A Handover Authentication Scheme based on Security Associations for NEMO in Aeronautical Telecommunications Network

Jianlong Li\textsuperscript{1,a,*}, Jinchun Gao\textsuperscript{2,b}, Xiaolei Ma\textsuperscript{3,c}, Haiyang Liu\textsuperscript{4,d} and Yuan’an Liu\textsuperscript{5,e,*}  
\textsuperscript{12345}Beijing University of Posts and Telecommunications, Beijing, 100876, China  
\textsuperscript{a}lijianlong_bupt@163.com

Keywords: Network Mobility(NEMO), Handover, Security Associations(SA), Authentication Authorization and Accounting(AAA).

Abstract. As an extension of Mobile IPv6, the NEMO is needed to support session continuity for each mobile network node(MNN) across different access networks in aeronautical telecommunications network(ATN). However, the existing schemes of NEMO don’t mention the authentication issues in handover procedure, which make it unsuitable for the ATN. In this paper, a handover authentication scheme based on security associations(HASA) is proposed for NEMO in ATN environment. HASA authenticates care-of address and prefix separately. The performance analysis shows that HASA not only mitigates the tunneling burden and decrease the handover latency but also provides a higher level of security over NBSP and FMIPv6 .

Introduction

The Internation Civil Aviation Organization(ICAO) adopted IPv6 for use within its future IP-based ATN [1]. The communications in heterogeneous ATN environment includes the packets signaling between cockpit in the airplane and the air traffic controller in the ground, which are time-critical and security-sensitive [2]. The NEMO basic protocol(NBSP) is provided by Internet Engineering Task Force(IETF) to support the session continuity of a whole mobile network when changing the access point of Internet [3]. As an extension of Mobile IPv6, NEMO inherits the disadvantage that all packets have to be routed through the home agent(HA). This causes large latency between the communication peers, especially when the HA is far away from the local area in ATN. In addition, NEMO does not specify how authentication, authorization and accounting(AAA) should be handled in mobile networks, especially for handover procedure. Petrescu [4] described various attacks against NEMO, like traffic hijacking and man in the middle attack. Therefore the confidentiality of the identity and the integrity of the transmission packets are highly desired.

In this paper, we introduce NEMO framework into aeronautical communications and propose a handover authentication scheme based on security associations(HASA) for NEMO in ATN environment. HASA can achieve mutual authentication between MR and its access router(AR) to improve the identity confidentiality. The signaling and transmission packets are protected by the authentication during the handover procedure. In addition, we mitigate the tunneling burden in FMIPv6 [5] and eliminate the suboptimal routing problem in NEMO protocol that all packets between the MNN and correspondent node(CN) are routed through the HA. We simulate the proposed scheme to evaluate the handover delay compared with other schemes. Moreover, we analysis the security resilience and prove HASA can prevent various active and passive attacks .

Related work

NEMO protocol. NEMO provides a mobile network prefix(MNP) for the MR which is never changed in the communications and also a correspondent node prefix(CNP) for the correspondent node. The MNNs that attach to the MR inside the mobile network obtain their addresss from the MNP advertised by the MR. When the aircraft performs handover across different network, the MR moves to a foreign network and attach to an access router. A care-of address(CoA) is assigned to the MR. Then, Binding Update(BU)/Binding Acknowledge(BA) procedure is performed between the MR and HA to inform the fresh location of the MR. Fig. 1 shows the architecture of NEMO in ATN.
As NEMO doesn’t specify how AAA should be handled in mobile network, fewer studies consider the AAA authentication in NEMO environment. Fathi [6] presents a leakage resilient-authenticated key establishment (LR-AKE) scheme to supply authenticate between the MR and LFNs, the MR and its HA, and VMNs and HA or CNs. However, in ATN, HA is always far away from the foreign network, which could enlarge the transmission delay. Lim [7] proposes an authentication scheme that could reduce the authentication time while the computation overhead is high which make it unsuitable in ATN. Chuang [8] integrates LMAM and E-HMIPv6 to decrease the handoff latency, but the existing tunneling burden can increase the packet loss during handover.

The proposed HASA scheme

In this section, we will describe the proposed scheme HASA in detail. The operations of HASA include two parts: macro authentication and micro authentication. When the MR first moves into a new foreign network, HASA performs the macro authentication procedure. It executes the micro authentication if the MR moves within the same foreign domain.

The NEMO based ATN will carry ATS and AOC data. ATN is a closed network, not reachable from the public Internet because of the security-sensitive [9]. When performing prefix authentication in HASA, public-key cryptography with an associated catenary public key infrastructure (PKI) and certificates are used. Fig. 2 shows the single-root based certificate authority (CA) scheme. The sub-CA is signed by neighbor CAs as the flight line of the airplane is fixed. For performing the CoA authentication, a Care-of Test Init/Care-of Test (CoTI/CoT) is chosen to provide the MR with a symmetric key during the handover procedure [10].

