Extending Home Agent Migration To Mobile IPv6 based Protocols

Guillaume Valadon[1] and Ryuji Wakikawa[2]

[1] Université Pierre et Marie Curie-Paris 6 - guillaume.valadon@lip6.fr
[2] KEIO University - ryuji@wide.ad.jp

Abstract. Defined at the IETF, the Mobile IPv6 protocol allows a single mobile node to keep the same IPv6 address independently of its network of attachment. It was recently enhance so as to augment its applicability. One of these extensions, NEMO, NEtwork MObility makes it possible to move a whole network, such as sensors deployed in a car, in the Internet topology. On the other hand, Proxy Mobile IPv6 provides Mobile IPv6-like services to standard IPv6 nodes. While these three protocols are actually heavily supported by the industry and deployed in 3GGP2, WiMAX and ITS, they suffer from several performances issues. Most of them are caused by the Home Agent, a specific router located on the home network, that hides movements of mobile nodes to their correspondents. The restricted position of the home agent is responsible for longer communications delays and higher path lengths. In one of our previous work, Home Agent Migration, we described how to significantly reduce these issues by deploying multiple home agents in the Internet topology. In this paper, we discuss the possible extensions to this specific architecture in order to support and enhance NEMO and Proxy Mobile IPv6. Furthermore, we analyze Home Agent Migration in terms of security so as to provide detailed guidance for secure real life deployments and safe usages.

1 Introduction

Mobile phones are entirely part of our daily life. We use them not only for work but also to communicate with friends, access the Internet or play games. They are slowly changing the way people interact with each other [1] and how we access the information. Indeed in 2006, mobile devices in Japan represents 57%[3] of all user access to the Internet. Moreover, usages of mobile phones have recently changed thanks to dual-mode GSM/WiFi handsets and Voice over IP services. Customers are now used to make cheap phone calls wherever they are. Therefore, mobility is one of the key feature for future Internet based technologies. Following these trends, we expect that the next evolution of customers' usages will likely require vertical handovers to provide seamless voice calls between access technologies such as WiFi and HSDPA. Consequently, there is a need to develop efficient

[3] owned by approximately 48 million people, according to The Japanese Ministry of Internal Affairs and Communications

mobility services at the IP layer so as to keep phone calls valid after a change of IP address.

While not extensively deployed yet, mobility protocols were already standardized at the Internet Engineering Task Force (IETF). Here, we focus on the Mobile IPv6 [2] protocol. It provides a permanent IP address to a mobile node independently of its network of attachment thanks to a home agent, a dedicated Mobile IPv6 router. Several extensions such as NEMO [3] and Proxy Mobile IPv6 [4] were also normalized. They respectively delivered Mobile IPv6-like mobility service to whole networks, such as sensors deployed in a car, and to standard IPv6 nodes that do not implement Mobile IPv6 on the client side[4]. However, the base Mobile IPv6 protocol is inappropriate for efficient deployments as it has several issues. One of them, called dogleg routing, is especially important as it induces longer path and higher communications delays.

In our previous work, Home Agent Migration [5], we introduced a distributed architecture of home agents that effectively solves the dogleg routing in Mobile IPv6. Using anycast routing, home agents are distributed in the Internet topology, and advertise a unique IPv6 prefix from these different locations. Therefore, a mobile node is always associated with its closest home agent in terms of the network topology, reducing the effects of the dogleg routing. In this paper, we describe how Home Agent Migration could be extended to support both NEMO and Proxy Mobile IPv6 so as to enhance their performances. It is an important contribution as these two protocols are currently being studied to provide IP layer mobility to WiMAX networks [6]. Moreover, we also provide a comprehensive discussion on security related issues from an operator perspective. This is the second contribution of this paper that could be used to achieve efficient deployments of Mobile IPv6 based protocols that fulfills real life usages.

This paper is organized as follows. Section 2 presents the Mobile IPv6 protocol and its extensions NEMO and Proxy Mobile IPv6. In Section 3, we first introduce Home Agent Migration, then describe two typical deployments and finally discuss its use with the two extensions. Finally, in Section 4, security implications of Mobile IPv6 and Home Agent Migration concerning mobile, correspondent nodes and the network infrastructure are given.

2 Mobile IPv6 and its extensions

In this section, the Mobile IPv6 protocol is first described in details. Then, its two major extensions, NEMO, and Proxy Mobile IPv6, and their common uses are discussed. Finally, the limitations of these three protocols are given so as to understand what is the benefit of extending our previous work, Home Agent Migration, to enhance them.

[4] referred as mobile node in the Mobile IPv6's terminology

2.1 Mobile IPv6

On the Internet, the location of a node is strongly constrained by the routing architecture. An IPv6 address that belongs to an IPv6 prefix allocated to a French Internet Service Provider cannot be used to receive packets in Japan. Consequently, the current Internet architecture makes it impossible to keep the same address when a nodes move. This problem is linked to the dual function of the IP address. First, it implicitly provides the position of a node on the globe; this role is called *locator*. Then, it uniquely identifies the node in the whole Internet topology; this second role is called *identifier*. The Mobile IPv6 protocol provides a solution to separate this two functions. From now on, a mobile node uses two different IP addresses: the Home Address, HoA, and the Care-of Address, CoA.

