Mobility Agents: Avoiding the Route Optimization Signaling on Large Servers

Albert Cabellos-Aparicio, Jordi Domingo-Pascual
Departament d’Arquitectura de Computadors, Universitat Politècnica de Catalunya
Campus Nord c/ Jordi Girona 1-3, Barcelona, Spain
{acabello,jordid}@ac.upc.edu

ABSTRACT
Mobile IPv6 has been designed by the IETF to provide mobility to the Internet. With mobility a user can move and change his point of attachment to the Internet without losing his network connections. If Mobile IPv6 was deployed on the Internet, typically Correspondent Nodes would be large servers of current content providers. These large servers have thousands of clients and in such scenario many of them would be mobile clients. In Mobile IPv6 if a Mobile Node wants to communicate with a Correspondent Node directly (Route Optimization) it must perform the Return Routability procedure which includes sending and receiving signaling messages, cryptographic calculations and storing a state. This procedure must be performed for each mobile client connection and for each handover. The Return Routability procedure would introduce a very significant load on these servers. Moreover the servers must be modified in order to support Mobile IPv6 Route Optimization. These issues may be a drawback for Mobile IPv6’s deployment. In this paper we propose Mobility Agents, a centralized solution that performs Route Optimization on behalf the Correspondent Nodes. Mobility Agents reduce the deployment cost, do not require modifying the servers, they can benefit NEtwork MObility (NEMO) and other mobility protocols and allow deploying different Mobile IPv6 extensions such as Optimized MIPv6 without modifying the Correspondent Nodes. Finally our proposal reduces the data packet overhead up to 25% compared with existing solutions.

Categories and Subject Descriptors

General Terms
Management, Design.

Keywords
Mobility, Mobile IPv6, NEMO, OMIPv6, Mobility Deployment, Route Optimization, Return Routability

1. INTRODUCTION
Wireless technologies have evolved in recent years. IEEE 802.11 is one of the most used wireless technologies and it provides up to 54Mbps of bandwidth in an easy and affordable way. In current Internet status, a user can be connected through a wireless link but he cannot move without breaking the IP communications. That’s why the IETF designed Mobile IP which provides mobility to the Internet. With “mobility” a user can move and change his point of attachment to the Internet without losing his network connections.

In Mobile IP a Mobile Node has two identifiers. The first one identifies the Mobile Node’s (MN) identity (WHO). The second one identifies the MN’s current location (WHERE). The MN will always be reachable through its WHO identifier while it will change its WHERE identifier according to its movements. A special entity called Home Agent placed at the MN’s home network will maintain bindings between the MN’s WHO and WHERE identifiers. The MN will inform to its Home Agent each change on its location (WHERE) by using special signaling while it will maintain a fixed identity (WHO). The communications between the MN and its peers (Correspondent Nodes) will be routed through the Home Agent.

However packets routed through the Home Agent follow a non-optimal path. If the MN wants to communicate using a direct path (Route Optimization) it has to inform to its Correspondent Nodes (CN) about its location changes. Obviously this requires some sort of support on the Correspondent Nodes. The required functionalities are similar to those provided by a Home Agent.

The IETF has designed two versions of Mobile IP, one for IPv4 and another one for IPv6. Mobile IPv6 [1] is very similar to Mobile IPv4 [2]. However for IPv4, mobility issues were not considered in its initial design. When IPv6 was designed, mobility issues were taken into account and it is perfectly integrated into the protocol. Mobile IPv6 is more efficient and avoids some problems suffered by Mobile IPv4. Among others, Mobile IPv6 does not need special network support on the MN’s foreign network and it supports Route Optimization.

In order to expand mobility, the IETF is currently standardizing the NEtwork MObility (NEMO) protocol. In NEMO [3] not a single node but a whole network can change its point of attachment to the Internet without losing its network connections. The main difference between NEMO and Mobile IPv6 is that the WHO identifier identifies a network prefix instead of a single node. Although Route Optimization for NEMO has not been
standardized yet several proposals have been published. Most of them introduce the concept of the Correspondent Router. A Correspondent Router is a special entity located at the Correspondent Network that will run NEMO’s Route Optimization on behalf the Correspondent Nodes.

As it has been said before, Mobile IPv6 requires of protocol support at the Correspondent Nodes to perform Route Optimization. If Mobile IPv6 was deployed on the Internet typically Correspondent Nodes would belong to large content providers. MNs would be clients while CNs would be large servers. These large servers would need to perform several operations in order to provide Route Optimization. These operations include message processing, storing the bindings between the WHERE and WHO identifiers and cryptographic operations. Moreover, these operations must be carried out for each client’s movement (handover). We claim that these issues will difficult the mobility protocol’s deployment. Moreover these large servers are content providers and its hardware may not be intended to perform this sort of operations.

