Journal of Mobile Multimedia, Vol. 3, No.3 (2007) 218-234

# MULTIMEDIA FLOW MOBILITY IN HETEROGENEOUS NETWORKS USING MULTIHOMED MOBILE IP

ROBERT BRÄNNSTRÖM, CHRISTER ÅHLUND, KARL ANDERSSON, DANIEL GRANLUND

*Division of Mobile Networking and Computing*

*Luleå University of Technology*

*{ robert.brannstrom, christer.ahlund, karl.andersson, daniel.granlund}@ltu.se*

Received March 13, 2007
Revised May 17, 2007

Communication in next generation networks will use multiple access technologies, creating a heterogeneous network environment. To enable end-user terminals to move between access networks with minimal disruption, the terminals should be able to maintain multiple active network connections. Such a multihomed mobile host will experience differences in capabilities and coverage area depending on the access technologies. This paper proposes and evaluates an extension to Mobile IP enabling multihoming, regardless of the access technology. Mobility of multimedia communication in this environment should adapt to changing conditions and be based on dynamic measurements and user preferences. The proposed architecture gives opportunities for mobile multimedia applications to use multiple access networks simultaneously and the possibility to move individual flows between access networks and between user devices. Media flows are identified by destination IP address, protocol and port number. Evaluation results are presented both from a simulation study and from a real world prototype implementation using three different wireless access technologies: 802.11, UMTS and 802.16-2004.

*Key words*: Wireless communication, Heterogeneous Networks, Mobile IP, Flow mobility

## 1 Introduction

In new generations of wireless networks, seamless mobility across heterogeneous networks will be supported. A widespread vision of the fourth generation (4G) mobile networks or Next Generation Networks (NGN) includes coexistence of current wireless technologies such as WLAN, WiMAX, General Packet Radio Service (GPRS) and Universal Mobile Telecommunications System (UMTS). Different technologies will be bound together into a single network and IP will be the glue. A Mobile Node (MN) will be equipped with multiple access network interfaces and users will be able to roam transparently over networks in a seamless manner. Software defined radio have however recently gained new interest in research communities and may in the future be an alternative to using multiple interfaces.

### *1.1 Handover policies*

To manage mobility between Access Points (APs) there are basically two approaches, namely mobile-controlled handover (MCHO) and network-controlled handover (NCHO). NCHO requires network providers to manage handovers between different technologies and is not a feasible solution in today’s heterogeneous networks. On the contrary MCHO can easily be adopted by adding multiple interfaces to MNs and additional mobility management software. For heterogeneous networks, policies are required for the decision of which type of technology to use in different situations. These policies should be based on user preferences as well as continuously evaluating performance of available access networks.

The ideas and terms of an IETF proposed policy model [17] are widely spread. Figure 1 illustrates a policy model that is based on the IETF proposed Policy Decision Point (PDP) and Policy Enforcement Point (PEP) entities, extended with a Policy Repository (PR) entity.

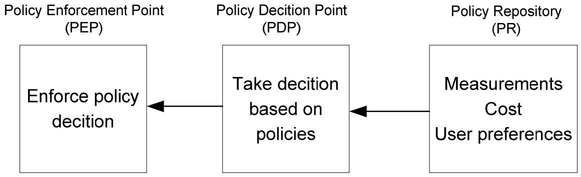

Figure 1 Policy-based decision model.

As show in Figure 1, the model consists of three entities:

- Policy Repository: The PR is responsible for delivery of requested policy parameters to the Policy Decision Point. The PR contains information such as user preferences, signal strength and cost of available access networks. The PR can obtain information through measurements of the environment.
- Policy Decision Point: The PDP is the control entity that evaluates access networks through policy decisions. The policy decisions are based on the parameters received from the PR. If the PDP decides that a handover is motivated, the PDP informs the PEP to perform a handover.
- Policy Enforcement Point: The PEP receives policy decisions from the PDP and performs the actual handover. The PEP is said to enforce the policy decision [9].

The actual location of the PDP (i.e. mobile node or network node) separates policy systems to perform an MCHO or an NCHO.

### *1.2 Mobility management*

To manage mobility for an MN connecting to IP networks, where applications and users are unaware of the network mobility, Mobile IP (MIP) is deployed. The MIP architecture incorporates a Home Agent (HA), and the MN, configured with an IP address at the home network (Home Address, HoA). An MN connected to the home network will operate according to normal IP network operations, without using MIP. When an MN connects to a foreign network it will register its new point of attachment by sending a Binding Update (BU) message containing the local address to the HA. This address is called the Care-of Address (CoA). The registration sent by an MN to the HA will create a binding in the HA between the HoA and the CoA.

When packets to the MN are discovered at the home network, the HA will forward the packets to the CoA using tunneling. A tunnel encapsulates the received packet as a payload in a new packet with an outer IP header having the CoA as the destination and the HA as the source. When the packet arrives at the MN, it will be decapsulated by the networking software. The outer packet header is removed before the packet is handed to upper layers. In MIPv6 a packet sent to a Correspondent Node (CN) will use the MN’s CoA as the source, and the HoA will be added in the home address destination option. Since the addresses are topology-correct, ingress filtering is avoided. The CN receiving the packet will replace the source address with the address in the home address destination option before handing the packet to the transport layer. The routing created by MIP is referred to as triangular routing (see Figure 2). Here packets from a CN are sent to the MNs home address (HoA).

The HA tunnels packets to the MNs CoA, and the MN sends its traffic directly from its current location to the CN, making a triangle. In the case of CN being unaware of MIP the traffic must be tunneled from the MN back to the HA and then forwarded by the HA to the CN. Bi-directional tunnelling is also the way MIPv4 handles Co-located CoAs.