1. the CoA changes when the mobile node moves; it is the *locator*. This is an IPv6 address belonging to the network where the mobile node is physically located. It allows IP packets to be routed to the mobile node.
2. the HoA is a fixed address that belongs to the home network of the mobile node; it is its *identifier*. It is transparently used by the upper layers, such as TCP and UDP, that do not perceive that Mobile IPv6 is used to communicate with correspondents nodes over the Internet.

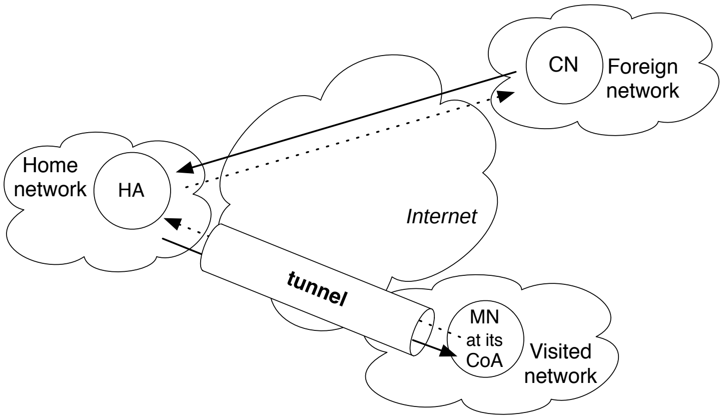

Fig. 1. Mobile IPv6

Correspondents of the mobile node are not aware of these two addresses, neither of its movements, and always communicate with the mobile node using the Home Address. A router called the Home Agent, HA, specific to Mobile IPv6, is located in the home network and performs the relation between the CoA and the HoA. As shown in Figure 1, the packets destinated to the HoA of the mobile node are routed to the home network. The goal of the home agent is therefore to intercept and forward them to the current location of the mobile node, its CoA, using and IPv6-in-IPv6 tunnel. Note that packets sent by the mobile node to its correspondent must go to the home agent before being routed to the Internet. When the mobile node moves to a new visited network, it notifies its home agent of this change using a packet called Binding Update containing the permanent Home Address and the recently acquired Care-of Address. Packets are then forwarded from the home agent to the new CoA using the tunnel. Unlike other mobility protocols, like HIP [7] or LIN6 [8], Mobile IPv6 only requires to modify the IPv6 stacks of the mobile nodes, and to deploy the home agent in the home network. This is the fundamental aspect of this protocol that makes its uses transparent regarding correspondent nodes, and the Internet architecture.

2.2 NEMO

Defined at the IETF in RFC 3963 [3], NEMO[5] is an extension to Mobile IPv6 that allows a whole network to move and change its point of attachment to the Internet as would a mobile node. A new entity similar to the mobile node and called a Mobile Router implements the NEMO protocol. Its goal is to hide the effect of mobility to the nodes connected to its ingress interface. The main concept of NEMO is to provide a mobility service to IPv6 nodes that do not implement Mobile IPv6 using an IPv6 prefix delegated from the home network. A typical usage scenario for this protocol is public transportation systems such as trains where end-nodes are connected to the Mobile Router using 802.11b.

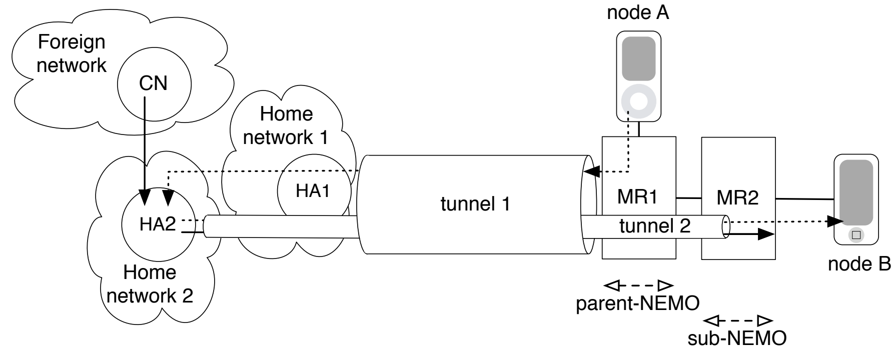

Fig. 2. Nested NEMO

Like a Mobile Node, the Mobile Router have a permanent Home Address that remains the same wherever it moves. In addition, it also manages a Mobile

[5] NEtwork MObility

Network Prefix delegated from the home network. This is the IPv6 prefix used by end-nodes connected to its ingress interface. In NEMO, the home agent is slightly modified so as to delegate home addresses as well as mobile network prefixes, and to process dedicated Binding Update messages. It does not only intercept packets destinated to the home address of mobile nodes and mobile routers but also intercepts packets sent to nodes belonging to the mobile network prefix. For example, with the home network's prefix *2001:db8::/48*, a network administrator could delegate the prefixes *2001:db8:0:1::/64* and *2001:db8:0:2::/64* to two different mobile routers MR1 and MR2.

As defined by the NEMO terminology [9], a mobile network is said to be nested (sub-NEMO) when it is directly attached to another mobile router (parent-NEMO). Figure 2 shows a simple case of nested mobile network where a mobile router, MR2, is connected to another mobile router, MR1; the networks interconnecting MR1 and HA1, and HA1 and HA2 are not represented. We consider that Binding Update messages were respectively send and receive by the mobile routers and their corresponding home agents. When node A in the parent-NEMO sends packets to a node B located in the sub-NEMO, they are forwarded to MR1 which encapsulates packets into tunnel 1. Then, HA1 decapsulates and routes them to the home network 2 which is the correct destination regarding the routing system. When packets reach this network, they are intercepted by HA2, immediately forwarded to MR2 via tunnel 2, and delivered to node 2. This is a typical use of NEMO that presents some performance issues. They will be described later in Section 2.4. This scenario is likely to happen when a passenger brings its own mobile router, MR2, into a train, and use it to provide access Internet access to its devices such as its laptop and its smart-phone.

