider (ACSP)

http://www.eurocontrol.int/link2000/gallery/content/public/files/documents/Generic%20ACSP%20Reqt%20v1.3.pdf

[7] EATM – DAP/SPR - LINK 2000+ PROGRAMME- LINK Baseline

http://www.eurocontrol.int/link2000/gallery/content/public/files/documents/Link%202000%20Baseline%20(1.4).pdf

[8] Internet Key Exchange (IKEv2) Protocol, RFC 4306

[9] IKEv2 Mobility and Multihoming Protocol (MOBIKE), RFC 4555

[10] IKEv2 Clarifications, RFC 4718

[11] Mobility Support in IPv6, RFC 3775

[12] Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents, RFC 3776

[13] Using IPsec between Mobile and Correspondent IPv6 Nodes, draft-ietf-mip6-cn-ipsec-07.txt, February 2008

[14] A Taxonomy and Analysis of Enhancements to Mobile IPv6 Route Optimization, RFC 4561

[15] IP Encapsulation within IP, RFC 2003

[16] Generic Packet Tunnelling in IPv6 Specification, RFC 2473

[17] A method of using IPsec to setup GRE tunnel, draft-wu-l3vpn-ipsec-gre-00, November 2007

[18] The Point-to-Point Protocol (PPP), RFC 1661

[19] ICAO Doc 9776: ICAO Manual on VHF Digital Link (VDL) Mode 2.

[20] ARINC SPECIFICATION 631-4 - VHF Digital Link (VDL) Mode 2 Implementation Provisions, August 2005

[21] EUROCONTROL Standard Document For On-Line Data Interchange (OLDI), edition 3

http://www.eurocontrol.int/oldi/gallery/content/public/doc/oldi_3-00.pdf

[22] LINK2000+ Uplink Newsletter #10, Nov 2007

http://www.eurocontrol.int/link2000/gallery/content/public/files/documents/Uplink_10.pdf

Appendix A Aeronautical Operational Scenarios

The purpose of this appendix is to provide a set of worked scenarios showing how the proposed IPsec extensions are used in an aeronautical context. Note that the Context Management (CM) and Controller to Pilot Data Link Communication (CPDLC) applications are specified in ICAO Doc9705 [3], and profiled for use in the LINK 2000+ baseline [7].

A.1 Operational Scenarios

In these scenarios, an aircraft is assumed to be routed through airspaces where it has to switch between more than one Air/Ground Communications Service Provider. This may be because of limited coverage, or because the availability requirement is only met when two independent services are available in the same airspace.

Each aircraft is assumed to be allocated a block of static IP Addresses with one or more common prefixes. These IP Addresses are globally unique (at least within the context of the ATN-IP). A PKI is assumed to exist that can both authenticate aircraft and authorise the use of their assigned IP Addresses.

A Mobile Router is present on each aircraft, providing a gateway between the on board systems and the Air/Ground Communications networks. An on board Local Area Network is used to link the Mobile Router to the aircraft's host computers. Each Host Computer on this network and the Mobile Router are assigned IP Addresses from the block of static IP Addresses assigned to the aircraft. The Mobile Router may also have separate dynamically assigned IP Addresses for each interface it has to an air/ground network.

Network Address Translation (NAT) is assumed to be neither required nor used.

The following scenarios need to be investigated.

1. Data Link Initiation
2. Transfer of Communications from the controlling ATSU to the next ATSU
3. Aircraft contact with a non-controlling ATSU
4. A non-controlling ATSU contacting an aircraft
5. Aircraft movement from one air/ground network to another
6. Concurrent use of multiple air/ground networks by an aircraft.
7. Establishing and Managing Communication with an Airline Operations Centre.
8. Termination of Data Link Communications

A.1.1 Data Link Initiation

This scenario is described in section 3.2.1.4 of the Eurocontrol IP Study Report [2]. The procedure is illustrated in Figure A-1 and described below.

The purpose of this procedure is to establish a communications path between the aircraft and an Air Traffic Service Unit (ATSU) and to enable an ATSU to identify the Flight, locate the Flight Plan, and bind it to the physical aircraft and any IP Addresses assigned to it. This procedure is always air initiated. ATC is oriented around Flights and not aircraft as such. It is thus not possible for an ATSU to contact a Flight before this procedure has been performed.

Once the aircraft has made contact with a suitable air/ground network and has been assigned an IP Address on this network, the pilot is informed that datalink communications are now available. On the pilot's instructions, Data Link Initiation is performed with the controlling ATSU, as selected by the pilot.

