fHA: A Flexible and Distributed Home Agent Architecture for Mobile-IP Based Networks,[☆☆]

Albert Cabellos-Aparicio[a], Dorin-Mircea Cioran[☆][b], Pere Barlet-Ros[a], Jordi Domingo-Pascual[a], Virgil Dobrota[b]

[a] *Universitat Politècnica de Catalunya, D. d'Arquitectura de Computadors,*
c/ Jordi Girona 1-3, D6-118, 08034 Barcelona, Spain
[b] *Technical University of Cluj Napoca, Dept.of Communications,*
26-28 George Baritiu St. Cluj-Napoca, Romania

Abstract

Home Agents (HA) represent a single point of failure in Mobile IP-based networks. In order to address this issue, researchers have proposed the deployment of redundant HAs on each sub-network. Although these approaches effectively mitigate this problem, they do not take into consideration the requirements of large networks with dozens of sub-networks. Both deploying and managing several HAs on each sub-network could prove to be too expensive. In this paper we present a novel HA architecture that only requires one set of HAs for the whole network. Our basic idea is that the location of mobile nodes can be announced to exit routers. This way, forwarding packets can be done without involving the HA. Our solution provides the same level of reliability as existing ones, while improving overall performance. We validate the proposed architecture by comparing its performance with that of a standard HA, using three network traffic traces collected in different networks. Our results show that, besides the architectural benefits, the proposed architecture would forward roughly 90% less traffic in a Mobile IPv4/NEMO network, and 15% less in a Mobile IPv6 one, when compared to a standard HA.

Keywords: Mobility, Home Agent, flexible Home Agent, Reliability

[☆] This work was done while the author was visiting Universitat Politècnica de Catalunya.

[☆☆] This work has been supported by Generalitat de Catalunya, under grant number 2009SGR-1140, and by the Spanish Ministry of Science and Innovation under grant TEC2010-10440-E.

Email addresses: acabello@ac.upc.edu (Albert Cabellos-Aparicio), dorincioran@student.utcluj.ro (Dorin-Mircea Cioran[☆]), pbarlet@ac.upc.edu (Pere Barlet-Ros), jordid@ac.upc.edu (Jordi Domingo-Pascual), Virgil.Dobrota@com.utcluj.ro (Virgil Dobrota)

1. Introduction

Mobile devices are evolving at an impressive pace, having smartphones, mobile Internet devices and netbooks with mobile broadband access breaking out of the high-end business markets to the everyday consumer. Technology has reached a milestone where the convergence to all-IP services (e.g., [9]) is becoming a reality and a rich mobile Internet experience is possible at low price for both devices and broadband access [21, 5]. This situation provides a unique context for the explosion of the future mobile Internet, where things like direct optimized paths, global reachability with the same identifier and fast handovers [2] will be a must.

To this day, mobile usage was restricted to but a few applications, which had to tolerate suboptimal network configurations imposed by the Mobile IP technology. Note that Mobile IP comes in two flavors, Mobile IPv4 [28] and Mobile IPv6 [18]. The limitations of Mobile IP have been largely analyzed in the literature (i.e., [34], [1]). One of the most important drawbacks of the Mobile IPv4 protocol [28] is that the Home Agent (HA) represents a single-point-of-failure and constitutes the main bottleneck in such networks [24]. This is because the communications between Mobile Nodes (MNs) and their peers are routed through the HA. Hence, MNs rely on their HA for reachability. In fact, a single HA may be responsible for multiple MNs on a Home Link[1] and, as such, a failure of a single HA may result in a loss of connectivity for numerous MNs. The communications of MNs through the HA may also lead to either the HA or the Home Link becoming the bottleneck of the system.

In order to alleviate this problem, the Mobile IPv6 protocol incorporates a route optimization mechanism that allows MNs to communicate directly with their peers. This mechanism avoids triangle-routing through the HA reducing its load. However, this mechanism introduces some signaling overhead and, therefore, it is not going to be used for short-term communications (e.g., a MN accessing a web page) [18]. In addition, the Mobile IPv6 standard allows the deployment of multiple HAs on the Home Link, providing reliability and load balancing. This is done in a way that upon the failure of the serving HA another HA can take over the functions of the failed one. This provides continuous service to the MNs registered with the failed HA. However, the transfer of service is problematic. The solution is MN-driven and forces the MN to detect the failure and select a new HA. This results in delayed failure detection and service interruption in the upper layer applications.

As a consequence, the research community has proposed different solutions to this issue [16, 13, 8, 11]. These proposals aim to increase the reliability and load balancing of a HA by deploying several redundant HAs at the Home Link. In all these solutions the HAs share the registration state and they define efficient mechanisms for HA recovery that reduce the service disruption time. Further, the MN's traffic is balanced among the deployed HAs. The main difference

[1] This is the link where the MN is attached to when it is at home.

between them is that some are MN-driven [16, 13, 8] while others are transparent to the MN [11].

Unfortunately, these proposals are focused on providing reliability and load balancing of HAs on just a single Home Link, hence they do not take into account the global requirements of an Autonomous System (AS). An AS that hosts MNs (e.g., a campus network or an ISP) may have dozens of sub-networks. Since mobility is considered a universal feature, and should be provided to all nodes, deploying reliable HAs requires several redundant HAs on each Home Link. It is important to note that the Mobile IPv6 protocol belongs to the IPv6 standard and, theoretically, any IPv6 node should have mobility capabilities. Thus, these approaches are too expensive to deploy and to manage.

A different proposal, which does not require deploying redundant HAs on each Home Link, is the Virtual Control Domain Protocol (VMCD) [33]. The VMCD allows multiple HAs to be placed at different domains. Then, a MN may use multiple HAs simultaneously. The basic idea behind this proposal is that each HA advertises, through eBGP, the same home network prefix from multiple routing domains. Each MN then picks the best HA according to its topological position. The main drawback of this proposal is that the impact on the exterior BGP routing system scalability can be severe.

In this paper, we present a novel flexible and distributed HA architecture that takes the mobility requirements of an AS into account. We consider the HA as an entity that performs several differentiated operations. We analyze each operation and assign it to an entity of the network. Our basic idea when distributing the operations is that a registration of a MN to a HA can be seen as an internal route from the point of view of the network. This means that, when a MN registers a new location to its HA, it is actually installing a new route (Home Address→Care-of Address). We think that this route can be announced throughout the network and thus, it is not necessary to deploy a HA on each link. As we will see, our solution only requires deploying one HA for the whole network. Moreover, our solution can take advantage of the redundancy mechanisms described in [16, 13, 8, 11] to increase the reliability and distribute the load among a set of HAs. With such architecture, besides the qualitative benefits, the load of the HA is significantly reduced, since packets are forwarded by the network and not by this entity.

In order to evaluate the proposed HA architecture, we use a trace-driven simulation. We collected two Netflow [7] traces from two different academic institutions. Our results show that the proposed solution forwards roughly 90% less traffic than a standard HA when considering Mobile IPv4/NEMO, and 15% less when considering Mobile IPv6. We also complement our evaluation using a publicly available dataset [**?**] obtaining comparable results.

