A Robust Return Routability Procedure for Mobile IPv6

R Radhakrishnan*, Majid Jamil[#], Shabana Mehfuz[#], Moinuddin[$]

*KIET, Ghaziabad, UP,India; #Department of Electrical Engineering, Jamia Millia Islamia, New Delhi, India; $ NIT, Jallandhar, India

Summary
Mobile IPv6 is a network-layer mobility protocol for the IPv6 Internet. Route optimization mechanism in IPv6 offers an efficient routing option to mobile IPv6 than that is available for mobile IPv4. The protocol includes security mechanisms, such as the return-routability tests for security of route optimization mechanism. This paper explains the threat model and existing security solutions for route optimization. An improved, robust and simple security solution is also presented based on IPSec, which is an inbuilt security feature of IPv6.

Keywords:
Mobile IPv6, Home agent, Care-of-address, Binding update, Route optimization

1. Introduction

Mobile IPv6 protocol [1], allows a Mobile Node (MN) to move from one network to another with packets getting routed to the MN through its Home Agent (HA), a router in its parent network. This happens regardless of MN's current point of attachment to the Internet because MN sends its current address (care of address (CoA)) to HA through Binding Update (BU) packets that are first authenticated by HA [2]. When a peer for MN, called as Correspondent Node (CN), unaware of MN's current location, first sends packets to MN at its home address, it is intercepted by HA and forwarded to MN. The MN sends the packets back to CN via HA or directly from its new location. Routing the data through a third entity like HA is not an efficient way of sending data. In Mobile IPv6, the packets can also be sent directly between the MN and its CN. This mode is called Route Optimization [1,3,4], which is not properly supported in Mobile IPv4 [5]. Route Optimization (RO) on a global scale between all MNs and CNs is an efficient routing mechanism supported by Mobile IPv6. RO is established by BU and Binding Acknowledgement (BA) between CN and MN. However a number of security threats like traffic redirection, replay attacks, inducing unnecessary binding updates, forcing of non-optimized routing and reflection attacks have been identified [13] due to improper verification of CoA and Home address (HoA).

Manuscript received May 5, 2008
Manuscript revised May 20, 2008

This paper is organized as follows. Section 2 presents RO mechanism and BU authentication in MIPv6. Security threats to BU authentication are discussed in section 3. Section 4 discusses the current solutions proposed in previous works for Return routability protocol. In section 5, the proposed solution called "Revised Return Routability procedure" for a simple, secure and robust solution for RO, is explained. An analysis of proposed solution with existing solution is carried out in section 6 followed by conclusion in section 7.

2. Route Optimization in Mobile IPv6[6]

The basic idea in Mobile IP is to allow a home agent (HA) to work as a stationary proxy for a mobile node (MN). Whenever the mobile node is away from its home network, the HA intercepts packets destined to the node and forwards the packets by tunneling them using IPv6 encapsulation [7] to the node's current CoA. The transport layer (e.g., TCP, UDP) uses the home address as a stationary identifier for the mobile node. Figure 1 illustrates this basic arrangement.

The basic solution requires tunneling through the home agent, thereby leading to longer paths and degraded performance. To avoid this degradation, Mobile IPv6 includes Route Optimization feature (shown in dotted path in figure 1) whereby the MN and CN can directly exchange packets, bypassing the HA completely after an initial set up phase in which the CN learns the CoA of MN. After the initial set up, the MN sends a Binding update message by which CN learns the authenticated CoA of MN.

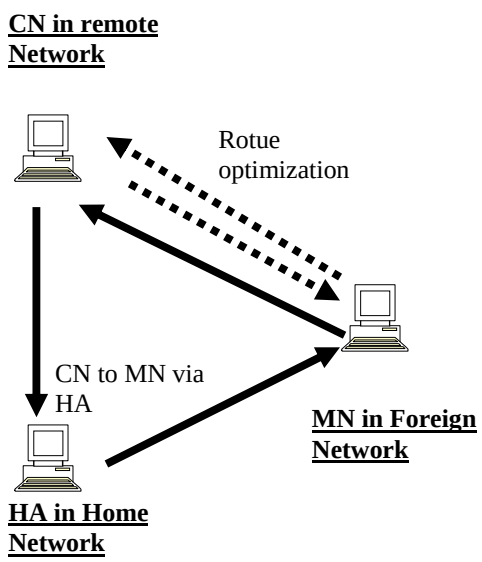

Figure 1: Illustration of triangular routing between CN, HA and MN

2.1 Set up for Route Optimization

The set up consist of Return Routability (RR) Procedure[1] which enables the correspondent node to obtain some reasonable assurance that the mobile node is in fact addressable at its claimed care-of address as well as at its home address.
There are four messages used to perform the return routability procedure between MN, HA and CN. These messages are :-

- Home Test Init (HoTI)
- Home Test (HoT)
- Care-of Test Init (CoTI)
- Care-of Test (CoT)

Figure 2 shows the message flow for the return routability procedure.

