fP2P-HN: A P2P-based Route Optimization Solution for Mobile IP and NEMO clients.

Albert Cabellos-Aparicio[1], Rubén Cuevas[2], Jordi Domingo-Pascual[1], Ángel Cuevas[2], Carmen Guerrero[2]

[1]Universitat Politècnica de Catalunya
Department of Computer Architecture
{acabello,jordid}@ac.upc.edu

[2]Universidad Carlos III de Madrid
Telematic Engineering Department
{rcuevas,acrumin,guerrero}@it.uc3m.es

Abstract— **Wireless technologies are rapidly evolving and the users are demanding the possibility of changing its point of attachment to the Internet (i.e. default router) without breaking the IP communications. This can be achieved by using Mobile IP or NEMO, however mobile clients must forward its data packets through its Home Agent (HA) in order to communicate with its peers. This sub-optimal route (lack of *route optimization)* reduces considerably the communications performance, increases the delay and the infrastructure load. Additionally, since the HA must forward all the mobile clients' data packets, it can become the bottleneck of such networks. In this paper we present the fP2P-HN architecture, a P2P-based solution that allows deploying several HAes throughout the Internet. With this architecture a mobile client can select a closer HA to its topological position in order to reduce the delay of the paths towards its peers. Furthermore it incorporates *flexible* HAes that, as we will see, reduce the load at these entities. The main challenge of our solution is signaling the location of the HAes in Internet. We provide an analytical model that evaluates the costs and the benefits of the fP2P-HN architecture. The model shows that the signaling grows logarithmically with the number of HAes and that the reduction is, at least, 20% (lower bound).**

***Index Terms*—Mobility, Mobile IP, NEMO, P2P**

I. INTRODUCTION

WIRELESS technologies have rapidly 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 an affordable way. In the current Internet status a user can be connected through a wireless link but he cannot move (i.e. change its access router) without breaking the IP communications. That's why the IETF designed Mobile IP (RFC 3344) 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 (MN) has two IP addresses. The first one identifies the MN's identity (Home Address, HoA) while the second one identifies the MN's current location (Care-of Address, CoA). The MN is always reachable through its HoA while it changes its CoA according to its movements. A special entity called Home Agent (HA), placed at the MN's home network, maintains bindings between the MN's HoA and CoA addresses.

The main limitation of Mobile IP is that communications between the MN and its peers are be routed through the HA. Unfortunately, packets routed through the HA follow a sub-optimal path. This reduces considerably the communications' performance, increasing the delay and the infrastructure load. In addition, since a single HA may be serving several MNs and forwarding several connections, the HA itself may become the bottleneck of the whole system and represents a single point of failure in Mobile IP-based networks [1].

Mobile IPv6 (RFC 3775) solves this limitation by allowing MNs to communicate with its peers directly (*route optimization*) exploiting special IPv6 extension headers. However the NEMO protocol (NEMOv4 [2] and NEMOv6 (RFC 3963)), which provides mobility to networks instead of nodes, does not support *route optimization*, even in IPv6. That is why we believe that this is an issue in the current Internet status (Mobile IPv4 and NEMOv4) and even in the future (NEMOv6).

Solving the *route optimization* problem has attracted the attention of the research community and several solutions have been proposed [3,4,5,6]. The main idea behind all these proposals is deploying multiple HAes at different Autonomous Systems (ASes). Then, a MN may pick the best HA according to its topological position thus, reducing the delay of the paths to its peers. The main challenge of this approach is signaling the location of the different HAes throughout the Internet in an scalable way. Some of authors use the exterior Border Gateway Protocol (eBGP) protocol [3,5,6] while others [4] use Anycast routing. However these approaches are not scalable. On the one hand, using the exterior BGP protocol means increasing the load in the already oversized global routing table [7]. On the other hand, anycast's defiance of hierarchical aggregation makes the service hard to scale [8]. In addition, these solutions force the MNs to send the data packets through the HAes, increasing the load on these devices that may become the bottleneck of the whole system [1].