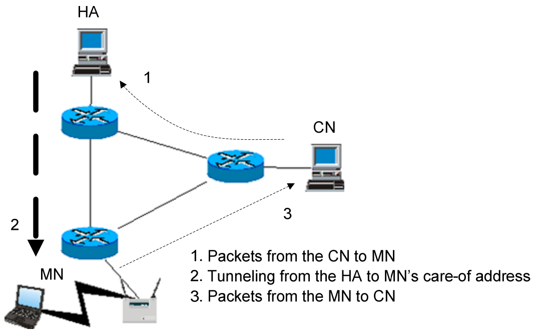
HA
1
CN
3
2
MN
1. Packets from the CN to MN
2. Tunneling from the HA to MN’s care-of address
3. Packets from the MN to CN

Figure 2 Triangular routing in Mobile IP.

To optimize routing between the MN and a CN, a route optimization procedure is used (see Figure 3). An MN receiving packets via the HA informs the CN about its current CoA in a BU. When a CN receives a BU it will start to send packets directly to the MN using the CoA as the destination address.

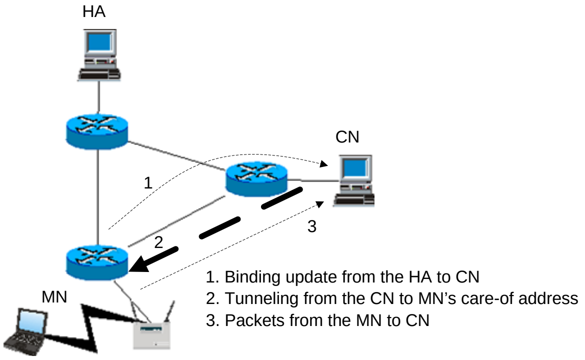
HA
CN
1
3
2
MN
1. Binding update from the HA to CN
2. Tunneling from the CN to MN’s care-of address
3. Packets from the MN to CN

Figure 3 Route optimization in Mobile IP.

In MIPv6, support for route optimization is built into IPv6. The CN uses the IPv6 routing header, where the destination of the packet is the MN’s CoA and the address in the routing header is the MN’s HoA. When the MN receives such a packet, the destination field will be updated with the MN’s HoA before handing the packet to the transport layer.

To secure MIPv6 route optimization the return routability procedure is used (see Figure 4). In the procedure four messages are sent; Home Test Init (HoTI), Care-of Test Init (CoTI), Home Test (HoT) and Care-of Test (CoT).

Before the MN sends a BU to the CN it sends a HoTI message through the HA. A CoTI message is also sent directly to the CN according to IP routing. When receiving these messages the CN responds with the HoT and CoT messages, where HoT is sent through the MN's HA and the CoT message is sent directly to the MN's CoA. The MN derives a binding management key from the information in the HoT and CoT messages. After this, the BU will be sent to the CN. The CN will derive the binding management key from the information in the BU.

The return routability procedure verifies that the MN is reachable both through its HoA and its CoA. To secure the information exchanged in the return routability procedure, IPSec [6] can be used between the MN and its HA for the HoTI and HoT messages. A malicious node has to intercept both HoT and CoT messages to create the binding management key. Return routability is required each time the MN changes its CoA. As long as the same CoA is used the same binding management key is valid.

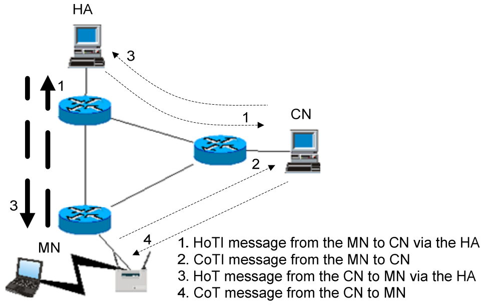
HA
3
1
CN
1
2
3
4
MN
1. HoTI message from the MN to CN via the HA
2. CoTI message from the MN to CN
3. HoT message from the CN to MN via the HA
4. CoT message from the CN to MN

Figure 4 Return routability in Mobile IP.

### *1.3 Research challenges*

The MIP solution is attractive since it enables mobility with the most widely used protocols at the transport layer, the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP). With MIP, protocols above the network layer are unaware of network mobility. However, one problem with MIP is the registration time when moving between networks, especially if there is a long distance between the HA and the foreign networks visited by an MN. MIP will probably be most used with MNs connecting wirelessly and this may cause problems because of rapidly changing conditions in the wireless network. An MN switching between APs connected to different networks will require a new registration each time. The time it takes performing a handover may cause UDP packets to be dropped and TCP flows to break.

To minimize these problems, the work described in this paper makes the following contributions:

- Extends and enhances Mobile IP to enable multihomed MNs to manage movement of individual traffic flows.
- Proposes and describes an extension to Mobile IP that enables users to switch terminal for individual or all ongoing traffic flows.

- Evaluates proposed solutions both through simulations and a real world prototype.

The rest of the paper is organized in the following way. Section 2 describes related work. Section 3 describes the handover selection algorithm and Section 4 Multihomed Mobile IP. Section 5 presents the port-based MIP architecture and Section 6 discusses the user mobility proposal. Sections 7 and 8 present conducted experiments and the results. Section 9 concludes the paper and describes future work.

## 2 Related work

The research activity in the field of IP mobility management is high. Extensions and amendments to the Mobile IP standard are common contributions. Work on bringing handover latencies down and reducing packet losses during handovers has resulted in Fast handovers for Mobile IPv6 (FMIPv6) [3] and Hierarchical Mobile IP (H-MIP) [11].