In this paper we present a new entity called Mobility Agent that it is able to process Mobile IPv6’s Route Optimization messages. This entity is located at the Correspondent Network border router and it will process Route Optimization messages on behalf the Correspondent Nodes. With Mobility Agents Mobile IPv6 can be deployed flawlessly because we do not require Correspondent Node support. Mobile IPv6 deployment at the Correspondent Network is as easy as plug and play with Mobility Agents. We also present how Mobility Agents can help NEMO’s Route Optimization and other Mobile IPv6’s extensions.

The remainder of this paper is organized as follows: section 2 presents an overview of Mobile IPv6 and NEMO. Our motivation is presented in section 3 while section 4 shows our proposal. An evaluation of our proposal is depicted in section 5. The related work is detailed in section 6 and finally, section 7 is devoted to the conclusions of our work.

2. MOBILITY PROTOCOLS OVERVIEW

This section presents an overview of the different mobility protocols that interact with our Mobility Agents.

2.1 Mobile IPv6

The main goal of the Mobile IPv6 (MIPv6) protocol is to allow Mobile Nodes (MN) to change its point of attachment to the Internet while maintaining its network connections. This is accomplished by keeping a fixed IP address on the MN (Home Address or HoA). This address represents the identity of the MN (WHO). When the MN is connected to a foreign network (not its usual network) it uses a temporal address (Care-of Address or CoA) to communicate. This address represents the location of the MN (WHERE). MIPv6 has three functional entities, the Mobile Node, the Home Agent (HA), a router of the home network that manages localization of the MN and finally, the Correspondent Node (CN), a fixed or mobile node that communicates with the MN. Figure 1 presents the basic operations of Mobile IPv6.

Mobile IPv6 has four phases:

1.- Agent Discovery: The MN has to discover if it is connected to the home network or to a foreign one. For this purpose it uses Router Advertisements [4], these messages are sent periodically by all IPv6 routers and include information for client autoconfiguration. Using this information the MN obtains a CoA.

2.- Registration: The MN must register (using the Binding Update and the Binding Acknowledgement messages) its CoA to its HA and to its CNs if it wants Route Optimization. In this case, CNs will know WHO the MN (HoA) is and WHERE it is (CoA). Route Optimization is secured through the Return Routability procedure.

3.- Routing and Tunneling: The MN establishes a tunnel with the HA if necessary, and it is able to receive and send data packets using the tunnel or directly by using Route Optimization.

4.- Handover: The MN changes its point of attachment. It must discover in which network it is connected (phase 1) and register its new CoA (phase 2). During this phase some data packets can be lost or delayed due to incorrect MN’s location.

2.1.1 Mobile IPv6’s Return Routability

The Return Routability (RR) procedure authorizes the direct communication between the MN and the CN. In other words, this procedure secures the Route Optimization for Mobile IPv6. The RR procedure enables the CN to obtain some reasonable assurance about the identity of the MN (WHO) and its location (WHERE). Only with this assurance the CN is able to accept Binding Updates from the MN allowing direct communications.

Basically, the RR is done by testing if packets addressed to the HoA (WHO) and CoA (WHERE) are routed to the MN. The MN can pass the test only if it is able to supply proof that it received both packets. Figure 2 shows the schema of the RR procedure.
Once the MN has finished the Agent Discovery and Registration phases (messages 1 and 2) the RR procedure starts. The MN sends two messages at the same time, the Home Test Init and the Care-of Test Init to obtain two “keygen tokens” from the CN. The first message is sent through the Home Agent while the second one is sent directly. The CN replies with the Home Test and the Care-of Test messages. The first one is sent to the MN’s Home Address while the second one is sent directly. Both “keygen tokens” are combined by the MN into a binding management key used to authenticate the Binding Update. At this point the MN and the CN are able to communicate directly.

2.2 Optimizations to Mobile IPv6

Recently several extensions to Mobile IPv6 have been published [5,6,7,8,9,10,11,12,13,14]. Basically, these extensions aim to reduce the handover latency and the signaling overhead between the MN and the CN in the Return Routability procedure. Deploying one of such extensions requires modifying each MN, HA and CN on the Internet. As we will see later our Mobility Agents are compatible with some of these extensions and allow deploying them without modifying the CNs.