In this paper we propose a scalable architecture, named fP2P-HN (**f**lexible **P2P** **H**ome agent **N**etwork), that solves the *route optimization* issue for Mobile IP and NEMO clients. We propose using an overlay Peer-to-Peer (P2P) network to signal the location of the different HAes. When a MN detects that its current HA is too far it queries it (the HA belongs to the fP2P-HN network) for a closer HA. Then, the fP2P-HN network uses BGP information in order to locate a HA that reduces the delay of the paths between the MN and its peers, for instance by choosing a HA located in the same AS than the MN.

Our solution allows deploying multiple HAes at different

AS without impacting the exterior BGP global routing table or requiring anycast routing; however the HAes are still responsible of forwarding all the MN's data packets. In order to alleviate their load we propose to deploy *flexible* HAes (fHA). The main idea behind the fHAes is that a registration from a MN into a HA can be viewed as an internal route from the network's point of view. That is, when a MN registers a new location into its HA it is actually installing a new route (*Home Address* → *Care-of Address*). We believe that this route can be announced throughout the network using the *interior* BGP (IBGP) protocol to each of the AS' Border Routers (BR). Then, the BRs are aware of the current location of the MN and can de-capsulate and forward any packets addressed to/from the MN directly, just as regular packets. Thus, MN's data packets are not forwarded by the HAes but by the routers.

The fP2P-HN architecture is simple, scalable and fully global. Moreover it does not require deploying any new entities on the Internet. At the Inter-domain level, we signal the location of the HA using a P2P network instead of using eBGP or anycast. At the Intra-domain level we signal the location of the MN using IBGP, this way the border routers are aware of the location of the MN and the load of the HA is significantly reduced. As we will see later we evaluate the performance of our proposal through a mathematical model that shows that the architecture is scalable since the amount of signaling grows logarithmically with the number of fHAes. In addition the reduction of the traffic processed by the fHAes is, at least, 20% (lower bound).

II. FLEXIBLE P2P HOME AGENT NETWORK

In this section we detail the fP2P-HN architecture. Please note that an fHA (*flexible* HA) is a Home Agent that belongs to the architecture and that has special features. In this paper we will refer to a HA or an fHA indistinctively.

A. Overview

The main goal of the fP2P-HN architecture is to reduce the delay of the communications of the MNs and the load at the fHAes. Figure 1 shows an overview of the architecture.

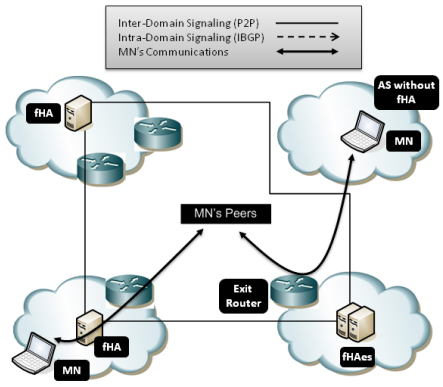


Figure 1. Overview of the fP2P-HN architecture

When a Mobile IP or NEMO client changes its point of attachment to the Internet it will establish a new tunnel with its HA to communicate. Depending on the MN's topological position this new path may suffer from a large delay. We propose to deploy several HAes throughout the Internet in order to reduce this delay. When the MN detects that the new path towards its currently assigned HA has an unacceptable performance (e.g. RTT > a given threshold) it queries its current HA for a closer one (i.e. a HA located in the MN's current AS). The architecture is flexible and allows using any metric to trigger the discovery of a closer HA. In this paper we use the RTT because it is a simple metric able to capture the performance of a path. It is worth noting here that any other metric can be used.

Our proposal requires deploying several HAes throughout the Internet and has four differentiated phases. The HAes organize themselves in a P2P network which stores the information regarding the HA's IP addresses and their topological position (HA's AS number). This P2P network is formed during the *P2P Setup phase*. The MNs are always bind to a HA belonging to this P2P network. Thus, when the MN detects that the RTT to its current HA is unacceptable it triggers the *fHA Discovery phase* and queries the P2P network for a closer one. Once the MN has the IP address of this closer HA it sends a registration message (Binding Update) and obtains a new HoA (*fHA Registration phase*). When this MN changes its point of attachment again it will keep using the same HA while the RTT remains below a given threshold.