Support for multihoming and cross-layer designed vertical handovers are currently being investigated by parts of the research community. Methods for horizontal and vertical handovers are discussed in [10,13]. These approaches use multicast to reach multiple nearby APs. MNs instruct APs to forward or buffer data packets for it. If not delivered to the MN, these packets are dropped after some time. Our solution uses multihoming to maintain multiple registrations and by this avoids forwarding between APs.

Soliman et al [11] present a proposal to lower the delay with MIP messages and thereby manage handover at the network layer more efficiently, considering the time for handovers. The proposal uses two care-of addresses; link local care-of address and regional care-of address. In our solution the possibility of maintaining multiple bindings enables a MN to perform soft handovers.

A solution for fast handovers is presented by Koodli et al [3]. It uses signalling between the MN, the old AP and the new AP entered to avoid loosing packets. Packets will be forwarded from the old AP to the new AP in order to avoid packet losses. Our solution avoids forwarding between APs and complicated signalling between access networks possibly owned by different providers.

Hseih et al [5] combine the proposals [11] and [3] and extend it to reduce the handover time even further. The handover time in this work is the same as the handover times for data-link layer handovers.

Wang et al [15] present a user-based policy to determine the currently best available access network in a heterogeneous network. The bandwidth is monitored and announced by APs so the MNs can calculate the utilization of each AP. Other parameters such as capacity and cost also affect the policy decisions. In our solution a new parameter (RNL) is used in the policy model for selection of which access network to use.

Chen et al [2] propose a Smart Decision Model to determine the best available network. The decision model considers factors such as user preferences, system information and properties of available access networks. The model's score function is described in detail.

Bi et al [1] propose an integrated IP-layer handover solution that targets the IP-layer handoff delay. Policies use criterion from user profiles, service requirements and network environment. An adaptive handover control scheme combines probed and monitored (dynamic and static) information. Cross-layer signalling (e.g. L2 triggers) enhances the IP-layer handover.

Soliman et al [12] propose a flow identification option in MIPv6. The identification is based either on IP addresses, protocol and ports or on the IPv6 flow label. The architectural ideas are similar to ours but our proposal also includes evaluation of available access networks and a decision model for network selection and handover timing.

## 3 Handover selection

In order to compare and select access networks in a heterogeneous environment the MN must perform continuous evaluation of the available networks. We use a metric called the Relative Network Load (RNL) to relatively compare the capacity of different access technologies at the network layer.

The evaluation of each network is expressed in formulas (1)–(4) shown below. A detailed explanation of the formulas can be found in [19].

RNL represents a quality value for each network based on Round Trip Time (RTT) and jitter values. $\bar{z}_n$ is the mean value of RTT metrics ($rtt_n$) for MIP registration messages between the MN and its HA. $\bar{x}_n$ is the mean value of times between arrivals of MIP registration messages at the MN, and $V_n$ is the variance between these messages. The variable $h$ determines the size of the history window for the weighted average calculations. For example, when $h$=5 the most recent value will contribute 20 per cent to the calculated $\bar{x}_n$, $\bar{z}_n$ and $V_n$ values.

$$\bar{z}_n = \frac{1}{h} rtt_n + \frac{h-1}{h} \bar{z}_{n-1} \qquad (1)$$

$$\bar{x}_n = \frac{1}{h} \delta_n + \frac{h-1}{h} \bar{x}_{n-1} \qquad (2)$$

$$V_n = \frac{1}{h}(\delta_n - \bar{x}_n)^2 + \frac{h-1}{h} * V_{n-1} \qquad (3)$$

$$RNL_n = \bar{z}_n + V_n \qquad (4)$$

The variables $h$, $\bar{x}_0$, and $V_0$ are initialized with the following values:

$$\frac{1}{h} = \{z : z > 0 \wedge z \leq 1\}$$

$$V_0 = 0$$

$\bar{x}_0 =$ defined advertisement time.

The variable $\delta_n$ is calculated as: $\delta_n = \{t_n - t_{n-1} : n > 0\}$

Where $t_n - t_{n-1}$ is the time difference between consecutive MIP registration messages received at the MN.

The RNL value for each network is stored in the policy repository and for the selection of which access network to use the monetary cost and radio energy consumption values for each interface is included. Cost and energy consumption for each interface is inserted by user configuration.

## 4 Multihomed Mobile IP

New terminals with multiple network interfaces introduce new requirements on mobility management. One such requirement is to enable parallel usage of several access technologies and to perform seamless handover between those.

In the scenario shown in Figure 5, an MN should be able to send traffic flows via different interfaces. In the proposed standard for MIPv6 a MN disconnecting from its home network (using one HoA) can only use one wireless connection (i.e. register one CoA) at a time. In the multihomed extension for MIP, M-MIP [18] multiple CoAs are managed. With M-MIP, CNs can associate the MN's HoA with multiple CoAs. In the case of an MN with two registered CoAs, the HA and CN may use different CoAs to reach the MN. However, M-MIP do not enable a CN or the HA to control the use of multiple CoAs by itself. Using multiple CoAs is beneficial if the total amount of traffic capacity needed extends the capability of one single interface. In that case flows can be sent via different interfaces. The mechanisms to realize multihomed MIP is further described in the next section.

