# On the Performance of Mobile IP in Wireless LAN Environments

Rastin Pries, Andreas Mäder, Dirk Staehle, and Matthias Wiesen

University of Würzburg, Institute of Computer Science, Germany
{pries, maeder, staehle, wiesen}@informatik.uni-wuerzburg.de

**Abstract.** Wireless Local Area Networks (WLANs) based on the IEEE 802.11 standard have become more and more popular in the last few years. In such networks, a handover has to be performed when moving from one cell to another. When considering small-scale scenarios like an office building, these handovers can be performed on the ISO/OSI layer two solely. However, the size of one subnet is rather restricted. Therefore, the handover has to be lifted to the network layer as well. The performance of this network layer handover will be shown in this paper.

## 1 Introduction and Related Work

With the increasing number of wireless LAN deployments at universities and companies, one IP subnet is often not sufficient. Therefore, we have to perform the handover on the network layer. Some standards like Cellular IP [1], HAWAII [2], and Mobile IP [3] try to perform the handover on layer three and above. In this paper, we focus on the performance of Mobile IP. IP mobility has been the topic of many researchers for several years. The basic approach by Perkins dates back to the year 1996 [3]. Meanwhile, another two standards [4,5] emerged from this basic approach. All three together are referred to as Mobile IP and they constitute the most promising solution in order to support mobility within the internet protocol. A good overview of Mobile IPv4, Mobile IPv6, and further extensions are given in [6,7].

A large variety of papers have been published which have analyzed the basic Mobile IPv4 handover. Their results show a handover latency of at least 6 seconds which is too high for any type of traffic. In this paper, we want to simulate which parameters cause these long handover delays and will show how to optimize these settings. Furthermore, we do not only look at Mobile IPv4 but also simulate Mobile IPv6 and Fast Mobile IPv6. In the context of Fast Mobile IPv6, we just like to point out two promising approaches. The first one [8] proposes a new mechanism called ARIP (Access Router Information Protocol) to speedup the Fast Mobile IPv6 handover. In their experimental setup, the handover latency of the Fast Mobile IPv6 with ARIP was bounded below 250 ms. With this handover delay it should be possible to support real-time traffic when the mobile user is changing its point of attachment rarely. The second approach, proposed by Sharma et al. [9] introduces a new low latency Mobile IP handover mechanism which they have implemented. They show that they can reduce the handover latency to less than 100 ms which is completely sufficient for real-time traffic. In this study we

J. García-Vidal and L. Cerdà-Alabern (Eds.): Wireless and Mobility, LNCS 4396, pp. 155–170, 2007.

will show how the actual IP connectivity loss and the overall handover delay can be reduced to less than 100 ms with an optimal setting of the layer 2 and layer 3 handover parameters without introducing a new handover mechanism.

The rest of the paper is organized as follows. Section 2 briefly explains the main concept of Mobile IP including Mobile IPv4, Mobile IPv6, and Fast Mobile IPv6. This is followed by Section 3 which describes the simulation model, the used traffic models, and the parameter settings. Section 4 presents our simulation results and finally, Section 5 concludes the paper.

## 2 Mobility Within the Internet Protocol

The primary goal of Mobile IP's design is to make the network-layer handover transparent to above layers. In order to assure the session continuity, the IP address of a mobile node has to remain the same after a network layer handover. When using Mobile IP, this IP address is called the mobile nodes home address and the subnet this address belongs to is called the home network. A router in this home network is called the *Home Agent* (HA). The network where the *Mobile Node* (MN) is moving to is called the foreign network and the router the *Foreign Agent* (FA).

### 2.1 Mobile IPv4

*"IP Mobility for IPv4"* [4] defines a way to always identify a node by its home IP address regardless of its current location. As soon as a mobile node leaves its home network and enters a foreign network, it is not able to receive packets addressed to its home agent anymore. Therefore, Mobile IPv4 describes a mechanism of forwarding data from a MN's home network to its current foreign network. This forwarding mechanism makes use of an IP-in-IP tunnel. The outer datagram of the IP tunnel carries the inner one from the tunnel start point to the tunnel end point. The MN's home address is used as the IP address of the tunnel start point, but the MN still lacks of a temporary foreign network IP address denoting the tunnel end point. This address is called the MN's care-of-address. Mobile IP distinguishes between two care-of-addresses, one is called co-located care-of-address and the other foreign agent care-of-address. When using the co-located care-of-address, the IP tunnel ends at the mobile node and for the foreign agent care-of-address, the foreign agent is the end point of the tunnel. Fig. 1 shows the tunnel after the network layer handover with the end point at the mobile node and Fig. 2 for the tunnel up to the FA.