2.3 Proxy Mobile IPv6

In Mobile IPv6, a mobile node is responsible for sending a Binding Update to the home agent in order to achieve its own sessions continuity. IPv6 stacks of legacy nodes must be modified to support Mobile IPv6 and turn them into mobile nodes. However, there is a need to provide IP mobility without any modification to legacy nodes. This could for example provide seamless sessions continuity to WiMAX based devices while roaming between base stations. Network based mobility protocol has been discussed in IETF and supported by several Standards Development Organizations such as WiMAX and 3GPP2. Proxy Mobile IPv6 is an extension to Mobile IPv6 that achieves network based mobility support. As shown in Figure 3, a Local Mobility Anchor, LMA, is placed in a network and acts as a home agent. Mobility Anchor Gateway, MAG, are located in every access networks. Their goal is to send Binding Update messages to the LMA on behalf of IPv6 nodes. As soon as an IPv6 node roams into its access network (arrow 1), the MAG detects it and sends a proxy Binding Update message to the LMA (arrow 2). The binding registration is then performed and the Binding Acknowledgment sent by the LMA (arrow 3). An IPv6-in-IPv6 tunnel is consecutively established between the MAG and the LMA and is used to carry the

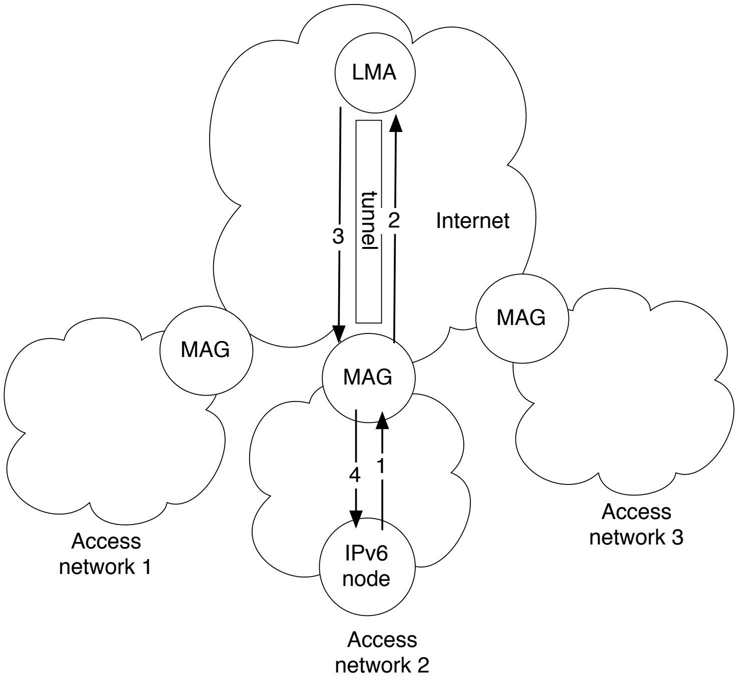

Fig. 3. Proxy Mobile IPv6

traffic of the IPv6 node. The IPv6 node will obtain and keep the same IP address wherever it moves within the same administrative domain (arrow 5).

2.4 Limitations of Mobile IPv6 based protocols

The Mobile IPv6 protocol suffers from the following three problems. Specifically, they are related to the use of the home agent to intercept packets sent to the mobile node. These problems weaken both the protocol scalability and the performance of the communications.

1. **Limitation for the home link** In order to intercept packets sent to the mobile node, the home agent acts as a neighbor discovery protocol proxy (Proxy NDP [10]). This represents a severe scalability issue as the number of neighbor discovery packets sent by the home agent is equivalent to the amount of mobile nodes it serves. Likewise, the individual bandwidth allocated to each mobile node is proportional to this number. Therefore, a home agent will possibly serve a fairly limited number of mobile nodes. Classic deployments of Mobile IPv6 are thus problematic as they can lead to limited performance. Partial solutions to these issues are available, and consist of suppressing the Proxy NDP using a virtual home link, as well as limiting

the number of mobile nodes served by each home agent. However, they are cumbersome and inconvenient to use in an operational network.

2. **Restricted location of the home agent** The position of the home agent is strictly limited by the routing architecture. It must be deployed where the home prefix is advertised to the Internet in order to intercept packets sent to its mobile nodes. This strong requirement on the home agent's location is especially problematic when the home link becomes unreachable as the mobile nodes cannot be reached anymore through their home address. Solutions to provide redundancy and reliability to Mobile IPv6 by duplicating home agents on the home link were proposed at the IETF [11–13]. They ensure that when a home agent fails, another one automatically takes over to guarantee the continuity of mobile node's communications. However, the main problem of these solutions is that only one home agent is activated at a time.
3. **Dogleg routing** As shown in Figure 1, a mobile node communicates with a correspondent via its home agent. All packets, sent and received, must go through the IPv6-in-IPv6 tunnel. Therefore, it is likely that the packets will take a non-optimal path. This problem, known as dogleg routing, induces higher communications delays, and longer paths when the mobile interacts with its correspondents. Preceding Home Agent Migration, works in route optimization [14, 15] involve caching the binding between the Home Address and the Care-of Address on-demand in routers and in correspondent nodes. However, these solutions are not transparent to end-nodes and the Internet architecture as they require changes to correspondent's and router's IPv6 stacks, as does the Return Routability Procedure [2].

