Applying IKE/IPsec Context Transfer to Aeronautical Networks

Serkan Ayaz  
German Aerospace Center  
Institute of Communications and Navigation  
Wessling, Germany  
serkan.ayaz@dlr.de

Christian Bauer  
German Aerospace Center  
Institute of Communications and Navigation  
Wessling, Germany  
christian.bauer@dlr.de

Max Ehammer  
University of Salzburg  
Institute of Computer Science  
Salzburg, Austria  
mehammer@cosy.sbg.ac.at

ABSTRACT

The International Civil Aviation Organization (ICAO) is currently standardizing an IPv6-based Aeronautical Telecommunications Network (ATN/IP) as a next generation communication network for air traffic management. Thereby, ATN/IP considers Mobile IPv6 (MIPv6) as a basic mobility management protocol which provides host mobility. Considering a large number of hosts within an aircraft, the need for network mobility (NEMO) arises. However, the base NEMO protocol does not support route optimization (RO), a feature which provides better end-to-end delay performance. In this paper, we considered the Global Home Agent to Home Agent (HAHA) protocol as a NEMO RO solution for the aeronautical environment. MIPv6/NEMO requires a security association (SA) between MR and HA in order to protect the mobility signalling. In a Global HAHA network, in case MR switches from one HA to another, it has to re-establish the IKE/IPsec SA and perform mobility signalling with the new HA. In this paper, we propose to use the context transfer protocol (CTXTP) for re-establishing the SA between MR and the new HA which provides better signalling overhead and delay performance.

Categories and Subject Descriptors

C.2.1 [Computer - Communication Networks]: Network Architecture and Design—Wireless Communication

General Terms

Design

Keywords

Network Mobility, IKEv2, IPsec, CXTP, Aviation

1. INTRODUCTION

The International Civil Aviation Organization (ICAO) is responsible for the standardization of the Aeronautical Telecommunications Network (ATN) that is used for Air Traffic Services (ATS) and Airline Operational Services (AOS) [5]. ATS Correspondent Nodes (CNs) are used to provide navigation, control and situational awareness services to the aircraft and AOS CNs are mainly used for business operations of airline companies. The ICAO is currently standardizing an IPv6-based Aeronautical Telecommunication Network (ATN/IP) [10] that considers Mobile IPv6 (MIPv6) [11] as a basic mobility management protocol. Since MIPv6 is standardized for hosts, it is not scalable in terms of mobility signalling overhead if we consider an aircraft with multiple Mobile Network Nodes (MNNs) on board. In this case, it is better to consider network mobility (NEMO) protocol [4]. NEMO introduces a new entity called Mobile Router (MR) in order to perform mobility signalling for all Mobile Network Nodes (MNNs) connected to the MR. However, the base NEMO specification does not support route optimization (RO), which means that the packets exchanged between MNNs (on MR side) and Correspondent Nodes (on ground side) always traverse the Home Agent (HA). Up to now, different NEMO RO methods were proposed by the IETF and we will consider one of these solutions for aeronautical case: Global Home Agent to Home Agent (Global HAHA) [14].

In aeronautical environment, legacy link technologies have severe bandwidth constraints. Hence aviation community is currently designing a future radio system (FRS) which will be operational around 2015-2020. Table 1 shows the capacity requirements of the FRS for different service volumes (SVs) (e.g. Terminal Maneuvering Area (TMA), Enroute (ENR) Large, Super Large etc.) [7] where PIAC shows Peak Instantaneous Aircraft Count numbers for each service volume. In this paper, we assume that one FRS cell covers one service volume and provides the capacity required by that service volume mentioned in the table. It is also important to keep in mind that the available capacity mentioned in the table is shared among all the aircraft within that cell. As opposed to today air traffic communication (which is based on analog voice), most of the air traffic communication will be handled by the data links after 2015-2020. Considering this fact, the FRS capacity values given in the table, is not very promising and the system should be designed in order to minimize any kind of signalling overhead over the wireless link. For this reason, we consider context transfer protocol (CTXTP) in order to minimize the signalling over-
head created due to establishing a new IKE/IPsec security association (SA) in case the MR switches from one HA to another one.