A DNS lookup is performed to determine the IP address to use for Data Link Initiation, and a secure communications path is now established with the ATSU. The secure communications path is established between the aircraft's Mobile Router (AMR) and the ATSU using the IKEv2 protocol with MOBIKE extensions. If more than one air/ground network is active, then one of these is selected as the airborne end-point of the communications path.

The IKE SA is established as illustrated below, with the AMR's dynamically assigned IP Address on the air/ground network, as the AMR's IKE SA IP Address. Note that an N(ADDITIONAL_*_ADDRESSES) payload is only present if the AMR is currently attached to more than one active air/ground network.

Aircraft		**ATSU**
HDR, SAi1, KEi, Ni -->		
	<--	HDR, SAr1, KEr, Nr, [CERTREQ]
HDR, SK {IDi, [CERT,] [CERTREQ,] [IDr,] AUTH, SAi2, TSi, TSr, N(MOBIKE_SUPPORTED) N(ADDITIONAL_*_ADDRESSES)}-->		
	<--	HDR, SK {IDr, [CERT,] AUTH, SAr2, TSi, TSr, N(MOBIKE_SUPPORTED }

An aircraft should normally have cached all required ATSU X.509 certificates prior to flight and so should not normally include a CERTREQ payload in the second message sent (IKE_AUTH). The aircraft's certificate should normally have been filed with the Flight Plan or should otherwise be available through a directory, and hence the ATSU should similarly not include a CERTREQ payload in its first response (IKE_INIT). It anyway cannot identify the aircraft from the initial message. The aircraft thus does not normally include a CERT payload in its IKE_AUTH.

The Child SA requested by the aircraft is for a Host to subnet transport mode SA (see 3.3). The airborne traffic selector (TSi) is for the static IP Address range assigned to the aircraft. The ground traffic selector (TSr) is for the ATSU's IP Address. The Child SA will be ESP protected, with an integrity check, but no encryption.

The ATSU validates the aircraft's IKE SA request using the certificate identified by the identity (IDi) payload. If this certificate cannot be found, then the request is refused. The certificate must include explicit authorisation for use of the IP Address range proposed by TSi, otherwise the request for the Child SA is refused.

Once the Child SA has been established, the secure communication path is available and the Context Management (CM) Login Request message is sent to the ATSU. The source address of the packet will be an IP Address on the aircraft LAN (i.e. one of the static IP Addresses assigned to the aircraft). The packet will thus be selected by the AMR's Security Policy Database (SPD) and forwarded using the Host to subnet SA to the ATSU.

The CM Login Request message identifies the Flight, by its callsign (Flight Identifier), Departure and Destination Airports and Estimated Time of Departure. This information is sufficient for the ATSU to locate the aircraft's Flight Plan and establish the binding between Flight and Aircraft.

The CM Logon Response is now returned, reporting either successful login or failure. It is returned from the ATSU's IP Address to the sending address of the CM Login Response. It is thus similarly selected by the ground SPD and transferred using Host to subnet SA to the AMR, from which it is forwarded to its destination on board system.