All the HAes deployed in the fP2P-HN architecture are in fact *flexible* HAes. This means that they belong to the IBGP domain of its AS. When their assigned MNs are attached directly to their AS they act as a regular HA. However, when the MNs are outside their AS they announce the location of the MNs (Care-of Address) through IBGP to the AS' BRs. This announcement is just a new route: To reach the MN (*Home Address*) packets must be addressed to its topological position (*Care-of Address*). This way packets addressed from/to the MN are directly processed by the BR and thus, the load at the HA is considerably reduced. This is the last phase of the proposal known as *Data Packet Forwarding*.

Changing the MN's HoA may break the existing connections. In order to solve this issue we propose that these connections are forwarded through the previous HA while new connections are be forwarded through the new HA. A MN changes its HoA only when it is outside of its currently assigned HA's AS *and* the RTT is above a given threshold. ASes usually provide connectivity to large geographical areas, thus this will occur rarely. In addition 98% of the connections last less than 15 minutes [16].

Regarding the inbound connections, the MN may still use its original HoA (the one from its Home Network). It is worth to note that MNs are clients (not servers) and with the current deployment of firewalls and NATs inbound connections are almost non-existent.

Finally the proposed architecture does *not* impact the handover latency of mobile clients. In case that the MN changes its HA (i.e RTT is above a given threshold) then we propose that it uses the previous HA until attaching to the new one. Furthermore, as shown in the next section the time to

search in the P2P network is $O(log_2 N)$ (where N is the number of HAes).

B. P2P Setup Phase (Inter-Domain)

This subsection details how the P2P network is created. The P2P network is used to store the location of the fHAes (AS number) and their IP addresses. This information is used by MNs to locate a closer fHA to its topological position.

fHAes organize themselves forming a structured P2P overlay (also known as DHT-based P2P overlay). The fP2P-HN is fully flexible and can be deployed using any of the proposed structured P2P schemes [13]. In the remainder of the paper we will consider Chord [14] as the P2P scheme, thus, the overlay's structure is a ring.

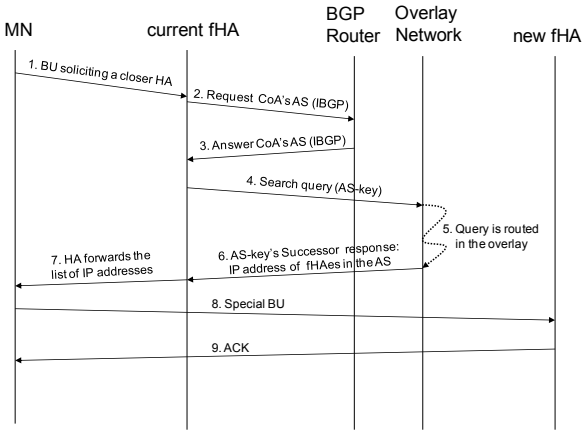


Figure 2. fHA Discovery Phase in the fP2P-HN architecture

In the fP2P-HN the search key is the *AS-key* which is computed as *hash(AS number)*. When a new fHA joins the fP2P-HN it chooses an identifier (*Peer-ID*). In this case this is the *hash(fHA's IP Address)*. The fHA's position in the ring is determined by its Peer-ID: the fHA is placed between the two overlay nodes with the immediately higher and lower Peer-ID to its own id. Each overlay node has direct references to its two neighbors and also to other overlay nodes (crossing the ring) thus making the routing within the fP2P-HN faster. These nodes are named *fingers*. Each overlay node uses these fingers to create its fP2P-HN routing table.

Finally, each fHA must register its AS number within the fP2P-HN. The fHA obtains the AS-key by computing the *hash(AS number)*. Then, it looks for the overlay node with the immediately higher Peer-ID to the AS-key, named *Successor*, and sends to this node the AS-key, its IP address and its AS number. Moreover, the fHA may send some security information. The *Successor* stores an entry with all this information.

C. fHA Discovery Phase (Inter-Domain)

This subsection details (figure 2) how a MN can use the fP2P-HN to discover a closer fHA.

An MN connected to fHA_1 eventually detects (after a handover) that the RTT to fHA_1 is above a given threshold. Then, it triggers the procedure to discover a closer HA. The MN sends to the fHA_1 a special BU soliciting the IP address of a closer fHA. At this point, fHA_1 discovers (using BGP) the AS number associated to the MN's CoA. Afterwards, it obtains the AS-key by computing the *hash(AS number)*.