NEMO As described in the NEMO problem statement document [16], along with the previous Mobile IPv6 issues, this protocol also suffers from the nested mobile network scenario described in Section 2.2. This is an important problem as all of the packets exchanged between correspondents and nodes behind the mobile router must go through the tunnel. Figure 2 shows a typical worst case scenario: two nodes A and B respectively attached to MR1 and MR2 exchange packets. As the mobile routers are not managed by the same home agent, the communication's path and delay are altered by the mandatory derivation to the home agents HA1 and HA2. Moreover, the bandwidth usage increases as the number of nested networks, wasting network resources and augmenting the probability of the tunnel congestion. The impact of this problem is even more serious when the home agents are far away, for example if HA1 is located in Tokyo and HA2 located in Paris. In addition to this first issue, if the egress interface of MR1 fails, node A can no longer send packets to node B. In other words, the egress interface of the root mobile router, here MR1, limits communications from all sub-NEMOs in terms of bandwidth and stability.

So far, the NEMO working group at the IETF did not come up with a solution to these issues. The only consensus is that the Routing Routability Procedure of Mobile IPv6 can not be used with NEMO. However, the most advanced works concern another scenario in which two mobile routers located in different vehicles try to communicate directly using a wireless interface instead of the tunnel. Solutions to this problem are actually discussed in the MANET[6] and NEMO working groups and labeled as MANEMO [17]. They tend to use well-known MANET routing protocols such as OLSR [18] to discover direct routes to other mobile routers. The goal of MANEMO based solutions is therefore to use a free wireless-based *MANET interface* when mobile routers are in communications range, and use the tunnel otherwise.

Proxy Mobile IPv6 Unlike Mobile IPv6, this protocol do not suffer from issues previously described as *limitation for the home link*. Indeed, due to its design, the notion of home link disappeared from Proxy Mobile IPv6. However, communications between nodes located behind the Mobile Anchor Gateway, and their correspondents are still targeted by the dogleg routing. None of the previously detailed solutions can be applied to solve this issue. The location of the home agent is also limiting the performance of the protocol. However, if it fails, the consequence are more serious than with Mobile IPv6: nodes can not communicate at all as they only reveal their home address to their correspondents. In a regular deployment, the redundancy of home agents is therefore critical. Finally, the Mobility Anchor Gateway brings an issue similar to the mobile router's one: it limits communications from all nodes behind it.

Like the mobile router NEMO the Basic Support, the LMA must process the traffic of each mobile node and transmit it over the tunnel. Therefore Proxy Mobile IPv6 and NEMO share the same problems. The LMA is located where the home prefix is advertised to the Internet and acts as the default router for this prefix consequently it represents a single point of failure. This is a critical issue for a real life deployment as it directly targets the availability of the Proxy Mobile IPv6 architecture.

3 Home Agent Migration

In this section, concepts behind Home Agent Migration are first described so as to understand which issues of Mobile IPv6 it solves and how. Typical deployments of this architecture are then discussed for a single Autonomous System and for the whole Internet. Finally, we consider NEMO and Proxy Mobile IPv6 and explain in which ways they can also benefit from Home Agent Migration while not being modified.

3.1 Conceptual description

Home Agent Migration is a network-based solution to the dogleg routing issue that also solves limitations for the home link. It is able to optimize the

[6] Mobile Ad-hoc Network

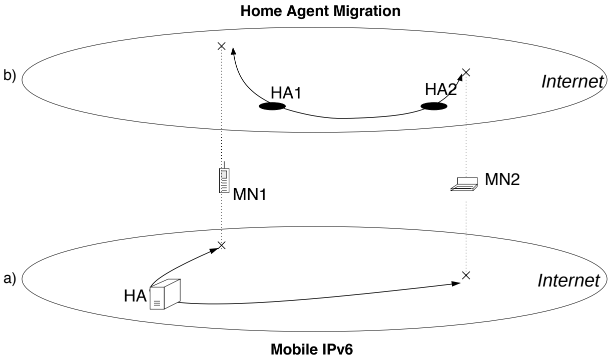

Fig. 4. Mobile IPv6 and Home Agent Migration architectures

routes while remaining fully compatible with existing Mobile IPv6 implementations. This key feature is especially important as many networking vendors had already integrated the Mobile IPv6 protocol into their products. Moreover, correspondents of mobile nodes can benefit of this route optimization without any modification of their IPv6 packets nor communication performances. In Home Agent Migration, home agents are distributed in the network so as to disengage them from the home link. Unlike in regular Mobile IPv6 deployments, several home agents are serving the same home prefix, as shown in Figure 4. To do so, the home prefix, also referred as mobile prefix, is advertised at diverse locations around the network in an anycast [19] fashion so as to create routing *shortcuts*.

Anycast is a common routing based mechanism that associates an IPv6 prefix to a dedicated service such as a DNS servers, or in this discussion home agents. Therefore when a mobile node sends a packet to the home agent IPv6 address, the routing plane decides which incarnation of the home agent will receive it. As a result, the mobile node is always associated with the closest incarnation of the home agents in terms of the routing topology.