Optimized MIPv6 (OMIPv6) [7] is one of the extensions proposed to improve Mobile IPv6. It uses Cryptographically Generated Addresses (CGAs) to authorize the Binding Update. As described in [15] a CGA is an IPv6 address which is generated by hashing the IPv6 address owner’s public key. CGAs allows to the user to provide a reasonable proof of ownership of its IPv6 address. In other words, the CGA offers a method for binding a public key to an IPv6 address. A peer can verify the binding between the public key and the IPv6 address by re-computing and comparing the hash value (and other parameters) of the public key with the user’s IPv6 address.

The OMIPv6 extension is divided into two separate cases, establishing the initial contact and subsequent messaging. The subsequent messaging is much more efficient than the initial one. Figure 3 present the OMIPv6 operations for the initial contact.

Once the MN and the CN have established the initial contact and computed the key if the MN changes its point of attachment it has to send the following signaling messages (figure 4). First it has to send the Care-of Test Init to proof that it is reachable at its new location. Next it has to compute a binding management key by combining the key computed in the initial contact and the “keygen token” of the Care-of Test message. Finally it has to send the Binding Update signed with this key.

The OMIPv6 extension has many benefits in front of MIPv6. First, OMIPv6 provides better security by using CGAs allowing longer binding lifetimes. Second, when the MN has established a binding with its CNs it does not need to rely on its Home Agent to update it. This means that in case of handover the MN does not need to send any packet to its Home Agent. Finally it reduces the signaling overhead (for each handover) and thus, the handover latency.

2.3 Network Mobility

Network Mobility [3] (NEMO) is currently being standardized at the IETF and it has been designed as an extension of Mobile
IPv6. Currently, the NEMO Basic Supports ensures session continuity for all the nodes in a mobile network, even as the Mobile Router changes its point of attachment. It also provides connectivity and reachability for all nodes in the mobile network as it moves. The solution supports both mobile nodes and hosts that do not support mobility in the mobile network.

In NEMO Basic Support a Mobile Router (MR) act as a Mobile IPv6 Node obtaining Care-of-Addresses and registering them on its Home Agent. The MR configures a tunnel with its Home Agent and all the packets from the mobile network are routed through this tunnel. NEMO Basic Support does not implement any sort of Route Optimization. Figure 5 presents a schema.

![Figure 5. NEMO Basic Support](image)

Several proposals have been published [16,17,18,19,20] to provide Route Optimizations for NEMO. Most of them have in common the concept of the Correspondent Router. A Correspondent Router is an entity located at the Correspondent Network that performs Route Optimization on behalf the Correspondent Nodes.

When a host of the mobile network initiates a communication with a Correspondent Node the MR locates by some sort of service discovery the Correspondent Router. Next, the MR initiates an extended Return Routability procedure where it has to prove its location (WHERE) and its identity (WHO). Please note that its identity is not a single address but a network prefix. There are several proposal to extended the Return Routability procedure [21,22] Once the Correspondent Router has authorized the MR, they establish a tunnel and the packets are sent using the optimal path. Figure 6 presents a schema of the NEMO Route Optimization.

![Figure 6. NEMO Route Optimization](image)

Table I and II show the amount of Return Routability signaling messages that a CN has to process (send or receive) for each mobile client.

<table>
<thead>
<tr>
<th></th>
<th>MIPv6</th>
<th>Total Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection</td>
<td>6</td>
<td>378</td>
</tr>
<tr>
<td>Establishment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Handover</td>
<td>4</td>
<td>258</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th></th>
<th>OMIPv6</th>
<th>Total Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Connection</td>
<td>5</td>
<td>514</td>
</tr>
<tr>
<td>Establishment</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Handover</td>
<td>4</td>
<td>280</td>
</tr>
</tbody>
</table>

A CN must process 6 messages (378 bytes) for each Route Optimization connection establishment and, in the best case, 4 messages (258 bytes) for each MN’s handover. The binding maximum lifetime is 7 minutes and thus, the CN will need to re-key with its MNs each 7 minutes (6 messages, 378 bytes). The values are similar when using OMIPv6. However OMIPv6 does not need to send messages through the Home Agent for each handover. Moreover, with OMIPv6 the binding maximum lifetime is 24 hours. The values have not been computed for NEMO because no Route Optimization solution has yet been standardized. Nevertheless, for instance, in [22] each CN needs to process 8 messages (549 bytes) for each connection establishment. For each Mobile Router handover it has to process (best case) 4 messages (258 bytes). Values are similar for other proposals.

Figure 7 shows an analytical evaluation of the amount of signaling messages that a CN must process. The figure shows the number of signaling messages processed by a CN during a time interval where a percentage of MNs are changing its point of attachment. We assume that Mobile IPv6 is being used and that...
30% of the MNs are establishing a connection with the CN during this time interval. With these assumptions we can see that if a CN is serving 8000 mobile clients where 20% of them are changing its point of attachment the CN has to process 20800 signaling messages.