The search method within the fP2P-HN is as follows. fHA_1 sends a query with the AS-key. The search query is routed in the overlay towards the AS-key's *Successor*. This fHA (e.g. fHA_2) is responsible of storing the information regarding the AS-key. Thus, it stores the IP addresses of all the fHAes located in the AS where the MN is currently attached to. Then, fHA_2 sends these IP addresses to fHA_1 which in turn forwards them to the MN. Finally, the MN selects one of them and sends a special BU message to the new fHA in order to obtain a new HoA.

Although the fHAes are expected to be very stable entities, the fP2P-HN includes the mechanisms to make the solution dynamic and adaptive. For this purpose, every fHA periodically checks if its neighbors and fingers are still reachable and running. If necessary, the fHA reconfigures its fP2P-HN routing table and establishes new neighbors or fingers.

Moreover, to make the solution more robust, reliable and load-balanced we use redundancy. Therefore, each AS-key is stored for several *Successors* instead of just one. Then, in case of failure of a *Successor* the others are still available and can reply to the queries. In addition, each MN has the list of the fHAes obtained during the last *fHA discovery phase*. Thus, if its current fHA fails, the MN can re-connect to one placed on the same AS.

D. fHA Registration Phase (Intra-Domain)

This subsection details the registration phase of a MN into a new fHA.

At the Intra-Domain level each MN selects a given fHA through the above-mentioned mechanism. The fHA has the same functionalities than a regular HA but it uses IBGP to signal the location of the MNs to reduce the load. The fHA acts just as a regular HA when the MN is directly attached to its network.

When the MN is not directly attached to its AS the fHA has to announce the new location of the MN (CoA) to the AS' BRs. To distribute this type of information we use the *interior* Border Gateway Protocol (RFC 1771). In our solution the fHAes and the BRs create an IBGP domain. This IBGP domain may be an already existing one or a separate one. The routes announced through this IBGP domain always have the longest prefix (/32 or /128) and never affect regular BGP routes. It should be noted that the routes announced by the fHAes will *never* be distributed outside the AS. Finally, the entities participating in the IBGP domain have pre-configured keys to provide confidentiality, integrity and authentication to the communications.

For each received registration message (Binding Update) from outside the AS, the fHAes send an IBGP UPDATE message to the BRs. We introduce new options in the IBGP UPDATE message. The UPDATE message sent to the BRs includes the following information: *<Home Address, Care-of Address, Lifetime>*. Upon reception of this message, the BRs setup a tunnel endpoint with the MN. The tunnel source address is the one of the BR's address while the destination address is the Care-of Address. In addition, each BR adds the following route to its routing table: *HomeAddress\32* →

Tunnel. The tunnel and the route are automatically deleted after "*Lifetime*" seconds. Finally the fHA will reply to the MN informing that the registration was successful and with the list of addresses of the BRs, this way the MN can address its tunneled packets towards the BRs (see section below for details).

Once the MN is assigned to a new fHA or returns home it sends a registration message to the previous fHA. Upon reception, the fHA sends an IBGP WITHDRAWAL message to the BRs to immediately remove all the routes and tunnels related to the MN's Home Address.

Finally, since several fHAes can be deployed at the same AS all of the fHAes should belong to the same IBGP domain (along with the BR). The MNs will receive a list of the available fHAes and will choose one based on any criteria (load balancing, RTT…).

E. Data Packet Forwarding Phase (Intra-Domain)

Finally this subsection details how MN's data packets are forwarded.

If the MN is connected to the fHA's AS then packets are forwarded just as in Mobile IP or NEMO. However when the MN is connected to a foreign AS then it has to forward the packets through its fHA.

In this case MNs encapsulate their data packets towards the BRs (figure 1). Since the fHA has previously configured (using IBGP) a new tunnel (*HomeAddress\32 → Tunnel*) in the BRs, packets sent by the MNs are automatically de-capsulated and forwarded towards the packet's destination address (the MN's peer address). If the exit point of the MN's peer address is another BR then the packet traverses the network as a transit packet.

Regarding the packets addresses towards the MN's (HoA) they will reach the fHA's AS. The BRs have learned the location (CoA) of the MN through IBGP and will automatically encapsulate and forward the packet directly towards the MN.