In short, the contribution of this paper is twofold. First, we review the flexible Home Agent architecture, which was previously presented in [3]. And second, we present a trace-driven evaluation using data collected from three different networks. In [3] we evaluated our architecture using a simulator with a synthetic workload.

2. The flexible Home Agent Architecture

This section describes the flexible Home Agent (fHA) architecture.

2.1. Design Rationale

In this subsection, we analyze the different operations of a Home Agent (HA) and how they can be distributed from the network's point of view. In the rest of the paper, we will use the following terminology. We define Home Network as the set of Home Links managed by our HA. We define Exit Routers (ER) as the routers that connect the Home Network to the rest of the Internet. These ERs may or may not be the AS's Border Routers and an AS may contain one or more Home Networks.

Home Agents are responsible for maintaining bindings between the MN's identity and its location. The HAs forward the signaling messages and the data packets of the MNs. MNs send data packets through their HA when communicating with their Home Network or with peers (Correspondent Nodes, CNs). In the particular case of Mobile IPv6, MNs can communicate directly with their CNs and it is expected that communications through the HA are mainly used for short-term connections.

The Mobile IP RFCs [18, 28] state that packets sent through the HA may be secured through IPSec [19]. It should be taken into account that the MN can use any secure transport protocol (such as SSL) with its peers regardless of the IPSec connection with their HA. Taking this into account, it is not efficient to secure MN to CN communications because the packets are only secured on half of the path (MN→HA) while the rest of the path (HA→CN) is not secured. Regarding the MN's communications with the Home Network, protecting the path is efficient. In this case the HA acts as a Virtual Private Network (VPN) gateway.

Under these assumptions and following the basic idea that a registration from a MN to a HA can be seen as an internal route, we can distribute the HA's operations throughout the network. In our architecture, a single HA is required for the whole network; we refer to it as flexible Home Agent (fHA). This fHA processes (using IPSec) mobility-related signaling, and maintains binding information. It also distributes this information throughout the network as internal routes. This way, the network directly forwards the MN's communications with its CNs while the fHA only forwards communications with the Home Network (using IPSec), acting as a VPN gateway.

2.2. Overview

Figure 1 presents an overview of the fHA architecture. The proposed architecture has only one HA (we refer to it as fHA) that will serve all MNs of the network. This proposal allows deploying more than one fHA (see Sect. 2.3) to distribute the load. This fHA will be identified by a unicast address and the MNs will address their registration messages towards it. Upon reception of a registration message, the fHA validates it and configures the new route towards the MN at the ER. In addition, the fHA advertises the route to the Home Link's

Access Router (AR). At this point, the network is aware of the location of the MN.

When communicating with a CN through the HA, MNs do not address packets towards the fHA but to an IP address configured at the ERs. This way, a given ER receives the MN's data packets and decapsulates them, looks up the address, and forwards them towards the CN. Similarly, CNs send packets to the Home Address of the MN. Upon reception, the ER looks the destination address (the Home Address) of the packet up. Since the fHA has previously installed a route at the ERs, they are aware that the MN it is not at home. Therefore, the ERs encapsulate and forward the packet towards the location of the MN. Our architecture efficiently manages MN-to-CN communications, because a subset of the packet are directly forwarded by ERs. This way, the internal traffic of the network is significantly reduced.

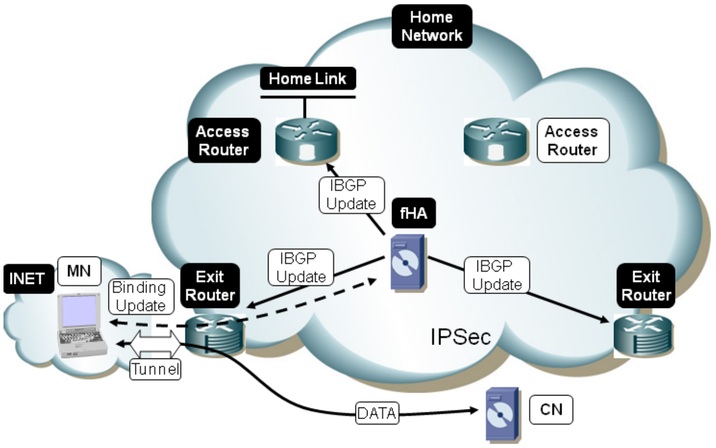

Figure 1: Overview of the proposed flexible Home Agent architecture

Regarding the communications from the MN to the Home Network, the MNs address their IPSec protected packets towards the fHA that, in turn, decapsulates and forwards them to the MN's peer. The peers address their data packets to the Home Address of the MN. Since the fHA has announced to the Home Link's AR a route for the MN, the AR is aware that the MN is away and it encapsulates the packet towards the fHA. Finally, the Home Link's AR also acts as a proxy-ARP for the MN. This enables communications between nodes located at the Home Link with the MN.

In the following subsections, the specific operations of our architecture are described in more detail.

2.3. Dynamic fHA Address Discovery

This subsection specifies how the fHA announces its presence and the mechanism used to boostrap the MNs. In the standard Mobile IPv6 protocol, HAs announce their presence through Router Advertisement messages. This way, the MNs can automatically select a HA. Our architecture implements this functionality in exactly the same way that Mobility Anchor Points (MAP) announce their presence in the Hierarchical Mobile IPv6 (HMIPv6) protocol [30]. This mechanism is also compatible with legacy MNs.

Each fHA sends Router Advertisement messages announcing its presence to the routers operating in the network. These messages include a preference value. The routers propagate these announcements towards ARs that, in turn, forward them to the Home Link. Each router decrements the preference value, so that MNs are not only able to automatically discover the address of the fHAs, but also to choose the best one according to the preference value.

This mechanism has many benefits. On the one hand, it enables ARs to automatically discover the fHA, thus avoiding manual configuration. On the other hand, it allows us to deploy more than one fHA on the network and distribute the load among them. The fHA's Router Advertisement messages include the prefix(es) of the Home Network that it is serving and the IP address configured at the ERs. Including the Home Network's prefix enables the MNs to be aware whether their peers are on the Home Network or not. Depending if the peer is on the Home Network or not, MNs will address the data packets to the fHA or to the ERs.

2.4. Signaling Processing

Each MN selects a given fHA through the above-mentioned mechanism. All the fHAs have pre-configured keys with the MNs as stated by the Mobile IP RFCs. Note that ARs and ERs do not share any keys with the MNs. The fHAs receive registration messages from the MNs as established by Mobile IP.

Upon reception of a successful registration message, the fHA has to announce this information (route) to the ERs, the Home Link's AR and the rest of the fHAs. To distribute this type of information we use a routing protocol. Instead of designing a new routing protocol, we use an already existing and deployed one. The routing protocol that best fulfills our requirements is the Interior Border Gateway Protocol (IBGP) [29]. In our solution the fHAs, the ERs and Home Link's ARs create an IBGP domain. It is very important to remark that this IBGP domain may be an already existing IBGP domain or a separate one. The routes announced through this IBGP domain always have the longest prefix (/128 or /32) and never impact the global routing system (eBGP). It should be noted that the routes announced by the fHAs are never propagated outside the network. Finally, the entities participating in the IBGP domain have pre-configured keys to provide confidentiality, integrity and authentication to the communications.