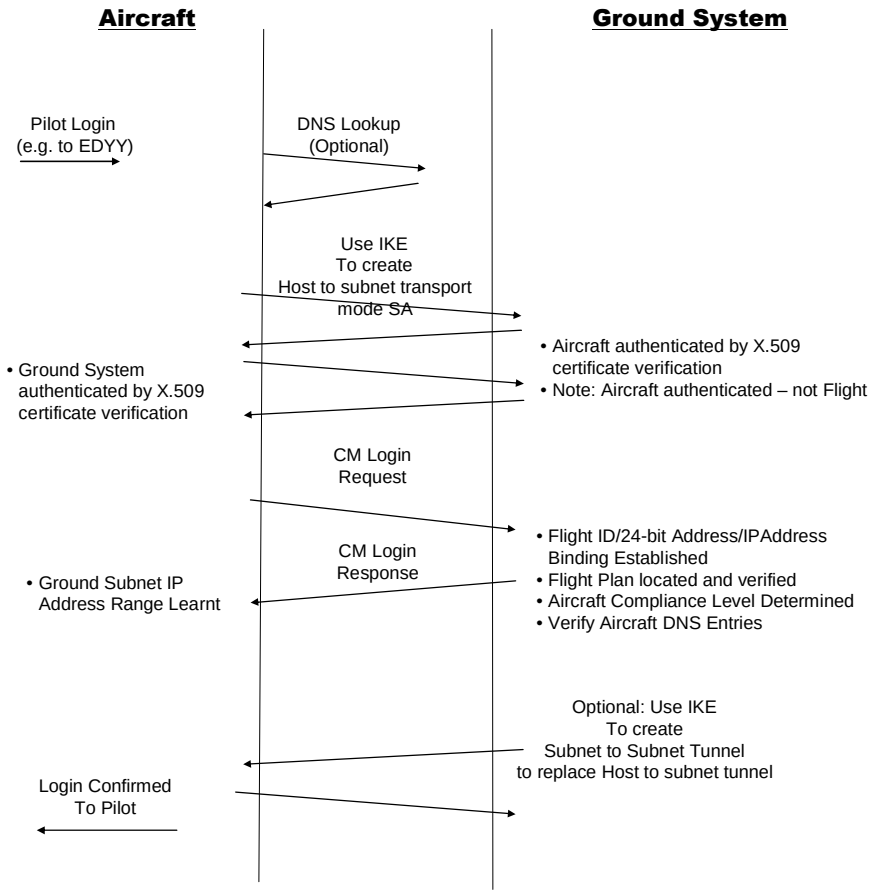

Figure A-1 Data Link Initiation Process

A.1.1.1 Aircraft X.509 Certificate not available

The above procedures assume that the aircraft's X.509 certificate will be available to an ATSU. In exceptional cases, the ATSU will not be able to locate the certificate and will have no option but to reject the aircraft's IKE_AUTH message with an authentication failure notification.

In this case, the aircraft should respond by repeating its IKE_AUTH message but should, this time, include its own X.509 certificate in the message. This should allow the ATSU IKE to correctly authenticate the message.

A.1.1.2 ATSU X.509 Certificate not available

In exceptional cases, the aircraft will have not cached the ATSU's X.509 certificate prior to take-off. In such situations, the Airborne IKE should know that the certificate is not available when it generates its IKE_AUTH message. It should thus include a certificate request field in this message. The ATSU should then respond with its own certificate included in its IKE_AUTH message.

A.1.1.3 Support of a Ground Subnet

The above procedures assume that a single static IP Address is assigned to the ATSU. This is satisfactory for all communication with the ATSU, as long as the same IP Address is used for the Flight Server etc. However, where a ground subnet rather than a single IP Address is used for the ATSU, there is a need to

replace the SA with a tunnel mode SA between the aircraft IP Address/subnet and the ATSU subnet. This will occur following a successful CM Login exchange, and is performed by the Ground System.

This is also required if the ground system needs to be multi-homed as this is not possible in Host to subnet Transport Mode.

Note that [2] proposed including the ground subnet addresses in the CM Login Response and hence it was the aircraft's responsibility to establish the subnet to subnet tunnel. Either approach is feasible.

A.1.1.4 Denial of Service Attacks

The IKE is known to be vulnerable to Denial of Service attacks that attempt to flood a responding system with spurious IKE_INIT packets from spoofed IP Addresses. When responding to an IKE_INIT, the responder calculates keying material from the Diffie-Hellman exchange. This is computing intensive and a flooding attack could lead to resource exhaustion at the responder.

The aircraft should be able to avoid this problem by rejecting all IKE_INIT requests. This is feasible as long as it never has to respond to incoming IKE_INIT requests, which appears to be true from inspection of these scenarios.

The ATSU is at risk and may need to protect itself if there is a risk of an attacker being able to send it spoofed packets. The "cookie exchange" procedure described in section 2.6 of RFC 4306 appears to be the most appropriate way to mitigate this attack. However, if always used, an otherwise unnecessary two packet exchange will be added every time Data Link Initiation is attempted. On low bandwidth air/ground networks, this could be an issue.

A better strategy is thus for the ATSU to monitor the rate at which IKE_INITs are being received and not completed with an IKE_AUTH exchange, and switch to using the cookie exchange procedure if this exceeds a pre-determined rate.

A.1.1.5 Additional Child SAs

The Child SA established during the Data Link Initiation procedure provides ESP integrity protection. However, in the future some applications may require encryption, while other applications may not need any protection and hence performance may benefit from avoiding ESP overhead.