III. Evaluation Methodology

The fP2P-HN architecture introduces a major improvement in Mobile IP and NEMO: the reduction of the delay of the paths and the load at the HA. However these improvements increase the signaling load both at Intra (IBGP) and Inter-domain (P2P) levels. In order to evaluate this amount of signaling we have developed a complete analytical model that evaluates the costs (signaling) and the benefits (reduction of the load).

A. Nomenclature

This section introduces the nomenclature used in the analytical model:

- $\boldsymbol{A}$: Number of Autonomous Systems.
- $\boldsymbol{h}$: Mean number of fHAes per AS.
- $\boldsymbol{N = h \cdot A}$: Number of nodes (i.e. fHAes) in the overlay.
- $\boldsymbol{B}$: Mean number of Border Routers per AS.
- $\boldsymbol{nBU}$: Mean number of received BU per fHA per second
- $\boldsymbol{p_{FR}}$: Probability that a handover is *not* to the MN's Home Network.
- $\boldsymbol{p_{fHA}}$: Probability that a handover produces a change of the MN's fHA.
- $\boldsymbol{p_{AS}}$: Probability that a handover produces a change of AS.

B. Types of Handovers

The analytical model must consider all the possible handovers types in order to produce accurate results. In this section we describe the different types of handovers and provide their mathematical expression based on our nomenclature:

1.- *Home Registration Handovers*. The MN returns back to its Home Network. The mean number of Home Registration handovers is expressed as $nBU(1 - p_{FR})$.

2.- *Internal AS Handovers*. These handovers produce a change of the CoA within the same AS: $nBU \cdot p_{FR} \cdot (1 - p_{AS}) \cdot (1 - p_{fHA})$.

3.- *fHA Handovers*. These handovers produces a change of fHA: $nBU \cdot p_{FR} \cdot p_{fHA}$.

4.- *AS Handovers*. These handovers produce a change of AS but do not produce a change of fHA: $nBU \cdot p_{FR} \cdot (1 - p_{fHA}) \cdot p_{AS}$.

C. Signaling Load

In this subsection the Inter-Domain signaling (P2P) and the Intra-Domain signaling (IBGP) are analyzed.

C.1 Inter-Domain Signaling (P2P)

The fHA discovery process is only triggered by the *fHA Handovers* ($nBU \cdot p_{FR} \cdot p_{fHA}$). Figure 2 shows the messages exchanged during the P2P search process. All the transactions require sending or receiving a single message except the routing of the search-query (Step 5). In this step each search-query is routed by $O(log_2 N)$ nodes in the DHT [13]. Since, the nodes have been randomly distributed in the DHT we can assume that the probability that a given node routes a search-query from any of the other N-1 nodes in the overlay is $(log_2 N)/(N-1)$. The model assumes that (on average) each fHA sends $nBU \cdot p_{FR} \cdot p_{fHA}$ search-queries per second, then the mean number of messages/s an overlay node has to route is expressed by Equation 1.

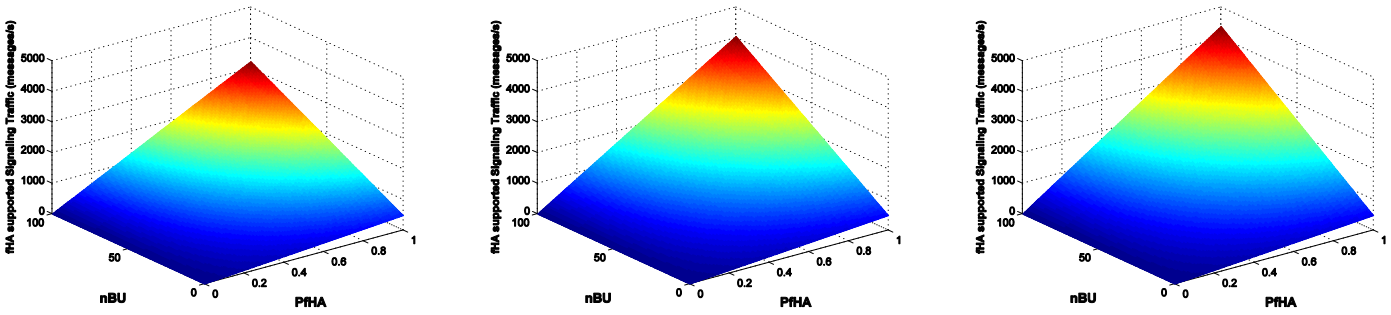
$$(nBU \cdot p_{FR} \cdot p_{fHA}) \cdot \log_2(N)\ msg/s \qquad (1)$$