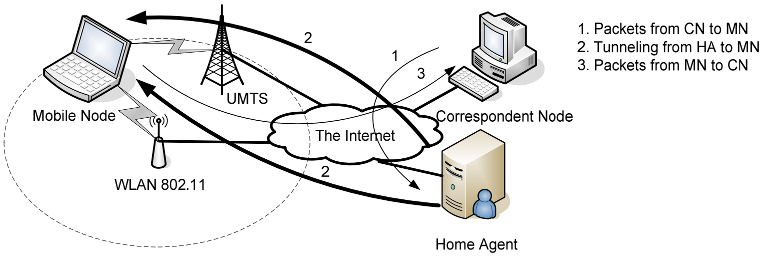

Figure 5 System overview when the MN is connected to both an 802.11b and a UMTS network.

## 5 The Port-based Mobile IP Architecture

In order to manage which interface should be used by individual traffic flows we introduce extensions to the MIP protocol. These extensions are needed for multihoming and identification of individual traffic flows. The extension only affects binding update messages and the management of binding information.

To enable UDP/TCP flow identification we extend the M-MIP proposal to include a flow mobility option header, specifying the protocol and port number when registering a binding. Other examples of flow identification could be the IPv6 flow identifier, or other protocol specific identifiers. By doing this an MN can register a binding that informs the CN or the HA that only a single flow shall be forwarded to the specific CoA. To control multiple flows the MN can include several flow mobility option headers in the BU. Beyond enabling flow mobility at the network layer the extension also enables flow mobility between devices (described in Section 6).

The modifications consist of two flags added in the BU message and a new option header hosting the protocol number and the port number. Figure 6 illustrates the modified BU header.

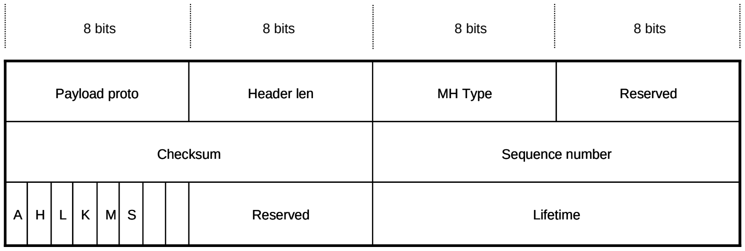

Figure 6 Binding update header with M and S flag.

The flag named the M-flag indicates a multihomed binding. This means that with the M-flag, currently registered bindings will be kept and without the M-flag they will be deleted. The S-flag is used by the MN to inform the HA and CNs of which CoA to use as default. Figure 7 illustrates the flow mobility option header.

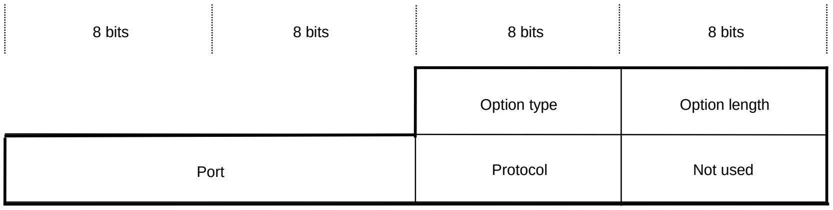

Figure 7 Flow mobility option header.

The port field identifies the destination port at the MN. The protocol field represents the transport protocol number. In Figure 8, bindings are shown for both an IP address as well as for a protocol and a port.

| **HoA** | **CoA** | **Protocol** | **Port** | **Lifetime** | **Flags** |
|---|---|---|---|---|---|
| 3ffe::a:b:c:d | 3ffc::1:5:a:b:c:d | -1 | -1 | 150 | A/H/L/K/M/S |
| 3ffe::a:b:c:d | 3ffc::1:6:a:b:c:a | 6 | 6935 | 200 | A/H/L/K/M |
| 3ffe::a:b:c:d | 3ffc::1:a:a:b:c:d | 17 | 7830 | 150 | A/H/L/K/M |

Figure 8 Binding cache.

The proposed solution requires the network layer to look for port numbers in the transport header. This is however nothing unique and is for example used to enable fast forwarding and to filter packets in access control lists.

When an MN discovers a foreign network, it acquires an IP address and registers the CoA with it's HA. If this is the first registration a BU is sent without the M or S flag. A BU without the M-flag means that previously added registrations are deleted and that this binding is the one selected (without using the s-flag).

If a second foreign network is discovered, another registration is sent to the HA. In this registration the MN adds the M-flag in the BU. When registering a new interface it should not be selected until an evaluation of the interface is conducted, assuming a previously added interface is operational. If the new interface performs better than the interface previously used, a new binding update is sent for the new CoA with the M- and S-flag.

Without the option header adding protocol and port to the BU, all traffic (from the same or other CNs) is sent to the same CoA. By adding such an option, a single flow can be redirected to another interface (CoA). If e.g. the WiMAX interface is used and traffic from CNs via the HA congests the WiMAX connection, one or more flows should then be moved to an alternative interface, e.g. WLAN. Such a scenario could be an e-meeting [8], where voice communication requiring rather strict jitter and delay values should be given high priority and kept at the WiMAX interface, while video showing presence of participants can be given lower priority and be moved to an WLAN interface. In this case a BU is sent to the HA with the option header informing the HA of what protocol number and destination port number to be redirected to another CoA.

For route optimization a BU is sent to the CN. This BU can be valid for all traffic sent from the CN or just for a specific flow. This means that some traffic may go via the HA and some traffic can be sent directly.

In the case of all traffic being redirected, a BU is sent to the CN without the S- and M-flags and without the flow mobility option. In this case all traffic is sent from the CN to the registered CoA. To direct a flow from a CN to another CoA a BU is needed using the M- and S-flags as well as the flow mobility option.

For each new CoA, return routability is invoked. No changes in messages are needed except for the added option and the two extra flags in the BU. Return routability is only needed when adding a new CoA. In the case of handover for specific flows (by adding the flow mobility option to the BU) to an already registered CoA, no new return routability needs to be invoked.

