Securing Route Optimisation in NEMO

María Calderón, Carlos J. Bernardos, Marcelo Bagnulo and Ignacio Soto
University Carlos III of Madrid
Avda. Universidad 30, 28911 Leganés, Madrid, SPAIN
E-mail: {maria, cjbc, marcelo, isoto}@it.uc3m.es

Abstract

The Network Mobility (NEMO) Basic Support protocol enables mobile networks to change their point of attachment to the Internet, while preserving established sessions of the nodes within the mobile network. When only a non-nested mobile network is considered, the so-called triangle routing is the main problem that should be faced. In Mobile IPv6, the Route Optimisation mechanism solves this problem, and the Return Routability mechanism aims to limit the security concerns originated because of the Route Optimisation. Nowadays Return Routability is considered a weak solution (i.e., based on strong assumptions). In this article we explore different approaches to Route Optimisation in NEMO and we devise how to adapt some of the Terminal Mobility solutions to a NEMO environment, where, as we will propose, a delegation of signalling rights from the Mobile Network Node to the Mobile Router is necessary.

1 Introduction and Problem statement

We are witnessing how the demand for Internet access in mobile platforms such as trains, buses and ships is constantly increasing. In order to satisfy such demands, the technical community is working on the design of the required protocols to provide what has been called Network Mobility support. In particular, a working group called NEMO has been created within the IETF [2] to extend the basic end-host mobility support protocol, MIP [12] [9], to provide network mobility support.

In more precise terms, a Network that Moves (NEMO) - a mobile network - can be defined as a network whose attachment point to the Internet varies with time. The router within the NEMO that connects to the Internet is called the Mobile Router (MR). It is assumed that the NEMO has a Home Network where it resides when it is not moving. Since the NEMO is part of the Home Network, the Mobile Network has configured addresses belonging to an address block assigned to the Home Network. These addresses remain assigned to the NEMO when it is away from home. Naturally, these addresses only have topological meaning when the NEMO is at home. When the NEMO is away from home, packets addressed to the Mobile Network Nodes (MNNs) will still be routed to the Home Network. Additionally, when the NEMO is away from home, i.e., it is in a visited network, the MR acquires an address from the visited network, called the Care-of Address (CoA), where the routing architecture can deliver packets without additional mechanisms.

The goal of the network mobility support mechanisms is to preserve established communications between the MNNs and external Correspondent Nodes (CNs) through movement. Packets of such communications will be addressed to the MNNs addresses, which belong to the Mobile Network Prefix (MNP), so additional mechanisms to forward packets between the Home Network and the NEMO are needed. The basic solution for network mobility support [7] essentially creates a bi-directional tunnel between a special node located in the Home Network of the NEMO (the Home Agent), and the Care-of Address of the MR (Fig. 1).

This solution is derived from the solution proposed for host mobility support, MIPv6 [9], without including the Route Optimisation support. Actually, the protocol is similar and the existing Binding Update (BU) message is extended to inform the Home Agent (HA) about the IP address of the NEMO side of the tunnel (that is, the CoA of the MR), through which the HA has to forward the packets addressed to the Mobile Network Prefix.

When only a non-nested NEMO is considered, the so-called triangle routing[1] is the main problem that should be faced (see Fig. 1). In Mobile IPv6, this problem has been solved using a Route Optimisation mechanism, which allows a Mobile Node to update the information about its current location (i.e., its Care-of Address) on the Correspondent Nodes, therefore enabling the traffic to bypass the HA, but still using some kind of encapsulation/overhead (i.e., the

[1] This term, used because of historical reasons, can lead to confusion. The path experimented by the packets is not triangular, but actually angular: CN<->HA<->MR<->MNN