For each successfully received registration message, the fHAs send an IBGP UPDATE message to the ERs and to the AR responsible of the MN's Home Link. The fHAs are able to determine the appropriate AR by inspecting the MN's Home Address.

We introduce new options in the IBGP UPDATE message. The UPDATE message sent to ERs includes the following information: {*Home Address, Care-*

of Address, Lifetime}. Upon reception of this message, the ERs setup an endpoint for a tunnel with the MN. The tunnel source address is the IP address shared by the ERs while the destination address is the Care-of Address. In addition, each ER adds the following route into its routing table: HomeAddress→Tunnel. The tunnel and the route are automatically deleted after "Lifetime" seconds.

The UPDATE message sent to the AR includes the following information: {*Home Address, Lifetime*}. Upon reception of this message, the AR knows that the MN is away (note that the AR does not know the location of the MN). Next, the AR configures an endpoint for the tunnel towards the fHA that announced the route and adds the following route to its routing table: HomeAddress→Tunnel. The AR also starts acting as a proxy ARP for the MN. If a node of the Home Network (or Home Link) sends a packet to the MN, the AR intercepts and encapsulates it towards the fHA. Once again, the tunnel and the route are automatically deleted after "Lifetime" seconds.

Once the MN returns home, it sends a registration message to the fHA. Upon reception, the fHA sends an IBGP WITHDRAWAL message to the ERs and to the corresponding AR in order to immediately remove all the routes and tunnels related to the Home Address of the MN. The implementation of these options in IBGP is further discussed in Section 6.

2.5. Data Packet Processing

This subsection presents how packets are routed from/to the MNs.

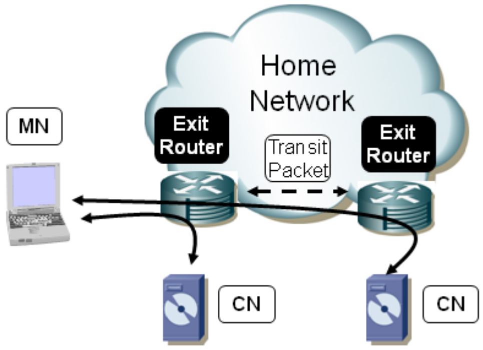

Figure 2: MNs to CNs communications

MNs communicating with CNs encapsulate their data packets towards the IP address configured at the ERs (Figure 2). The packets are received by the nearest ER (according to the inter-domain routing) that will de-capsulate and forward them towards the packet's destination address (i.e., the address of the CN).

MNs communicating with nodes located into their Home Network (Figure 3) encapsulate their packets towards the fHA. However, packets sent by MN's

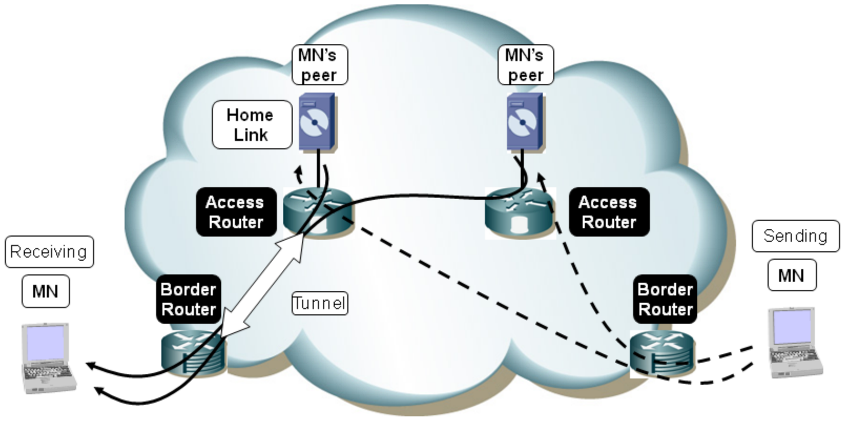

Figure 3: MNs to Home Network communications

peers are addressed to the Home Address of the MN. The MN's AR intercepts these packets. Since the AR is aware that the MN is away, it encapsulates the packets towards the fHA, that in turn re-encapsulates them towards the MN.

2.6. flexible Home Agent Location

This subsection discusses the possible locations of the fHAs. Each fHA can be placed anywhere in the network, as a separate server or colocated with an ER.

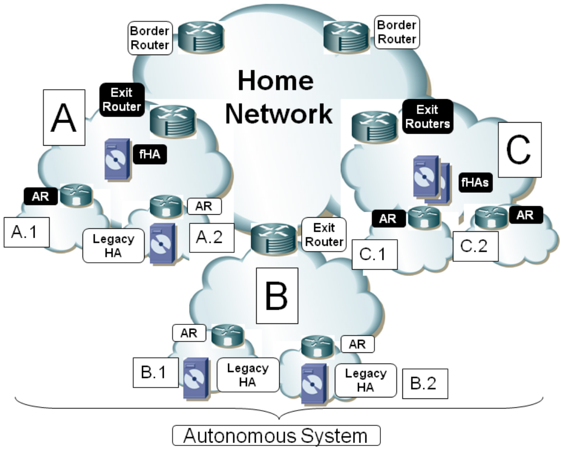

Figure 4: fHA location example

One of the major benefits of our proposal is its flexibility. On the one hand, our architecture can serve all the MNs of a network with one or more fHAs. If more than one fHA is deployed, MNs will select the nearest one based on the preference value. This way the load is spread among them. Each fHA thus only processes signaling messages and communications from/to the Home Network (like a VPN gateway). Communications from MNs to CNs are then processed by ERs. On the other hand, our architecture is transparent to MNs running with legacy Home Agents and both technologies may coexist on the same network.

Figure 4 shows an example of the flexibility of our architecture. The AS shown in the figure has three networks and each one can independently select the approach to deploy. For instance, the network “A” can deploy both technologies. The fHA could serve MNs belonging to the sub-network “A.1” while MNs belonging to the sub-network “A.2” could be served by a legacy HA. The network “B” can deploy only legacy Home Agents on each sub-network. Finally, the network “C” can deploy two fHAs and all the MNs from “C.1” and “C.2” could be served by them.

Only routers labeled in black will belong to the IBGP domain together with the fHAs of their network. There will be a separate IBGP domain for each Home Network. MNs served by an fHA send their data packets to an IP address configured at the ERs. Since the prefix of the IP address belongs to the Home Network’s prefix, the Border Router knows how to forward the packets and does not need to be aware of our protocol.