Table 1: Capacity Requirements of Different SVs

<table>
<thead>
<tr>
<th>Service Volume Type</th>
<th>Type</th>
<th>Small</th>
<th>Large</th>
<th>EnL</th>
<th>EnL</th>
<th>Super Large</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total (kbps)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. BACKGROUND

This section provides information about general functionalities that are considered in this paper.

2.1 Network Mobility

Network Mobility (NEMO) [4] introduces the Mobile Router (MR) which extends the mobile host functionality [11] in such a way that it provides IP addresses to the connected MNNs from the assigned mobile network prefix (MNP). The assigned MNP is associated with the Home Address (HoA) of the MR.

2.1.1 Basic NEMO Operation

In NEMO [4], when a CN sends a packet to a MNN of the MR, the packet is first routed to the HA that advertises MNP (MNNs are configuring their IP address from the MNP). After the HA receives the packet, it checks its binding cache entry (BCE) 1 in order to tunnel the packet to the current point of network attachment of MR (i.e. Care-of Address (CoA) of the MR). On the reverse path (i.e. when a MNN sends a packet to its CN) the MR receives the packet from the MNN and tunnels it to the HA. When HA receives the packet it decapsulates the packet and sends it to the CN.

2.2 Global HAHA

In this paper, we considered the Global HAHA protocol [14] as a NEMO RO solution in the aeronautical environment. Figure 1 shows an example network architecture where HAs are exchanging mobility information among themselves by using the Inter-HAHA protocol [15] via HA-HA tunnel. HAs announce their common /32 prefix (i.e. Extended Home Network (EHN)) via an Exterior Gateway Protocol (EGP) to the global Internetwork. In addition, each HA advertises its own /36 prefix to other HAs via an Interior Gateway Protocol (IGP). In our network, each HA works as either primary HA (Pri_HA) or proxy HA (Pro_HA) for a MR and each MR has a home address (HoA) configured from either the home network prefix (HNP) or the mobile network prefix (MNP).

Figure 1 shows two communication scenarios (i.e. ATS and AOS) and the aircraft is registered with the HA in Subnetwork B (i.e. Pri_HA in B). Considering the ATS CN communication scenario, packets sent by ATS CN will be intercepted by topologically closest HA (i.e. Pri_HA in B) and will be tunneled to MR via MR-HA tunnel. Considering the AOS CN communication scenario, packets sent by AOS CN are first routed to the topologically closest HA (i.e. Pri_HA in B) and will be tunneled (via the HA-HA tunnel) to the Pri_HA since MR registered to it. When the Pri_HA receives the packet, it first decapsulates the packet and then tunnels the packet to the MR. On the reverse path (from a MNN to the AOS CN), the MR tunnels the packets to Pri_HA, and Pri_HA decapsulates the packets and forwards them to the AOS CN without using a HA-HA tunnel.

Dynamic Home Agent Address Discovery (DHAAD) Procedure.

In [11], mobile nodes use the DHAAD procedure in order to find the topologically closest HA. NEMO [4] extends the DHAAD so that the procedure can be used by MR. DHAAD uses the anycast routing feature which means that the MR sends a DHAAD request message with the HA anycast address as destination address. The topologically closest HA will receive the message and sends a DHAAD reply to the MR with its IP address. Normally the anycast address is specified with a /64 home subnet prefix, however in our case the anycast addresses are constructed with a /32 prefix since our extended home network is using a /32 prefix.

The Home Agent Switch Message.

RFC 5142 provides a new mobility header message which is used for notifying the mobile node about a new home agent assignment. After the MN receives the HA switch message, it should establish a new SA with the new assigned HA before sending the home registration (i.e. BU/BA). However, since we are considering the context transfer of SA from previous HA (pHA) to next HA (nHA) in our scenarios, there is not any need to establish a new SA from MR side.

2.3 Internet Key Exchange

In order to secure mobility signalling between a MN and a HA, IPsec is mandated in [3]. IPsec provides numerous possibilities for confidentiality, data integrity, access control, and data source authentication. These services are provided by maintaining a shared state between the source and the sink of IP datagrams. Establishing such a state manually is not only error prone and tedious, but also not scalable.