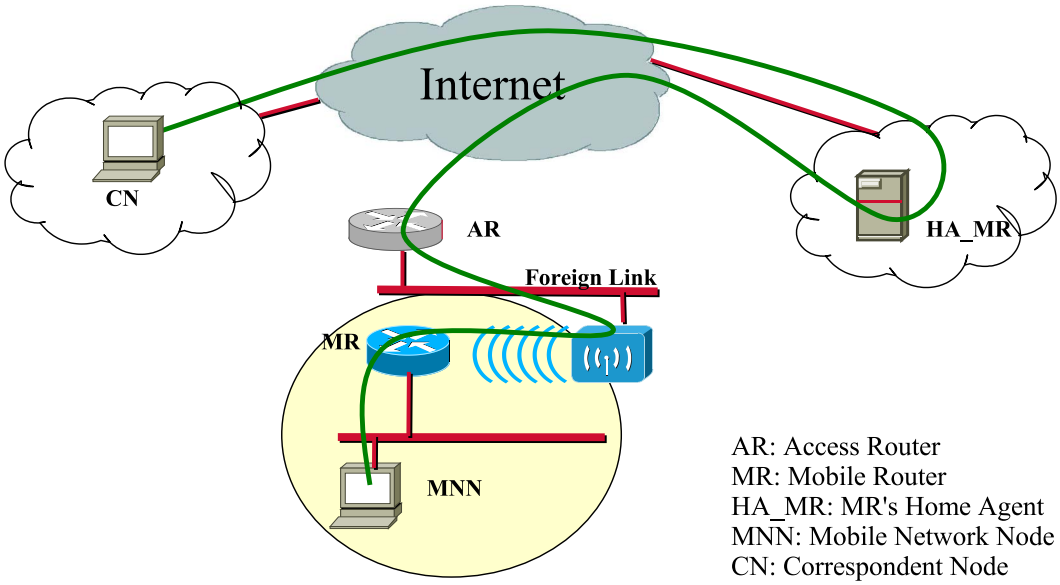

Figure 1. Triangular routing

use of the Home Address Destination Option and the Type 2 Routing Header), needed to provide a mobility support transparent to the layers above IP.

A mechanism, named Return Routability (RR) [11], was specified by the MIPv6 Route Optimisation security design team with the aim of limiting the security concerns originated because of the Route Optimisation. Basically, this mechanism verifies that there is a node that is able to respond to packets sent to a given address. This mechanism can be deceived only if the routing infrastructure is compromised or if there is an attacker between the verifier and the address to be verified. With these exceptions, the test is used to ensure that the MN's Home Address (HoA) and MN's Care-of Address (CoA) are collocated.

It is known that in different contexts there have been doubts about the goodness of the Return Routability mechanism. An important fact is that many mobile operators seem to be reluctant to use a solution based on RR as compared to "strong cryptography" to protect the location information updates (i.e., Binding Updates sent to Correspondent Nodes) in their Mobile IPv6 deployments. Essentially the RR is considered a "weak security mechanism" and it is accused of introducing a non-negligible burden of signalling in the network, which is a relevant handicap in links where resources are scarce (i.e., the wireless access link from a NEMO to the infrastructure). This poses an important challenge for the solution of the Route Optimisation problem in NEMO environments, and brings up the need of studying new mechanisms to adequately secure (integrity protection & source authentication) the communication between a MNN and a CN.

A strong cryptography approach to protect Binding Updates must be based on a security association between the two nodes participating in the communication (i.e., MNN and CN). When signalling messages (e.g., Binding Updates) are sent, the problem is then how to efficiently create a security association between these nodes. Some solutions have been already proposed to solve that in Mobile IPv6 (i.e., a Terminal Mobility scenario). We consider the following important solutions: solutions based on the availability of a Public Key Infrastructure (PKI), solutions based on the use of Cryptographically Generated Addresses (CGAs) [4] [8], and solutions based on Crypto Based Host Identifiers (CBHIs) [13].

In this article we explore different approaches to Route Optimisation in non-nested NEMOs and we devise how to adapt some of the Terminal Mobility solutions to a NEMO environment, where as we will propose, a delegation of signalling rights from the MNN to the MR is necessary.