Figure 7. Amount of Signaling Messages

Finally, regarding the amount of mobility signaling messages it is important to remark that there is currently a rapid development in the area of new wireless standards. Nowadays, mobile clients which have radio and protocol support for two or even more standards are appearing. This opens the possibility of using multiple interfaces simultaneously. For instance, a mobile client with two IEEE 802.11 interfaces can speed up the Mobile IPv6 handover by binding one different CoA for each interface [32]. The IETF’s MONAMI6 Working Group [33] is standardizing the use of multiple addresses and interfaces for mobile clients. This means that this type of mobile clients will double (or triple) the amount of signaling messages sent to its CNs.

The RR procedure also requires cryptographic computations. In Mobile IPv6 each MN’s connection establishment or handover requires that the CN computes four SHA1 [23] hashes. In OMIPv6 the CN must compute for each MN’s connection establishment: 5 hashes (SHA1), sign a message using a RSA public key and verify a signed message encrypted with a RSA private key. For each MN’s handover, the CN must compute three hashes (SHA1). Please, take into account that RSA security algorithms require very expensive calculations in terms of CPU/Memory consumption [24].

As we have seen large servers could be overloaded by the Return Routability procedure. Even more, Mobile IPv6 clients require support at the CN. This means that the large server’s kernel must be modified. Moreover several Mobile IPv6 extensions have been published and in order to support them the kernel must be modified again. This would increase the Mobile IPv6’s deployment cost. We believe that a centralized solution such as Mobility Agents solve these issues while providing other benefits.

4. MOBILITY AGENTS

This section presents Mobility Agents (MA), a new entity located at the Correspondent Network that performs Mobile IPv6 operations on behalf the CNs. When a MN initiates a Route Optimized connection with a CN it will run the Return Routability (RR) procedure. The RR’s messages will be intercepted by the Mobility Agent that will process them on behalf the CN. The Mobility Agent will reply to these messages, it will compute the required cryptographic operations to authenticate the MN’s Binding Update and finally it will store the binding between the MN’s Care-of Address (CoA) and the MN’s Home Address. With Mobility Agents the CNs are unaware of mobility issues.

Section 2 has shown how the RR procedure is signaled for Mobile IPv6 and Optimized Mobile IPv6. In an optimized-route data packets exchanged between the MN and the CN use special IPv6 Mobility Extension Headers. Figure 8 shows which extensions headers are used for packets sent by the MN to the CN.

Figure 8. Extension Headers for data packets (MN to CN)

With standard Mobile IPv6 or Optimized Mobile IPv6, if a MN has performed the RR procedure with its CNs the packets are sent using the Home Address Option Extension Header defined in the Mobile IPv6 RFC [1] (figure 8). Packets sent by the MN to the CN have the CoA as source address. This avoids ingress filtering problems at the MN’s foreign network. Destination address for these data packets is the CN’s address. The MN’s Home Address is included into the Home Address Option. This way, when the CN receives the packet it will know the identity of the MN (WHO) by inspecting the Home Address Option Extension Header and the location of the MN (WHERE) by inspecting the packet’s source address. If the CN has a binding between the MN’s CoA and the MN’s Home Address the packet will be accepted and sent for upper layer processing.

Packets sent by the CN to the MN use the Routing Header Type 2 Extension Header as defined in the Mobile IPv6 RFC [1]. Figure 9 shows these data packets.

Figure 9. Extension Headers for data packets (CN to MN)

Packets sent by the CN to the MN must be addressed to a given location (the MN’s CoA) but to a given identity (the MN’s Home Address). The RFC defines that packets will have the MN’s CoA as destination address to avoid egress filtering at the MN’s
foreign network while the Home Address will be included into the Routing Header. When the packet reaches the MN it will forward it to the address defined in the extension header, in this case its own identity. Then the packet will be processed by upper layers as it was sent to the MN’s Home Address.

Optimized Mobile IPv6 follows the same rules than Mobile IPv6 to exchange data packets between the CN and the MN. NEMO uses tunneling to exchange packets between the Mobile Router and the Correspondent Router as it has been shown in figure 6. Actually, packets are also conceptually “tunneled” in Mobile IPv6 Route Optimization. The Mobility Extension Headers represent the outer IP header of this conceptual “tunnel”. This “tunneling” technique has less overhead than the traditional IP over IP one.