From the figures you can see the triangular traffic shape. From the mobile node to the *Correspondent Node* (CN), from the CN to the MN's home agent, and from the home agent back to the MN. When a MN enters a FN and obtains a new care-of-address, it has to inform the HA about the new address in order to enable the HA to establish a tunnel to the MN's new location.

The Mobile IPv4 handover starts when the MN recognizes that it has lost the connection to his previous point of attachment. Therefore, Mobile IPv4 introduces *Agent Advertisements* (AAs). These AAs inform about the existence of the HA or a FA and the services it offers. The AAs are broadcasted by the HA and the FAs in periodical

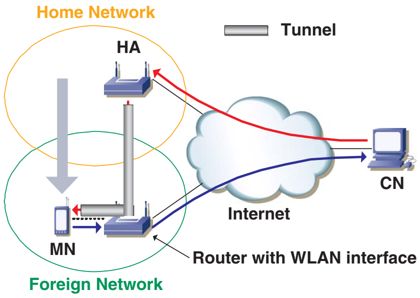

**Fig. 1.** Co-located care-of-address scenario after the handover

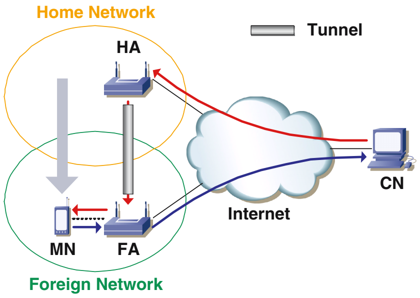

**Fig. 2.** Foreign agent care-of-address scenario after the handover

intervals. When a MN does not receive any AAs from its agent anymore for a period of time called agent advertisement lifetime, it considers that the connection is lost. The lifetime of an AA is supposed to be as long as at least three times the interval between the transmission of two consecutive agent advertisements. For example, when the HA sends an AA every four seconds, the lifetime field of the AA should be set to at least twelve seconds. Thus, the MN recognizes that a link layer handover has taken place when three consecutive AAs are lost and the MN receives AAs from another mobility agent instead. After analyzing the AAs from the new mobility agent, the MN registers with the agent and the tunnel between the home agent and the new foreign agent or to the MN, depending on the care-of-address, is created. Now, the MN is able to continue with the session. A complete description of the Mobile IPv4 handover procedure can be found in [10].

### 2.2 Mobile IPv6

Mobility Support in IPv6 [5] is the adaptation of *”IP Mobility Support for IPv4”* [4] to an internet using IP version 6. The design of Mobile IPv6 is very similar to Mobile IPv4 and both standards share the functionality of basic entities like a mobile node, its home agent, and correspondent nodes.

### 2.3 Bidirectional Tunneling and Route Optimization

In Mobile IPv6, there are two possible modes for communication between a MN and its CNs, namely bidirectional tunneling and route optimization.

The first mode, bidirectional tunneling, does not require Mobile IPv6 support from the CN and is available even if the MN has not registered its current binding with the CN. Packets from the CN are routed to the home agent and then tunneled to the MN. Packets to the CN are tunneled from the MN to the home agent and then routed normally from the MNs home network to the CN. The latter procedure of tunneling packets back to the MNs home address is called reverse tunneling. In this mode, the home address uses proxy neighbor discovery to intercept any IPv6 packets addressed to the MNs home address on the home network. Each intercepted packet is tunneled to the MNs care-of-address. This tunneling is performed using IPv6-in-IPv6 encapsulation [11]. Fig. 3 depicts bidirectional tunneling, which is used when route optimization is not available or intentionally turned off.

The second mode, route optimization, allows to use the shortest communications path between CN and MN by routing packets directly to the MNs care-of-address. This eliminates congestion at the MNs home agent and home network. In addition, the impact of any possible failure of the home agent or networks on the path to or from it is reduced.