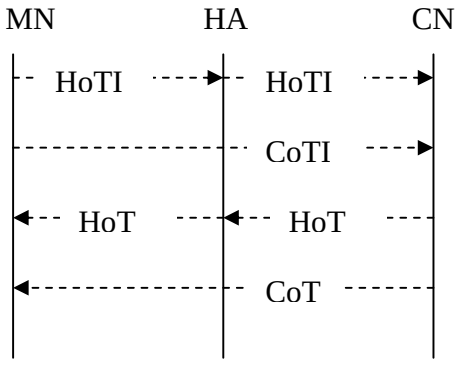

Figure 2 : RR messages flow.

The HoTI message, which is reverse tunneled through HA, conveys the MN's home address to the correspondent node. The MN also conveys its CoA directly to CN by the CoTI message. The CN on receipt of HoTI generates a Home keygen token, which is the first 64 bits of MAC of a secret key of CN (kcn) and HoA as follows:

Home keygen token := First (64, HMAC_SHA1 (Kcn, (home address | nonce | 0))) ----(1)

This home keygen token is sent by CN to MN via the HA through a HoT message in response to a HoTI message.

The CN on receipt of CoTI generates a Care of keygen token based on a secret key of CN (kcn) and CoA as follows:

Care-of keygen token :=
First (64, HMAC_SHA1 (Kcn, (care-of address | nonce | 1))) ---------(2)

This Care of keygen token is sent by CN to MN directly through a CoT message in response to a CoTI message. When the mobile node has received both the HoT and CoT messages, the return routability procedure is complete.

2.2 Binding update (BU) and Binding Acknowledgement (BA)

A Binding Update is used by a MN to notify a CN or the mobile node's HA of its CoA at its new location. To authorize a Binding Update, the mobile node creates a binding management key, Kbm, from the keygen tokens as described in the previous section. The mobile node hashes the tokens together to form a 20 octet binding management key (Kbm):

Kbm = SHA1 (home keygen token | care-of keygen token) ------(3)

After the mobile node has created the Kbm, it can supply a verifiable BU to the correspondent node. Message flow of BU and BA are shown in figure 3.

The content of BU message include a sequence number, nonce CoA and a MAC of (Kbm, (CoA | Address of CN | BU)). Once the CN has verified the MAC, it can create a Binding Cache entry for the mobile. Optionally, CN sends a BA, the content of which include a sequence number and a MAC of (Kbm, (CoA | Address of CN |

BA)). After the integrity and authenticity of the Binding Update message to CN is verified by CN, Route optimization is established between CN and MN and data transfer takes place between CN and MN directly, bypassing the HA. The complete RR protocol combined with the BU and BA is called as bombing resistant protocol.

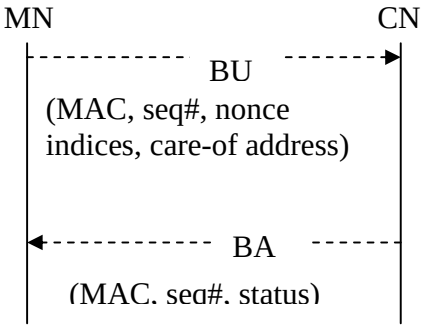

Figure 3: Binding Update and Binding Acknowledgement messages flow

3. Security threats to BU authentication

The RR protocol mainly provides two checks. Firstly, the HoTI and HoT messages, called the RR test for the HoA, authorizes the sender of the binding update to change the binding for the home address. Secondly, CoTI and COT messages called the RR test for the CoA authorize the sender of the BU to request data to the care-of-address. Though this RR for HoA and RR for CoA solved threats such as unauthorized traffic redirection, replay attacks and reflection attacks there are attacks like state-storage exhaustion and unwanted Binding Authentication still to be resolved [8].