## 6 User mobility scenario

This section describes the user mobility proposal. In order to fully take advantage of flow mobility the user should be able to move an ongoing traffic flow from one terminal to another. A typical scenario would be moving a VoIP call from the desktop to a mobile device when leaving the office.

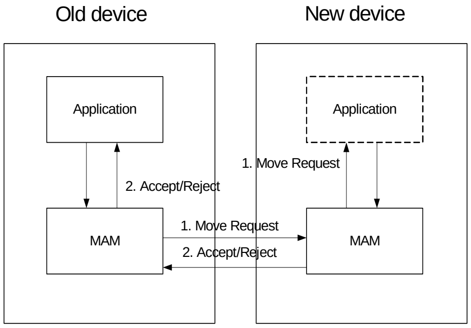

Figure 9 Flow mobility between devices.

We define user mobility as moving a traffic flow between devices using Mobile IP. The request to move can be issued at the source device (from where the flow will be moved) or at the destination device (to where the flow will be moved). The request to move a flow is given from the application (by user interaction) and sent to a Mobility Application Manager (MAM) process within the device. The MAM must discover the location of the peer device and send a request to the peer MAM (see Figure 9). The MAM at the peer device forward a request to the application to see if it is willing to accept the flow. If accepted, the application replies with an accept message that will be forwarded to the requesting application. After the source MAM sent the accept notification to the application, the MAM will update the HA and CNs with information about the destination host. A binding update is sent to update the binding lists with the flows new CoA.

A user moving flows between different devices must maintain a device list that binds between logical device names and numerical identifications. This device list must be replicated on all devices. When a biding update is sent to the HA or CN it contains the integer id of the device.

Mobility between devices requires extra system support. While the trigger for flow mobility between interfaces is based on predefined policies and measurements of dynamic metrics (RNL), the mobility between devices requires instant user action interaction. A Mobility Application Manager (MAM) manages flow mobility requests from applications wanting to move from one device to another. The request may look like, move from “myLaptop” to “myPDA”.

The MAM in the device requesting a move is responsible for finding the peer device and to start the negotiation to move a flow from the application at “myLaptop” to the application at “myPDA”. If the application is serializable (as in Java) the application itself with all variables and their states can of course also be moved. This paper however assumes that an application is running and is ready to accept a flow.

If the application at the new device accepts to receive the flow, the MAM at the new device will update the HA (by sending a BU) and possibly the CN if route optimization is used.

Upon receiving the request from the application in the source device, the MAM have to locate the current location (CoA) of the destination device before starting the negotiation. To be able to ask for the CoA of a specific device, a mapping from a user defined name to the actual device is needed. This is enabled by naming each device with a name (e.g. “myLaptop”, “myPDA”) and giving each device an identification number (e.g. 1,2,…,n). The mapping between the name and ID must be maintained in all devices where flow mobility between devices is required. The BU will contain a field that hosts the id of the node sending the message. Xxx

## 7 Simulations

This section evaluates the usefulness and efficiency of the multihomed flow based selection strategy compared to sending all flows through a “default gateway”. In the simulation we study the use of a parallel link with lower capacity to simulate a heterogeneous environment. For a detailed study of M-MIP and RNL we refer to [19]. Our simulation study uses the GloMoSim simulation model version 2.4 [14]. The simulation uses 802.11 radios with the default RADIO-TX-POWER (15dBm) which gives a transmission range of 376.8 meters. The MN is equipped with two wireless interfaces, one is configured at 2Mbps on channel 1 (2.412 GHz) and the other at 11Mbps on channel 6 (2.437 GHz).

Our simulation study has selected the packet-size 512 bytes. Packets about this size are used for example for Voice over IP (VoIP). The advertisements used in the simulations have a size of 32 bytes.

Figure 10 shows the simulation topology. There are two routes the MN could use to communicate with an Internet CN. One route is via GW1 at 11Mbps and the other via GW2 at 2 Mbps. When "default gateway" selection is used, the 11Mbps link was selected.

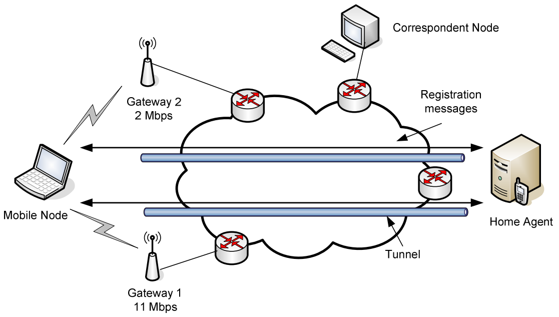

Figure 10 Simulation topology.

Traffic is sent between an Internet located CN and the MN. A new traffic flow is started every 10 seconds until there are seven parallel flows. All flows end after 200 seconds. Every traffic flow has the same characteristics, i.e. CBR traffic with 50, 71, 100, 125 or 200 packets per second (200, 285, 400, 500, 800 kbps).

### *7.1 Simulation Results*

The simulation study results are presented in figures 11, 12 and 13. The graphs represent the mean value of multiple simulations with different seeds. The solid line represents flow based gateway selection and the dashed line "default gateway" selection (i.e. all flows are sent via the same GW). Figure 11 show the aggregated throughput for all flows in each scenario and the CN increases the traffic for each scenario.