In order to correctly deliver packets to mobile nodes, distributed home agents must also share the same information about received Binding Update messages in a unique Binding Cache. For every mobile node, this cache maintains the relationship between the Care-of Address, the Home Address and the home agent associated with a mobile node. The home agent associated with a mobile node is called the primary home agent. As a means to synchronize the Binding Cache, each home agent establishes a secured tunnel with the other home agents and uses it to exchange signaling and traffic of mobile nodes.

3.2 Typical deployments

There is two possible deployments for the Home Agent Migration architecture. They are linked to the protocol operated to perform the anycast routing and advertise the mobile prefix. When an Interior Gateway Protocol, IGP, is used, the scope of Home Agent Migration is limited to a single Autonomous System, AS. The achieved route optimization concerns communications destinated to mobile or correspondent nodes associated to the AS. When an Exterior Gateway Protocol, EGP, is used, the prefix is distributed globally on the Internet. The optimization therefore concerns nodes located all over the Internet topology.

In an Autonomous System In this deployment, the mobile prefix is picked up from the set of IPv6 prefixes associated with the AS. This mobile prefix is advertised from different locations in the network using an IGP such as OSPF. The choice of these locations and their numbers is left to network administrators. However, so as to provide an effective route optimization, the prefix should be advertised from routers with the highest centrality in terms of graph theory as shown in our on-going studies. Routers with high centrality are gathering most of the shortest paths in the network, and are therefore on the path to most of the communications. The home agents are placed close to these routers. Depending on the Autonomous System, home agents could be interconnected using direct links or VLAN, so as to provide a fast and reliable distribution system to synchronize the Binding Cache and exchange mobile node's data traffic. This IGP based deployment is more flexible than the EGP based one as network administrators are able to efficiently place the home agent in the locations that provide the best performance within their network.

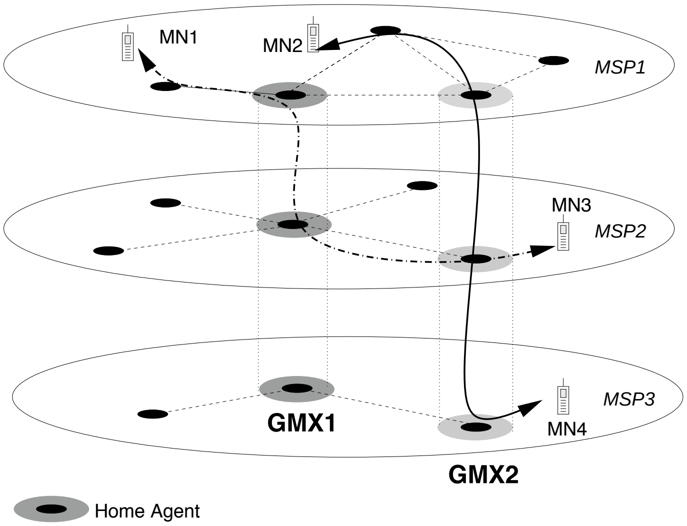

Fig. 5. Global Mobile eXchange

In the Internet Compared to the Autonomous System' one, this deployment is more difficult to achieve due to its bigger scale. The mobile prefix must be associated to a dedicated AS number. The Home Agent Migration architecture would therefore look like a distributed AS regarding the Internet topology. The mobile prefix will be advertised from many different locations around the globe using an EGP such as BGP. This deployment relies on Internet Exchange Points (IXPs) to locate the distributed home agents. They are operated with a concept similar to IXP; therefore we call this architecture Global Mobile eXchange (GMX). The primary goals of GMX are to decrease the cost of the transit traffic related to mobile nodes and to allow Internet-Scale Mobility services. In Figure 5, there are three Mobile Service Providers managing different sets of home agents, MSP1, MSP2 and MSP3. All of them are interconnected by home agents located in GMX1 and GMX2. In a GMX, a home agent exchanges traffic and routing information as a regular router would do in an IXP. However, this EGP based deployment could be difficult to achieve as it requires peering agreements with Internet Service Providers located in IXPs where home agents are located.

3.3 In details

Mobile IPv6 Figure 6 represents flows of packets generated when a mobile node, MN, associates with the Home Agent Migration system and communicates with its correspondents, CN1 and CN2. A mobile node (MN) first registers to its primary home agent (Seq1). The primary home agent then creates a binding for the Home Address of the mobile node, and subsequently distributes a copy to other home agents to synchronize the Binding Cache. When a mobile node communicates with a correspondent node, outgoing packets from the mobile node are tunneled to the primary home agent, here HA1 (Seq4). Then, as it is not possible to know which home agent is closer to the MN, the packets are simply routed to CN1 using the regular routing system. Incoming packets to the mobile node are intercepted by the home agent HA2, which is closer to the correspondent node. Intercepted packets are then tunneled to the primary home agent. The primary home agent delivers the packets to the mobile node through the tunnel (Seq5). If the mobile node decides to switch its primary home agent because of its movement, it sends a Binding Update to the new primary home agent (Seq7). The new primary home agent then synchronizes the binding with other home agents (Seq8). After receiving the Binding Update copy, all the home agents update the binding as well as the new primary home agent address.

