CRYPTRON: CRYptographic Prefixes for Route Optimization in NEMO

Ana Kukec *, Marcelo Bagnulo† and Antonio de la Oliva†
*University of Zagreb
Email: anchie@fer.hr
†Departamento de Ingeniería Telemática, Universidad Carlos III de Madrid, Spain
Email: marcelo,aoliva@it.uc3m.es

***Abstract*— The aviation community is in the process of designing the next generation Aeronautical Telecommunications Network (ATN), based on Internet standards, to provide air-ground communications for the aircraft. Support for mobile networks in the current Internet architecture is provided by the NEtwork Mobility (NEMO) protocol. As currently defined, NEMO Basic Support protocol lacks of Route Optimization support which is an essential requirement for its adoption as part of the next generation ATN. This paper presents a novel security tool, the Crypto Prefixes, and their application to the Route Optimization in Nemo (CRYPTRON). The Crypto Prefixes are IPv6 prefixes with embedded cryptographic information that enable the Mobile Network Prefix proof-of ownership without any centralized trust infrastructure. In CRYPTRON, the Crypto Prefixes are used to protect the establishment of the bindings on the Correspondent Nodes for the whole Mobile Network Prefix.**

I. Introduction

The aviation community is on the process of defining the next generation of the Aeronautical Telecommunications Network (ATN). The ATN is the network used to provide air-ground and ground-ground communication services for the aviation. While the current ATN is based on a modified version of the Inter-Domain Routing Protocol and the ISO CLNP protocol for the support of aircraft mobility [1], the next generation ATN will be based in IETF protocols. In particular, the International Civil Aviation Organization (ICAO) is proposing the use of IPv6 for data communications and Mobile IPv6 (MIPv6) [2] to support aircraft mobility [3]. MIPv6 supports network mobility through the NEMO extensions [4]. However, the current NEMO specification lacks some features required for the aviation scenario. In particular, as opposed to MIPv6, NEMO lacks of route optimization (RO) support to enable direct communication between the nodes in the mobile network and their communicating peers located in the fixed infrastructure. The Internet community has acknowledged the problem and the work on solutions has been chartered in the Mobility EXTensions working group (MEXT)[1] in the Internet Engineering Task force (IETF).

The objective of this paper is twofold, first we propose a novel security tool, the Crypto Prefixes. And second we present a Route Optimization solution based on Crypto Prefixes which is especially well suited for the aeronautical requirements. Crypto Prefixes are IPv6 prefixes that contain embedded cryptographic information, namely, a hash of a public key. The Crypto Prefix has notable properties that are suitable for securing the route optimization procedure. The basic idea is that thanks to their cryptographic nature, it is possible to prove the prefix ownership without requiring additional infrastructure. By using the Crypto Prefixes, the proposed NEMO extensions can securely establish a direct route between the mobile network and the communicating peers located in the fixed infrastructure.

The paper is structured as follows. Some background about the NEMO protocol is presented in Section II. Section III provides an overview of the proposed mechanism, which is explained in more detail in Sections III-A (Crypto Prefixes) and III-C (CRYPTRON Operation). Section IV evaluates our solution against the NEMO RO requirements. In Section V, we explore alternatives for NEMO RO and compare them to our approach. Finally, Section VI concludes the paper.

II. Network Mobility (NEMO) protocol Overview

The Network Mobility protocol as defined in [4] has been designed to provide support for moving networks in the Internet. It is a general tool that is well fitted for most common scenarios. It has been defined as an extension to Mobile IP [2] in order to perform bindings between prefixes assigned to the mobile network (called Mobile Network Prefixes) and the current location of the Mobile Router (MR) that provides access to the mobile network. In the general NEMO scenario, Mobile Network Nodes (MNN) configure an address from the Mobile Network Prefix, obtaining Internet connectivity from the MR. The Mobile Network Prefix is part of the Home Network Prefix, which is announced to the Internet through the ISP of the Home Network. This means that packets addressed to the mobile network will be routed to the Home Network. In the case that the mobile network is roaming, the MR will inform the HA about its current location by means of the Binding Update (BU) message which contains the Care-off Address i.e. the topologically correct address obtained by the MR in its current location. Upon the reception of the BU message, the HA will create a binding for the Mobile Network Prefix and the CoA. From then on the HA will forward packets addressed to the mobile network to the current MR's CoA.