In order to do so, route optimization requires the MN to register its current mobility binding at the CN. This means that the MN sends a binding update to every CN, telling it about its current care-of-address. The CNs are then able to create a mobility binding between the MNs home address and the MNs care-of-address in their mobility binding cache. When sending a packet to any IPv6 destination, a CN checks its cached mobility bindings for an entry for the packet's destination IP address. If a cached mobility binding is found, the CN will use a new IPv6 extension header [12] to route the packet to the MN by using the care-of-address indicated in this mobility binding. The main purpose of the extension header is to carry the MNs home address and replace the packet's destination IP address with the home address, once the packet has arrived at the MN. Vice versa, the MN adds a new IPv6 destination option [12] to every packet it sends to a CN. This new option is called the home address option and it is used to inform the CN of the MNs home address. The inclusion of the MNs home address in these packets allows a transparent use of the care-of-address above the network layer.

Fig. 4 depicts the simplification that can be achieved by deploying the route optimization procedure. Please note that the MN has not changed its home address and it still uses the home address of its home network. Furthermore, the arrows symbolize a traffic flow whose IPv6 packets are extended with the extension header. Just as well, the IPv6 packets from the MN to the CN are extended with the home address option.

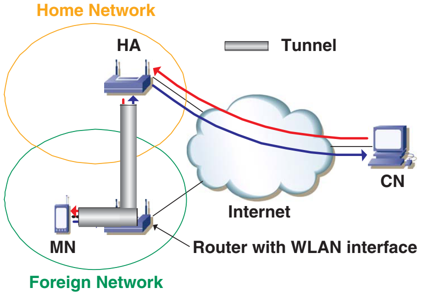

**Fig. 3.** Bidirectional tunneling in Mobile IPv6

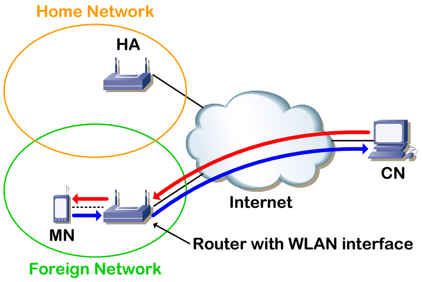

**Fig. 4.** Mobile IPv6 scenario after network layer handover and route optimization

Route optimization as described so far, has one major weakness. Any node knowing the MNs home address can transmit a binding update to the MNs CN and claim its own source IP address to be the new care-of-address. As a result, the CN stops sending the MNs traffic to the MN and starts delivering it to the malicious node instead. Thus, to assure that only valid MNs are sending binding update messages, route optimization in Mobile IPv6 uses a mechanism called the return routability procedure. It strongly reduces the amount of locations from where potential attackers can transmit malicious binding updates to a CN. A detailed explanation of the return routability procedure is given in [13].

The bidirectional tunneling and route optimization can also be applied for Mobile IPv4. However, there are also some differences between Mobile IPv4 and Mobile IPv6. The agent advertisements from Mobile IPv4 are replaced by router advertisements which can be transmitted with a shorter period. Furthermore, the lifetime of these advertisements is not fixed but can be varied using the so called *Mobility Detection Factor* (MDF). After a MN has detected that it has moved from its home network to a foreign network or from one foreign network to another, the MN generates a care-of-address. Before assigning this new care-of-address to the interface, the MN has to check if the chosen address is not already in use. This is done using a duplicate address detection scheme. To check for duplicates of an IP address, a node sets the neighbor solicitation's target IP address to the address being checked. The source IP address is set to the unspecified address [14] and the destination IP address is set to the solicited-node multicast address of the target IP address. If a node receives a neighbor solicitation message whose target IP address matches the nodes own IP address and whose source address is set to the unspecified address, it will answer by sending a neighbor advertisement. With this method, the MN recognizes that the IP address is already assigned. If there are no duplicates of the target IP address assigned in the local network, the MN performing the duplicate address detection will not receive any responding neighbor advertisements. Thus, it waits for a certain amount of time for responding neighbor advertisements to arrive. However, neighbor discovery for IPv6 recommends a default value of 1000 ms before assuming that the target IP address is unique. Thus, the overall handover is delayed by one second.