Both situations can be accommodated by establishing additional Child SAs between the AMR and ATSU, with more specific protocol and port selection criteria, and using either ESP with encryption, or "No Protection". By ensuring that the protocol and port selection criteria match the application requirements for encryption or "No protection", the desired objective can be achieved.

A.1.1.6 Use of a Home Agent

As the PKI is assumed to include authorisation of the aircraft's IP Address range (believed to be essential as a Mobile Router is used), a Home Agent is only needed as a rendezvous point. The only scenario that could take advantage of this, is contact from a non-controlling ATSU (see A.1.4) and here it is only optional. There is thus no requirement for an aircraft to bind to a Home Agent.

However, this may still be desirable, in which case the binding would take place in parallel to the Data Link Initiation procedure. As the SA Traffic Selection criteria for aircraft to ATSU SAs will always be more specific than to the Home Agent, thus these SAs will always be selected in preference to the SAs with the Home Agent for aircraft to ATSU traffic.

A.1.1.7 CPDLC Message Exchange

Once Data Link Initiation is complete, Controller to Pilot Data Link Communications (CPDLC) messages may be exchanged (e.g. to request and/or receive clearances). CPDLC communications starts with a CPDLC start request message being sent from the ATSU to the aircraft and the aircraft returning a CPDLC

start response. The source and destination IP Addresses of these messages may be any IP Address on the aircraft and ATSU's subnets, respectively.

A.1.2 Transfer of Communications from the controlling ATSU to the next ATSU

In ATC, the Transfer of Communications between ATSUs corresponds to the ATC transfer of control and is distinct from any change in air/ground network transitions. The communications path between the aircraft and the Receiving ATSU (R-ATSU) must be set up before control is transferred from the Current ATSU (C-ATSU). The procedure is illustrated in Figure A-2 and is described in section 3.2.1.11 of [2].

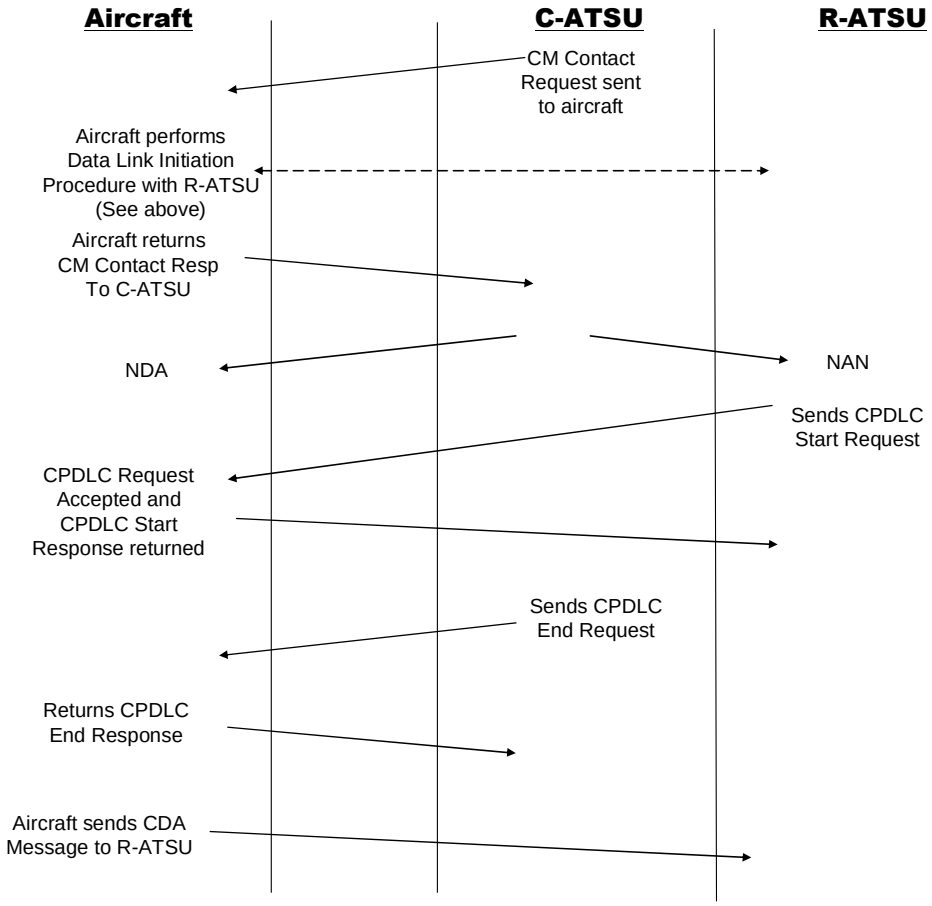

Figure A-2 Transfer of Communications

Transfer of Communications proceeds in a controlled manner and starts with the controlling ATSU sending a CM Contact Request message to the aircraft's CM Application. This message is sent in anticipation of the transfer of control from the controlling ATSU to the ATSU identified in the CM Contact Request. It is sent using an existing SA between the C-ATSU and the aircraft.