4.1 Mobility Agents Operations

4.1.1 Mobility Agents Signaling Interaction

Figure 10 shows how the Mobility Agents perform RR on behalf the CNs for Mobile IPv6.

![Figure 10. Mobility Agents interaction with RR](image)

The Mobility Agent will act as a transparent proxy for the MN, receiving and processing all the signaling messages. When the MN’s Binding Update has been authorized it will store it and it will reply with a Binding Acknowledgement. Mobility Agents can work with other RR procedures such as OMIPv6 or NEMO in the same way.

4.1.2 Mobility Agents Data Exchange Interactions

When the MN sends packets to the CN it includes the Home Address Option. Figure 11 shows how it is processed by the Mobility Agent.

![Figure 11. Home Address Option processing](image)

When a data packet including a Home Address Option is received by the Mobility Agent it will first check if it has a binding between the packet’s source address (CoA) and the Home Address. If it has a binding it will remove the extension header and it will replace the packet’s source address CoA for the MN’s Home Address included into the Home Address Option. This way the CN will receive a packet from the MN’s Home Address and it will process it normally. This procedure is very similar to the Mobile IPv6 CN support.

When the CN sends packets to the MN in Mobile IPv6 it includes the Routing Header, however with Mobility Agents CNs do not have Mobile IPv6 support and thus, they send the packets as stated by the IPv6 RFC [25]. As shown in figure 12 the packet will be received by the Mobility Agent and it will check if it has a binding for the packet’s destination address (the MN’s Home Address). If it does not have a binding it will forward it as defined in the IPv6 standard. However if a binding exists it will replace the packet’s destination address with the MN’s CoA and will add the Routing Header Type 2 Extension Header. This extension header will include the MN’s Home Address. The Mobility Agent will also set the Next Header field accordingly to the new extension header. This procedure is very similar to the Mobile IPv6 CN support.

![Figure 12. Routing Header processing](image)

Our Mobility Agents act as the “tunnel” endpoints. The “tunnel” is established between the MN and the Mobility Agent. Please note that this “tunnel” is conceptual and does not use the traditional IP over IP technique.

4.1.3 Mobility Agents Location

Our Mobility Agent has to receive all the packets exchanged between the MN and the CN, and thus it must be placed on the path between both nodes. Due to MN’s movement the path between both nodes will change and thus the Mobility Agent must be placed at the Correspondent Network border router. We assume that the Correspondent Network is single-homed. In the case that the Correspondent Network is very large the Mobility Agents can be placed in each access router (figure 13) to avoid scalability issues.

![Figure 13. Mobility Agents Location](image)
3. The AH authentication data (ICV) is calculated as is the following was true. The packet’s destination address contains the MN’s Home Address and the Routing Header contains the MN’s CoA.

Please note that the Mobile IPv6 RFC defines that the ICV calculation must be done exchanging the destination address field with the Routing Header field.

Our Mobility Agents can not deal with IPSec protected packets because they modify the packet. If Mobility Agents were used with an IPSec connection the ICV verification would fail at the destination.

NEMO solves this issue by creating a tunnel between the Mobile Router and the Correspondent Router. This way, inner packets are not modified. However, as it has been said before, the Mobile IPv6 data exchange is actually a “tunneling” technique. Instead of inserting a whole new IP header Mobile IPv6 uses the Home Address Option and the Routing Header. The traditional tunneling technique [28] uses four IP address: the source and destination addresses and the two tunnel endpoint IP addresses. Mobile IPv6’s “tunnel” requires just three addresses: the MN’s CoA, the MN’s Home Address and the CN’s address. The Mobile IPv6’s “tunnel” is configured between the CN’s address and the MN’s CoA while the “inner” packet has the CN’s address and the MN’s Home Address. This “tunneling” [29] technique was specially designed for Mobile IPv6 because it has less overhead. Figure 14 presents a comparison.

In fact, in standard Mobile IPv6, packets are processed at the destination as if they were tunneled. In this case, the extension headers (Home Address Option or Routing Header) represent the outer IP header of the traditional tunnels. This header is removed and the IP source or destination address is replaced by the address contained in the extension header. Finally, after this replacement, the modified IP header represents the inner IP header. The resulting packet of this process reaches its destination as if the mobile node was at home and it was sent from or to the Home Address.

We claim that, if we accept that Mobile IPv6 “tunnels” packets, data packets exchanged between the MN and the CN with Route Optimization should be processed as tunneled packets. With this
assumption, a Mobile IPv6 data packet should be assembled without including the Home Address Option or the Routing Header into the ICV calculation. Please note that the ICV calculation does not include the outer IP header of a tunnel [26]. In this case, the outer IP header is included after the ICV calculation and it will be removed before it arrives to its destination. Thus, we propose that Mobile IPv6 packets sent by the MN to the CN are assembled as follows (figure 15):

1.- The data packet is created by higher layer protocols and applications (e.g., by TCP) as if the mobile node were at home and Mobile IPv6 were not being used. The packet’s source address contains the MN’s Home Address while the packet’s destination address contains the CN’s address.