RR protocol assumes that an attack does not originate from a CN. Such a situation that an attacker can be a CN has not been brought out so far. This section brings out one more attack in which the attacker is CN and the victims are HA, MN and node whose address is stolen by the attacker. This attack is called Amplification attack. These unresolved threats are discussed below.

3.1 CPU, State-storage exhaustion

Authentication protocols are often vulnerable to flooding attacks that exploit the protocol features to consume the target node's computing power. In the case of RR procedure, a rogue node posing as a MN can flood a target (CN) with HoTI and CoTI messages that cause the CN to perform expensive repeated generation of Home keygen and Care of keygen tokens. This can cause exhaustion of computing power especially if the CN is a low-end mobile device.

3.2 DOS attack

BU authentication is a stateful protocol and it exposes the protocol participants to denial of service attacks. In particular, if a host stores a state as a result of an unauthenticated message, an attacker can initiate the protocol many times and cause the host to store a large number of unnecessary protocol states. Figure 4 shows such an attack relating to BU authentication protocol. The attacker, which may be a rogue MN, sends a HoTI message with a false home address and a CoTI message with false care-of address. The CN responds with two randomly chosen secret values, which it has to remember until it receives the authenticated BU. If the attacker repeats this many times, the victim CN may not be able to store all the state data and may drop some initial messages. This may prevent legitimate MNs from using route optimization with the CN. The attack is similar to the SYN-flooding attack against the TCP protocol.

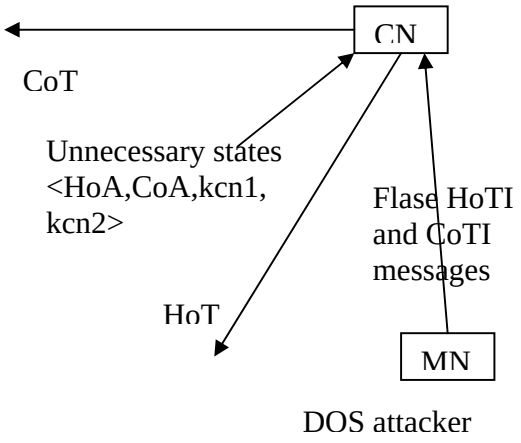

Figure 4: DOS attack

3.3 Amplification Attack

Figure 5 shows the CN as an attacker. The CN spoofs the address of a victim node V and sends a message (1) to a node, which has moved away from its home network. The HA forwards the CN's message (2) to MN, which then initiates the RR protocol for Route optimization between MN and CN's spoofed address of V. Message 3 is HoTI from MN to V. Message 4 is CoTI from MN to V. In response, V generates Home keygen and care of keygen tokens (equations 1 & 2 in sec 2.2) sends messages, 5 and 6, which are HoT and CoT respectively.

MN now calculates kbm (equation 3 in sec 2.2) and send BU in message 7. Message 8 is BA from V to MN.

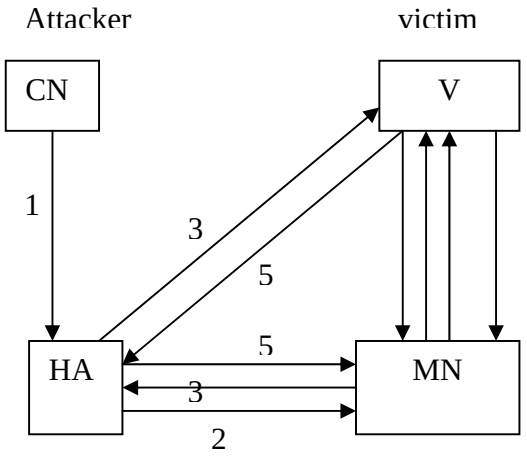

Figure 5: Shows how a single message from attacker CN results in 8 unwanted messages.

In this attack a single message from the attacker gets amplified into 8 unwanted messages and also results in unwanted computations in MN and victim V.

4. Current solutions

The state storage exhaustion attack [8] mentioned in section 3.2 is similar to the SYN-flooding attack against the TCP protocol. Adding memory and managing the state storage carefully can prevent the attack. A better solution is to design the protocol to be stateless. The CN need not store a state for each mobile but instead after sending the HoT and CoT messages, the keygen token values can be deleted from memory. These values can be recomputed when it receives the BU. This way the CN can remain stateless until it has authenticated the mobile. The CPU exhaustion mentioned in section 3.1 is not a big issue since calculations involved in generation of keygen tokens do not consume too much CPU power.