The CM Contact Request message is received by the airborne CM Application which now performs a Data Link Initiation exchange with the identified ATSU, as described in A.1.1. Once this has completed, the CM Application returns a CM Contact Response Message to the controlling ATSU, reporting the outcome of the Data Link Initiation exchange.

Assuming that success has been reported, the controlling ATSU sends a Next Data Authority (NDA) message to the aircraft in order to formally nominate the next ATSU en route as the NDA. In the European System, a Next Authority Notify (NAN) message is also sent to that ATSU using the OLDI [21] network and, as a result, the next ATSU will send a CPDLC start message to the aircraft. A suitable communications path may be assumed to exist for this message as a result of the CM Contact Request exchange. The aircraft can likewise respond with a CPDLC start response, and the NDA CPDLC association is now created. As required by ICAO, such a CPDLC association cannot be used to exchange any other CPDLC messages until the NDA becomes the controlling ATSU.

The final step in the transfer of communications occurs when control is passed from the controlling ATSU to the NDA. In CPDLC terms, this is realised by the controlling ATSU sending a CPDLC End Request to the aircraft, which responds with a CPDLC End Response. The Airborne CPDLC Application then completes the transfer of communications, by instructing the Application Security Manager that the ATC Data Link with the current controlling ATSU is terminated. It now sends a Current Data Authority (CDA) message to the next ATSU to indicate that it is now the controlling ATSU.

The IKE SA with the ATSU and any Child SAs with the C-ATSU may now be terminated.

A.1.3 Aircraft contact with a non-controlling ATSU

Contact with a non-controlling ATSU is required for both Downstream Clearances (DSC) and Flight Information Services (e.g. D-ATIS[1]). This is always aircraft initiated and on demand from the pilot. This scenario was not explicitly discussed in [2] as it is not in current use.

Downstream Clearances cannot be obtained before the Data Link Initiation procedure has been performed with the non-controlling ATSU. This is so that the non-controlling ATSU can locate the Flight Plan for the aircraft. The Data Link Initiation is the same as that used with a controlling ATSU and is as described in A.1.1. The CM Application will execute Data Link Initiation with a non-controlling ATSU when requested to by the pilot. Once the Data Link Initiation has completed successfully then a CPDLC message exchange may take place to request and receive a Downstream Clearance.

In the case of D-ATIS, there is not necessarily a requirement to perform Data Link Initiation prior to making a D-ATIS request. It may be sufficient for the D-ATIS Data Link Application to simply:

1. Perform a DNS name/address resolution to determine the IP Address for the required D-ATIS Information Provider.

2. Send the D-ATIS request to the D-ATIS Information Provider. This may be an example of where TCP is used, especially if MET data is retrieved.

Only if the D-ATIS exchange needs to be protected, need any of the Data Link Initiation (communications path establishment) procedures be performed.

A.1.4 A non-controlling ATSU contacting an aircraft

A non-controlling ATSU may need to initiate communication with a Flight, for example, in support of ADS-C based Data Link Applications. This scenario was also not explicitly discussed in [2] as it is not in current use.

Because the aircraft's (dynamically assigned) IP Address cannot readily be predicted from a Flight Identifier, the non-controlling ATSU must, in addition to the Flight Plan, also have access to up-to-date information about the aircraft and its current IP Address. This may, for example, have been learnt from the controlling ATSU via a CM Logon Request copied to the ATSU by an OLDI LOF message [21].

---

[1] Automatic Terminal Information Service

If a Home Agent or a similar rendezvous point was available then this could be used to communicate with the aircraft. Alternatively, the controlling ATSU can be requested to send a CM Contact Request to the aircraft, in order to request it to contact the non-controlling ATSU.

If a Home Agent is available, then the non-controlling ATSU can send to the aircraft's Home Address a CM Update message. This message identifies the non-controlling ATSU and updates the aircraft with information about it. The aircraft should react to the receipt of the message by performing the Route Optimisation procedures and creating a protected communications path with the ATSU. ATC Messages can now be exchanged directly between the aircraft and the non-controlling ATSU.