2.- The AH authentication data (ICV) is calculated.

3.- Next the packet is “tunneled” by inserting the Home Address Option Extension Header. The packet’s source address is set to the MN’s CoA and the Home Address Option is set to the MN’s Home Address.

With Mobility Agents, the CN does not need mobility support. In this case, the CN will assemble the packet following the rules defined in the IPv6 RFC [25]:

1.- The data packet is created by higher layer protocols and applications (e.g., by TCP) as if the mobile node were at home and Mobile IPv6 were not being used. The packet’s destination address contains the MN’s Home Address while the packet’s source address contains the CN’s address.

2.- The AH authentication data (ICV) is calculated.

3.- Next the packet is “tunneled” by inserting the Home Address Option Extension Header. The packet’s source address is set to the MN’s CoA and the Home Address Option is set to the MN’s Home Address.

The MN will replace the destination address with its own Home Address. Finally it will verify the ICV by calculating it on the same way than the CN did.

With this simple modification our Mobility Agents are also compatible with Mobile IPv6 IPSec connections. It is important to remark that we propose to modify how Mobile IPv6 data packets are assembled, not the IPSec or the IPv6 standard. This modification only affects Mobile IPv6 implementations.

4.2.1 Security Considerations

Modifying how Mobile IPv6 packets are assembled when they interact with IPSec can introduce new security threats. In this subsection we will analyze these threats.

It is very important to remark that although the Mobility Extension Headers are not protected by the ICV the contained Home Address is indeed protected. The ICV was computed as if the MN was at home. Then, the Mobility Agent or the MN replaced the Home Address for the CoA. This means that actually the CoA is not protected by the ICV.

We will consider two separated cases. First we will analyze the security considerations when packets are sent from the CN to the MN. Next when packets are sent from the MN to the CN, packets sent by the CN to the MN are as follows:

- Packet’s source address: CN’s address
- Packet’s destination address: MN’s CoA address
- Routing Header : MN’s Home Address

However, the ICV has been computed with the following IP header and without including mobility extension headers:

- Packet’s source address: CN’s address
- Packet’s destination address: MN’s Home Address

This means that an attacker could change the packet’s destination address (CoA) by using a Man-in-the-Middle attack. This would route the packet to a different destination. This attack is also possible even if the ICV computation includes the mobility extension header.

Packets sent by the MN to the CN are as follows:

- Packet’s source address: MN’s CoA address
- Packet’s destination address: CN’s address
- Home Address Option : MN’s Home Address

However, the ICV has been computed with the following IP header and without including mobility extension headers:

- Packet’s source address: MN’s Home Address
- Packet’s destination address: CN’s address

This means that an attacker could change packet’s source address (CoA) using a Man-in-the-Middle attack. The packet will reach the Mobility Agent. This entity would check if a binding exists between the packet’s source address and the MN’s Home Address. As the packet’s source address has been modified by the attacker the binding does not exists and thus the packet is discarded. If the binding exists because the attacker is trying to impersonate another MN then the CN will also drop the packet.

As it has been explained before, the Home Address is included into the ICV computation and the attacker is not able to forge and encrypt an ICV which includes the victims Home Address. In
fact, the MN’s CoA is protected by the binding stored at the Mobility Agent which is at the same time protected by the Return Routability procedure. The MN’s Home Address is protected by the ICV value.

An attacker could also modify the packet sending malformed mobility extension headers. This would drop the packet at the destination. This is also possible even if the ICV computation includes the mobility extension header.

As it has been demonstrated our modification of data packets assembly in Mobile IPv6 when Route Optimization and IPSec are used does not introduce new security threats.

### 4.2.2 Mobility Agents Legacy Support

Modifying how Mobile IPv6 data packets are assembled when IPSec and Route Optimization are used can introduce incompatibility issues with legacy Mobile IPv6 nodes. In this subsection these issues are considered. It is important to remark that our Mobility Agents are compatible with legacy Mobile IPv6 nodes when IPSec is not used. Only if IPSec is used incompatibility issues arise.

To provide compatibility with legacy Mobile IPv6 nodes we will use the reserved field of the Care-of-Test Init message (figure 16). This message is the first one sent in the Return Routability procedure. By using this message we are minimizing the amount of useless signaling sent by unmodified Mobile IPv6 nodes. The Mobile IPv6 RFC [1] defines that this field must be set to zero.