The work of Marcelo Bagnulo is partly supported by Catedra Telefonica en Internet del Futuro para la Productividad of the University Carlos III de Madrid. The work of Antonio de la Oliva is supported by the European Community's FP7 under grant agreement 214994 (CARMEN project)

[1]http://www.ietf.org/html.charters/mext-charter.html

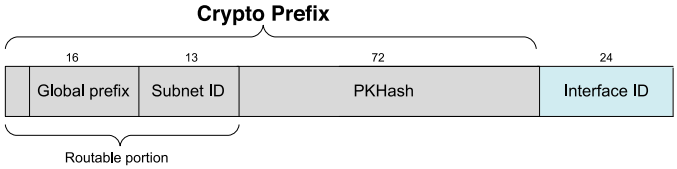

Fig. 1. CGPA: Cryptographically Generated Prefix Address

III. CRYPTRON: CRYPTOGRAPHIC PREFIXES FOR ROUTE OPTIMIZATION IN NEMO

In this paper we propose a novel security tool, the Crypto Prefixes and its application to NEMO Route Optimization. The Cryptographic Prefix (Crypto prefix) is a security tool that enables to prove the ownership of the prefix. The Crypto Prefix binds a public component of a public-private key pair to IPv6 network prefix. The binding is created by embedding the hash information of a public key in the prefix itself. The Crypto Prefix then allows the private key holder to claim the prefix ownership by proving its knowledge of the corresponding private key. The ability of the Crypto Prefixes to provide proof-of ownership of a prefix makes them specially suited for securing the communication between CNs and MNNs in network mobility scenario. Hence, in this paper, we also present the application of the Crypto Prefixes to the Route Optimization problem in NEMO. CRYPTRON (CRYptographic Prefixes for Route Optimization in NEMO) is a new approach to provide route optimization for mobile networks. The main innovation of CRYPTRON is that it provides high-level security for the route optimization operations without requiring any infrastructure, this makes CRYPTRON specially suited for aeronautical applications. In the following sections we present the Crypto Prefix tool along with its security analysis. Afterwards the CRYPTRON solution is described in detail.

A. Crypto Prefixes

Crypto Prefixes are IPv6 prefixes containing embedded cryptographic information. They are 104 bits long prefixes and their format is depicted in figure 1. The *PKHash* parameter is generated as the output of a one-way hash function computed over the set of parameters called the Crypto Prefix Parameters. The Crypto Prefix Parameters are defined as the concatenation of the public key (K_m) and the random value:

$$\textit{Crypto Prefix parameters:} K_m | RV$$

The 72-bit long PKHash is then generated as:

$$\textit{PKHash = H(Crypto\_Prefix\_parameters)}$$

Crypto Prefixes consist of a routable portion (the Global Prefix and Subnet ID) and the *PKHash*. The routable portion is topologically significant, hierarchically-structured and aggregatable part of the address. The Subnet ID is 13-bits long allowing for each mobile network that is configured with a Crypto Prefix to have 2^{13} (8192) subnetworks. This is in the same order than current address allocation policies that assign a /48 per end-site supporting 2^{16} subnetworks per site. Contrary to the routable portion, *PKHash* is topologically insignificant, it acts as a network identifier, and thus recedes route aggregation, but at the same time, it provides a possibility to prove prefix ownership as described in section III-C. End host addresses containing the Crypto Prefix are formed by concatenating the Crypto Prefix and a 24 bit long interface identifier (figure 1). The interface identifier is chosen randomly and unique within each subnetwork of the Crypto Prefix. We will denote the IPv6 address built in the way described in this section as Cryptographically Generated Prefix Address (CGPA).