3. Evaluation Methodology

In order to evaluate the performance of the fHA architecture, we have carried out a trace-driven simulation. The results have been obtained by replaying a set of real-world traces with our ad-hoc simulator that was developed using the Perl programming language. We collected Netflow traces at two different campus networks from two different academic institutions. Both networks provide connectivity to the academic staff and to the students, and include common services such as Web or DNS. The traces were collected during six consecutive days and contain 36.94 and 8.19 million flows respectively. Regarding the size of both monitored networks, Inst-A has 1500 nodes attached and roughly 700 users, while Inst-B has 200 nodes servicing the same amount of users.

Both institutions include a subnetwork that provides connectivity to servers. These nodes were not considered in our experiments. The remaining subnetworks in Inst-B provide connectivity to wireless clients and, as such, were considered mobile clients that are away and roaming. Hence, we are assuming that the traffic profile of a mobile node is similar to that of a wireless node. This is a reasonable assumption since both types of nodes share the same types of users. It is therefore safe to assume that wireless and mobile nodes will run similar applications. Concerning Inst-A, a large percent of the clients were also attached wirelessly. Finally, we also complement our evaluation using a publicly available dataset [**?**] from a different network scenario. This set of three traces allowed the Perl simulator to emulate the performance of a theoretical fHA deployed at all these networks.

The performance of the fHA was evaluated considering both Mobile IPv4/NEMO and Mobile IPv6. We also considered the performance of a standard HA for comparison. In particular, we evaluated the benefits and the costs of our proposal. The benefits were analyzed comparing the load of the standard HA with that of a fHA in terms of bandwidth and packets/s. In order to evaluate the load we considered the flows and the signaling that, depending on the selected mobility protocol, are forwarded through the Home Agent (either standard HA or fHA). We did not consider handovers since such events impose the same signaling load to both entities. Regarding the costs, we computed the intra-domain signaling overhead in terms of IBGP messages/s and stored state at the routers. Finally, it is worth mentioning that the experimental traffic data sets used in this work can be found at [22].

4. Description of the Traces

In this section, we present a brief description of the datasets used in this study. The data captured comprise Netflow records from two different campus networks at two academic institutions (Inst-A and Inst-B) for six days of traffic: from March 9 to March 14 (2007) at Inst-A and from March 13 to March 18 (2009) at Inst-B. Overall, both datasets contain 144 hours of traffic with 903.7 GB at Inst-A and 159.2 GB at Inst-B. Both networks include a set of sub-networks (7 for Inst-A and 6 for Inst-B) connected through a single router that also provides Internet access. Both academic networks include servers and end-hosts (1500 and 200 nodes respectively) and roughly 700 and 200 users respectively. The bandwidth consumption in Inst-A and Inst-B is 4.3Mbps and 0.7Mbps on average respectively. In both cases, bandwidth exhibits seasonal patterns related to the time of day and to the day of the week. Since both networks only include one router, the traces contain all internal and external flows. Unfortunately, with this setup we were unable to capture flows transmitted within a subnet. Nevertheless, we expect this traffic to be low since the servers are located in separated subnets.

First we focus our attention on the ratio of internal vs. external flows (Figure 5). As shown in the figure, roughly 95% of the flows, octets and packets belong to traffic to/from the Internet, and only 5% represents traffic between hosts inside the institutions. It is worth noting that Inst-B has a slightly larger percentage of internal flows (9% vs. 4%), although these flows carry little traffic (about 4% of the total packets).

Table 1 presents the breakdown of traffic by type of flows. As explained earlier, we consider that the nodes of the network are actually away and roaming. The only hosts that are not considered to be roaming are the servers of the campus network, which we identified manually. As expected, the traffic between servers and between MNs is negligible. The bulk of the traffic consists of MN-to-server flows (i.e., internal clients accessing the mail server) and MN to

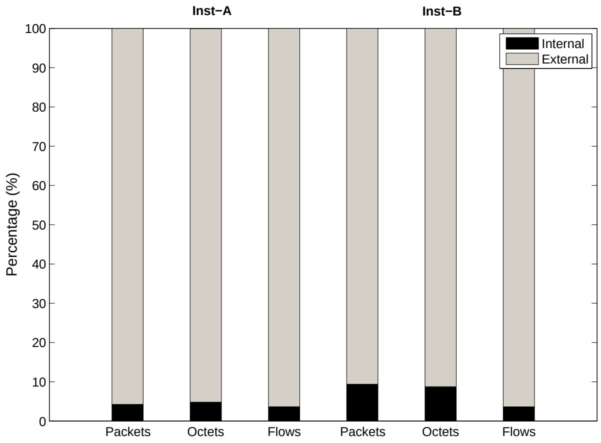

Figure 5: Internal vs. External Traffic

the Internet (i.e., standard clients accessing remote servers). It is worth mentioning that the servers deployed at both institutions include mainly internal applications and, therefore, the traffic from/to the Internet of these servers is extremely low.

Finally, we also used a publicly available dataset [**?**] captured in two internal network locations at the Lawrence Berkeley National Laboratory in the USA. The trace, obtained in April 2004, includes 100 hours of traffic and the activity of 8,000 nodes and 47,000 external addresses. A detailed description of the trace can be found at [27].

Table 1: Fraction of Flows, Octets and Packets for different types of flows

Data Set	Inst-A Traces			Inst-B Traces		
Type	Flows	Octets	Packets	Flows	Octets	Packets
Internal flows						
Server to Server	2.33%	0.39%	1.30%	0.01%	0.01%	0.05%
Server to MN	2.02%	3.13%	2.70%	9.37%	8.78%	3.58%
MN to MN	0.46%	0.13%	0.24%	0.01%	0.01%	0.01%
External flows						
Server to INET	34.22%	9.76%	11.39%	9.41%	9.25%	3.20%
MN to INET	60.97%	86.59%	84.37%	81.20%	81.95%	93.16%

5. Evaluation

In this section, we evaluate the performance of the proposed fHA architecture in front of a standard HA. The evaluation is based on the traces and aims to show the costs in terms of signaling overhead and stored state at the routers, and the benefits in terms of saved resources: octets and packets. In the last part of this section we complement the evaluation using the publicly available dataset described in [**?**].

5.1. Costs

As discussed in Section 2.4, for each mobile node and handover, the fHA has to transmit a signaling packet to the ERs. This is done using an IBGP message, either IBGP_UPDATE or IBGP_WITHDRAWAL. Therefore, we can state that the cost of the fHA in terms of signaling is $O(H)$, where H is the amount of handovers per unit of time and mobile node. H will be highly dependent on the specific deployment of the Mobile IP technology. In this section we aim to discuss realistic values for H. In particular, this parameter depends on two different metrics: (i) the amount of active mobile nodes served by a single Home Agent and (ii) the movements of these mobile nodes and, in particular, to the amount of handovers per second and mobile node.

Regarding the first one, consider as an example Figure 6, which plots the amount of *active* mobile nodes per second in both Inst-A and Inst-B networks. Recall that Inst-A has a total of 1500 nodes while Inst-B has 200. As shown in the figure, the average number of active nodes is 193.44/s for Inst-A and 18.93/s for Inst-B (averaged over one minute) while the maximum is 295.03/s and 35.58/s respectively. This indicates that, on average, 12.89% and 9.46% of the total nodes are active, which provides a hint of the fraction of nodes that are active from the total number of nodes served by a single Home Agent. Note that this may vary depending on the network and user profiles. However, this value helps us to better understand H. Additionally, this value can be decreased by deploying more fHAs or by spreading the mobile nodes across several subnetworks (see Section 2.6 for further details).