The rest of the paper is structured as follows: in section 2 different approaches to Route Optimisation in non-nested NEMOs are analysed. In section 3, three different approaches to the delegation of signalling rights, adapted for using strong cryptography to protect the Route Optimisation, are devised. Finally, section 4 is devoted to conclusions.

2 Route Optimisation in non-nested NEMOs

In this section, different approaches to mitigate/solve the problem of the triangle routing in NEMOs are presented and analysed.

2.1 End-to-end Route Optimisation

A first approach to solve the triangle routing issue is to perform an end-to-end management of the Route Optimisation (RO). When a whole NEMO moves (i.e., the MR changes its point of attachment to the fixed Internet), every MNN inside the NEMO that supports this sort of end-to-end RO has to update its location information on all the CNs it is communicating with (see Fig. 2).

Without any doubt, performing source address authentication would be the easier approach. The MNN by itself can demonstrate, using one of the different proposed schemes (e.g., a PKI certificate, or a CGA), that it owns its address (HoA). Nevertheless this approach presents the following drawbacks:

- Signalling (e.g., Binding Update) bursts. These storms can lead to congestions and drops, and would usually involve wasting scarce bandwidth in wireless environments.
- The MNN has to be mobility-capable (i.e., implement the Mobile IPv6 protocol), which is, in general, an undesired requirement in a NEMO. This makes more difficult the deployment of mobile networks because it prevents the non-aware NEMO nodes taking advantage of the RO.
- In each visited network, a CoA per MNN in the NEMO is needed, whereas with the NEMO Basic Solution [7] just one CoA is needed to support the mobility of the whole NEMO.
- Without extra mechanisms, the MNNs are not aware of the movement of the NEMO (i.e., the moments when the NEMO changes its point of attachment to the Internet). So, unless additional procedures are provided, MNNs cannot know when they have to send the location update signalling.

2.2 MR-CN Route Optimisation

There are several good reasons to let the Mobile Router in the NEMO to send the signalling on behalf of the MNNs belonging to that NEMO. In this case, whenever a MNN-CN RO is needed, the MR sends a Binding Update to the CN binding the MNN's HoA to the MR's CoA (see Fig. 3) [5].

This approach has the following characteristics. First, the solution is applicable to nodes without mobility support. Second, the signalling overhead within the NEMO is eliminated, improving the overall performance. This is specially important when the NEMO is composed of Ad-Hoc nodes (i.e., the NEMO is a Mobile Ad-Hoc Network - MANET [6]).

In order to let the MR send the location update signalling on behalf of the MNN, a delegation of the signalling rights to the MR is needed. To be able to send the signalling on behalf of the MNNs in a secure way, the MNNs have to delegate their signalling rights to the MR, i.e., some procedure must be carried out to allow the MR to send signalling messages on behalf of a MNN, in a way that enables the CN to verify that the MR is actually allowed to send this signalling. We should remark that Mobile Nodes visiting a NEMO, i.e., Visiting Mobile Nodes (VMNs), cannot benefit of the secure Route Optimisation provided by this approach (i.e., the MR performing the RO on behalf of the MNNs), because a delegation of the signalling rights between a MR and a MNN belonging to different administrative domains may not be easily deployed.

The delegation of signalling rights to authenticate BUs can solve the identity attacks (e.g., an attacker that claims to own a stolen address). Nevertheless, it cannot solve the location attacks (e.g., an attacker that claims to be located at a certain place). A possibility that has been suggested in Mobile IPv6 and that may be also applicable to the the NEMO scenario would be performing the Return Routability procedure once per handover [8].

3 Approaches to the delegation

In this section we analyse different solutions proposed to use strong cryptography in the signalling of Mobile IPv6, and how to adapt them to a NEMO environment in which a delegation of signalling rights from the MNN to the MR is necessary. This kind of mechanisms is essential to allow the deployment of Mobile Networks solutions in real environments. A general analysis to Delegation of Signalling Rights can be found in [10].