B. Security analysis for the Crypto Prefixes

This section is devoted to the security analysis of the Crypto Prefixes. We assess the security robustness of the Crypto Prefixes by analyzing the impact of the birthday, brute-force and pre-computed dictionary attacks on Crypto Prefixes. We also prove the trustworthiness of our authentication mechanism by applying BAN logic, which can be found in the appendix. Regarding the birthday attack, one must define the probability that two random selections result in the same hash value. In our case, we define the probability that two different users generate the same hash value from two different public keys. In order to quantify the probability, we take into account the birthday paradox [5]. In order to assess the suitability of the selected hash length for statistical uniqueness, we contrast the selected hash length with the number of expected mobile networks that will use Crypto Prefixes. However, since it is very hard to predict the actual number of mobile networks some years ahead, we will take a very conservative approach and compare it to a very clear upper bound. In particular we consider a scenario where every node obtains a Crypto Prefix and evaluates the collision probability. If all nodes in the current Internet ($6 * 10^8$ hosts according to ISC Internet Domain Survey data about current number of hosts[2]) obtained a Crypto Prefix, the collision probability for 72-bit hash will be $p = 3,81 * 10^{-05}$. This probability is in the same order of magnitude as the probability of the core melt for a modern nuclear reactor ($p = 1 * 10^{-05}$ according to [6]).
Either to perform the brute-force attack or the pre-computed attack, an attacker needs more then 30 years to attack the 72-bit hash value. The successful brute-force attack on Crypto Prefix requires $O(2^{72})$ calculations of the *PKHash*. In each iteration an attacker hashes 144 bytes (the 1024-bit public key and the 128-bit random value). According to `openssl speed`, a computer with a Pentium(R) III CPU family (1266MHz) processor and 1GB of RAM hashes 25177 kB per second, when doing SHA1 for 3s on 64B size blocks. In order to perform brute-force attack, an attacker would spend more then $8 * 10^8$ years hashing all the possible inputs.
In the pre-computed dictionary attack, an attacker pre-computes a list of dictionary words, in our case Crypto Prefixes. The preparation requires a considerable amount of the preparation time, but accelerates the actual attack. However, the storage requirements for all the pre-computed values are incredibly high. Taking into account that the *PKHash* is 72 bits long, and the length of the rest of the Crypto Prefix is 32 bits, the dictionary would consist of $2^{72} * 2^{32}$ entries, i.e.

[2]https://www.isc.org/solutions/survey

$2.45*10^{23}$ GB. In case of the 1 GB SDRAM memory modules (6.2 cm x 2.3 cm x 0.2 cm) an attacker needs $7*10^{17}m^3$, or $7.13*10^9$ Empire State Buildings (260000 m^2 x 381 m) to store all the memory modules.

C. CRYPTRON Operation

In this section we present the process of securing NEMO Route Optimization with Crypto Prefixes in detail, starting from the initialization of the Mobile Network, the movement to a foreign link, the secured Binding Update sent from a foreign link, the verification performed by the Correspondent Node (CN) and the handover in case of the subsequent movements. During the initialization process, a /19 prefix is assigned to the Home Network. For each Mobile Network, a /104 mobile prefix is generated, following the procedure described in section III-A. The Crypto Prefix is assigned to the Mobile Network and the Mobile Router is provisioned with the Private Key and Crypto Parameters associated to the Crypto Prefix assigned to that mobile network. Mobile Network Nodes obtain their permanent addresses from the Crypto Prefix so all the mobility procedures are transparent to them. In addition, the Mobile Router configures its Home Address (MR_HoA). When the mobile network moves away from home, the Mobile Router obtains a new, topologically correct Care-of address, MR_CoA. The Mobile Router informs the HA about its new Care-of Address (MR_CoA) in the Binding Update message. As a consequent of the Binding Update message, the Mobile Router and the Home Agent set up the IP-in-IP tunnel between them, secured with IPsec. After that, the communications initiated by the Mobile Network Node with a Correspondent Node flow through the Mobile Router and the Home Agent to the Correspondent Node.