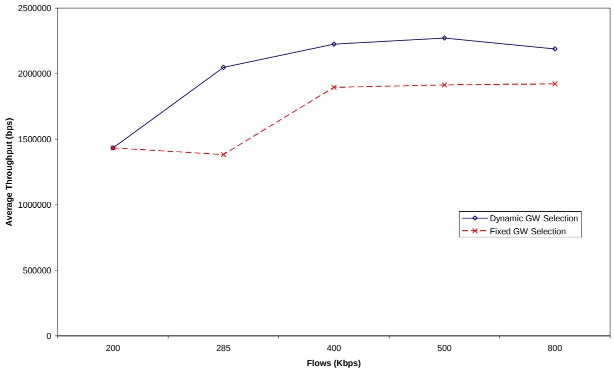

Figure 11 Average throughput for different traffic characteristics.

As expected the average aggregated throughput is higher when the MN is able to direct some of the flows via the second GW. This traffic does not have to compete with the other flows since it uses a different frequency. As shown in Figure 12 the delivery ratio is also higher when multiple gateways are used.

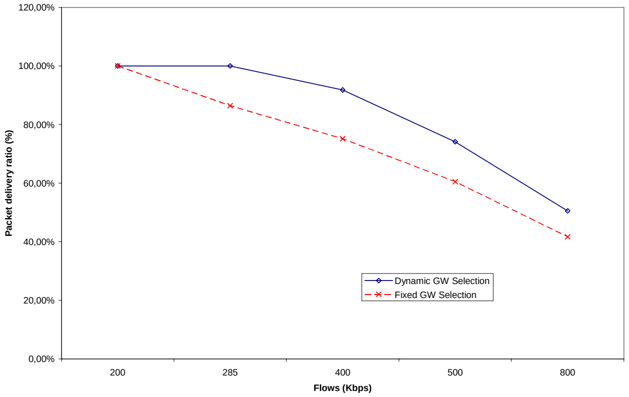

Figure 12 Average delivery ratio for different traffic characteristics.

Figure 13 show the average packet delay between the CN and the MN for each scenario. The delay increase for the highest traffic scenario with dynamic GW selection relates to the limited capacity of the 2Mbps link and the big step in adding another flow (800 kbps).

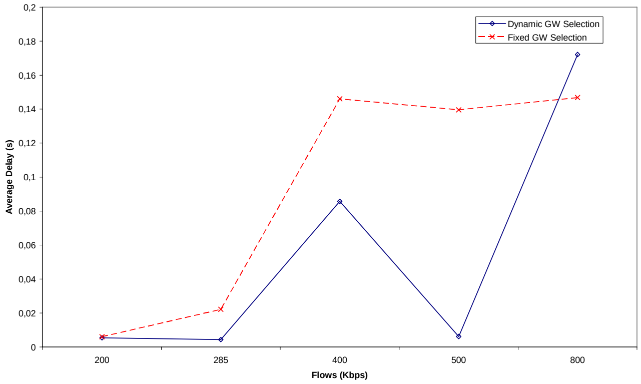

Figure 13 Average delay for different traffic characteristics.

## 8 The software prototype architecture

The prototype developed is composed of a HA running on Linux distribution Fedora core 5 [4], with kernel 2.6.15. The HA software is developed using ANSI C and PCAP [7] for packet capture. The binding cache holds home address and active care of address for each connected MN. The HA is multi-threaded with one socket listening for incoming traffic and one socket used for outgoing traffic. One common socket handles BU messages.

The MN software is running on Windows XP using WinpkFilter 3.0 [16] for packet filtering. In this prototype all traffic is sent via the HA in a bidirectional tunnel, i.e. route optimization is not used and the MN use a Co-located CoA. BU messages are sent prior to tunnel setup and transmitted out of band, i.e. sent directly to the HA outside the tunnel. The BU message contains CoA, HoA, life time, sequence number, check sum, and flags.

The tunneling mechanism is implemented using a virtual network interface on the MN. The tunneling mechanism use UDP datagrams in order to support NAT and firewall traversal at the cost of an UDP header overhead. Policy values are used to decide what physical interface to send traffic through. The selection of what interface to use is based on the policy value calculated using RNL (Relative Network Load) [19], energy consumption, and monetary cost. The user is able to set weights on those parameters.

The architecture allows MNs behind firewalls and NAT boxes to reach the HA. The solution basically provides connectivity to the home network via the virtual interface using datalink layer communication. The virtual interface is configured with home network parameters (IP address being the HoA, network mask, and default gateway). It appears to the user as being directly connected to the home network. The HA address and port number are configured in the prototype’s GUI.

The fact that no additional dependencies like IP forwarding, IP tables, and TUN/TAP drivers are used makes the prototype feasible to run on a variety of platforms. The virtual adapter is a standard loopback adapter. Besides the HA address no manual configuration is needed in the MN. Home network settings can be fetched via the DHCP protocol.

By using Internet Connection Sharing on the MN’s virtual adapter mobile routing is also provided. This way multiple users may use the MN’s global connectivity enabling e.g. flight connection services.

### *8.1 MN software architecture*

The Policy Engine calculates and updates policy values continuously for all active interfaces. Information on what is the best interface is sent to the MIP Driver. The MIP Driver then enforces the best interface to be used.

The routing functionality handles the routing table, i.e. adding and deleting entries in the Windows routing table. When a new route is added it is assigned a lower routing metric than automatically generated routes. This way a new route is preferred over existing ones. The MIP Driver is set as default gateway. A full match mask (255.255.255.255 for IPv4) is used in order to make sure the tunnelled traffic destined to the HA is sent through the selected interface.

The tunnel functionality captures frames on the virtual interface (i.e. the default gateway interface) and encapsulates them in UDP datagrams.

The interface functionality is a software entity, representing the physical interface selected in a graphical user interface. Each physical interface runs a thread that handles BU messages sent out of band (i.e. not tunneled). The BU message mechanism is also used to measure network performance.