NEMO Home Agent Migration could easily be extended in order to provide route optimization to NEMO. Small modifications to the shared Binding Cache are sufficient so as to also take mobile network prefixes into account. Moreover, the network prefixes associated with mobile routers must belong to the IPv6 prefix advertised by the distributed home agents using anycast. However, the sub-NEMO scenario, described in Section 2.2, can not fully benefit from our proposal. In Figure 2, with Home Agent Migration, when node B wants to communicate with node A in the parent-NEMO, the performance is similar to the

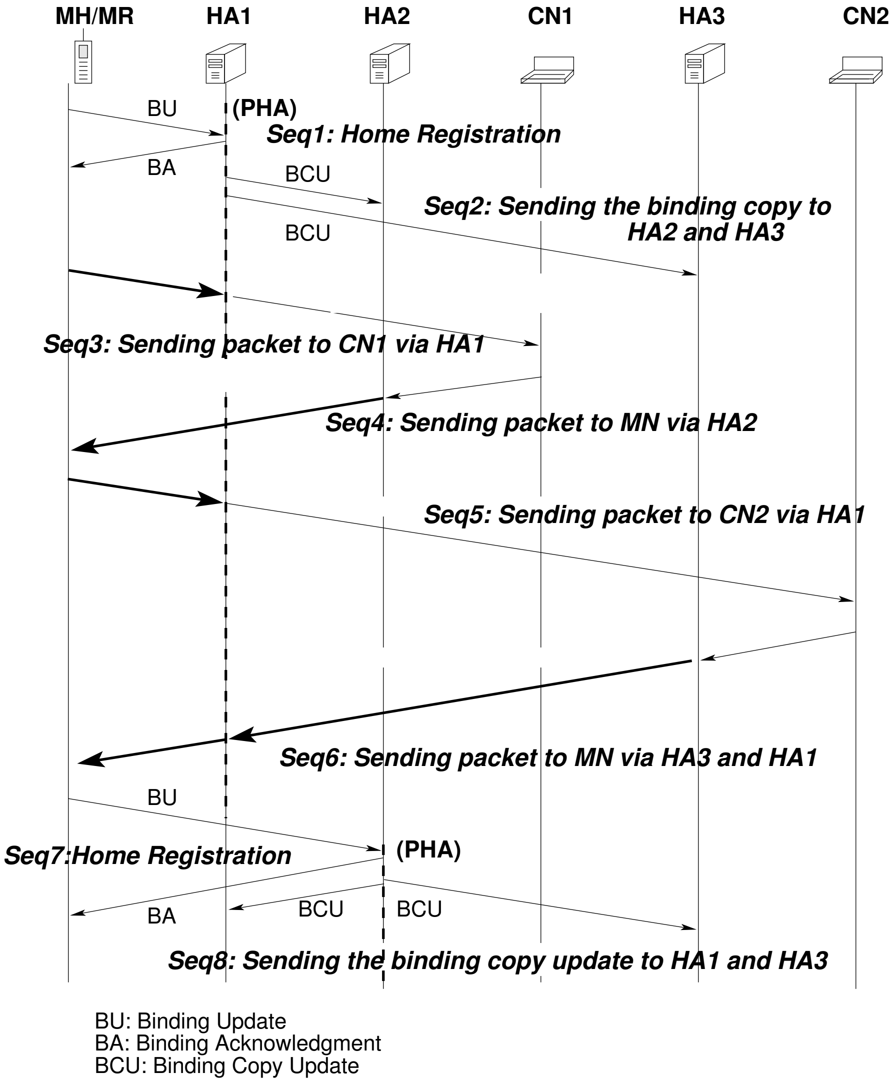
MH/MR
HA1
HA2
CN1
HA3
CN2
BU
(PHA)
Seq1: Home Registration
BA
BCU
Seq2: Sending the binding copy to HA2 and HA3
BCU
Seq3: Sending packet to CN1 via HA1
Seq4: Sending packet to MN via HA2
Seq5: Sending packet to CN2 via HA1
Seq6: Sending packet to MN via HA3 and HA1
BU
(PHA)
Seq7:Home Registration
BA
BCU
BCU
Seq8: Sending the binding copy update to HA1 and HA3
BU: Binding Update
BA: Binding Acknowledgment
BCU: Binding Copy Update

Fig. 6. Multiple Home Agents

performance of two mobile nodes communicating together: packets are not anymore routed to a distant home agent as both tunnels terminates on the closest home agent. The overhead is thus equivalent to the round trip time between the parent mobile router and the home agent. While this could be considered as huge in environments sensible to delay, our proposal do not alter the privacy and the security of the communications as the packets are protected by IPsec between the home agent and the two mobile routers.

Proxy Mobile IPv6 In order to use Proxy Mobile IPv6 with Home Agent Migration, both protocols need to be modified. Indeed, this is not a problem as the former protocol does not require any specific implementation on the client's side, and as the later one only specifies changes on the home agent. Therefore, modifications to these protocols are transparent to clients. Since LMA is similar to a Home Agent in Mobile IPv6 and NEMO Basic Support, LMAs can be distributed with the Home Agent Migration. LMAs are scattered in the same Proxy Mobile IPv6 administrative domain or in the Internet as an anchor point. Each LMA exchanges the proxy binding information with others. The LMA intercepted packets of mobile node can directly tunnel packets of a mobile node to the MAG which the mobile node is currently belong to. Compared to the Home Agent Migration for Mobile IPv6, the tunnel end points are between LMA and MAG. While the home agent intercepting packets must forward the packets to the primary home agent of the corresponding mobile node in Mobile IPv6 and NEMO Basic Support, LMA can tunnel the packets directly to the MAG without going to the primary LMA. This is because the mobile node does not receive any tunneled packets from LMA and is not aware of the bi-directional tunnel established between MAG and LMA. This is more advantageous to provide route optimization than other mobility protocol. Alternatively, for communication between mobile nodes in the same Proxy Mobile IPv6 administrative domain, we can extend MAGs to manage the binding information of mobile nodes in the same domain. Since the MAG is an entity securely managed by network operators, having the binding information on the MAG does not cause any security vulnerability. If two mobile nodes attached to the same MAG communicate, the MAG can redirect the packets without LMA involvement. In this case, the path can be fully optimized compared to the regular Proxy Mobile IPv6. As a result, for Proxy Mobile IPv6, both LMA and MAG can be extended to manage the bindings of all the mobile nodes and to route the packets of the mobile node by using Home Agent Migration.