Since the routing in the case of a communication between the Mobile Network Node and the Correspondent Node through the Home Agent is suboptimal, the Mobile Router decides at some point to trigger the Route Optimization procedure, i.e. to send packets directly to CN. Thus, it sends the Binding Update message, containing the Mobile Network Prefix and the MR_CoA, secured by the Crypto Prefix to the Correspondent Node (figure 2).

The Binding Update message is secured with the Crypto Prefix mechanism by introducing two new options for the Binding Update message:

- Crypto Prefix Signature (CPS) option: it is used to carry a signature computed over the Mobile Router's Care-of Address (A_M), Correspondent Node's address (A_C) and the Mobility Header (MH) in the Binding Update message using the private key associated to the Crypto Prefix (K_m^{-1}):

$$\textit{CPS option} = H(A_M, A_{CN}, MH, RV)K_m^{-1}$$

- Crypto Prefix Parameters (CPP) option: which contains the public key (K_m) corresponding to the *PKHash* and the random value *RV* used to compute the *PKHash*:

$$\textit{CPP option} = K_m|RV$$

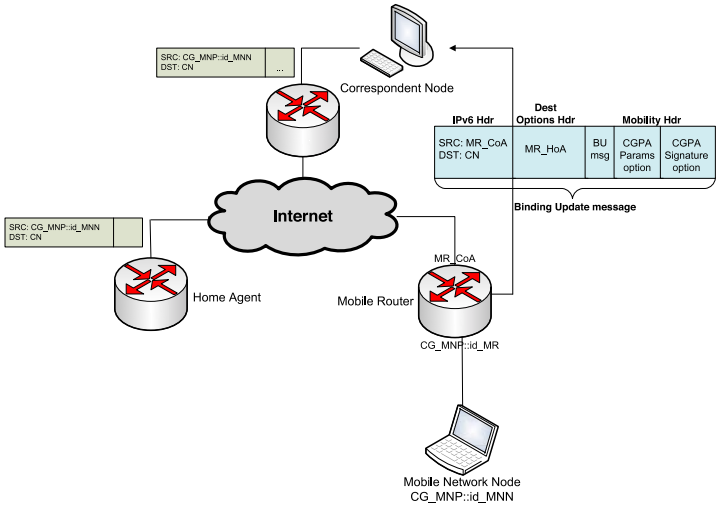

Fig. 2. NEMO Route Optimization with Crypto Prefix protected Binding Update message

This yields the CRYPTRON message:

$$MR \rightarrow CN : A_M, A_{CN}, MH, RV, H(A_M, A_{CN}, MH, RV)K_m^{-1}$$

These options allow securing the BU messages from the MR to the CN. The basic idea is that the MR will convey the following three elements to the receiver along with the BU: i) the Crypto Prefix, ii) the associated Crypto Prefix Parameters and iii) a Crypto Prefix Signature. The receiver validates the BU performing a set of verifications; First, it computes the hash of the public key and random value contained in the CPP option and compares it to the Crypto Prefix in the received Binding Update message. Second, after the verification of the Crypto Prefix, the verifier checks the signature in the Crypto Prefix Signature option. For that, it computes the cryptographic hash over the Mobile Router's Care-of Address, its own address and the mobility header, and verifies the signature of the hash using the public key K_M received in the CPP option. In case of the successful verification, the sender proves that it is the owner of the Crypto Prefix.

The trust chain is then as follows: The Crypto Prefix is bound to the public key (K_M) through the hash ($PKHash$). The public key is inherently bound to the private key (K_m^{-1}). The private key is bound to the Signature option, since only the private key holder can generate it. Then there is a trust chain between the holder of the private key and the Crypto Prefix, hence the receiver can validate that the sender is the owner of the prefix. A formal derivation, using BAN logic, of the CRYPTRON trust chain can be found in the appendix.