The RR procedure, as shown above, has the overhead of messages (CoTI, CoT, HoTI and HoT) besides computations of keygen tokens and kbm. One solution, which has been previously proposed, called as Improved Bombing Resistant protocol [9] has less packet count than the RR procedure, hence consume lower bandwidth and is more efficient. Another solution called Enhanced cga based Route Optimization [13] applies cryptographically generated home addresses for proof of ownership of address in addition to RR procedure. Enhanced Route Optimization also protects against redirection-based flooding attacks through the use of Credit-Based Authorization.

5. Revised Return Routability procedure

The return routability procedure provides authentication to binding updates. But this procedure still lacks a comprehensive mechanism to validate and prove the correctness of CoA. An attacker can lie about MN address as mentioned in section 3.2 and cause a victim CN to generate CoT and HoT messages to carry out DOS attack. There is no mechanism in RR protocol to validate the address of CN, resulting in Amplification attack as mentioned in section 3.3.

This article suggests a solution called Revised Return Routability procedure to provide a secured mechanism to ensure that all the players involved in mobility i.e., HAs, MNs and CNs are all verified authenticated nodes and thus leaves almost nil security holes to be exploited by an attacker. The procedure is based on following:-

a) Secured link between HA and MN[12]
b) A public key infrastructure (PKI) for IPv6 [10]
c) Validation of MN and CN
d) Revised Return Routability procedure

5.1 Secured link between HA and MN

It is assumed that a HA will have secured association with all its nodes in the home network. Manual configuration of IPsec security associations must be supported between HA and its nodes. The configuration of the keys is expected to take place out-of-band, for instance at the time the mobile node is configured to use its home agent. When any node moves out of the link to any foreign network, the secured association between the MN and HA continues to exist and communication between them take place through this secured pipe. ESP encapsulation of Binding Updates and Acknowledgements, Home Test Init and Home Test messages, ICMPv6 messages and Payload packets tunneled between HA and MN must be supported and used. This ensures the validation of MN to HA in a mobile IPv6 scenario.

5.2 A public key infrastructure (PKI) for IPv6.

A public key infrastructure, called UMU-PKIv6 developed by the University of Murcia, is a suitable infrastructure for all those organizations that want to offer secure communications and data protection to their users. UMU-PKIv6 is compliant with the Internet X.509

Public Key Infrastructure [11] and offers services that can be reached via Internet, such as certification requests, retrieval, revocation or renewal PKCs, etc over IPv6 network. Authentication will rely on UMU-PKIv6 system

The components and structure of UMU-PKIV6 is given in fig 6. The main components are:

- Certification Authorities (CAs) process requests of issue, renewal and revoking of PKCs stored in Request Server(RS)
- Registration Authorities (RAs) authenticate off-line users and add certificate's properties.
- Request Servers(RS) picks up all requests from system entities to be processed by CA
- Certificate Repository (CR) server provide directory service of all users certificate, CA Certificates and Certificate Revocation Lists.

The services provided by UMU-PKIv6 enables a user client to carry out any operation type from his own navigator: to request a certificate, renewal or revoke it, to look for another user certificate which wants to establish a secure communication, etc.

In the proposed solution the Authentication Server (AS) acts as a user client to above PKIv6 system. Such an AS for every link is assumed to function as a Home Agent. Such an HA will be a trusted node in a mobile scenario.

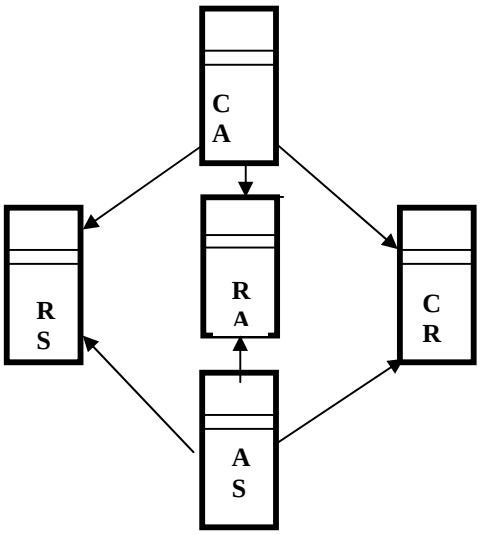

Figure 6 : Main components of UMU-PKIv6

5.3 Validation of MN and CN

A CN (initiator) wishing to communicate with a MN first sends a message to MN's Home address. The HA then forwards the message to MN at its care of address. It is assumed that the MN when it moved to its foreign network would have already sent its BU to HA through the secured channel. Hence the MN is already validated. Now the HA through the PKIv6 infrastructure validates the genuineness of CN and obtains its certificate and hence its public key (m2,m3 in figure 7). HA is a known trusted server in the PKI system. Thus MN and CN are validated by HA before checking the routability.