4 Security

Mobile IPv6, its extensions, and Home Agent Migration should not bring new security related issues into the Internet architecture. From its conception, the Mobile IPv6 protocol was developed to limit its impacts on the network and the correspondents. This section initially describes the protection of the communications that should be performed in real life deployments. Moreover, it discusses the security implications of Mobile IPv6, and Home Agent Migration for the network infrastructure.

4.1 IPsec

The communications between a mobile node and its home agent are interesting targets for an attacker. If she manages to inject fake Binding Update messages, he can control the Binding Cache of the home agent, and alter the relation between the Care-of Address and the Home Address. As a result, she is able to retrieve the traffic sent to the mobile node, forbid it to communicate, or redirect its traffic to a target to perform a Denial of Service attack. In order to be protected from this injection, the RFC 3776 [20] defines how IPsec must be used to protect signaling messages[7] as well as the tunnel between the mobile node and the home agent. Real life deployments of Mobile IPv6 outside closed networks can not be done without using IPsec.

In a simple Home Agent Migration deployment, each home agent generates a distinct home agent address from the same home network prefix. Concerning the protection provided by IPsec, this means that every mobile node is pre-configured with four security policies for each Home Agent. Two ensures the protection of Binding Update and Binding Acknowledgment, and two others one the protection of the tunnel. The pre-configuration of these policies could be problematic, and could lead to operational issues if home agents are added after the first deployments of mobile nodes.

An advanced deployment of Home Agent Migration could solve this problem. If all the Home Agents share the same IPv6 address, only two security associations must be pre-configured for each mobile node. While promising, this architecture could lead to problems concerning the interaction of the IPsec and Mobile IPv6 stacks especially on the home agent side. In fact, so as to keep the IPsec sessions alive after a movement, the home agent would have to synchronize information about the negotiated security associations. The use of IPsec to secure the distribution system is however much simpler. In order to synchronize the Binding Cache, home agents are interconnected using IPv6-in-IPv6 tunnels in a mesh like fashion. Consequently, if the distribution system includes N home agents, each home agent must be pre-configured with $N-1$ security associations to the other home agents.

Concerning the integration of Mobile IPv6 in the 3GPP2 architecture, a simple authentication mechanism [21] modeled from Mobile IPv4 is preferred to IPsec. Indeed, the implementation and use of IPsec and IKE is considered as being too heavy to be integrated into small devices such as mobile phones. This mechanism is promoted by telecommunications operators as it simplifies the billing when roaming occurs between them. Moreover, operators considers that IPsec is not mandatory in their core networks IPsec if efficient packets filtering is performed.

[7] Binding Update and Binding Acknowledgment messages

4.2 Protection of the infrastructure

The deployment of Mobile IPv6-based protocols is related to their performances as well as their impacts on the network infrastructure. From a security point of view, Mobile IPv6 integrates protection against denial of services, easier filtering capabilities and prevents problems associated with bypassing the ingress/egress filtering [22]. For a network administrator, Mobile IPv6 is a protocol that allows a node to send packets from his network using a source address that do not belong to the prefix of the site. While this could look like a perfect way to bypass filtering that prevents address spoofing, it do not work in practice. Indeed, as the traffic of the mobile node is always transferred via the tunnel, no spoofing occurs and Mobile IPv6 remains compatible with filtering policies.

Amongst the IPv4 options, the ones concerning *source routing* have always be considered as dangerous as they provide easy methods to discover network topologies, or divert firewalls. With IPv6, a similar source routing option is available as a specific extension called Routing Header Type 0 which was recently deprecated as it leads to serious amplification attacks [23]. Mobile IPv6 also uses a routing header, Type 2, that includes limitations that makes it safe[8]. The difference between Type 0 and Type 2 allows a specific filtering on firewalls. A network administrator can therefore decide to protect his infrastructure against Type 0 related attacks, and authorize Mobile IPv6 as well. The semantic of the routing header Type 2 was limited: only one address is carried by this extension, and it must correspond to the Home Address of the destination. Moreover, this routing header is not examined by nodes that do not support Mobile IPv6, and its usage is limited to specific packets such as Binding Acknowledgments. Independently of these extensions, specific headers or ICMPv6 codes were defined for Mobile IPv6 to enable a simplified and dedicated filtering.