After the Correspondent Node verifies the BU message, it creates the binding for the Mobile Network Prefix and replies to the Mobile Router with the Binding Acknowledgement (BA) message. After reception of the BA, the Mobile Router is ready to send data packets directly to the Correspondent Node through the optimized path. Data packets from the Mobile Network Node, are sent through the Mobile Router to the Correspondent Node. They contain the HoA Destination option defined by MIPv6 carrying the MR-HoA. Upon the reception of the packets by the CN, it replaces the source

address from the packet (MR_CoA) with the Mobile Router's Home Address (MR_HoA), since the upper layer protocols are aware only of the Mobile Router's Home Address. In the opposite direction, when the Correspondent Node sends a packet to the Mobile Network Node, it adds the MR_HoA address into the routing header, hiding the use of topologically correct MR_CoA from the upper layers.

IV. Evaluation

In order to evaluate our proposal, we will contrast CRYPTRON against the requirements defined by the aviation community for the NEMO route optimization support for the next generation ATN. The requirements of a Route Optimization (RO) solution for NEMO, as specified in [7] [8], are the following:

- Flow separability; The local policy must be able to decide which traffic flows through the optimized path and which traffic flows through the HA path, providing flow granularity for optimization decision. CRYPTRON can easily satisfy the separability requirement for different traffic flows by adding the local policy database within the Mobile Router.
- Multihoming; A Route Optimization solution must support a multi-interfaced MR and must allow a domain to be bound to a specific interface. CRYPTRON satisfies the multihoming requirement since it is possible to apply it to the multi-interfaced Mobile Routers with bindings of its different MR_CoA addresses to the Crypto Mobile Network Prefix.
- Latency and Availability; This requirement imposes that the Route Optimization solution must not add any extra delay in the transfer of data, hence the MR must be able to keep on using the non-optimized path while it is setting up the optimized one. As described in section III-C, CRYPTRON supports the NEMO Basic Support protocol and allows for the use of the tunnel between the Mobile Router and the Home Agent (MRHA tunnel) in the process of Home Network initialization, or reconfiguration, hence supporting the latency requirement. Additionally, our solution supports the Mobile Router to fall-back to the MRHA tunnel in case of any failure, and thus satisfies the availability requirement as defined in the requirements document.
- Packet Loss; The use of a Route Optimization solution should not incur in a higher loss or duplication of data than the use of the NEMO basic support. CRYPTRON prevents from the additional packet loss caused by the Route Optimization mechanism. The Binding Update message has to be followed by the Binding Acknowledgment, and if that is not the case, the Mobile Router continues to use the MRHA tunnel, so no packets are lost during the setting of the optimized path.
- Scalability and Efficient Signaling; The Route Optimization solution must be able to scale to hundreds of thousands mobile nodes without overloading the ground network, it must also be efficient in the signaling part, in terms of number of packets and their size. CRYPTRON solution is also in accordance with the scalability requirement and efficient signaling requirements, since one of its goals is to reduce the signaling overhead to only one round trip (the Binding Update message and the Binding Acknowledgment message) and the signaling message size by the use of the Crypto Prefix tool. In particular, each BU message will create a binding for the whole prefix of the mobile network, resulting in efficient signaling. In addition, CRYPTRON, has no impact whatsoever in the global routing system (i.e. no routes are injected though BGP as the result from movement). Thus, our solution minimizes the overload of the ground network and the routing system.
- Security and Adaptability; Because of the cryptographic nature of Crypto Mobile Network Prefixes, the CRYPTRON solution automatically supports the security requirements, e.g. the proof of ownership of the MR_CoA address. Additionally, CRYPTRON satisfies the security requirement in the optimized way, since with the Crypto Prefix tool protects the whole mobile network, and not just a particular Mobile Network Node. In addition, CRYPTRON is transparent to the upper layer protocols, providing the possibility to use new transport protocols (IPsec or new IP options within it) and thus satisfies the adaptability requirement.