Macro authentication. Macro is initiated when a layer-2 trigger occurs. After the RtSolPr and PrRtAdv, MR creates a CoA and sends a fast BU (FBU) message to PAR, which contains $SA_{MR}$, the security association of MR, $CERT_{MR}$, MR’s certificate and $N_{MR}$, a randomly generated nonce. The FBU is signed by the private key of the MR. Fig. 3 shows the macro authentication signaling. Then, PAR sends a handover initiate (HI) to NAR. After that, NAR and LAAA exchanges the CoTI/CoT to authenticate the CoA of the MR. LAAA generates the symmetric care-of test key $k_{MR}$ in the following way:

$$k_{MR} = H(N_{MR} | CoA | S'_C).$$ (1)

And $S'_C$ refers to a secret key only know to LAAA and has a limited lifetime. $I_S$ in CoT message points out the key i which is used to generate $k_{MR}$. On receiving the CoT message, NAR generates $k_{SK}$ to secure the transmission of $k_{MR}$ based on the formula (2):

$$k_{SK} = H(N_{NAR} | N_{MR} | RPI).$$ (2)

Replay protection indicator (RPI) means the ID or timestamp of NAR. The signature message $SM_1$ signed by $k_{SK}$ contains $CERT_{NAR}$, $SA_{NAR}$ and $k_{MR}$ . NAR then sends Hack message to PAR and PAR
transfer FBack to MR. MR can regenerate $k_{SK}$ by formula (2) and then receive $k_{MR}$ and MR proves to be the owner of this address. The authentication of CoA is done.

The next step is BU/BA message to authenticate MNP. $A_{MR}$ and $A_{LAAA}$ refers to the cryptographic algorithms support by MR/LAAA. The signature message $SM_2$ is calculated with the private key of MR $k^{PRIV}_{MR}$. On receiving the BU message, LAAA verifies the legality owner of the BU by regenerate $k_{MR}$ based on the formula (1) : $N_{MR}$ is contained in BU, $CoA$ is the source address of BU and $I_3$ point out the accurate $S'$ in the previous procedure of generating $k_{MR}$. Therefore LAAA does not need to keep any information in the CoTI/CoT message exchange. LAAA verify the MNP by $SM_2$. If the CERT$_{MR}$ is valid according to the root CA of catenary PKI and the public key $k^{PUB}_{MR}$ from certificate can be used to verify the $SM_2$ appended to BU, LAAA could make sure the legal owner of the MNP.

LAAA then generates a random, symmetric home key $k_{SH}$ and sends a BA to MR. CERT$_{LAAA}$ includes the certificate of local AAA and CNP refers to local correspondent node prefix. $SM_3$ which claims the legal owner of CNP, is calculated with the private key of LAAA $k^{PRIV}_{LAAA}$. The key $k_{SH}$ is signed by $k_{MR}$ and the BA message is signed by the private key of LAAA. On receiving the BA, MR verifies CERT$_{LAAA}$ according to the root CA and $SM_3$ by the public key in CERT$_{LAAA}$. MR stores the $k_{SH}$ permanently and the macro authentication is completed.

**Micro authentication.** HASA performs the micro authentication if the MR moves within the same foreign domain. Fig. 4 shows the signaling of Micro authentication after a handover has occured. The NAR executes CoTI/CoT just like the procedure in Macro to authentication the CoA and get the $k_{MR}$. Then HI and Hack message are exchanged between NAR and MR3 to get $N_{MR3}$, $SA_{MR3}$, CERT$_{MR3}$. NAR generates the $k_{SK}$ in the following way:

$$k_{SK} = H(N_{MR3} | N_{MR} | RPI).$$  (3)

$SM_1$ here signed by $k_{SK}$ contains CERT$_{MR3}$, $SA_{MR3}$ and $k_{MR}$. Then NAR sends FBack message back to MR signed by the private key of NAR and the CoA authentication is done.

As the MNP is fixed during the handover, the MNP authentication in Micro is not the same as that in Macro. The symmetric home key $k_{SH}$ now is used as a session to generate key $k_5$ as follows :

$$k_5 = H(k_{MR} | k_{SH}).$$  (4)

The new key $k_5$ is used to calculate the signature message $SM_2$ in $A_{LAAA}$ attached to BU. And the BU message doesn’t contain any certificate or signature because the MNP has been authorized in Macro. If LAAA could verify the $SM_2$, the new CoA of the MR is proved to be legal and a BA message will be sent back to MR. The prefix authentication procedure is done.

**Simulation and analysis**

Security analysis of HASA. Before the analysis, we suppose the key length is robust for the system and the one-way hash function is irreversible which means that it is easy to figure $H(x)$ when the value
of $x$ is given, while given the value of $H(x)$, computing $x$ is very difficult [8]. We compare the security feature of HASA with LR-AKE scheme, SeNERO scheme in Table 1.