![Figure 16. Care-of Init Message](image)

Modified Mobile IPv6 nodes must compute the Reserved field using the following rules (figure 17):

![Figure 17. Modified Reserved Field](image)

The first byte indicates whether the Mobile IPv6 node has Mobility Agents IPSec support or not. The second byte indicates which version of the Return Routability procedure is supported by the MN. Table III presents the proposed values for the different Return Routability procedures:

<table>
<thead>
<tr>
<th>Reserved Field Value</th>
<th>Support</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000000000000000</td>
<td>Unmodified MIPv6 node</td>
</tr>
<tr>
<td>0000000100000000</td>
<td>Mobility Agent support with standard RR</td>
</tr>
<tr>
<td>0000000010000000</td>
<td>Mobility Agent support with OMIPv6</td>
</tr>
</tbody>
</table>

When an unmodified Mobile IPv6 node sends the Care-of-Test Init message with the Reserved field set to zero the Mobility Agent will recognize it as an unmodified node and will send an ICMP parameter problem code 1. The Mobile IPv6 node will then revert to bidirectional communication with the Home Agent to reach the CN. The unmodified MN will be able to communicate with the CN but without Route Optimization. This particular case is the same than when the CN does not have mobility support.

When a modified Mobile IPv6 node sends the Care-of-Test init with the first byte set to 00000001 and the second byte set to the supported Return Routability procedure the Mobility Agent will act as explained in subsections 4.1 and 4.2.

### 4.3 Mobility Agents and NEMO

Mobility Agents can also be used with NEMO. In NEMO the Mobility Agent can be placed at the Correspondent Router to run the RR procedure on behalf the CNs.

Moreover in all the NEMO’s Route Optimization proposals such as [16,18,19,20] the Correspondent Router tunnels the packets with its Mobile Routers. However if Mobility Agents where used, packets could be sent using the mobility extension headers. These extension headers provide better efficiency in terms of data overhead. The traditional tunneling technique uses two IPv6 headers [28]: 80 bytes in total. The mobility extension headers use just one IPv6 header with options. Packets sent with the Home Address Option have 60 bytes in total while packets sent with the Routing Header have 64 bytes in total. This means that our Mobility Agents reduce up to 25% of data packet’s overhead when used with NEMO Route Optimization.

### 5. MOBILITY AGENTS EVALUATION

Mobility Agents are actually a Mobile IPv6 transparent proxy that runs the Return Routability procedure in a centralized fashion. This section presents the typical benefits and drawbacks of centralized solutions in front of the distributed ones. Moreover it also presents the specific benefits provided by Mobility Agents.

#### 5.1 Centralized Vs. Distributed Solution Discussion

**Deployment Cost:** On one hand, centralizing the RR procedure with Mobility Agents for all the Correspondent Nodes of a network would reduce the Mobile IPv6’s deployment cost. Mobile IPv6 requires CN’s specific support to run the RR procedure. This means that if a large content provider wants to support Mobile IPv6 clients it needs to modify the kernel of each of its servers. Probably this cost is similar to the IPv6’s deployment cost. In fact Mobile IPv6 support should be included into IPv6 kernel implementations. However, as the OMIPv6 proposal has demonstrated other RR protocols may exist. Even more, a large content provider may want to implement a proprietary RR procedure with its own costumers. By introducing Mobility Agents the deployment cost is reduced. A large content provider has just to upgrade its border router with a new Mobility Agent implementation. Even more, a later upgrade of the RR procedure for any mobility protocol such as NEMO or Mobile IPv6 can be easily deployed.

**Policy, Configuration and Management:** Large content provider administrators may need to configure and manage the mobility protocol support. With Mobility Agents the cost of configuring and managing is reduced because it is centralized.
Hardware Support: Large server’s hardware may not be intended to process the RR’s signaling messages and its cryptographic operations. Mobility Agents can be implemented on a router that may have specific hardware to run these operations.

Single Failure Points: It is also important to consider that centralized solutions introduce single failure points. However our Mobility Agents are placed at the border router and thus, the whole system is as reliable as the distributed one. A failure at a border router would interrupt the Internet connectivity in any case.

Scalability Issues: Finally, centralized solutions usually have scalability issues. However, as it has been explained before (subsection 4.1.3), our Mobility Agents can be placed at the CN’s access router instead of at the border router. In this case each Mobility Agent would serve very few CNs avoiding the scalability problems.