The Crypto Prefix also satisfies additional desirable characteristics defined by the aviation community for NEMO Route Optimization solutions: i) CRYPTRON allows the protection of the binding establishment without increasing the configuration complexity on Correspondent Nodes and ii) it does not require any trust infrastructure and process of prefix proof-of ownership is self-adjusting from the Correspondent Node's point of view. Similarly, since the Mobile Router provides NEMO Route Optimization feature on behalf of the Mobile Network Nodes, our solution does not increase the configuration complexity of the Mobile Network Nodes.
At the end, CRYPTRON is a general solution for securing the binding establishment between the Mobile Router's Care-of Address and Mobile Network on each Correspondent Node, and can be applied to any other context, outside of aeronautics and space exploration.

V. Comparison with other proposals

With the current NEMO Basic Support, all the communication between the Mobile Network and the CN goes through the bidirectional tunnel between the MR and the HA. When the Mobile Network is not at home, this result in sub-optimal routing, increased packet delay, congestion in the Home Network and increased packet overhead in the MRHA tunnel. In order to solve these problems, different partial NEMO RO solutions were offered, with focus on different problems. In the following lines we present the advantages of CRYPTRON over the most relevant RO proposals being developed at the moment:

- CRYPTRON is more efficient in terms of number of signaling messages and handover delay than solutions based on extending the Return Routability Procedure of MIPv6 such as [9] and [10]. Since the Mobile Network is

self-authenticated through the Crypto Prefix mechanism, CRYPTRON avoids the need for the Home Address Test, as a protection from the hijacking attacks, and thus reduces the number of signaling messages and the handover delay.
- CRYPTRON is more efficient in terms of packet overhead than solutions which use extra-tunnels to provide routing between the CN and MNN such as the NEMO Basic protocol and RO proposals [11] and [12].
- By proving the possession of the private key, the MR using CRYPTRON is automatically delegated for signaling right to authenticate BUs, which solves both the identity attacks and location attacks, contrary to [10].
- Contrary to our proposal, some NEMO RO mechanisms are based on the prefix delegation [13] [14] and increase the complexity of other protocols (e.g. Neighbor Discovery) or other network elements (e.g. the access router).
- The suggested proposal does not require any centralized trust infrastructure (PKI), contrary to other proposals [15].

VI. Conclusion

This paper proposes a novel security tool, the Crypto Prefixes. Crypto Prefixes are 104-bit IPv6 prefixes which consist of the routable portion and a cryptographic portion, allowing the proof-of ownership of a given prefix. This paper also presents the application of the Crypto Prefix to the Route Optimization problem in mobile networks (CRYPTRON). The cryptographic nature of the Crypto Prefix allows the prefix proof-of ownership to the whole mobile network, in the way transparent to the Mobile Network Nodes. CRYPTRON is a scalable solution, since it ensures the required trust between the Correspondent Node and the whole mobile network, and it does not depend on other infrastructures, since the process of the secure binding establishment does not require any centralized trust infrastructure. It also reduces the handover latency by avoiding the need for the part of the Return Routability procedure - Home Address Test. We have contrasted the proposed solution to the requirements defined by the aviation community for the support of network mobility in the next generation ATN and we have verified that CRYPTRON is perfectly suited for the proposed scenario, providing high level security and reduced deployment costs.

Appendix: BAN analysis of CRYPTRON

We will use BAN logic [16] statements over principals CN (correspondent node), MR (mobile router) and MNN (mobile network node), and encryption keys K_m (MR's public key) and K_m^{-1} in order to evaluate the proposed authentication mechanism, CRYPTRON. In the BAN logic, principal starts with the initial belief in at least one key. In our case, CN *b*elieves that MR *o*wns K_m as a public key:

$$CN \models \stackrel{K_m}{\rightarrow} MR \textit{ (Assumption 1)}$$

The next assumption we make is that the random value RV is fresh, since RV is a nonce and it has not been used at any time before the current binding update message:

$$CN \models \#(RV) \textit{ (Assumption 2)}$$

The goal of the CRYPTRON is to ensure the statement "CN *believes* MR *believes* A_M to be MR's Care-of Address with associated mobile network prefix stored in the mobility header (MH)". Besides, CRYPTRON ensures that "CN *believes* MNN" based on MR's jurisdiction over the mobile network:

