MOBILITY AGENTS: AVOIDING THE SIGNALING OF ROUTE OPTIMIZATION ON LARGE SERVERS

Albert Cabellos-Aparicio and Jordi Domingo-Pascual*
Technical University of Catalonia,
Department of Computer Architecture
Barcelona, Spain

ABSTRACT
A foreseeable scenario is where, on the Internet, Mobile IPv6 is deployed and a large percentage of the clients are mobile nodes. These mobile clients will communicate with large servers, which under the point of view of Mobile IPv6 will be Correspondent Nodes. 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 the Route Optimization of Mobile IPv6. These issues may be a drawback for the deployment of Mobile IPv6. 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 are compatible with NEMO and other mobility protocols. Moreover they allow deploying different extensions of Mobile IPv6 such as Optimized MIPv6 without modifying the Correspondent Nodes.

I. INTRODUCTION
Mobile IPv6 [1] is considered to be one of the key technologies 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.

In Mobile IPv6 a Mobile Node has two identifiers. The first one identifies the identity (WHO) of the Mobile Node (MN). The second one identifies the current location (WHERE) of the MN. 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 home network of the MN will maintain bindings between the WHO and WHERE identifiers. The MN will inform 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 sub-optimal path. This sub-optimal path has many drawbacks [17]. First, the longer route increases delay and infrastructure load. Such increase may not be tolerated by time sensitive applications. Moreover, the total network resource utilization is higher due to the longer path. Second the MN encapsulates packets to the Home Agent and thus, the sub-optimal path leads to an increased packet overhead. This tunnel may also lead to an increase of the processing delay due to the encryption/decryption and other verifications of the packets. In addition, it may also increase the chances of the packets being fragmented due to the increased packet size. Third, as the sub-optimal path is longer it is less robust against link-failures. And finally, since all the packets to and from MNs are forwarded through the Home Agent, the Home Agent itself or the Home Link may be overloaded.

If the MN wants to communicate using a direct path (Route Optimization) it has to inform its Correspondent Nodes (CN) about its location changes. These CNs (usually 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 make more difficult the deployment of Mobile IPv6. Moreover these large servers are content providers and their hardware may not be intended to perform this sort of operations.

In this paper we extend our Mobility Agents [2,3]. A Mobility Agent (MA) is able to process the messages of the Mobile IPv6 Route Optimization. This entity is located at the Correspondent Network border router and it will process the messages of the Route Optimization procedure on behalf of the CNs. With MAs, Mobile IPv6 can be deployed flawlessly because it does not require support of the CNs. The deployment of Mobile IPv6 at the Correspondent Network is as easy as plug and play with MAs.

In our previous work [2] we detailed an important incompatibility between the Route Optimization of Mobile IPv6 and several load balancing techniques. Then, we first introduced MAs in order to solve this issue. In that work, a MA was embedded into a load balancing device. Next [3] we extended our MAs to Home Networks in order to provide a novel Home Agent architecture. This architecture provided reliability and load balancing to Home Agents.

In this present paper we extend our MAs to Correspondent Networks. The most significant contributions of this paper are:

- Support of Route Optimized connections without involving the CN
- Compatibility with legacy MNs
- Support of IPSec connections

II. MOBILITY AGENTS
This section presents our Mobility Agents (MA), a new entity located at the Correspondent Network that performs the operations of Mobile IPv6 on behalf the CNs. When a MN initiates a Route Optimized connection with a CN it will run the Return Routability procedure. The messages of this procedure will be intercepted by the MA that will process them on behalf the CN. The MA will reply to these messages.

*This work was partially funded by IST under contract IST-2006-NoE-0384239 (IST-CONTENT), MEC (Spanish Ministry of Education and
it will compute the required cryptographic operations to authenticate the Binding Update and finally, it will store the binding between the Care-of Address (CoA) of the MN and the Home Address of the MN. With MAs the CNs are unaware of mobility issues. In fact, they do not need Mobile IPv6 support at all.