The second metric is the amount of handovers per second and per mobile node. Again, this depends on the specific deployment of the Mobile IP technology. Theoretically, a mobile node performs a handover each time it changes from one sub-network to another. A single subnet may provide connectivity to a large geographical area, and this depends on the particular wireless technology deployed. For instance UMTS [32] provides connectivity to very large areas (hundreds of km) while IEEE 802.11 provides connectivity to smaller areas, ranging from meters to a few kilometers (e.g., a wireless campus network). Therefore, depending on the speed of the mobile node, and the specific wireless technology deployed, a mobile node will handover more or less often. Further, there are some protocols, such as HMIPv6 [30], that reduce the amount of handovers signaled towards the Home Agent by deploying a special entity (Mobility Anchor Point) at the visiting network.

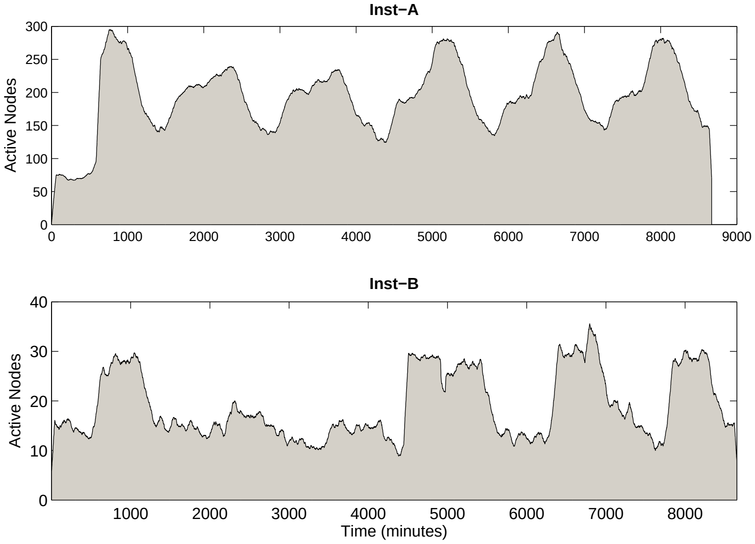

Figure 6: Active Nodes/s (averaged per minute)

Even though it is difficult to provide a realistic value for the amount of handovers per second, we carried out a simulation to evaluate our proposal. Specifically, we configured a highly mobile environment using a Random Trip mobility model [26]. In particular, we used the Random Waypoint on Generalized Domain model with a set of 8 domains (we refer the reader to [26] for further details). Each domain represents a layer-2 network where a MN can move without changing its point of attachment (i.e., default router). Only when the MN changes from one domain to another it performs a handoff, signals its new location, and in turn the fHA informs the ER using an IBGP message. The first domain is considered to be the Home Network (either Inst-A or B) while the rest of the domains are foreign networks. We consider 1000 mobile nodes and we simulate this environment during 10.000 seconds (roughly 2.7 hours). The simulation, considering all the mobile nodes, produced a mean of 4.68 handovers/s and, in the worst case, 24.25 handovers/s. This means that, in the worst case, each mobile node performs 0.024 handoffs per second.

Taking all these results into account and considering our evaluation scenarios (both institutions), in the worst case, the mobile nodes would produce a total of $H = 7.08$ and $H = 4.64$ handovers respectively. Therefore, the fHA should send, in the worst case, 7.08 and 4.64 IBGP messages within the same second. Additionally, regarding the stored state at the router, each mobile node that is away requires 1 tunnel and 1 route towards it, which is a maximum of 29.9KB for the Mobile IPv4/NEMO case, and 119.6KB for the Mobile IPv6 case.

As a summary, we have seen that the signaling overhead of the fHA is linear with respect to the amount of handovers per mobile node, and the traces and simulations show that this amount is in the order of tens per second. In addition, we investigated if a commercial router could support such a load, and according to the measurements presented in pierre, commercial routers can install 10^4 routes/s. This value is several orders of magnitude above our requirements.

5.2. Benefits

Besides the architectural benefits of the fHA described in the previous sections, the fHA processes a lower load compared to a standard Home Agent. This is because a large percentage of the traffic is directly processed by Exit Routers. In this subsection, we evaluate these benefits in terms of saved packets and octets with respect to a standard HA, considering both Mobile IPv4/NEMO and Mobile IPv6 clients.

5.2.1. Mobile IPv4/NEMO

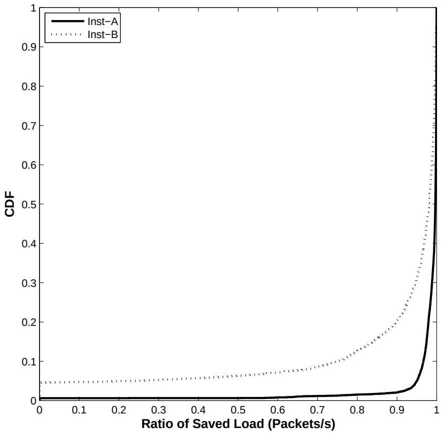

Figure 7: Cumulative Distribution Function (CDF) of the ratio of saved load in packets/s. The ratio refers to the percentage of traffic saved by a fHA in front of a standard HA.

First we focus on Mobile IPv4/NEMO. Figures 7 and 8 plot the Cumulative Distribution Function (CDF) of the ratio of saved load (i.e., $ratio = \frac{Load_{HA} - Load_{fHA}}{Load_{HA}}$). The figures compare the amount of load in terms of packets and octets processed by the HA and by the fHA. Also, the figure considers both datasets (Inst-A and Inst-B) during the six days of the experiment. In this case, the difference in the load is very significant because the fHA only processes traffic from the MNs towards internal servers. As indicated in Table 1, this represents a small fraction of the total traffic.

The figure also shows that the amount of resources required to run a fHA compared to a HA is much lower, given that our architecture has to process only 67 packets/s and 5.8kbps on average for Inst-A, while the standard HA forwards

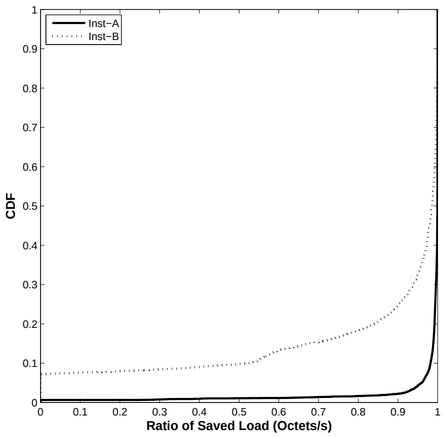

Figure 8: Cumulative Distribution Function (CDF) of the ratio of saved load in octets/s. The ratio refers to the percentage of traffic saved by a fHA in front of a standard HA.