Equation 2* shows the mean Inter-domain signaling load (P2P load) supported by the fHA in the fP2P-HN. This is the sum of all the signaling messages generated during the P2P search procedure (figure 2).

$$P2PLoad = \left(\frac{1}{p_{FR}} + p_{fHA} \cdot (7 + 2\log_2(N))\right) \cdot p_{FH} \cdot \text{nBU}\ msg/s \qquad (2)$$

We must also consider the maintenance traffic; this is the refreshing information messages and the keep-alive messages to check the availability of the *fingers* and neighbors. Since the fHAes are supposed to be very stable entities these messages should have a periodicity of minutes or even hours. Therefore this signaling traffic can be neglected. Furthermore due to the high stability of the fHAes, the traffic required for

*This equation includes the nBU original messages as part of the P2P signaling communication



a) fP2P-HN formed by 1000 ASes b) fP2P-HN formed by 20000 ASes c) fP2P-HN formed by 65536 ASes

Figure 3. Total Signaling Traffic in the fP2P-HN

recovering a failure (i.e. an fHA leaving the network) is also negligible. A failure is expected to occur at large timescales.

C.2 Intra-Domain Signaling (IBGP)

Each type of the handover defined on Section II-B can generate different number of IBGP signaling messages depending on the situation. In this model we consider always the worst possible case. The *Home Registration Handovers* and the *fHA Handovers* produce an IBGP WITHDRAW message. The *Internal AS Handovers* and the *AS Handovers* produce both an IBGP WITHDRAW and an IBGP UPDATE messages. These IBGP messages must be sent to all the routers in the fHA's IBGP domain. Without loss of generality in the obtained results we consider that each AS is a unique IBGP domain that includes B Border Routers.

Equation 3 presents the mean Intra-domain signaling load (IBGP load) supported by each fHA in the fP2P-HN (considering the worst possible case).

$$IBGPload = [(1 - p_{FR}) + (p_{FR} + p_{fHA}) + 2p_{FR}(1 - p_{fHA})]nBU \cdot B \quad (3)$$

C.3 Total Signaling (P2P + IBGP)

The average signaling load supported by each fHA in the fP2P-HN is the sum of the $P2PLoad$ (Equation 2) and the $IBGPload$ (Equation 3). Whereas in the Mobile IP and NEMO based solution the signaling load suffer from the HA is defined by the BU messages and their correspondent ACKs. Based on the model this can be expressed as $2 \cdot nBU$.

D. Data traffic routed by the fHA

In this section we extend the analytical study in order to evaluate the data traffic routed by each fHA. This will be compared with the amount of traffic processed by a regular HA.

The different possible situations have been described by the four types of handovers introduced in Section II-B. Thus, all the traffic generated after a *Home Registration Handover* $(1 - p_{FR})$ will be normally routed since the MN is at home. In this case the fHA does not forward the MN's traffic.

The traffic generated after an *fHA Handover* $(p_{FR} \cdot p_{fHA})$ is routed by the new fHA since the MN and the new fHA are in the same AS. Regarding the traffic generated after an *AS Handover* $(p_{FR} \cdot (1 - p_{fHA}) \cdot p_{AS})$ the fHA establishes a new route into the BRs which will deal with it.

Finally, in the case of the *Internal AS Handovers* the fHA may (or may not) be responsible of routing the MN's data traffic. Since the model considers the worst possible case we assume that the traffic generated after each *Internal Handover* is routed by the fHAes.

Regarding the Mobile IP or NEMO's, HAes are responsible of routing each data packet except those generated after a *Home Registration Handover*. Therefore, the average data traffic load saved by the fHA in the solution (in the worst possible case) is expressed by Equation 4.

$$Saved\ Traffic = 1 - [p_{fHA} + (1 - p_{fHA}) \cdot (1 - p_{AS})] \quad (4)$$

IV. Evaluation Results

We have implemented the analytical model defined above in Matlab in order to provide numerical results of the performance of the fP2P-HN architecture. Specifically we evaluate the signaling overload and the saved data traffic on each fHA. For this purpose some weak assumptions are made.