A. Mobility Agents Signaling Interaction

Figure 1 shows how the MAs performs the Return Routability procedure on behalf the CNs for Mobile IPv6.

![Figure 1: Mobility Agents Interaction with Return Routability](image)

The MA will act as a transparent proxy for the MNs, receiving and processing all the signaling messages. When the Binding Update of the MN has been authorized it will store it and it will reply with a Binding Acknowledgement. MAs can work with other Return Routability procedures such as OMIPv6 [4] or NEMO [5] in the same way.

B. Mobility Agents Data Exchange Interaction

When the MN sends packets to the CN it includes the Home Address Option [1]. Figure 2 shows how it is processed by the MA.

![Figure 2: Home Address Option processing](image)

When a data packet including a Home Address Option is received by the MA it will first check if it has a binding between the source address of the packet (CoA) and the Home Address. If it has a binding it will remove the extension header and it will replace the source address of the packet (CoA) with the Home Address of the MN included into the Home Address Option. This way the CN will receive a packet from MN as if it were at home, and it will process it normally. When the CN sends packets to the MN in Mobile IPv6 it includes the Routing Header, however with MAs, CNs do not need Mobile IPv6 support and thus, they send the packets as stated by the IPv6 RFC [6]. As shown in figure 3, the packet will be received by the MA and it will check if it has a binding for the destination address of the packet (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 destination address of the packet with the CoA of the MN and it will add the Routing Header Type 2 Extension Header. This extension header will include the Home Address of the MN. The MA will also set the Next Header field according to the new extension header.

![Figure 3: Routing Header processing](image)

Our MAs act as the “tunnel” endpoints. The “tunnel” is established between the MN and the MA. It is important to remark that this “tunnel” is conceptual and does not use the traditional IP over IP technique.

C. Mobility Agents Location

Our MA 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 movements of the MN the path between both nodes may change and thus, the MA must be placed at the border router of the Correspondent Network. We assume that the Correspondent Network is single-homed. In the case that the Correspondent Network is very large or multihomed, the MAs can be placed in each access router to avoid scalability issues.

D. Mobility Agents Interaction with IPSec

Our MAs should take into account what happens when the Route Optimization of Mobile IPv6 is used with IPSec in transport mode (IPSec is tunnel mode is fully compatible with MAs). IPSec in transport mode uses one parameter that affects the operations of our MAs. This parameter is the Integrity Check Value (ICV) which belongs to the Authentication Header [7,8] protocol. The ICV field is used to provide integrity to the communications and covers the entire packet. The Mobile IPv6 RFC [1] specifies that packets sent by the MN that use IPSec in transport mode must be assembled in the following way:

1. The data packet is created by higher layer protocols and applications (e.g., by TCP) as if the MN were at home and Mobile IPv6 were not being used.
2. The Home Address Option Extension Header is inserted. The source address of the packet is set to the CoA of the MN and the Home Address Option is set to the Home Address of the MN.
3. The Authentication Header authentication data (ICV) is calculated as is the following was true. The source address of the packet contains the Home Address and the Home Address Option contains the CoA.
Please note that the Mobile IPv6 RFC defines that the ICV calculation must be done exchanging the source address field with the Home Address Option field. The packets sent by the CN to the MN when Route Optimization and IPSec are used are assembled in the following way:

1. The data packet is created by higher layer protocols and applications (e.g., by TCP) as if the MN were at home and Mobile IPv6 were not being used.
2. The Routing Header is inserted. The destination address of the packet is set to the CoA and the Routing Header to the Home Address.
3. The AH authentication data (ICV) is calculated as is the following was true. The destination address of the packet contains the Home Address and the Routing Header contains the CoA.