Figure 1: Global HAHA Network Architecture
The Internet Key Exchange (IKEv2) protocol [12] is used to create this state dynamically which performs mutual authentication and establishes a Security Association (SA). An SA offers security services to the traffic passed through the SA and needs at least two message exchanges for a successful establishment. The first exchange, IKE-SA_INIT, is responsible for the initialization and negotiates cryptographic algorithms, exchanges nonces and does a Diffie-Hellman (D-H) exchange. With the D-H exchange a shared secret key between the source and the sink is established. Based on this secret the keys for encryption and integrity algorithms are derived. From now on all messages that follow are encrypted and integrity protected (except the outer header). In the following the second message exchange, IKE_AUTH, is performed. This message authenticates the previous communication, exchanges identities and possibly certificates, and creates an IKE-SA and a first CHILD-SA. CHILD-SAs are created for IPsec ESP and/or AH.

In order to approximate the overhead caused by IKEv2/IPsec, we assumed an example configuration, including the IKE (28 Bytes), UDP (16 Bytes), and IPv6 (40 bytes) headers. For the IKE-SA_INIT we assumed the Diffie-Hellman group 2 (16+128 bytes), a nonce length of 136 bytes, a proposal of three encryption variants (56 bytes), a single proposal for the pseudo random function (20 bytes), and a single proposal for the integrity check (20 bytes). For the IKE_AUTH we assumed a fully qualified domain name string for identification (30 bytes), proposals for encryption and integrity (68 bytes), three proposals for a traffic selector initiator range (272 bytes), three proposals for a traffic selector responder range (272 bytes), and an authentication signature of 100 bytes. Further we assumed that AES-CBC 256 (cyclic block cipher, which has a 16 byte initialization vector and a 16 byte aligned payload length) and HMAC_SHA_96 (12 byte integrity check) was selected from the proposal.

For the CHILD-SA, we assumed no new D-H value and one additional proposal for encryption and integrity. Hence we come up with the overhead shown in Table 2 for the IKE initialization phase.

<table>
<thead>
<tr>
<th>Message</th>
<th>Size (Bytes)</th>
</tr>
</thead>
<tbody>
<tr>
<td>IKE-SA_INIT Request</td>
<td>468</td>
</tr>
<tr>
<td>IKE-SA_INIT Response</td>
<td>436</td>
</tr>
<tr>
<td>IKE_AUTH Request</td>
<td>1656</td>
</tr>
<tr>
<td>IKE_AUTH Response</td>
<td>1698</td>
</tr>
<tr>
<td><strong>Total IKEv2 Exchange</strong></td>
<td><strong>4160</strong></td>
</tr>
</tbody>
</table>

### 2.4 Context Transfer Protocol

Reference [13] describes the Context Transfer Protocol (CXTXP) that we used for IKEv2/IPsec context transfer between HAs in the Global HAHA network. The protocol defines the following messages:

- **Context Transfer Activate Request (CTAR):** CTAR is sent by the MN to the target HA (i.e. next HA) for requesting the context transfer activation. It carries an authorization token which authorizes the sender (i.e. MR) to request this operation. In order to calculate the authorization token, the MR and HAs should share a secret key.

- **Context Transfer Activate Acknowledge (CTAA):** This message is sent by the HA to the MR to acknowledge the CTAR message.

- **Context Transfer Data (CTD):** This message is sent by previous HA (i.e. pHA) to nHA that carries the context data. An acknowledgement flag, 'A', included in this message, indicates whether a reply is required by pHA. This message requires IPsec protection.

- **Context Transfer Request (CT-REQ):** This message is sent by nHA to pHA in order to request the start of context transfer (if needed). This message is sent after CTAR message is received.

### 2.5 IPsec Context

The data of interest is stored in the Security Policy Database (SPD) and in the Security Association Database (SAD) [9]. The SPD contains entries (i.e. general policies) which need to be maintained by the operator of the network. Note that these entries need to be the same on all HA within the network. Additionally, the SPD contains selector values in order to support SA management. The selectors used to define the SA must be context transferred [8]. Selector fields are, among others, source and destination address, source and destination port, transport layer protocol, etc. Treatment fields such as sequence numbers, sequence overflow flag, antireplay window, ESP encryption algorithm, etc. are used by the IPsec stack in order to process the incoming data packets properly. All these fields, necessary for the SA, need to be context transferred. The second database is the SAD that contains parameters associated with each (active) security association. Each entry in the SAD is uniquely identified by three parameters: Security Parameter Index (SPI), destination IP address and ESP/AH mode information. It is of utmost importance that the context transfer of an IPsec SA is secured (i.e. assuming already established security tunnels between the previous and the next HA).