Regarding the signaling overload we assume that there are 4 fHAes and 2 Border Routers per AS (on average). In addition, we assume p_{FR} equal to 0.95. This means that only 5% of the MN's handovers correspond to Home Registrations. Finally in order to set a realistic range for nBU (mean number of handovers per second processed by each fHA) we have used the Random Waypoint Mobility simulator presented in [15]. Assuming a set of 8 domains and that each fHA serves 1000 MNs the simulator produced a mean of 18.72 handovers per second. This is a highly mobility environment where each domain represents a layer-2 network. In the evaluation we set the range of nBU from 0 to 100. We believe that this range represents a stresfull scenario.

Figure 3 presents the average signaling traffic (generated + received messages) supported by each fHA on the fP2P-HN architecture as a function of p_{fHA} and nBU. Different phases of the fP2P-HN deployment have been considered. As the figure shows the fP2PHA architecture is scalable. If the number of ASes is increased from 1000 to 65536* (65 times) the number of messages just increases 25% (0.25 times).

In order to roughly numerically evaluate the values of the graphics we are going to consider the worst case of figure 3 (case c, nBU = 100 and $p_{fHA} = 1$). In this case each fHA has to process around 4400 messages/s. In this situation, if we assume an average signaling message size of 50 bytes (a Mobile IP's BU is 44 bytes (RFC 3344)), the consumed upload and download bandwidth would only be 0.88 Mbps. Moreover this is for a worst case scenario and must be considered as an upper bound of the signaling overload.

In a nutshell, we can conclude that the signaling traffic processed by each fHA in the fP2P-HN solution is scalable. It grows logarithmically with the number of fHAes and it could be even supported by a domestic DSL connection.

Regarding the saved data traffic on the fHA compared to a

* The maximum number of ASes currently supported by the Internet is 65536 (RFC 1771).

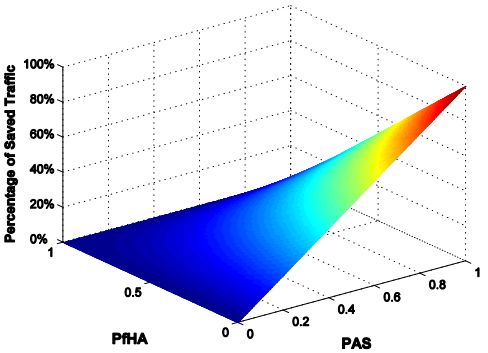


Figure 4. Saved Traffic at the fHA in our architecture

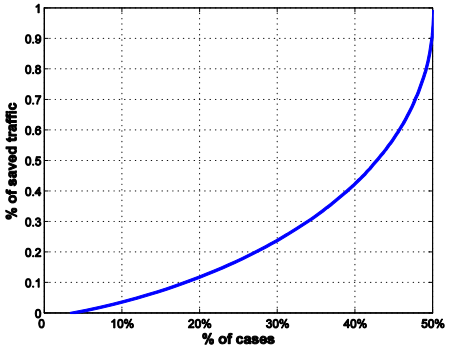


Figure 5. CDF of the saved traffic

regular Mobile IP or NEMO HA we do not need to assume anything since Equation. 4 depends only on p_{fHA} and p_{AS}.

Figure 4 shows the percentage of saved data traffic as a function of both probabilities whereas figure 5 represents the saved data traffic considering all the possible cases of figure 4.

From figure 5 we can see that only in the 6'6% of the cases the fHA suffer from the same load than the Mobile IP or NEMO HA. Besides, from figure 4 we discover that these cases are those where $p_{fHA} = 1$, which is not a real case. Again, it must be noticed that the model considers the worst possible case and provides a low bound of the saved data traffic. Even under these circumstances figure 5 shows that in the 50% of the cases the data traffic routed by the fHA is reduced in at least the 20% compared to a regular HA. Furthermore in the 75% of the cases the reduction increases up to 37'4% (upper bound).