5.2 Mobility Agents Benefits
The Mobility Agent main advantage and goal is to avoid processing all the Return Routability signaling messages and the related cryptographic computations at the Correspondent Nodes. Our solution is basically intended for large content providers where each Correspondent Node may have thousands of simultaneous mobile clients.

A very interesting functionality of Mobility Agents is that they allow pre-established shared secrets with the MNs. The Return Routability procedure can be easily implemented using preconfigured shared keys. Standard Mobile IPv6 does not have this functionality because it is not feasible to distribute shared keys among all MNs and CNs on the Internet. However with Mobility Agents a large content provider can distribute shared secrets among its clients and implement its own Return Routability procedure. Another typical example scenario where this mechanism is applicable is within a corporation or between specific users. A Return Routability procedure based on symmetric keys [6] is much faster and secure than the traditional one. This RR procedure requires just 2 direct messages (132 bytes) for each MN’s connection establishment or handover. This means that the RR based in shared keys reduces the handover latency to one round trip time and the signaling overhead to just 2 messages. Moreover it requires less cryptographic computations than OMIPv6.

6. RELATED WORK
Several papers have presented solutions that run the Return Routability procedure on behalf the Correspondent Nodes. In [30] the authors present an agent-based route optimization for Mobile IPv4. In their proposal, a special entity located at the Correspondent Network border router achieves Route Optimization on behalf the Correspondent Nodes. Data packets are tunneled between the special entity and the MNs. Our Mobility Agents is intended for Mobile IPv6 instead of Mobile IPv4. Moreover, with our solution packets are not tunneled but sent using the mobility extension headers. These headers provide less overhead (25%) than the traditional tunnelling technique.

In [31] authors propose a bi-directional route optimization for Mobile IPv4. With the author’s solution, a special entity called Correspondent Agent is placed at the correspondent network border router. This entity also achieves Route Optimization on behalf the Correspondent Nodes. Another special entity (Foreign Agent) is placed at the MN’s visited network. The Correspondent Agent establishes a bi-directional tunnel with the Foreign Agent to send and receive data packets. Authors also present a binding optimization. In this case the Correspondent Agent can send the network prefix of its correspondent network to the Foreign Agent. This binding allows optimizing routes for entire networks. However, in the author’s proposal this binding is not secured or authorized in any way. This is an important issue because a malicious correspondent node could send a fake network prefix to the Foreign Agent redirecting all the traffic to a victim.

The NEMO protocol also introduces an entity called Correspondent Router that achieves Route Optimization on behalf the correspondent nodes. This entity was proposed in [16]. Since NEMO has not yet a standard Return Routability procedure most of the research efforts have focused on this. Different papers such as [21,22] propose different algorithms for the NEMO Return Routability procedure. All the proposed solutions establish a tunnel between the Mobile Router and the Correspondent Router. Our Mobility Agents can act as Correspondent Routers using the mobility extension headers instead of tunneling.

7. CONCLUSIONS
The Return Routability procedure is used to achieve Route Optimization for the different mobility protocols. Different mobility protocols have different Return Routability procedures according to their special requirements. This procedure is typically performed by CNs. As recent publications demonstrate the Return Routability procedure is still an on-going research topic.

If one of such mobility protocols was deployed on the Internet, typically CNs would be large serves with thousands of mobile clients. The CNs would need to perform the Return Routability procedure for each mobile client connection establishment and handover. We believe that this work may overload the serves and may be a drawback for the protocol’s deployment.

We propose Mobility Agents, a special entity located at the correspondent network border router that centralizes the Return Routability procedure. In this paper we have shown how to centralize the Return Routability procedure for different mobility protocols without modifying the CNs. As it has been demonstrated, our centralized solution is compatible with IPsec connections and does not introduce new security threats. Moreover it does not use tunnels like the previous proposals reducing the data packet’s overhead up to 25%. Finally, our solution reduces the deployment cost of the different mobility protocols allowing upgrading the Return Routability procedure. Even more, it allows Return Routability solutions based on preconfigured shared secrets.

Many open issues still need further investigation. One promising area is to evaluate how our Mobility Agents can benefit server load balancing with mobile clients. We also plan to investigate the benefits of allowing aggregated bindings for all the CNs served by a Mobility Agent. Finally, we aim to expand our solution to multihomed correspondent networks.

8. ACKNOWLEDGMENTS
This work was partially funded by the Spanish Ministry under contract TSI2005-07-250-C03-02, the Generalitat de Catalunya
under contract 2005-SGR-00481 and the European Commission under contract FP6-0384239-CONTENT.

9. REFERENCES
[27] S. Kent. IP Authentication Header. RFC 4302, December 2005