#### 3. PROBLEM STATEMENT

As mentioned in Section 2.3, IKE/IPsec SA establishment has a certain impact on the overhead and handover delay in the ATN, and considering Global HAHA network, these procedures have to be repeated in case the MN binds with another HA. Therefore, there is a need to consider CXTXP protocol in order to transfer the IKE/IPsec context from one HA to another, in order to decrease the signalling overhead and delay in the wireless link.

#### 3.1 Number of Home Agent Switches

In a Global HAHA network, one question is how many times a mobile node perform HA switch while it is on the move. In aeronautical environment, we could assume each ICAO region has its own HA which means there will be 22 HAs deployed around world. Among those 22, there will be 2 HAs in Europe; one in Northern Europe and one in Southern Europe. However if we distribute the HAs considering air traffic data volume, then it is probably reasonable to consider more than 2 HAs in Europe, since Europe is one of the densest air traffic regions in the world.

#### 3.2 SPI Collision Problem

In order to transfer the IPsec context from pHA to the nHA, it is necessary to examine all the states concerning the current SA. The authors of [2] identified a SPI collision problem which occurs in case the target node already uses the same SPI for another context (i.e. for another mobile node). In our scenario, HAs exchange SPI information with each other before they assign a new SPI for a new context.
This information is exchanged via HELLO messages defined in the Inter-HAHA protocol [15]. Before assigning a SPI for an SA, HA should inform other HAs and then wait for some time (e.g., one second) in order to be sure that the corresponding SPI is not used by other HAs. Therefore in our case, there is not any need for extending MOBIKE [6] for carrying SPI information since its uniqueness is satisfied by synchronizing SPI assignment among HAs.

### 3.3 Authorization Token Generation

As mentioned in [13], the CTAR message requires the MN and the HA to have a shared secret key to generate the authorization token. In our scenario, we are assuming that the currently registered HA generates the shared secret and sends it to the MR inside a binding acknowledgement message as an option\(^4\). It is also good to mention that the binding registration is IPsec protected, hence the shared secret key can be transferred safely. In addition, during the context transfer, the pHA transfers the shared secret to nHA inside the CTD message, so that the nHA can generate the authorization token as well.

### 4. SOLUTIONS PROPOSED

In this section, we will provide two different context transfer methods: namely network-initiated and node-initiated. The basic operations are shown in Figure 2 and Figure 3.

#### 4.1 Node Initiated Proposal

As shown in Figure 2, the MR configures a new CoA from a newly attached network, and performs a binding registration with the pHA. In the binding update (BU) message, the K bit is set (Key Management Mobility Capability) in order to move the SA to the new care-of address [11]. In parallel, MR starts the DHAAD procedure in order to know whether there is another, topologically closer HA. In case the MR receives a DHAAD response from another HA (i.e., nHA), it initiates context transfer operations by sending a CTAR message to the nHA as shown in Figure 2. This CTAR message is used to trigger the context transfer from the pHA to the nHA. When nHA receives the CTAR, it checks two address fields which are pHA address and MR home address (HoA). Afterwards, it requests the corresponding context and the binding information from pHA via CT-REQ and Binding Information Request messages respectively (MR HoA is used to identify the MR). pHA responds with two messages: CTD message which includes the context and Binding Information Update (BIU) message which includes corresponding MNP information. When context transfer is completed, nHA sends a BU to other HAs in order to inform them about the newly established binding information and a CTAA message to MR. When MR receives CTAA, it starts MOBIKE SA address update procedure in order to change the HA address information (from pHA to nHA) inside the SPD entry.