5 Conclusion

In this paper, we provided detailed descriptions of Mobile IPv6 and its two extensions NEMO and Proxy Mobile IPv6. We have also shown that Home Agent Migration could be reshaped so as to enhance these extensions with no modification of their implementations. We explained that using distributed home agents might not fully optimize every possible scenario deployments of these extensions. However, the achieved performances are sufficient for most customers as optimizations concerns typical uses of these technologies. Furthermore, unlike other proposals, ours remains fully compatible with the use of IPsec with Mobile IPv6 based protocols. Considering network operators, this is an important feature as it allows safe and secure deployments of mobility services on the Internet, as well as billing possibilities.

Future work based around the ideas described in this paper will focus on practical experiments. So far, we only focused our tests on Mobile IPv6, and we would like to perform them with NEMO at first; and then with Proxy Mobile

[8] the same discussion applies to the Home Address Option

IPv6. In fact, we would like to efficiently quantify the impact of the IPsec on the latency of handovers. Experiments using regular Mobile IPv6 already showed that it is possible to minimize this latency, but more tests need to be performed.

Acknowledgment

The authors would like to thank Arnaud Ebalard for his valuable discussions on IPsec and security related topics.

References

1. Mizuko, I., Okabe, D., Matsuda, M.: Portable, pedestrian: Mobile phones in japanese life. In: MIT Press, Cambridge, MA. (2005)
2. Johnson, D., Perkins, C., Arkko, J.: Mobility Support in IPv6. RFC 3775 (Proposed Standard) (June 2004)
3. Devarapalli, V., Wakikawa, R., Petrescu, A., Thubert, P.: Network Mobility (NEMO) Basic Support Protocol. RFC 3963 (Proposed Standard) (January 2005)
4. Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., Patil, B.: Proxy mobile ipv6 (work in progress, draft-sgundave-mip6-proxymip6-02). Internet Draft, Internet Engineering Task Force (March 2007)
5. Wakikawa, R., Valadon, G., Murai, J.: Migrating home agents towards internet-scale mobility deployments. In: CoNext06, Lisbonne, Portugal. (Dec 2006)
6. Jang, H., Jee, J., Han, Y., Park, S., Cha, J.: Mobile ipv6 fast handovers over ieee 802.16e networks. Internet Draft, Internet Engineering Task Force (January 2007)
7. Moskowitz, R., Nikander, P.: Host Identity Protocol (HIP) Architecture. RFC 4423 (Informational) (May 2006)
8. Kunishi, M., Ishiyama, M., Uehara, K., Esaki, H., Teraoka, F.: Lin6: A new approach to mobility support in ipv6. In: Wireless Personal Multimedia Communication (WPMC). (Nov. 2000)
9. Ernst, T., Lach, H.: Network Mobility Support Terminology (work in progress, draft-ietf-nemo-terminology-06). Internet Draft, Internet Engineering Task Force (December 2006)
10. Narten, T., Nordmark, E., Simpson, W.: Neighbor Discovery for IP Version 6 (IPv6). RFC 2461 (Draft Standard) (December 1998) Updated by RFC 4311.
11. Wakikawa, R.: Home Agent Reliability Protocol (work in progress, draft-ietf-mip6-hareliability-01.txt). Internet Draft, Internet Engineering Task Force (March 2007)
12. Chambless, B., Binkley, J.: Home agent redundancy protocol (harp) (expired, draft-chambless-mobileip-harp-00.txt). Internet Draft, Internet Engineering Task Force (October 1997)
13. Faizan, J., El-Rewini, H., Khalil, M.: Virtual Home Agent Reliability Protocol (VHAR) (expired, draft-jfaizan-mipv6-vhar-02.txt). Internet Draft, Internet Engineering Task Force (April 2004)
14. Myles, A., Johnson, D.B., Perkins, C.: A Mobile Host Protocol Supporting Route Optimization and Authentication. In: IEEE Journal on Selected Areas in Communications, special issue on Mobile and Wireless Computing Networks, vol.13, No.5. (Jun. 1995) 823–849
15. Wakikawa., R., Koshiba, S., Uehara, K., Murai, J.: ORC: Optimized Route Cache Management Protocol for Network Mobility. In: IEEE 10th International Conference on Telecommunication (ICT) 2003. (February 2003) 119–126

16. Ng, C., Thubert, P., Watari, M., Zhao, F.: Network mobility route optimization problem statement (work in progress, draft-ietf-nemo-ro-problem-statement-03). Internet Draft, Internet Engineering Task Force (September 2006)
17. Ng, C., Thubert, P., Watari, M., Zhao, F.: Analysis of manet and nemo (work in progress, draft-boot-manet-nemo-analysis-01). Internet Draft, Internet Engineering Task Force (June 2007)
18. Clausen, T., Jacquet, P.: Optimized Link State Routing Protocol (OLSR). RFC 3626 (Experimental) (October 2003)
19. Abley, J., Lindqvist, K.: Operation of Anycast Services. RFC 4786 (Best Current Practice) (December 2006)
20. Arkko, J., Devarapalli, V., Dupont, F.: Using IPsec to Protect Mobile IPv6 Signaling Between Mobile Nodes and Home Agents. RFC 3776 (Proposed Standard) (June 2004) Updated by RFC 4877.
21. Patel, A., Leung, K., Khalil, M., Akhtar, H., Chowdhury, K.: Authentication Protocol for Mobile IPv6. RFC 4285 (Informational) (January 2006)
22. Ferguson, P., Senie, D.: Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing. RFC 2827 (Best Current Practice) (May 2000) Updated by RFC 3704.
23. Biondi, P., Ebalard, A.: IPv6 Routing Header Security. In: CanSecWest Security Conference. (April 2007)