Once again, the RFC defines that the ICV calculation must be done exchanging the destination address field with the Routing Header field. Our MAs can not deal with IPSec protected packets because they modify the packet. If MAs were used with an IPSec connection the ICV verification would fail at the destination. Different approaches to the Route Optimization of NEMO [17] solve this issue by creating a tunnel between the Mobile Router and the Correspondent Router. This way, inner packets are not modified. However, packets sent in an optimized route of Mobile IPv6 are actually “tunneled”. Instead of inserting a whole new IP header, Mobile IPv6 uses the Home Address Option and the Routing Header. The traditional tunneling technique [9] uses four IP address: the source and destination addresses and the two tunnel endpoint IP addresses. The “tunnel” of Mobile IPv6 requires just three addresses: the CoA, the Home Address and the address of the CN. The “tunnel” of Mobile IPv6 is configured between the address of the CN and the CoA while the “inner” packet has the address of the CN and the Home Address. This “tunneling” [10] technique was specially designed for Mobile IPv6 because it has less overhead (25%).

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, the modified IP header represents the inner IP header. The resulting packet of this process reaches its destination as if the MN 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. Under 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 [7,8]. In this case, the outer IP header is included after the ICV calculation and the header will be removed before it arrives to its destination. Thus, we propose that packets sent by the MN to the CN are assembled as shown in figure 4:

1. The data packet is created by higher layer protocols and applications (e.g., by TCP) as if the MN were at home and Mobile IPv6 were not being used. The source address of the packet contains the Home Address while the destination address of the packet contains the address of the CN.
2. The AH authentication data (ICV) is calculated.
3. Next the packet is “tunneled” by inserting the Home Address Option Extension Header. The source address of the packet is set to the CoA and the Home Address Option is set to the Home Address.

With MAs, the CN does not need mobility support. In this case, the CN will assemble the packet following the rules defined in the IPv6 RFC [6].

The CN will send the packets addressed to the Home Address. This packet will be intercepted by our MAs. As explained before, the MA will check if it has a binding for this particular Home Address. If it does not have a binding it will forward it as defined in the IPv6 RFC [6]. Otherwise it will “tunnel” the packet by inserting the Routing Header. The MA will also change the destination address of the packet to the CoA. Then, the Routing Header of the packet will include the Home Address. Finally, when the packet reaches the MN it will remove the Routing Header and 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 MAs are also compatible with 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 to the implementations of Mobile IPv6.

E. Security Considerations

Modifying how data packets of Mobile IPv6 are assembled when they interact with IPSec in transport mode can introduce new security threats. In this subsection we 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 MA or the MN replaced the

Figure 4: Proposed packet assembly at the MN

![Diagram of proposed packet assembly at the MN](image-url)
Home Address with the CoA. This means that actually the CoA is not protected by the ICV.

We consider two separated cases. First we 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:

- Source address of the packet: Address of the CN
- Destination address of the packet: CoA
- Routing Header : Home Address

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

- Source address of the packet: Address of the CN
- Destination address of the packet: Address of the CN
- Home Address Option : Home Address

This means that an attacker could change the destination address of the packet (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:

- Source address of the packet: CoA
- Destination address of the packet: Address of the CN
- Home Address Option : Home Address

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

- Source address of the packet: Home Address
- Destination address of the packet: Address of the CN

This means that an attacker could change the destination address of the packet (CoA) by using a Man-in-the-Middle attack. The packet will reach the MA. This entity would check if a binding exists between the source address and the Home Address of the MN. As the 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 Home Address of the victim. In fact, the CoA is protected by the binding stored at the MA which is, at the same time, protected by the Return Routability procedure. The Home Address is always protected by the ICV value.

An attacker could also modify the packet, sending a malformed mobility extension header. 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 how data packets are assembled in Mobile IPv6 when Route Optimization and IPSec in transport mode are used does not introduce new security threats.

F. Mobility Agents Legacy Support

Modifying how Mobile IPv6 data packets are assembled when IPSec in transport mode 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 MAs are compatible with legacy Mobile IPv6 nodes when IPSec in tunnel mode is used. Only if IPSec in transport mode is used incompatibility issues arise.