If a Home Agent is not available then the non-controlling ATSU requests the controlling ATSU to send a CM Contact Request to the aircraft, requesting that the aircraft performs ATC Data Link Initiation with the non-controlling ATSU. This request could be made through an OLDI message. The aircraft now performs Data Link Initiation with the non-controlling ATSU and communication may then proceed as required.

A.1.5 Aircraft movement from one air/ground network to another

When an aircraft moves from one air/ground network to another the SA end-point IP Address will change for each of its active SAs. This scenario is described in 3.2.1.8 of [2]. It must now notify the ATSU of the change, using the following IKEv2 packet exchange. The AMR sends these packets from the new SA end-point IP Address, i.e. the IP Address assigned to the interface on the new air/ground network.

Aircraft	**ATSU**
HDR, SK {N(UPDATE_SA_ADDRESSES), N(ADDITIONAL_*_ADDRESSES) N(COOKIE2)} -->	
	<-- HDR, SK{N(COOKIE2)} //response <-- HDR, SK{N(COOKIE2)} //request
HDR, SK{N(COOKIE2)} -->	

The first packet exchange is used to report the change of IP Address to the ATSU, and the change is signalled by the N(UPDATE_SA_ADDRESSES) payload. If the AMR still has other air/ground network connections then its IP Addresses on these are signalled by an N(ADDITIONAL_*_ADDRESSES) payload. The ATSU responds to this message by returning the N(COOKIE2) payload.

If the new SA end-point IP Address had been reported in a previous N(ADDITIONAL_*_ADDRESSES) payload sent by the AMR to the ATSU, then this exchange is sufficient to move the IKE SA end point. However, if this had not been done, then the ATSU cannot yet fully trust the new SA end-point IP Address. A genuine IKE SA packet may have been intercepted and the (unprotected) source IP Address replaced. A second ATSU initiated exchange is needed in this case to verify return routability with the AMR via the new SA end-point IP Address. This is a simple ATSU initiated IKE exchange using another N(COOKIE2) payload. Once completed successfully, the new IP Address can be trusted and all Child SAs are now switched to using the new IP Address.

A.1.6 Concurrent use of multiple air/ground networks by an aircraft

This scenario is described in section 3.2.1.10 of [2].

IKEv2/MOBIKE currently has only limited support for multi-homing. Additional IP Addresses can be reported using IKE Informational Messages. However, there is no support at present for making use of this information for load sharing. The only use that the MOBIKE Specification has for this information is to permit the initiator to recover from an apparent responder failure by trying the alternative addresses, and this procedure is, anyway, not compatible with Host to subnet Transport Mode.

The responder (ATSU) can, however, make use of the reported Additional IP Addresses to attempt to contact an otherwise uncontactable aircraft.

At present, genuine multi-homing will require a separate IKE SA between the aircraft and ATSU for each Air/Ground network in concurrent use, and separate Child SAs for each such case. Local load balancing rules can then be applied.

A.1.7 Aeronautical Operational Communications (AOC)

An aircraft's AOC communication requirements are generally much simpler than those for ATC. In support of AOC applications, the aircraft needs to be able to contact its Airline Operations Centre at the start of flight and remain in contact during a flight. Various information, status and control messages may then be exchanged during a flight.

This scenario is described in section 3.2.2 of [2].

A.1.7.1 Initial Contact

As with ATS Communications, initial contact is performed by the aircraft either on pilot command or automatically, once air/ground communications services are available. A DNS lookup may be used to determine the IP Address of the Airline Operations Centre and a secure communications path established with the Airline Operations Centre.

An IKE SA and Host to subnet transport mode SA may now be established as described in A.1.1.

Once the communications path has been established, the aircraft will send a communications advisory message to its Airline Operations Centre, advising it that it is now contactable.

The Airline Operations Centre is also vulnerable to a Denial of Service attack as described in A.1.1.4, and a similar mitigation strategy appears to be appropriate.

A.1.7.2 Aircraft movement from one air/ground network to another

This is identical to the ATC case except that the ground end-point is the Airline Operations Centre rather than an ATSU.

Note that an aircraft may have separate SAs with an ATSU and an Airline Operations Centre when it moves from one air/ground network to another. These are independent of each other and have to be moved separately.