Therefore, we can conclude that the fP2P-HN generates a very low signaling overload while it reduces considerably the data traffic routed by the fHA. In addition it clearly outperforms Mobile IP and NEMO in terms of Route Optimization and Communications Delay.

V. Related work

Incorporating *route optimization* to Mobile IP and NEMO clients is a key issue when considering the deployment of a truly mobile Internet. That's why this topic has attracted the attention of the research community and many solutions have been proposed.

First the research community focused on solving this problem specifically for Mobile IPv4 [9] and NEMO clients [10,11,12]. The main idea behind these proposals is to deploy a new entity at the correspondent network that helps the MN to communicate directly with the CN. Usually this new entity authenticates the location (CoA) and the identity (HoA) of the MN. In addition this device acts as a tunnel endpoint, this way the MN can send the packets tunneled directly to the correspondent network. The main drawback of all these proposals is that they require deploying a new entity on each correspondent network. In the current Internet status this would imply deploying a new entity on each network or at least, on each AS (currently there are roughly 22.000 ASes on the Internet). Therefore the deployment cost of these solutions is very high.

As we mentioned in Section I *R. Wakikawa* presented recently a different approach [3] used by other researchers [4,5,6]. Since these proposals are not scalable [7,8] we propose using a P2P network that it is fully scalable and we benefit from the fHA that reduces the load at the HAes significantly.

VI. Conclusions

In this paper we have presented the fP2P-HN architecture that solves the *route optimization* problem of Mobile IP and NEMO clients. Since the main concern of this approach is the scalability we have presented a complete analytical model that evaluates the amount of signaling messages as a function of the number of deployed HAes. The model shows that the signaling overload grows logarithmically with the number of HAes. In fact, we have shown that if we deploy (on average) 4 HAes at 65535 ASes (the maximum number of ASes currently allowed in the Internet) each HA would just need to process 0.88 Mbps of signaling messages. In addition the architecture uses flexible HAes that reduce the amount of traffic processed by the HAes. We have extended the analytical model and shown that the traffic can be reduced up to 20% in most of the cases.

References

[1] T. Clauser et al. "*NEMO Route Optimisation Problem Statement*" RFC 4888 October 2004

[2] K. Lueng et al. NEMOv4 "*Network Mobility (NEMO) Extensions for Mobile IPv4*", (Work in progress) January 2008

[3] R. Wakikawa et al "*Virtual mobility control domain for enhancements of mobility protocols*". IEEE INFOCOM 2006

[4] Y.S.Yet et al "*Global Dynamic Home Agent Discovery on Mobile IPv6*", in Wireless Communications and Mobile Computing. August 2006

[5] Boeing Connexion Service, http://www.connexionbyboeing.com

[6] Marcelo Bagnulo et al. "*Scalable Support for Globally Moving Networks*", ISWCS 2006

[7] G.Huston, "*Commentary on Inter-Domain Routing in the Internet*" RFC 3221, December 2001

[8] Katabi, Dina et al., "*A Framework for Scalable Global IP-Anycast (GIA)*", SIGCOMM 2000.

[9] Chun-Hsin Wu et al. "*Bi-directional Route Optimization in Mobile IP over Wireless LAN",* Vehicular *Technology Conference, Sept, 2002.*

[10] C. Ng et al. "*Network Mobility Route Optimization Problem Statement*" (Internet Draft, Work in Progress), February 2006

[11] M. Calderon et al, "*Design and Experimental Evaluation of a Route Optimization Solution for NEMO*" IEEE JSAC 2007

[12] Ng, J. Hirano. "*Extending Return Routability Procedure for Network Prefix (RRNP)*" (Internet Draft, Work in Progress), October 2004

[13] K. Lua et al, "*A Survey and comparison of peer-to-peer overlay network schemes".IEEE Communications Surveys & Tutorials. 2005*

[14] I. Stoica et al,"*Chord: A scalable peer-to-peer lookup service for internet applications*" ACM SIGCOMM'01, 2001

[15] PalChaudhurri, S et al. "*Perfect Simulations for Random Trip Mobility Models*", 38th Simulation Symposium, 2005

[16] N.Brownlee et al. "*Understanding Internet traffic streams: dragonflies and tortoises*" IEEE Communications Magazine, 2002