The policy repository holds user preferences on weights for policy calculation parameters.

The graphical user interface allows the user to select what interfaces to be included in the mobility management handling. It is therefore possible to let the user exclude interfaces.

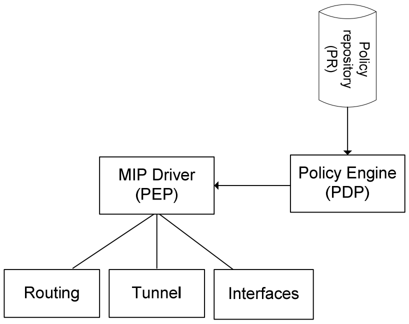

Figure 14 MN software architecture.

### *8.2 HA software architecture*

The HA is a combined tunnelling end point, a router, and a simple server. It holds a binding cache with entries for each connected MN.

When a BU message is received the HA checks if the MN is already in the cache and if not, it is added. The BU message is mirrored back as a BA message. If the received BU is incorrect it is discarded.

Outgoing traffic (i.e. traffic from MNs to CNs) is decapsulated at the tunnel end-point and sent out on the home link using raw socket. This way IP routing in the HA is not necessary.

Incoming traffic (i.e. traffic from CNs to MNs) is captured in the HA using proxy Address Resolution Protocol (ARP) functionality. This is handled by making a published static ARP entry in the Linux kernel. The HA responds to ARP requests on the home link on behalf of the MN. The captured frame is inspected to determine the destination MN, encapsulated and sent to the MN through the tunnel.

### *8.3 Real world evaluation*

To evaluate the prototype, three access network technologies were used; WLAN (802.11b), WiMAX (802.16-2004) and UMTS. The topology is shown in Figure 15. To simulate a Skype video call of 20 kbps (UDP) we used the Iperf traffic generator.

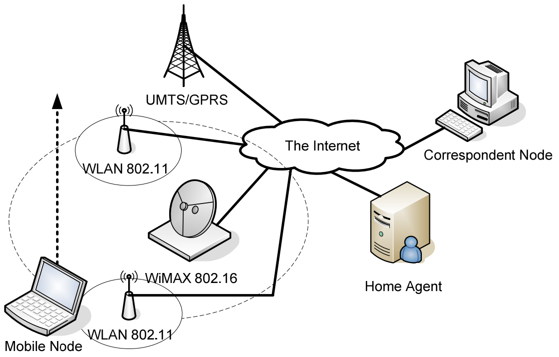

Figure 15 Evaluation topology.

Traffic from the CN is sent to the MN's home network, where the HA intercepts packets destined for the MN and tunnels them to the selected CoA. For each registered CoA a tunnel is installed. Experiments conducted used h = 5 (in formulas 1-3). The cost- and energy consumption parameters where set to be equal on all interfaces in order to evaluate a policy based only on RNL. The registration messages were sent with a one second interval on all interfaces. The interval relates to how fast the MN reacts to variations in RTT and jitter and an even shorter interval improves reactivity (at the cost of higher overhead). A shorter interval would be motivated especially for highly fluctuating networks with high throughput (e.g. 802.11). The movement pattern during the experiment is as follows: the MN starts at a place nearby an 802.11 AP and moves with a constant velocity of approximately 1 m/s towards another 802.11 AP. Between these two APs there is bad WLAN coverage. Beyond the second 802.11 AP, both 802.11 and 802.16 have bad coverage. The 802.16 cell cover the area of both 802.11 cells and the UMTS network cover both the 802.11 and 802.16 cells. After some time using the UMTS access the MN turns and starts to approach the (second) 802.11 AP again. Results are presented in Figure 16.

Each vertical line illustrates the time when a handover was performed. The blue curve illustrates the policy value for the 802.11 access, the red curve illustrates policy value for the UMTS access and the yellow curve plots the policy value for the 802.16 access. The access network having the lowest policy value is selected.

The upper (dashed) black plot shows the bandwidth (kbps) received at the MN and the lower (dotted) black plot shows the jitter (in ms) of the received traffic. The CN send constant bit-rate traffic (UDP) of 20 kbps. The 802.11 APs have a capacity of 11Mbps (5.5 Mbps in practice) and the 802.16 AP was set to 2.22 Mbps (BPSK ½ modulation). The UMTS network performed about 300 kbps downlink (depending on other ongoing traffic).

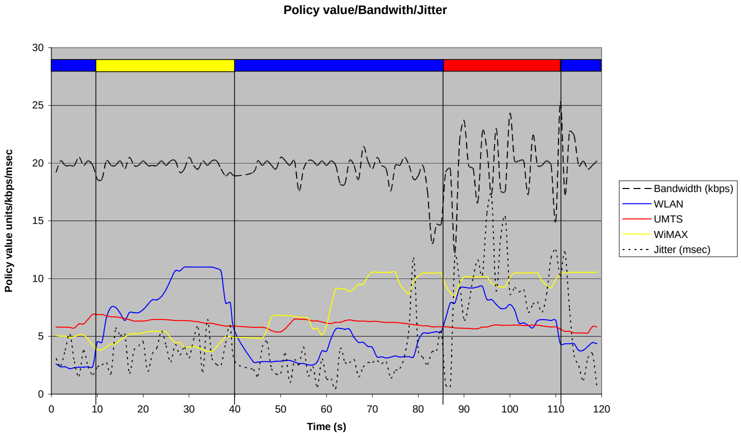

Figure 16 Calculated policy values, bandwidth and jitter for each access network at the MN.