### 2.4 Fast Handovers for Mobile IPv6

Fast handovers for Mobile IPv6 [15] is an optional standard proposed by the IETF to speed up handover times on the network layer when deploying Mobile IPv6. The main goal of Fast Mobile IPv6 is to improve the standard Mobile IPv6 protocol in a way that enables a MN to send IP packets as soon as it detects a new IP subnet and to receive packets as soon as the new access router has detected the MNs attachment. Therefore, Fast Mobile IPv6 defines new IPv6 and neighbor discovery messages, necessary for its operation. However, the protocol is designed to interwork with Mobile IPv6. Once attached to its new access router, the MN engages in Mobile IPv6 operations including the return routability procedure. Furthermore, Fast Mobile IPv6 works without depending on specific link-layer features but it recommends to make use of inter-layer communication between the link layer and the network layer as often as possible. Inter-layer communication is realized via function calls in the MNs link- and network-layer.

They offer a means of event notification between the two layers and are referred to as triggers. In the following paragraphs, we will explain the Fast Mobile IPv6 handover procedure.

Fig. 5 depicts a standard Fast Mobile IPv6 scenario. Since the access routers in both, the MNs old and its new IP subnet, do not necessarily have to be home agents, Fast Mobile IPv6 assigns the new denotions *Previous Access Router* (PAR) and *Next Access Router* (NAR). Accordingly, the IP subnet the MN is leaving is called the previous network and the one it is moving to is called the next network. At the previous network, the MN uses the previous care-of-address, at the next network the next care-of-address.

The main design idea of Fast Mobile IPv6 is to handle as much handover-related IP communication before the actual link layer handover occurs. In order to do so, the MN somehow has to learn, that a link layer handover is forthcoming. The protocol states that this notification may be achieved by conventional router discovery. However the use of a trigger is a more effective solution. A complete description about the exchange between the link layer and the network layer using triggers can be found in [15].

There are two approaches how the Fast Mobile IPv6 handover can be performed, a predictive mode and a reactive mode. In this paper, we focus on the predictive mode which is shown in Fig. 6. The handover starts with the MN asking the PAR about the next network. This is done via the exchange of a router solicitation for proxy advertisement and its response, the proxy router advertisement. Fast Mobile IPv6 does not specify how the PAR obtains the information for according proxy router advertisements. However, the MNs link layer discovered a neighboring AP, by some means. Since every AP provides some kind of identifier, the trigger sends this AP-ID to the network layer, which in turn provides the AP-ID in its router solicitation for proxy advertisement request. If the PAR has subnet-specific information of the discovered AP, it returns an [AP-ID, NAR-Info] tuple back to the MN. The information about the NAR consists of its link layer address, its IP address and the prefixes of the next network. Thus, the MN already possesses all information equivalent to the data stored in a router advertisement of the next access router, while still connected to the previous network.

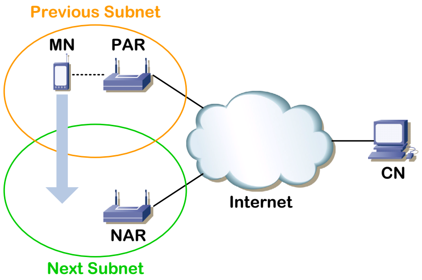

**Fig. 5.** Reference scenario for Fast Mobile IPv6

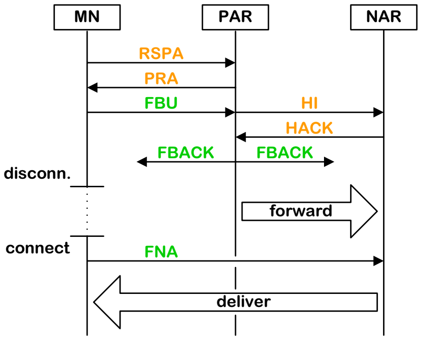

**Fig. 6.** Predictive Fast Mobile IPv6

With the information provided in the proxy router advertisement message, the MN is able to form a prospective next care-of-address, which is sent inside the fast binding update to the previous access router. The sending of the fast binding update may be triggered and its response from the PAR is called a fast binding acknowledgment. However, the main purpose of the fast binding update is to enable the PAR to create a mobility binding between the MNs previous care-of-address and its next care-of-address. Thus, from this time on, the PAR is able to tunnel the MNs packets to the next network. However, before establishing this tunnel, the PAR exchanges a handover initiate message and its according response, the handover acknowledgment with the NAR. The PAR may resolve the NAR's IP address by performing the longest prefix match of the next care-of-address with the prefix list of neighboring access routers. However, the purpose of the handover initiate is to agree upon the prospective next care-of-address with the NAR. If the NAR accepts the prospective next care-of-address, it creates an according proxy neighbor cache entry and starts buffering incoming packets addressed to the next care-of-address. Now, the MN is ready to perform the link layer handover. After the handover, it is recommended that the MN immediately sends a so-called fast neighbor advertisement to the NAR. This is necessary in order to inform the NAR about the MNs successful attachment to the next network. The NAR then turns the MNs proxy cache entry into a standard cache entry and begins to transmit packets forwarded from the PAR and own buffered packets to the MN.