2160 packets/s and 1.6Mbps. For Inst-B, the fHA forwards a larger percentage of traffic because this network has a higher ratio of internal server-to-MNs flows.

Summarizing our findings concerning Mobile IPv4/NEMO, the advantages of the fHA architecture in front of a standard HA are very significant in terms of load. According to our experiments, the proposed fHA has to process only Kbps of traffic while the standard HA forwards Mbps.

5.2.2. Mobile IPv6

In this subsection, we extend the evaluation of the benefits of the fHA considering Mobile IPv6 clients. In this particular case, we have to take the built-in route optimization mechanism into account. Mobile IPv6 clients can initiate the return routability procedure in order to establish direct communications with their peers (see [25] for further details). In this case, these flows are not forwarded by the HA (neither by the fHA). However, in order to setup a direct route the MN has to send 6 signaling messages, and this takes roughly 2 Round-Trip-Times[2]. During this time the communications are forwarded through the HA.

In our evaluation, we consider that Mobile IPv6 clients benefit from route optimization, reducing the load at the HA. The Mobile IPv6 standard suggests that developers should decide when to trigger route optimization [18]. This procedure has a cost in terms of signaling overhead and the RFC suggests avoiding to trigger it for very short flows (e.g., a DNS query). Designing an efficient route optimization triggering algorithm is out of the scope of this paper. In this evaluation we consider that *all* flows are route optimized and that only

[2] $max(RTT_{MN-CN}, RTT_{MN-HA} + RTT_{HA-CN}) + RTT_{MN-CN}$

packets transmitted during the return routability establishment are processed by the HA. This means that our evaluation considers a worst-case scenario for the proposed fHA.

In order to consider route optimization for Mobile IPv6, we have to choose a realistic value for the RTT between the MN and its peers. This is a problematic choice since it will highly depend on the topological distance between both nodes. We performed the following experiment to find a representative set of values. We collected a dataset with 200k one-way-delays between arbitrary pairs of nodes at the Internet. The dataset comes from the iPlane infrastructure [20][3]. Next, we geo-located each host using a commercial database maxmind and processed the dataset distributing the delays into the following categories: (*i*) end-hosts located in the same country, (*ii*) end-hosts located in the same continent and, finally, (*iii*) end-hosts located in different continents. Considering the different scenarios and the results of this simple experiment, we choose three different representative (90% of the cases) one-way-delays between the MN and its peers: 75ms, 125ms and 500ms. This leads us to consider three different durations for the return routability procedure: 300ms, 500ms, 2s. Recall that we estimate the duration of the return routability procedure as $2 \times RTT$.

Next, we proceed with the evaluation of the load for Mobile IPv6 clients in terms of packets and octets. We use the same methodology as in the previous subsection. Figure 9 shows the CDF of the ratio of saved load in packets and octets. The figure shows that the reduction of the load is less evident, mainly because the route optimization mechanisms greatly reduce the load for the standard HA. Interestingly, in the Mobile IPv4 case, the Inst-A HA forwards on average 1.67Mbps while, for the Mobile IPv6 case, it forwards only 60.43Kbps. This also shows the benefits of the IPv6 built-in route optimization mechanisms, which are irrespective of the proposed fHA.

Recalling Figure 9, and assuming a 500ms RTT, the fHA saves roughly 13% of the packets and 20-31% of the octets on average (Inst-A and B respectively). The duration of the return routability process also has a significant impact on the saved load. Higher RTTs (e.g., 2s) save more traffic, 50% of the octets for Inst-A on average. This is explained by the fact that during this time packets are forwarded by the standard HA. Lower RTTs (e.g., 300ms) slightly reduce the gains of the fHA. It is worth mentioning that this is a worst-case scenario and probably not all the flows will benefit from route optimization.

5.3. Evaluation in Other Network Environments

In previous sections, we evaluated the performance of the proposed fHA in front of traditional HAs using two different traces. The objective of this section is to evaluate if similar results are also obtained in other network environments.

[3] iPlane is a scalable service providing accurate predictions of Internet path performance. To achieve these goals, the iPlane project uses hundreds of vantage points distributed across the Internet for measurements, and they update their dataset daily.

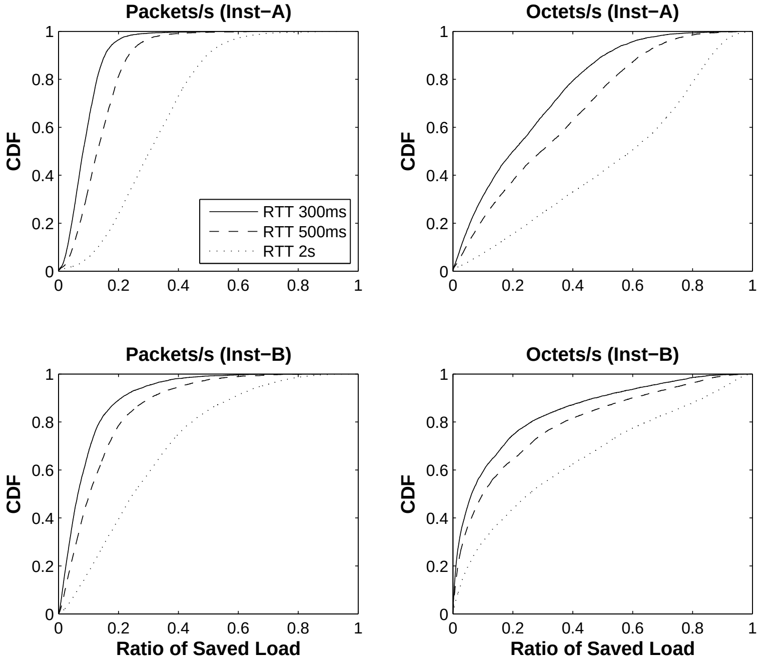

Figure 9: Cumulative Distribution Function (CDF) of the ratio of saved load (standard HA vs fHA in MIPv6, averaged per second). The ratio refers to the percentage of traffic saved by a fHA in front of a standard HA.

For this purpose, we use a publicly available dataset [**?**] captured in two internal network locations at the Lawrence Berkeley National Laboratory.

The trace was analyzed by *V. Paxson et al.* in [27] focusing on the enterprise data traffic. For this reason, the trace contains a larger amount of internal traffic when compared to external traffic. We refer the reader to [27] for further details about the trace.

Figure 10 plots the ratio of saved bandwidth both in Mobile IPv4 (left) and Mobile IPv6 (right). The figure shows that the performance of the fHA is comparable to that observed with the Inst-B trace. In particular, the ratio of saved load is, on average, roughly 90% for Mobile IPv4/NEMO and 10% for Mobile IPv6. This is an expected result since this trace, as in the trace from Inst-B, contains a larger amount of internal traffic. The remaining results for packets and flows are also comparable with those obtained with Inst-B.