#### 4.2 Network Initiated Proposal

As shown in Figure 3, the MR performs a layer 3 handover and sends a binding update (BU) to the pHA. Similar to the node initiated proposal, K bit is set for moving the

\[^{4}\text{Here a new option is added to the HELLO message so that SPI is carried with it.}\]

\[^{3}\text{Similar to binding authorization data option in [11].}\]

SA. Since we are assuming that the nHA is topologically closer to the MR, the nHA will intercept the BU and tunnel it to the pHA via HA-HA tunnel. When pHA receives the encapsulated packet, it checks source address of the outer header (i.e., nHA IP address), and realizes that the packet is coming from another HA. In that case, pHA sends a home agent switch message to the MR including nHA address inside it. In parallel, pHA sends the context to nHA via CTD message. When the MR receives the HA switch message, it sends a CTAR message to nHA in order to activate the context. Since nHA already received the CTD message, it does not send a CT-REQ message and it immediately responds with CTAA message to acknowledge the CTAR message. In parallel, nHA sends BIU to other HAs in order to update the binding information. Finally, MR performs a MOBIKE SA Address update in order to update the SPD entry related to HA information.

### 4.3 Overhead and Delay Comparisons

As can be seen from Table 3, context transfer overhead on the wireless link is negligible compared to the new IKE/IPsec SA establishment shown in Table 2. In order to see the capacity gain of the proposed scheme in aeronautical environ-
ment, we have considered a worst case scenario where the peak instantaneous aircraft count (PIAC) number of aircraft [7] (in two different service volumes; namely Enroute (ENR) large and super large) are located within a cell. Here we assume that each aircraft stays within the cell around half an hour, so that T number of aircraft should establish a new SA per minute where T is defined as:

\[
T = \frac{\text{PIAC number of aircraft within a cell}}{30}
\]

(1)

Table 4 shows the overhead comparison of the new SA establishment and proposed context transfer procedure considering the forward and return link capacities that are mentioned as requirement for the FRS in [7]. The proposed method provides around ten times capacity gain both in the forward and return link. In addition, the proposed method’s benefit is seen more clearly in the return link analysis since the new SA establishment uses almost ten percent of the capacity for super large service volume.

<table>
<thead>
<tr>
<th>Table 3: Context Transfer Overhead</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message</td>
</tr>
<tr>
<td>CTCA R Message to aHA</td>
</tr>
<tr>
<td>CTAA Message to MR</td>
</tr>
<tr>
<td>SA Address Update Request</td>
</tr>
<tr>
<td>SA Address Update Response</td>
</tr>
<tr>
<td>Total Exchange</td>
</tr>
</tbody>
</table>

Table 4: Overhead Comparison Depending on PIAC and Link Capacity

<table>
<thead>
<tr>
<th>PIAC</th>
<th>Overhead due to SA establishment (Kbps)</th>
<th>Overhead due to Context Transfer (Kbps)</th>
<th>Capacity Forward Link (Kbps)</th>
<th>Capacity Return Link (Kbps)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ENR Large</td>
<td>1.85</td>
<td>0.14</td>
<td>300</td>
<td>40</td>
</tr>
<tr>
<td>ENR Super Large</td>
<td>4.91</td>
<td>0.14</td>
<td>500</td>
<td>50</td>
</tr>
</tbody>
</table>

Considering delay analysis, both approaches (i.e. node and network initiated) require two round trip time (RTT): one RTT for context transfer exchange and one RTT for MOBIKE SA address update which is the same as the new IKE/IPsec SA establishment. However, in case multiple CHILD_SAs are already created then our proposal will provide better performance since it is always restricted to two RTTs without considering the number of CHILD_SAs. However, in case the new IKE/IPsec establishment, each additional CHILD_SA creation requires one additional RTT (i.e. CREATE_CHILD_SA request/response). Here, we only considered the delay introduced by message exchanges and ignore processing delays due to cryptographic operations.

5. CONCLUSION

In Global HAHA network, establishing a SA every time the MR changes its HA causes not only overhead but also additional handover delay. Therefore, we proposed an IKE/IPsec context transfer mechanism for such networks in order to better utilize the bandwidth constrained links. In the worst case scenario, with our proposal, less than 1 percent of the cell capacity is used in the return link however, with the regular approach almost 5 and 10 percent of the capacity is used for SA establishment for Enroute(ENR) large and super large service volumes respectively. As a future work, we are planning to build a testbed in order to see the performance gain in a real environment. We are also planning to investigate IEEE 802.21 Media Independent Handover (MIH) Information Server (IS) services in order to decrease the handover signalling delay associated with the context transfer mechanism that is presented. By using the MIH IS services, the MR can get the required information about the next access network proactively and perform some parts of the handover and context transfer signalling in advance.

6. REFERENCES