3.1 Delegation based on PKI certificates

As a first approach, the delegation may be expressed in the form of certificates generated by a PKI. This general concept can be easily adapted to be used in NEMO. Basically, the PKI assigns prefix certificates to MRs, binding a MR public key to a NEMO Mobile Network Prefix.

CERT = (MNP, K_MR+)

Basically, the certificate states that the MR owning the public key K_MR+ is authorised to bind a CoA to a HoA with network prefix MNP. This certificate is signed by a Certification Authority.

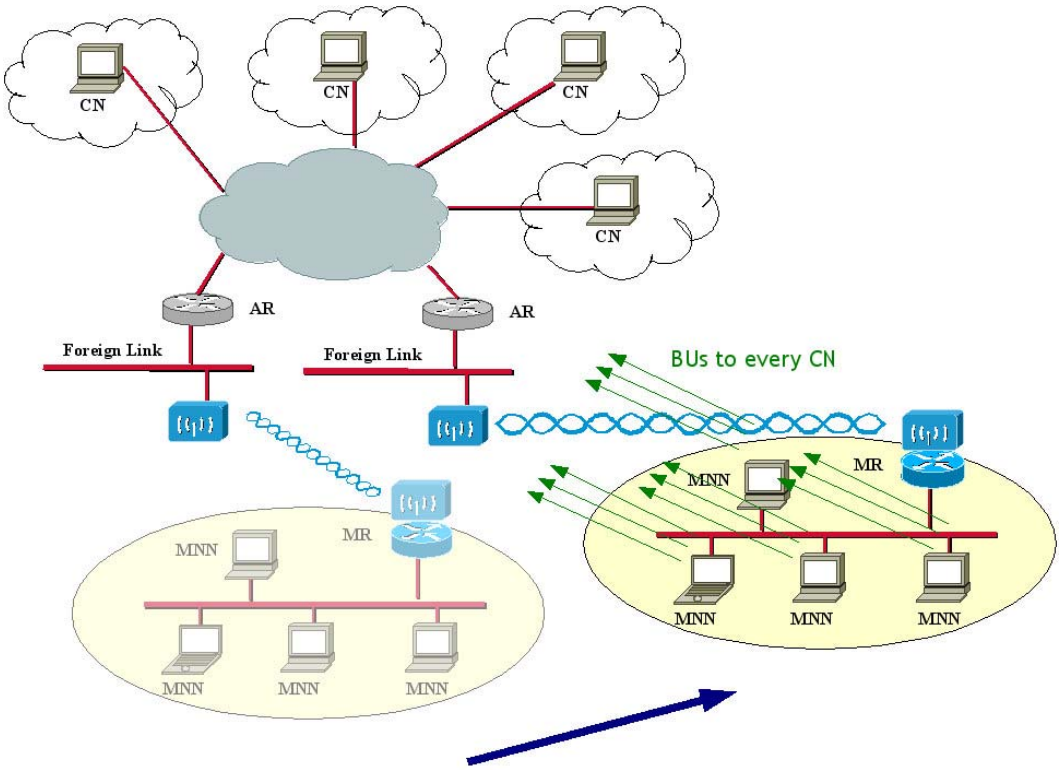

Figure 2. MNN-CN end-to-end Route Optimisation

3.1.1 Procedure of operation

- The MR obtains a certificate from the PKI, containing the Mobile Network Prefixes associated to the MR.
- Each Binding Update sent by the MR to a CN on behalf of a MNN is signed with the MR's private key. The message also contains the MR's prefix certificate.
- The Correspondent Node, when receiving a Binding Update, obtains the prefix certificate associated with the HoA contained in the BU, and verifies it. If the Binding Update is valid, the CN adds an entry in its Binding Cache.

3.1.2 Analysis of the solution

In this approach, a high protection against identity attacks is provided, but the major drawback of this solution is the requirement of a global key infrastructure, which is an unrealistic requirement for the whole Internet nowadays (although it is a solution feasible in more restricted environments).