(1) Mutual authentication: In HASA, the MR authenticates its prefix to LAAA, the LAAA also proves to be the legal owner by verifying signature message in BA. This avoids an adversary to masquerade as a legitimate LAAA and hijack the prefix and packets will not be redirected to the illegal prefix.

(2) Tunneling burden: In MIPv6, a tunnel is established between NAR and PAR during handover and the packets destined to MR will be stored in or via the tunnel. It will cause the tunneling burden and packet loss because of the limited space of the tunnel. In HASA, after the CoTI/CoT, the packets from NAR to MR could be first forwarded to LAAA and then delivered to MR according to the CoA, which will mitigate the tunneling burden.

(3) Local authentication: In ATN communication, if the aircraft is far away from the home network, starting in China and ending in Europe, the large geographical distance will lead to unreachable of the HA. HASA performs local authentication without the participation of the HA. The authentication procedure in foreign domain doesn’t need to exchange signaling with HA.

(4) Modified attack resistance: The one-way hash function in HASA to generate different keys make sure that information cannot be modified. The RPI in the procedure could also record the ID or timestamp of the authentication. Therefore, a malicious modified packet will be easily identified by verifying the hash values.

(5) Replay attack resistance: The random number has a fresh lifetime in macro and micro authentication. It is difficult for hijacker to get the accurate value. Therefore, the proposed scheme has a nice performance when it comes to replay attack resistance because of the random number.

### Table 1 Comparasion of security feature

<table>
<thead>
<tr>
<th>Feature</th>
<th>HASA</th>
<th>SeNERO</th>
<th>LR-AKE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mutual authentication</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Tunneling burden</td>
<td>Yes</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>Local authentication</td>
<td>Yes</td>
<td>Yes</td>
<td>No</td>
</tr>
<tr>
<td>Modified attack resistance</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Replay attack resistance</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

**Handover delay of HASA.** We define the handover delay as the time interval between the moment that the layer-2 trigger is initiated and the moment that MR receive the first BA message in foreign network. Table 2 shows the parameter values used in analysis based on [8]. The authentication delays of NEMO, LR-AKE and HASA are calculated as follows:

### Table 2 System parameters used for analysis

<table>
<thead>
<tr>
<th>Time(ms)</th>
<th>$T_{L2}$</th>
<th>$T_{DAD}$</th>
<th>$T_{MR-LAAA}$</th>
<th>$T_{MR-HA}$</th>
<th>$T_{MR-AR}$</th>
<th>$T_{HR-LAAA}$</th>
<th>$T_{HR-HA}$</th>
<th>$T_{HR-AR}$</th>
<th>$T_{Min}$</th>
<th>$T_{Max}$</th>
<th>$T_{AUTH}$</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>50</td>
<td>1000</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
<td>10</td>
</tr>
</tbody>
</table>

**Fig. 5 The performance of authentication delay**

$$T_{AD}^{NEMO} = 2T_{MR-AR} + 2T_{AR-LAAA} + 2T_{HAHA-LAAA} = 4a + 2c + 2d + 2kb$$

$$T_{AD}^{LR-AKE} = 5T_{MR-AR} + 5T_{AR-HA} + 2T_{HAHA-HA} + 4T_{HAHA-LAAA} = 10a + 5c + 5d + 9kb$$

In HASA, the authentication delay is divided into macro $T_{AD}^{HASA-Macro}$ and micro $T_{AD}^{HASA-Micro}$:

$$T_{AD}^{HASA-Macro} = 2T_{MR-AR} + 4T_{HAHA-AR} + 2T_{MR-LAAA} = 2a + 4c + 2d$$

$$T_{AD}^{HASA-Micro} = 2T_{MR-AR} + 2T_{AR-LAAA} = 2a + 2c + 2d$$
\[ T_{\text{HA-SA-Micro}}^{AD} = 2T_{\text{MR-AR}} + 2T_{\text{MR-I-AAA}} = 2a + 2d \] (8)

Fig. 5 shows the simulation result of authentication for different distances between the home domain and local domain. The authentication delay of HASA keeps the same and is lower than NEMO and LR-AKE. However, NEMO and LR-AKE increases sharply when the distance from home to local is getting farther. In Micro, the prefix doesn’t need to be authenticated again because it has been done in Macro, which makes HASA achieves a better result.

**Summary**

In this paper, an authentication scheme HASA is presented for NEMO in ATN, that authenticates the identity of the MR based on security associations during handover procedure to improve the confidentiality and integrity in ATN. The CoA and MNP are authenticated separately. In addition, HASA can eliminate the tunneling burden of FMIPv6 which reduce packets loss and authentication delay. The analysis and simulation result show that the handover performance of the proposed authentication scheme can significantly outperforms those of NBSP and LR-AKE in mobile network.

**Acknowledgement**

This work was supported by the National Natural Science Foundation of China (No.61272518) and 2013RC0208 research of the information access technology for complex information system.

**References**