A.1.8 Termination

Ideally, data link termination for both ATC and AOC is a controlled procedure that takes place at the end of a flight and involves a normal termination of the IKE SAs and associated child SAs.

However, in many cases, the aircraft will go out of range of air/ground communications before a controlled termination can take place. It is thus necessary to place an upper bound on the lifetime of each SA.

Use of the INITIAL_CONTACT notify payload whenever an new IKE SA is established is also important as there may often be cases where a ground system has an unexpired IKE SA with an aircraft, when Data Link Initiation is attempted, and left over from an earlier flight that same day.

Appendix B Assessment Against the Requirements for Aeronautical RO

Reference [1] has identified a set of requirements for Route Optimisation in support of aeronautical requirements. This appendix assesses the proposed use of IPsec (plus extensions) to support Route Optimisation.

B.1 Required Characteristics

B.1.1.1 Req1 – Separability

An example of the need for separability may be found in A.1.1.5. This is when access to some types of information services does not require any form of IPsec protection.

The AMR recognises this from pre-configured policy and creates a Child SA with "No Protection" for the applications that do not require IPsec protection. In some cases, for example, when an aircraft contacts a non-controlling ATSU for access to weather information, the Child SA established by the IKE_AUTH exchange may have "No Protection".

B.1.1.2 Req2 – Multihoming

Multi-homing in support of increased availability is well supported by the proposed approach. An aircraft can have many concurrent air/ground networks available and move SAs and hence communications path from one to another using a simple "follow me" approach that leverages the use of strong authentication.

Different communications paths could also be routed over different air/ground networks by using separate IKE SAs and an appropriate choice of IP Address for the airborne SA endpoint. For example, in Oceanic Airspace, an AOC communications path might use HF Data Link, whilst an ATC communications path might use SATCOM.

Multi-homing of ground systems is also possible. However, this is not compatible with Host to subnet Transport Mode mode SAs, which would need to be replaced by tunnel mode SAs.

Load balancing across multiple air/ground networks to the same ground system is also possible if separate IKE SAs are used for each case. However, there is a need to investigate how MOBIKE can be extended to provide efficient load balancing in multi-homing scenarios.

B.1.1.3 Req3 – Latency

A low latency approach is proposed by this paper. The simple "follow me" approach of MOBIKE means that airborne SA end-points can be changed rapidly, and often with only a single message exchange, for each ground system that the aircraft is in contact with.

B.1.1.4 Req4 – Availability

The avoidance of single points of failure is a major rationale for the proposed approach.

When multiple air/ground networks are available, the simple "follow me" approach of MOBIKE allows the aircraft to quickly switch the communications path from a failed air/ground network to one that is still operational. In most cases, the aircraft is able to directly detect the loss of service and to react accordingly. In some cases, the wireless communications service is still available but a downstream problem prevents communications with the ground system. IKE/MOBIKE includes a Return Routability Check mechanism that may be used to confirm communications path failure, should it be suspected. Movement to an alternative air/ground network can then be performed, if required.

The other identified threats to availability are:

- Loss of IPSec state synchronisation following a system crash/recovery

- Loss of SA state following rekeying

The IKE INITIAL_CONTACT payload is very important in respect of avoiding the first problem. This is included in an IKE initial exchange (in the IKE_AUTH) whenever the aircraft establishes an IKE SA with a ground system except when parallel IKE SAs are being established for load balancing purposes. This forces synchronisation of both sides to an initial state.

Warm restarts with recovery of IPsec state information are always preferable. However, in the case where a ground system has cold started and lost all IPsec state information, this will only be detectable to the aircraft when unauthenticated error responses are received, if at all, from the ground system, including failure of the IKE/MOBIKE Return Routability Check and any attempt to move to a different Air/ground network. The aircraft may then attempt to re-synchronise with the ground system by use of an initial IKE SA establishment exchange with an INITIAL_CONTACT payload. Provided that the ground system is active, this should always succeed.

In general, rekeying should not be an issue, as most SAs will be short lived. Only those with Airline Operations Centres will last for the length of a Flight, and hence may be subject to rekeying.

Under IKEv2, rekeying is performed by creating a new Child SA to replace an existing one and then deleting the old one. Either side may rekey an SA. The main risk appears to be when both sides decide to simultaneously rekey an SA. This situation is discussed in detail in section 5.11.3 of RFC 4718 [10], and appears to be handled satisfactorily provided that both sides follow the recommendations in RFC 4718.