Using prefix certificates introduces the non-trivial issue of the Prefix Ownership and this problem is much more complex than the basic Address Ownership issue that arises with Mobile IP.

3.2 Delegation based on self-signed certificates

In this case, the MNN is assumed to have a Cryptographically Generated Address (CGA) as its HoA. As described in [13], a CGA is an IPv6 address, which contains a set of bits generated by hashing the IPv6 address owner's public key. This property allows the user to provide a "proof of ownership" of its IPv6 address. On the other hand the MR (i.e., delegate) has a certificate as follows:

CERT = (CGA, K_MR+)

Basically, the certificate states that the MR owning the public key K_MR+ is authorised to bind a CoA to the CGA (MNN's HoA) included in the certificate. In other words, the MNN, identified by the CGA, delegates the right to send Binding Updates (location update messages) to a trusted node, the delegate, identified by K_MR+. This certificate is signed with the MNN's private key associated to the CGA (K_MNN-).

3.2.1 Procedure of operation

In this scenario, whenever a MNN-CN RO is needed, the MR performs it on behalf of the MNN and sends to the CN

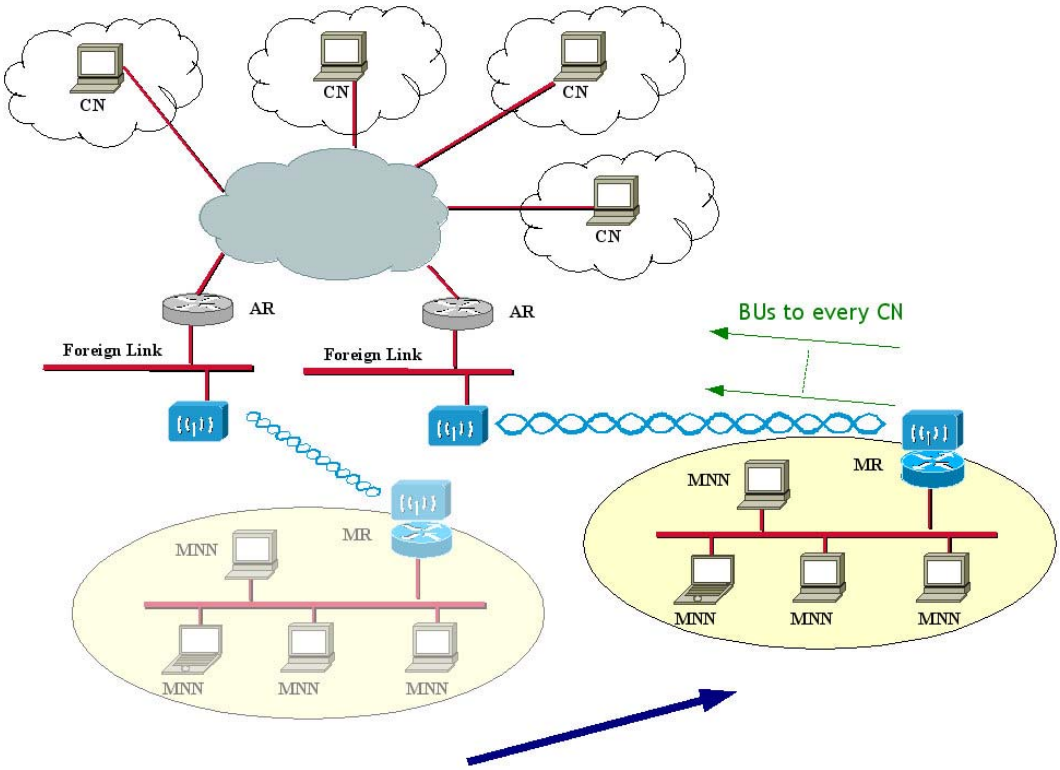

Figure 3. MR-CN Route Optimisation

a location update message (BU) linking the MNN's HoA to a CoA. The process is the following: the Binding Update is signed with the MR's private key and it includes the certificate. When the CN receives this location update message, it first verifies the certificate using the MNN's public key associated to the CGA (HoA of the BU) and then it verifies the received message using the MR's public key (K_MR+), included in the certificate.