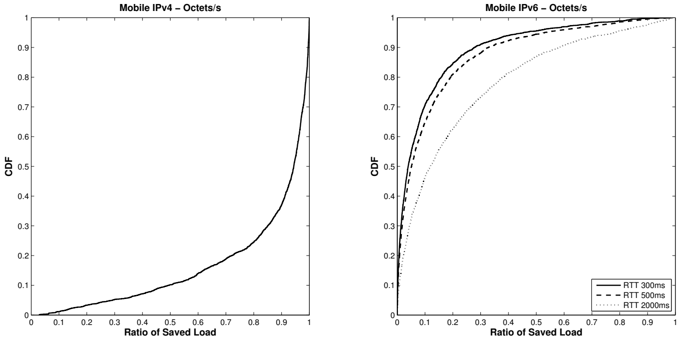

Figure 10: Cumulative Distribution Function (CDF) of the ratio of saved bandwidth by fHA compared to standard HA in MIPv4 (left) and ratio of saved bandwidth in MIPv6 (right). Results are averaged over one second.

6. Implementation and Deployment of the fHA

This section discusses relevant aspects of the implementation and deployment of the fHA architecture.

6.1. Implementation

The fHA architecture requires support in four different entities: MNs, fHA, Exit Routers (ER) and Access Routers (AR).

- *MN*: MNs do not have to be updated and only require changes in terms of configuration. MNs need to be configured to use the fHA address for signaling packets and ERs addresses for data packets.

- *fHA*: The implementation of the fHA can take base on existing Home Agent implementations [6, 31], since the required functionalities are similar. The implementation must also include an iBGP routing engine. For this purpose, a developer can take advantage of well-known open-source implementations, such as Zebra [15]. The relationship between the Home Agent software and the iBGP routing engine is rather simple: for each Binding Update message the fHA must transmit an iBGP message. In addition, there is no need to store any extra state and the remaining functionalities are already provided by the Home Agent software. The fHA can be implemented in a hardware-based router or in an inexpensive software-based router (a PC). According to our results, the fHA has to process, in the worst case, a peak of ≈10k pkts/s for Inst-A and ≈1k pkts/s for Inst-B. It has been reported that software-base routers, built on top of off-the-shelf PCs, can forward (at the time of this writing) up to ≈300k pkts/s [23]. Moreover, and assuming a linear relationship between the load in pkts/s and the amount of users, the fHA could serve an order of tens of thousands of MNs using a single PC. Although this is a rough estimate, it is a reasonable assumption since MNs do not usually exchange traffic among them, but rather connect to servers. It is worth mentioning that in any case, and regardless of the load, network operators may want to deploy multiple fHAs to achieve redundancy.

- *ER:* These routers have two basic requirements: (1) include an iBGP routing engine (typically routers already include this protocol) and (2) encapsulate/decapsulate data packets from/to MNs. In order to forward such packets, the router must encapsulate/decapsulate them on the fly. This means that the router should not be configured with a tunnel for each combination of MN/CN. Instead, it should simply check in its routing table if the packet is addressed towards the MN and encapsulate it (add a new IP header) or, in case it was originated by the MN, decapsulate it (strip the outer IP header). In order to implement this requirement the router software should be upgraded.

- *AR:* Access Routers must also include an iBGP engine and act as a proxy ARP. Both functionalities are commonly included in routers. It is worth noting that upgrading ARs is not a hard requirement for the fHA architecture, since ARs enable the communication between the MNs and fixed peers attached to the same Home Link. In some cases, a network operator may not want to enable this functionality.

Finally, the fHA architecture may require defining a new option for the iBGP protocol. This means that the router's firmware must be updated. This could be alternatively implemented with the basic iBGP support, and without updating the firmware. In this case, the MNs locations could be announced as routes towards the Home Address/32 (/128 in IPv6) and the next hop as the Care-of Address. In addition, the lifetime can be replaced by triggering an IBGP WITHDRAWAL message when the location has expired.

6.2. Deployment

The deployment cost of the fHA is low, mainly because the proposed architecture includes autoconfiguration capabilities. Network administrators willing to deploy this architecture should set up the iBGP routing protocol (or update the existing one) to include the fHA, the ERs and (optionally) the ARs. Both the fHA and the MNs only require basic configuration, such as the addresses of the MNs and the shared keys. Routers participating in the fHA architecture (ERs and ARs) do not need any explicit further configuration since they automatically learn the MN's location through iBGP. Finally, it is worth noting that efficient caching strategies, such as the one proposed in [4], could further improve the performance of the fHA.

7. Conclusions

In this paper, we presented a flexible and distributed HA architecture. Existing proposals [16, 13, 8, 11, 33] provide a reliable HA architecture by deploying redundant HAs on each Home Link. The architecture proposed in this paper has the same benefits as previous solutions, but only requires the deployment of one set of fHA for the whole network.

Our solution is reliable: a failure on the MN's ARs will not disconnect the MN. In this case, the MN will still be able to communicate with the Home Network (except for the Home Link) and with the rest of the Internet. Since our solution allows deploying several fHA for each network, a failure of a fHA does not disconnect the MN. In this case, our solution can benefit from the proposed efficient failure recovery mechanisms presented in [16, 13, 8, 11]. This way, we can minimize the service interruption time. Finally, a failure of an ER does not disconnect the MN. In this case, the network announces the failure of the ER through the exterior routing protocol and the packets will be re-routed. Our solution also provides load balancing because the MN's data packets are processed by ERs or by a set of fHAs.

Besides the architectural benefits, the fHA architecture also outperforms the standard HA. We compared the performance of both entities using three traces from three different networks. Our evaluation shows that for Mobile IPv4, the fHA forwards roughly 90% less traffic than the HA. In the case of Mobile IPv6, we showed that it highly depends on the return routability policy implemented by the MN. We used a worst-case approach that shows that the fHA saves roughly 15% of the resources, when compared to the standard HA. This indicates that deploying the proposed architecture has a lower cost in terms of CPU/memory and bandwidth usage.

In order to distribute the operations of a HA, some extra signaling has to be added at the exit routers. The costs depend on the amount of active mobile nodes and their movements (i.e., handovers per second). We simulated a highly mobile environment that shows that each router would need to process only tens of signaling messages per second. Experimental results show that commercial routers can support thousands of updates per second.

[1] I. Al-Surmi, M. Othman, B. Mohd Ali, Mobility management for IP-based next generation mobile networks: Review, challenge and perspective, Journal of Network and Computer Applications, Volume 35, Issue 1, January 2012, Pages 295-315, ISSN 1084-8045, 10.1016/j.jnca.2011.09.001.

[2] M. Alnas, I. Awan, R.D.W. Holton, Performance Evaluation of Fast Handover in Mobile IPv6 Based on Link-Layer Information, Journal of Systems and Software, Volume 83, Issue 10, October 2010, Pages 1644-1650, ISSN 0164-1212, 10.1016/j.jss.2010.03.080.