5.4 Revised Return Routability procedure

The MN now initiates Revised RR (RRR) procedure to authenticate BU before Route Optimization between MN and CN. It initiates a CoTI message (m1 in figure 7) to HA through the secured channel. On Receipt of CoTI, HA now understands that the MN wants to have RRR procedure for Route optimization with CN. MN now sends CoTI message even in the case when MN is the initiator of communication with CN. HA now generates a care-of keygen token as below:
Care-of keygen token:= First (64, HMAC_SHA1 (care-of address | nonce |))----(4)

This Care-of keygen token is now sent in CoT message (m5) to CN encypted by the public key of CN. The contents of the CoT message are:

- Source Address = address of HA
- Destination Address = address of CN
- Parameters:
  - care-of init cookie
  - Encrypt with public key of CN (care-of keygen token)

The same Care-of keygen token is also sent by HA to MN (m4) through the secured channel. The MN now generates a BU (m6) and sends to CN. The content of BU message include a sequence number, nonce, CoA and a MAC of (Care-of keygen token, (CoA | Address of CN | BU)). The messages are as given in figure 7.

5.5 Robustness and simplicity of RRR procedure.

When a MN moves out of its home network, it maintains the IPSec secured association with its HA. The CoA of MN is conveyed to HA through this secured channel. This ensures mutual trust and reacheabilty between MN and HA.

In the proposed solution the HA is an Authentication Server (AS) of PKIv6 system. Such an HA will be a trusted node in a mobile scenario.

Now the genuineness of CN is verified by HA through the PKI system. Only CNs with certificates issued within the PKI systems is allowed to participate in Mobile scenario.

Reacheability test of MN and HA with CN is carried out in a simplified manner by HA. The HOTI and HOT messages in RR procedure are eliminated. The CN does not have to generate Home keygen token and Care-of keygen token as is required in RR procedure. A CN, which can be a mobile device with low processing power, is saved of computation load. The CN receives care-of keygen token in CoT message from HA and MAC of this token from MN in BU message besides other parameters. Now the CN will be able to verify the care-of keygen token and also obtain the correct CoA of MN from CoT and BU messages. Thus all three players namely the HA, MN and CN are mutually authenticated and tested for routability in a simple and robust manner in RRR procedure.

6. Analysis

A comparative analysis of RRR procedure with RR procedure, Improved bombing resistant protocol and Enhanced cga based Route Optimization carried out in table 1. The salient feature of original RR procedure is that it does not depend on any infrastructure such as PKI for providing security to RO set up. But it has an overhead of total eight messages:

- HoTI from MN to HA.
- HoTI from HA to CN
- HoT from CN to HA
- HoT From HA to MN
- CoTI from MN to CN
- CoT from CN to MN
- BU
- BA

In contrast, RRR procedure has seven messages:

- CoTI from MN to CN
- CoT from HA to MN
- CoT from HA to CN
- Certificate request
- Certificate reply
- BU
- BA

All other three procedures do not validate the CN at all. RRR procedure absolutely validates all three players namely the HA, CN and MN and hence it is more robust. Computation load on CN and MN, which can be small hand-held devices, is very much reduced in RRR procedure since token generation is done by HA only which is a server.

7. Conclusion

The RR procedure sets up a secure BU for RO by validating HA and MN. Certain security threats still persist. A CN is not validated at all in RR procedure resulting in new threats like amplification attack. A revised RR procedure is proposed in this article, which is simple and validates CN also. Unlike RR procedure RRR procedure relies on UMU-PKIv6, which has a potential to emerge as a standard for PKI for IPv6. RRR procedure is thus suitable for networks, which support UMU-PKIv6. The latency in obtaining a certificate of a CN, which is topologically far, is assumed to be low in this article. This is an area which is needed to be explored in detail since PKIv6 is a new and untested technology so far.