3.2.2 Analysis of the solution

The main advantages of this approach are the following:

- It does not require the deployment of a PKI infrastructure. This is a crucial point because assuming the availability of a global PKI infrastructure is not very realistic in large networks (e.g., Internet), at least not nowadays.
- On the other hand it would be potentially compatible with SEND [3].

Also, some drawbacks can be pointed out:

- The solution is not transparent for the CN, i.e., any CN must understand the address format and the procedures involved, which requires changes to the software of the CN.

3.3 Implicit Delegation

In this approach to delegation of signalling rights, there is not an explicit delegation from the Mobile Network Node to the Mobile Router. Instead, the MNN gives to the MR the right to send signalling on its behalf by accepting the use of an address with a particular structure (the format of this address is proposed in [13]).

3.3.1 Address format

This address (an IPv6 address) is composed of the network prefix (64 bits) and the Interface Identifier (64 bits). The network prefix is simply the Mobile Network Prefix. The Identifier (IID) is called a Crypto Based Host Identifier [13] and is created in the following way:

IID = [4 control bits, 48 bit site identifier, 12 host bits]

The format for this IID is proposed and described in [13]. The 4 control bits are: one reserved, one to distinguish between 80 bit identifiers and 64 bit identifiers (in this application we are only interested in 64 bit identifiers), and the usual universal/local bit and group bit. To ensure EUI-64 compatibility, [13] proposes to set the u/l bit to "universal"

and the group bit to indicate a group address. Because we have 12 host bits, we will be able to address $2^{12} = 4096$ hosts, which seems to be large enough for a NEMO.

The site identifier contains cryptographic information that allows Correspondent Nodes to verify that the address is used legitimately. The site identifier must contain the following information (this is different from what is proposed in [13] because of the reasons explained in next section):

NEMO Site identifier = Hash (Mobile Network Prefix, MR public key)

3.3.2 Procedure of operation

A MR willing to serve a NEMO by sending the signalling on behalf of its MNNs, must generate a pair of keys: public/private. Then, it generates and provides addresses (Home Addresses or HoAs) to the MNNs. The addresses have the format explained in the previous section.

If the MR wants to send a Binding Update on behalf of a MNN of its NEMO to a Correspondent Node, the MR signs the BU with its own private key. The MR also informs the Correspondent Node of its public key and Mobile Network Prefix (that must match that of the HoA included in the BU).

The CN can verify the address by re-calculating the Site Identifier (it has the MR public key and the NEMO Mobile Network Prefix) and checking that it matches that of the HoA. Using the MR public key, the CN can also verify the authenticity of the BU.

An attacker cannot generate a fake BU that binds a certain HoA to a CoA. To be able to do that, the attacker would need to authenticate the BU with a private key that corresponds to the public key used to create the Site Identifier of the HoA.

An attacker can also try to generate pairs of public/private keys and create a dictionary of 2^{48} different Site Identifiers. Then, if the attacker detects a particular HoA that she wants to attack, she only has to look up in the dictionary the public/private key corresponding to the Site Identifier of the HoA. Using the Mobile Network Prefix in the calculation of the Site Identifier makes this attack much more difficult, because the dictionary must include not only Site Identifiers but also network prefixes: $2^{48} * 2^{64}$ entries.

Notice that in this section we focused on the conceptual ideas of this solution, a practical situation would use some improvements, for example a symmetric key could be generated from the public/private key for doing authentications less computationally costly. Also, the particular hash algorithm or public key cipher method are not analysed.

3.3.3 Analysis of the solution

The main advantage of this delegation solution is that is very simple. Nevertheless some disadvantages can be pointed out:

1. It is incompatible with stateless address auto-configuration and other solutions that work with the IID as CGAs (what can have a negative effect in SEND for example).