To provide compatibility with legacy Mobile IPv6 nodes we use the reserved field of the Care-of-Test Init message (figure 5). 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.

![Figure 5: Care-of Init message](image)

Modified Mobile IPv6 nodes must compute the Reserved field using the following rules (figure 6):

![Figure 6: Modified reserved field](image)

The first byte indicates whether the Mobile IPv6 node has MA IPSec support or not. When an unmodified Mobile IPv6 node sends the Care-of-Test Init message with the Reserved field set to zero the MA 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 the MA will act as explained in subsection II.

III. MOBILITY AGENTS EVALUATION

MAs are actually a Mobile IPv6 transparent proxy that runs the Return Routability procedure in a centralized fashion. This section presents the major benefits and drawbacks provided by our proposal.

The MA main advantage and goal is to avoid processing all the Return Routability signaling messages and the related cryptographic computations at the CNs. Our solution is basically intended for large content providers where each CN may have thousands of simultaneous mobile clients.

First our MAs reduce the deployment cost. Mobile IPv6 requires specific support of the CNs to run the Run Routability 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. However with MAs a large content provider has just to upgrade its border router (or access router) with a MA implementation.

Second, the hardware of large servers may not be intended to process the signaling messages of the Return Routability procedure and its cryptographic operations. MAs can be implemented on a router that may have specific hardware to run these operations.
A very interesting functionality of MAs 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 MAs, a large content provider can distribute shared secrets among its clients and implement its own Return Routability procedure. Another typical example of a scenario where this mechanism is applicable is within a corporation or between specific users. A Return Routability procedure based on symmetric keys [11] is much faster and more secure than the traditional one. This Return Routability procedure requires just 2 direct messages (132 bytes) for each connection establishment or handover. This means that the Return Routability procedure based on symmetric keys reduces the handover latency to one round trip time and the signaling overhead to just 2 messages.

Finally, our MAs may not be scalable, however, as it has been explained before (subsection II.C), our MAs can be placed at the access router of the CN instead of at the border router. In this case, each MA would serve very few CNs, avoiding the scalability problems.

IV. RELATED WORK

Several papers have presented solutions that run the Return Routability procedure on behalf of the CNs. In [12], 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 of the CNs. Data packets are tunneled between that special entity and the MNs. In [13], authors propose a bi-directional route optimization for Mobile IPv4. With the authors’ solution, a special entity called Correspondent Agent is placed at the correspondent network border router. This entity also achieves route optimization on behalf of the CNs. Another special entity (Foreign Agent) is placed at the visited network of the MN. The Correspondent Agent establishes a bi-directional tunnel with the Foreign Agent to send and receive data packets. The NEMO protocol also introduces an entity called Correspondent Router that achieves route optimization on behalf of the CNs. This entity was first proposed in [14]. Since NEMO has not yet a standard return Routability procedure most of the research efforts have focused on this. Different papers such as [15,16] propose different algorithms for the Return Routability procedure of NEMO. All the proposed solutions establish a tunnel between the Mobile Router and the Correspondent Router.

Our MAs are 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 tunneling technique. Finally, they support IPSec connections and legacy MNs.

V. CONCLUSIONS

A foreseeable scenario is where, on the Internet, Mobile IPv6 is deployed and a large percentage of the clients are mobile nodes. These mobile clients will communicate with large servers. The Return Routability procedure is used to achieve route optimization for Mobile IPv6. This allows direct communication between the MNs and the large servers. However, this procedure includes sending and receiving signaling messages, cryptographic calculations, storing a state and it must be performed for each connection and for each handover. This can represent a very significant load on these large servers and they must be modified in order to support it. 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 without modifying the CNs. In addition, our MAs are compatible with Mobile IPv6, NEMO, OMIIPv6 and other mobility protocols. 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 overhead of the data packets to 25%.

REFERENCES