B.1.1.5 Req5 - Packet Loss

There appears to be no characteristic in IPsec that increases the probability of packet loss or duplication beyond the level that would normally be expected. IPsec data integrity protection should decrease the undetected error rate which may appear to increase the packet loss rate. However, this is an improvement rather than an increase in actual packet loss.

The "follow me" mechanism used to change from one air/ground network to another should still allow for incoming packets to be received on the old air/ground network (if it is still available) during a transition period.

B.1.1.6 Req6 – Scalability

The use of IPsec for Route Optimisation does not affect the normal routing infrastructure of the network and does not add any additional messages to those that would otherwise be required to protect end-to-end communications using IPsec. There thus seems to be no scalability issue.

B.1.1.7 Req7 - Efficient Signalling

The "follow-me" approach to change of air/ground network seems to be as about as efficient as possible for managing the movement of an MN from one care of address to another. The establishment of initial communications takes only an exchange of two message pairs.

The main issue is likely to be over the size of messages:

- The IKE_INIT messages include Diffie-Hellman keying information, including a key exchange payload and a nonce payload. These messages will be of the order of 1.5 kbits, which should be acceptable.

- The IKE_AUTH messages can include X.509 certificates, a DER encoded X.509 certificate can be of the order of 800+ bytes each and are preferably avoided. Section A.1.1 describes procedures that aim to avoid having to transfer X.509 certificates.

- An IP-in-IP tunnelled message can double the header size of a message. The proposed use of Host to subnet Transport Mode mode should avoid this unless necessary, and will maintain the same level of efficiency as in RFC 3775 RO.

B.1.1.8 Req8 – Security

Three sub-requirements are contained here:

• The RO scheme MUST NOT further expose MNPs on the wireless link than already is the case for NEMO basic support.	This is the minimum level of security provided. Protection against masquerade of an MN is also much stronger than in NEMO basic support.
• The RO scheme MUST permit the receiver of a BU to validate the CoAs claimed by an MR.	This capability is inherent in the use of IPsec. Strong authentication of MNs is provided, and credentials based authorisation of the use of the Home Address in a Traffic Selector.
• The RO scheme MUST ensure that only explicitly authorized MRs are able to perform a binding update for a specific MNP.	This capability is inherent in the use of IPsec and the proposed PKI. Strong authentication of MNs is provided, allowing the enforcement of access controls.

B.1.1.9 Req9 – Adaptability

The RO strategy supports any transport protocol supported by ESP or AH, or by IP-in-IP encapsulation. There are no restrictions placed on the use of IP Options.

B.1.2 Desirable Characteristics

B.1.2.1 Des1 – Configuration

The configuration mechanism is the same as would be expected for IPsec. Use of X.509 certificates means that access control policies can be configured in a straightforward manner. For example, by permitting access to MNs only when their certificate is signed by an explicitly recognised Certification Authority.

In this scheme, the Binding Cache is the SPD and each binding equates to an SA. Standard tools for inspection and manipulation of the SPD may be used.

B.1.2.2 Des2 – Nesting

Nesting is possible, but does result in "tunnel in tunnel" configurations.

For ATC and AOC operations, a "nesting" requirement is not foreseen.

B.1.2.3 Des3 - System Impact

Using a single integrated mechanism for both security and mobility that is based on industry standards would appear to be the best approach for minimising complexity of systems software. IPsec is mandatory for the MN under both Mobile IP and NEMO. By removing the use of Binding Updates and the RFC 3775 Return Routability Procedure from the implementation requirements, complexity is reduced.

B.1.2.4 Des4 - VMN Support

The RO strategy can support Mobile Routers, supporting several blocks of IP Addresses on an aircraft. Provided LFNs and VMNs are allocated IP Addresses from these ranges, they can use the routing facilities provided by the MR.

B.1.2.5 Des5 – Generality

IPsec with MOBIKE has been optimised for what is arguably the most common mobility scenario today: the corporate road-warrior gaining secure remote access to a corporate intranet. This approach has been extended to provide a general purpose mobility and security solution. This is focussed on Route Optimisation but is also compatible with Home Agent operations.

Mobility frameworks are inherently vulnerable to a range of spoofing attacks and demand strong authentication mechanisms, leading to authorisation of Home Address(es). RFC 3775 already provides for strong authentication of an MN to a HA. This approach extends strong authentication to the MN to CN relationship, and uses this to avoid the need for an HA unless a rendezvous point is explicitly required.