2. The solution is not transparent for the CN, i.e., any CN must understand the address format and the procedures involved, which requires changes to the software of the CN.

3. It imposes a limit of 2^{12} to the number of hosts in a NEMO. This does not seem to be a great problem for a NEMO. A solution for this would be to use more than one prefix in the NEMO (this, of course, uses address space).

4 Conclusions and Final Remarks

In this paper we have analysed the need of a delegation of signalling rights in those environments in which a Route Optimisation for NEMO using strong cryptography is a requirement.

The delegation of signalling rights can be done in an explicit way, by means of authorisation certificates, or, as it has been devised here, in an implicit way, accepting the use of an address with some particular characteristics.

Probably, the simplest solution, implicit delegation, has also more limitations (as incompatibilities with other mechanisms like SEND or stateless address auto-configuration). The most flexible solution, the one based on PKI certificates, requires an important infrastructure. The solution based on CGAs can be a good compromise between complexity and flexibility. The solutions to be used in real deployments are very much dependant on operators preferences.

A handicap for delegation of signalling rights is that, irrespective of the approach followed, it is not transparent for Correspondent Nodes, i.e., it requires changes to the software of the Correspondent Nodes, which pose an important difficulty for its deployment.

5 Acknowledgements

The work described in this paper is based on results of IST FP6 Integrated Project DAIDALOS [1]. DAIDALOS receives research funding from the European Community's Sixth Framework Programme. Apart from this, the European Commission has no responsibility for the content of

this paper. The information in this document is provided as is and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

References

[1] FP6 IST Integrated Project DAIDALOS. http://www.ist-daidalos.org.

[2] The Internet Engineering Task Force (IETF). http://www.ietf.org.

[3] J. Arkko, J. Kempf, B. Sommerfeld, B. Zill, and P. Nikander. *SEcure Neighbor Discovery (SEND)*, April 2004. draft-ietf-send-ndopt-05.txt (work in progress).

[4] T. Aura. *Cryptographically Generated Addresses (CGA)*, April 2004. draft-ietf-send-cga-06.txt (work in progress).

[5] C. J. Bernardos, M. Bagnulo, and M. Calderón. MIRON: Mobile IPv6 Route Optimization for NEMO. In *4th Workshop on Applications and Services in Wireless Networks. ASWN 2004*. IEEE, August 2004.

[6] S. Corson et al. *RFC 2501: Mobile Ad hoc Networking (MANET): Routing Protocol Performance Issues and Evaluation Considerations*, January 1999.

[7] V. Devarapalli, R. Wakikawa, A. Petrescu, and P. Thubert. *Network Mobility (NEMO) Basic Support Protocol*, June 2004. draft-ietf-nemo-basic-support-03.txt (work in progress).

[8] W. Haddad, L. Madour, J. Arkko, and F. Dupont. *Applying Cryptographically Generated Addresses to Optimize MIPv6 (CGA-OMIPv6)*, June 2004. draft-haddad-mip6-cga-omipv6-02.txt (work in progress).

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

[10] P. Nikander and J. Arkko. Delegation of Signalling Rights. In *10th Annual Workshop on Security Protocols*, 2002.

[11] P. Nikander, J. Arkko, T. Aura, G. Montenegro, and E. Nordmark. *Mobile IP version 6 Route Optimization Security Design Background*, December 2003. draft-nikander-mobileip-v6-ro-sec-02.txt (work in progress).

[12] C. Perkins. RFC 3344: IP Mobility Support for IPv4, August 2002".

[13] I. van Beijnum. *Crypto Based Host Identifiers*, January 2004. draft-van-beijnum-multi6-cbhi-00.txt (work in progress). URL: http://mirrors.isc.org/pub/www.watersprings.org/pub/id/draft-van-beijnu%m-multi6-cbhi-00.txt.