[3] A. Cabellos-Aparicio, J. Domingo-Pascual, "A Flexible and Distributed Home Agent Architecture for Mobile IPv6-Based Networks" in Proc. of NETWORKING 2007. Ad Hoc and Sensor Networks, Wireless Networks, Next Generation Internet, Lecture Notes in Computer Science, pp. 333-344, Vol. 4479, 2007.

[4] P. Chuang, Y. Chiu, Efficient cache invalidation schemes for mobile data

accesses, Information Sciences, Volume 181, Issue 22, 15 November 2011, Pages 5084-5101, ISSN 0020-0255, 10.1016/j.ins.2011.07.005.

[5] M. Cimino, F. Marcelloni, Autonomic tracing of production processes with mobile and agent-based computing, Information Sciences, Volume 181, Issue 5, 1 March 2011, Pages 935-953, ISSN 0020-0255, 10.1016/j.ins.2010.11.015.

[6] CISCO IPv6 Solutions (online) http://www.cisco.com/en/US/technologies/tk648/tk872/tk373/technologies_white_paper09186a00802219bc.html

[7] CISCO NetFlow www.cisco.com/web/go/netflow (Last seen on 19th March 2009)

[8] H. Deng, X. Huang, K. Zhang, Z. Niu, M. Ojima. "A hybrid load balance mechanism for distributed home agents in mobile IPv6" Personal, Indoor and Mobile Radio Communications, 2003. PIMRC 2003. 14th IEEE Proceedings on, pp. 2842 - 2846 vol.3, DOI=10.1109/PIMRC.2003.1259264 , 2004.

[9] L. Duen-Ren, T. Pei-Yun, C. Po-Huan, Personalized recommendation of popular blog articles for mobile applications, Information Sciences, Volume 181, Issue 9, 1 May 2011, Pages 1552-1572, ISSN 0020-0255, 10.1016/j.ins.2011.01.005.

[10] Dynamics HUT Implementation http://dynamics.sourceforge.net/

[11] J. Faizan et al. “Efficient Dynamic Load Balancing for Multiple Home Agents in Mobile IPv6 based Networks” in Proc. Pervasive Services, 2005. ICPS ’05. Proceedings. International Conference on. 08/2005; DOI: 10.1109/PERSER.2005.1506409

[12] P. Francois, C. Filsfils, J. Evans, and O. Bonaventure. 2005. Achieving sub-second IGP convergence in large IP networks. SIGCOMM Comput. Commun. Rev. 35, 3 (July 2005), 35-44. DOI=10.1145/1070873.1070877 http://doi.acm.org/10.1145/1070873.1070877

[13] W. Fritsche and I. Guardini. "Deploying home agent load sharing in operational mobile IPv6 networks" In Proceedings of first ACM/IEEE international workshop on Mobility in the evolving internet architecture (MobiArch ’06). ACM, New York, NY, USA, 31-36. DOI=10.1145/1186699.1186711 http://doi.acm.org/10.1145/1186699.1186711, 2006

[14] Geolocation Maxmind http://www.maxmind.com/

[15] GNU Zebra Routing Software http://www.zebra.org/

[16] F. Heissenhuber, W. Fritsche, and A. Riedl. ”Home agent redundancy and load balancing in mobile IPv6” In Broadband communications, Kluwer Academic Publishers, Norwell, MA, USA 235-244, 2000

[17] HotPlanet 2009: The 1st ACM International Workshop on Hot Topics of Planet-scale Mobility Measurements (colocated with ACM Mobisys) `http://www.hotplanetconf.net/` 2009

[18] D. Johnson, C. Perkins, J. Arkko, ”Mobility Support in IPv6”, RFC 3775, June 2004.

[19] S. Kent, R. Atkinson. ”Security Architecture for the Internet Protocol”, RFC 2401, 1998

[20] H. V. Madhyastha, T. Anderson, A. Krishnamurthy, N. Spring, and A. Venkataramani. 2006. A structural approach to latency prediction. In Proceedings of the 6th ACM SIGCOMM conference on Internet measurement (IMC ’06). ACM, New York, NY, USA, 99-104. DOI=10.1145/1177080.1177092 http://doi.acm.org/10.1145/1177080.1177092, 2006

[21] S.S. Manvi, M.S. Kakkasageri, Multicast routing in mobile ad hoc networks by using a multiagent system, Information Sciences, Volume 178, Issue 6, 15 March 2008, Pages 1611-1628, ISSN 0020-0255, DOI: 10.1016/j.ins.2007.11.005.

[22] Mobility Dataset (online), http://personals.ac.upc.edu/acabello/fha

[23] R. Morris, E. Kohler, J. Jannotti, and M. Frans Kaashoek. 1999. The Click modular router. In Proceedings of the seventeenth ACM symposium on Operating systems principles (SOSP ’99). ACM, New York, NY, USA, 217-231. DOI=10.1145/319151.319166 http://doi.acm.org/10.1145/319151.319166

[24] C. Ng, P. Thubert, M. Watari, F. Zhao. ”Network Mobility Route Optimization Problem Statement”, RFC 4888, July 2007.

[25] P. Nikander, J. Arkko, T. Aura, G. Montenegro, E. Nordmark. ”Mobile IP Version 6 Route Optimization Security Desig”, RFC 4225, December 2005

[26] S. PalChaudhuri, J. Le Boudec, and M. Vojnovic. 2005. Perfect Simulations for Random Trip Mobility Models. In Proceedings of the 38th annual Symposium on Simulation (ANSS ’05). IEEE Computer Society, Washington, DC, USA, 72-79. DOI=10.1109/ANSS.2005.33 http://dx.doi.org/10.1109/ANSS.2005.33

[27] R. Pang, M. Allman, M. Bennett, J. Lee, Vern Paxson, and Brian Tierney. 2005. A first look at modern enterprise traffic. In Proceedings of the 5th ACM SIGCOMM conference on Internet Measurement (IMC ’05). USENIX Association, Berkeley, CA, USA, 2-2.

[28] C. Perkins (Ed), "IP Mobility Support for IPv4", RFC 3344, Aug. 2002

[29] Y. Rekhter, T. Li. "A Border Gateway Protocol 4 (BGP-4)", RFC 1771, 1995

[30] H. Soliman, C. Castelluccia, K. El Malki, L. Bellier. "Hierarchical Mobile IPv6 Mobility Management (HMIPv6)", RFC 4140, 2005

[31] The Kame Project (online) `www.kame.net`

[32] UMTS, "Radio interface protocol architecture" 3GPP, Technical Specification 25.301-v4.3.0 Release 4, June 2002.

[33] R. Wakikawa, Y. Ohara, J. Murai. "Virtual mobility control domain for enhancements of mobility protocols", INFOCOM 2005. 24th Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings IEEE, pp. 2792 - 2797 vol. 4, DOI=10.1109/INFCOM.2005.1498564, 2005

[34] Y. Wong, T. Wang, Y. Lin, Effects of route optimization on out-of-order packet delivery in Mobile IP networks, Information Sciences, Volume 169, Issues 3-4, 1 February 2005, Pages 263-278, ISSN 0020-0255, DOI: 10.1016/j.ins.2004.06.008.