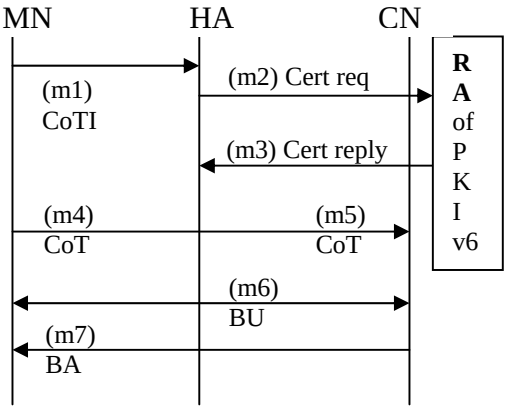

Figure 7: RRR procedure message flow

Table 1: Comparison of solutions

Security solution	Messages	Dependency on PKI	Computation load on devices	Verification of MN,HA and CN	Crypto capabilities for nodes
RR procedure	8	No	High on CN, MN	Reachability of MN, HA	Hash, MAC, generation of 3 keys
Improved Bombing Resistant protocol	6	No	Medium on MN, CN	Reachability of MN, HA	Hash, MAC, generation of 3 keys
Enhanced cga based RO	7	Yes	High on CN, MN	Reachability of MN, HA	HASH, MAC, RSA, generation of 3 keys
RRR procedure for RO (proposed)	7	Yes	Low on CN , MN	Absolute validation of MN, HA and CN	HASH, MAC, generation of one key
Security solution	**Messages**	**Dependency on PKI**	**Computation load on devices**	**Verification of MN,HA and CN**	**Crypto capabilities for nodes**
RR procedure	8	No	High on CN, MN	Reachability of MN, HA	Hash, MAC, generation of 3 keys
Improved Bombing Resistant protocol	6	No	Medium on MN, CN	Reachability of MN, HA	Hash, MAC, generation of 3 keys
Enhanced cga based RO	7	Yes	High on CN, MN	Reachability of MN, HA	HASH, MAC, RSA, generation of 3 keys
RRR procedure for RO (proposed)	7	Yes	Low on CN , MN	Absolute validation of MN, HA and CN	HASH, MAC, generation of one key

References

[1]. C. Perkins, Nokia Research Center; J. Arkko, Ericsson; June 2004, RFC 3775 “Mobility Support in IPv6”,

[2]. A.Patel, K. Leung, M. Khalil, H. Akhtar, K. Chowdhury; Authentication Protocol for Mobile IPv6;RFC 4285, January 2006.

[3] S.H. Hwang, B.K. Lee, Y.H. Han, C.S. Hwang; An adaptive hierarchical mobile IPv6 with route optimization; In Proceedings of Vehicular Technology Conference, April 2003

[4] CE Perkins, DB Johnson; Route Optimization for Mobile IP; In Proceedings of Cluster Computing, 1998 - Springer

[5] C Perkins; IP Mobility Support for IPv4; RFC 3344, 2002

[6] P. Nikander, J. Arkko, Ericsson Research NomadicLab; T. Aura, Microsoft Research, G. Montenegro, Microsoft Corporation, E. Nordmark, Sun Microsystems; December 2005, RFC 4225, Mobile IP Version 6 Route Optimization Security Design Background.

[7] Conta, A. and S. Deering, December 1998, RFC 2473, "Generic Packet Tunneling in IPv6 Specification".

[8] Tuomas Aura, Michael Roe, Designing the Mobile IPv6 Security Protocol, Annals of telecommunications, Vol. 61 no:3-4, March-April 2006, Network and information systems security.

[9]. Irfan Ahmed, Usman Tariq, Shoaib Mukhtar, Kyung-suk Lhee , S.W. Yoo, Piao Yanji, ManPyo Hong, “Binding Update Authentication Scheme for Mobile IPv6”, Third International Symposium on Information Assurance and Security, IEEE computer society, 2007

[10] Antonio F. Gómez Skarmeta, Gregorio Martínez Pérez, Óscar Cánovas Reverte. "New Security Services based on PKI", Elsevier Future Generation Computer Systems, Vol. 19, No. 2, 2003

[11] C. Adams, P. Silvestre, M. Zolotarev, M. Zuccherato, Internet X.509 Public Key Infrastructure Data Validation and Certification Server Protocols, RFC 3029, IETF, February 2001.

[12] J. Arkko, Ericsson,V. Devarapalli, Nokia Research Center, F. Dupon, RFC 3776 “Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents”, GET/ENST Bretagne, June 2004

[13] J. Arkko, Ericsson Research NomadicLab, C. Vogt, RFC 4866, “Enhanced Route Optimization for Mobile IPv6”, Universitaet Karlsruhe (TH), W. Haddad, Ericsson Research, May 2007.