The evaluation started indoors and the first 802.11 AP was selected the first 9 seconds. At that time the MN's distance to the 802.11 AP render in an increasing policy metric due to increased RTT and jitter metrics of MIP registration messages. At this time the 802.16 policy metric is the lowest and therefore is selected. The handover renders in a small increase in jitter metrics but the bandwidth is kept stable with small fluctuations. The short dip in bandwidth at 10 seconds from start indicates that the handover decision is taken at the right time.

After 40 seconds from start the connection to the second 802.11 AP is considered better than the 802.16 access regarding RTT and jitter metrics. This is illustrated by the jitter plot showing lower jitter metrics for the received traffic, after handover from the 802.16 access network to the 802.11 access network. The bandwidth is shown to be stable during this handover as well. However, a small increase in fluctuation of measured bandwidth is experienced.

After 83 seconds from start, the MN leaves the indoor environment (where the 802.11 and 802.16 access networks are installed) and enters an outdoor environment. Handover to the UMTS access network takes place after 86 seconds from start due to both the 802.11 and 802.16 radio signals being faded by the wall of the left building. Since today's UMTS networks prioritize circuit switched traffic before packet switched (IP) traffic, the jitter increases as well as the fluctuations of both the bandwidth and the jitter metrics. The trend of the bandwidth and jitter plots shows that the handover decision is taken at the right moment, since this trend is kept while using the UMTS network. When returning back into the building (after 111 seconds from start) handover takes place to the 802.11 access network, rapidly increasing both the bandwidth and jitter metrics.

## 9 Conclusion

In this paper, we described how Mobile IP can be extended to handle port-based multihoming. By such extension different flows can be destined through different interfaces on the MN leveraging differences in coverage, Quality of Service, cost, bandwidth, delay, et cetera among different wireless and fixed access networks. Our results presented in this paper show that load and capacity can be measured on the different interfaces. The results from the measurements can be used to perform load balancing between different interfaces, both between the MN and multiple CNs and multiple flows between MN and a single CN. In a near future, we intend to investigate load balancing between multiple flows and a single CN further.

We intend to develop our ideas even further by exploring and introducing different sorts of cross-layer signalling, extending and integrating the policy-based decision model, and implementing pilots where new innovative services like mobile IP telephony and pervasive games are evaluated. Hand-over between different mobile access network technologies will be studied in detail. Particularly, components from the 3GPP IMS (IP Multimedia Subsystem) will be considered.

## Acknowledgements

The work presented in this article is based on results from the HybriNet@Skellefteå project (http://www.hybrinet.org) supported by Skellefteå Kraft. The prototype is developed in collaboration with TietoEnator, Telecom & Media R&D Services.

## References

1. Bi, Y., et al., "An integrated IP-layer handover solution for next generation IP-based wireless network", Proc. of 60th IEEE Vehicular Technology Conference, 2004.
2. Chen, L.-J., et al., "A smart decision model for vertical handoff", Proc. of 4th ANWIRE International Workshop on Wireless Internet and Reconfigurability, 2004.

3. Koodli, R. (ed.), “Fast Handovers for Mobile IPv6,” RFC 4068, 2005.
4. Fedora Core, http://fedora.redhat.com/
5. Hseih, R., Zhou, Z.-G., and Seneviratne, A., "S-MIP: A Seamless Handoff Architecture for Mobile IP," IEEE INFOCOM 2003 - Conference on Computer Communications, pp. 1774-1784, 2003.
6. Kent, S., Atkinson, R., “Security Architecture for the Internet”, RFC 2401, 1998
7. libpcap, http://www.tcpdump.org/
8. Marratech, http://www.marratech.com/
9. Murray, K., Mathur, R., and Pesch, D., “Intelligent access and mobility management in heterogeneous wireless networks using policy”, ACM 1st Intl Workshop on Information and Communication technologies, pp. 181-186, 2003.
10. Seshan, S., Balakrishnan, H., and Katz, R., “Handoffs in Cellular Wireless Networks: Daedalus implementation and Experience”, Wireless Personal Computing, vol.4, pp.141-162, 1997.
11. Soliman, H., Castelluccia, C., El Malki, K., Bellier, L., “Hierarchical Mobile IPv6 Mobility Management (HMIPv6)”, RFC 4140, 2005.
12. Soliman, H., Montavont, N., Fikouras, N., Kuladinithi, K., Flow bindings in Mobile IPv6, Internet Draft, 2006
13. Stemm, M., Katz, R. H., Vertical Handoffs in Wireless Overlay Networks Mobile Networks and Applications, vol. 3, no. 4, pp. 335-350, 1998.
14. UCLA Parallel Computing Laboratory. Glomosim, http://pcl.cs.ucla.edu/projects/glomosim/.
15. Wang, H. J., Katz, R. H., and Giese, J., “Policy-enabled Handoffs Across Heterogeneous Wireless Networks”, Proc. of Second IEEE Workshop on Mobile Computer Systems & Applications, pp. 51-60, 1999.
16. Windows Packet Filter, http://www.ntkernel.com/w&p.php?id=7
17. Yavatkar, R., Pendarakis, D., and Guerin, R., “A Framework for Policy-based Admission Control”, RFC 2753, 2000.
18. Åhlund, C., Brännström, R., and Zaslavsky, A., “M-MIP: Extended Mobile IP to Maintain Multiple Connections to Overlapping Wireless Access Networks”, International Conference on Networking, 2005, Reunion Island. Lecture Notes in Computer Science (LNCS), Springer-Verlag.
19. Åhlund, C., Brännström, R., and Zaslavsky, A., “Traffic load Metrics for Multihomed Mobile IP and Global Connectivity”, Telecommunication Systems Journal, Springer-Verlag, 2006.