$$CN \models MR \models A_M, MH \text{ and } CN \models MNN \textit{ (Goal)}$$

The CRYPTRON message:

$$MR \rightarrow CN : A_M, A_{CN}, MH, RV, \{H(A_M, A_{CN}, MH, RV)\}K_m^{-1}$$

Together with the message-meaning rule, the nonce-verification rule and the jurisdiction rule this yields:

$$CN \triangleleft H(A_M, A_{CN}, MH, RV)$$
$$CN \models MR \mid\sim H(A_M, A_{CN}, MH, RV)$$
$$CN \models MR \models (A_M, A_{CN}, MH, RV),\ i.e.\ CN \models A_M, MH$$
$$CN \models MR \models> MNN, CN \models MR \models MNN,\ i.e.\ CN \models MNN$$

References

[1] ICAO, "Manual of Technical Provisions for the Aeronautical Telecommunications Network (ATN)," May 2002, third Edition.

[2] D. Johnson, C. Perkins, and J. Arkko, "Mobility Support in IPv6," RFC 3775, June 2004.

[3] ICAO, "Document 9896, Manual for the ATN using IPS Standards and Protocols," May 2008, work in progress.

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

[5] B. Schneier, "Applied Cryptography," 1996, second edition, John Wiley & Sons.

[6] N. E. Agency, "Externalities and Energy Policy: The Life Cycle Analysis Approach," 2001, OECD, Workshop Proceedings, Paris.

[7] W. Eddy, W. Ivancic, and T. Davis, "NEMO Route Optimization requirements for Operatinal Use in Aeronautics and Space Exploration Mobile Networks," IETF Draft, Jan. 2009. [Online]. Available: http://www.ietf.org/internet-drafts/draft-ietf-mext-aero-reqs-03.txt

[8] C. Bernardos and M. Bagnulo, "Analysis on how to address NEMO RO for Aeronautics Mobile Networks," IETF Draft, Nov. 2008. [Online]. Available: http://www.ietf.org/internet-drafts/draft-bernardos-mext-aero-nemo-ro-sol-analysis-01.txt

[9] C. Ng and J. Hirano, "Extending Return Routability Procedure for Network Prefix (RRNP)," IETF Draft, Oct. 2004. [Online]. Available: http://tools.ietf.org/html/draft-ng-nemo-rrnp-00

[10] M. Calderon, C. Bernardos, M. Bagnulo, and I. Soto, "Securing the Route Optimization in NEMO," 2005, proc. of WIOPT.

[11] R. Wakikava, S. Koshiba, K. Uehara, and J. Murai, "ORC: Optimized Route Cache Management Protocol for Network Mobility," 2003, 10th International Conference on Telecommunications, ICTEL.

[12] J. Na, S. Cho, C. Kim, S. Lee, H. Kang, and C. Koo, "Route Optimization schemene based on Path Control Header," IETF Draft, 2004. [Online]. Available: http://draft-na-NEMO-path-control-header-00

[13] K. Lee and et al., "Route Optimization for Mobile Nodes in Mobile Network based on Prefix Delegation," IETF Draft, 2003. [Online]. Available: http://www-users.cs.umn.edu/~jjeong/publications/ietf-internet-draft/draft-leekj-nemo-ro-pd-00.txt

[14] J. Song, S. Han, and K. Park, "Route Optimization in NEMO Environment with Limited Prefix Delegation Mechanism," 2009, iCSS.

[15] F. Bao, R. Deng, Y. Qiu, and J. Zhou, "Certificate-based binding update protocol (CBU)," IETF Draft, 2005. [Online]. Available: http://www.join.uni-muenster.de/Dokumente/drafts/draft-qiu-mip6-certificated-binding-update-03.txt

[16] M. Burrows, M. Abadi, and R. Needham, "A logic of Authentication," 1989, proc. of the Royal Society of London Series A, 426, pp. 233 - 271.