## 3 Simulation Setup

In order to simulate the Mobile IP handover performance, we have used the OPNET Modeler [16]. The tool already offers the basic Mobile IPv4 and Mobile IPv6 models. Due to the fact that we want to see if it is possible to support QoS even during a network layer handover, first of all we need a fast and reliable handover mechanism on the wireless LAN MAC layer. The performance of the layer 2 handover is studied in [17]. It is shown that only two mechanisms support these demands, the fast active scanning and the active scanning with neighborhood detection. Since only the fast active scanning is included in the standard, we have decided to use this wireless LAN handover mechanism with an average link layer handover time of 34.93 ms. The wireless LAN model was modified in order to implement fast handover for Mobile IPv6. As the FMIPv6 standard suggests, we make use of triggers as often as possible. The first trigger is used after the scanning process is completed. The wireless LAN association process is postponed and the FMIPv6 pre-handover messaging is initiated by a trigger. Afterwards, the wireless LAN association process is started and the link layer again sends a trigger to the network layer to initiate the binding update messages. Fig. 7 depicts the three triggers in the context of the overall handover procedure.

The basic structure of all simulation scenarios is shown in Fig. 8. Three access routers and one correspondent node are interconnected through an IP network. The access routers are connected by a T3 line to the IP core network and the distance between the routers is 200 m. The IP core network, illustrated as an IP cloud in the middle of the scenario can be configured to delay or drop data packets in order to simulate background load. However, we focus in our simulations on the wireless link because

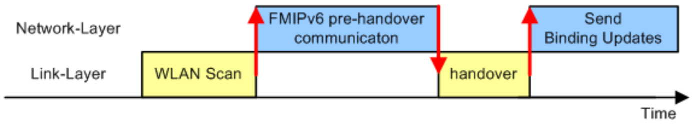

**Fig. 7.** Triggers used for Fast Mobile IPv6

the major packet delay results on the wireless link and so we have set the background load to zero and do not add any delays on the packets, routed via the IP cloud. The mobile node moves from the previous access router to the next access router with a moving speed of 18 kmph and the handover is initiated at a distance of about 160 m to the PAR based on the SNR. All access routers are configured with the IEEE 802.11g standard and use different, non overlapping channels. The PAR uses channel one, the NAR channel six, and the home agent channel eleven. Hence, fast active scanning and normal association is used on the link layer.

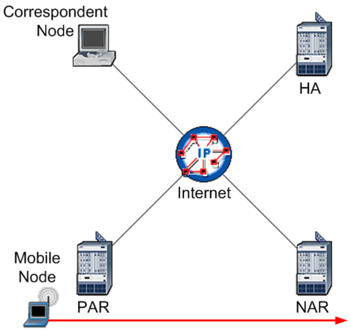

**Fig. 8.** Typical simulation scenario

For the communication between the MN and the CN, we choose the G.711 [18] voice codec. The codec has a data rate of 64 kbps and the packetization interval is set to 10 ms. For the simulation runs of Fast Mobile IPv6, we want to see the impact of background traffic on the handover performance in the cells and therefore, configure a number of clients within the cells using the same voice traffic profile as the MN. Further parameter settings are shown in Table 1.

## 4 Simulation Results

### 4.1 Agent Advertisement Interval of Mobile IPv4

In the first simulation study, the performance of Mobile IPv4 is evaluated. The handover performance mainly depends on the moving speed of the mobile and the interval of the

**Table 1.** Simulation parameter settings

| Parmeter | Value |
|---|---|
| Data rate | 54 Mbps |
| Channel assignment | Non overlapping channels |
| Layer 2 scanning | Fast active scanning [17] |
| Layer 2 authentication | Pre-authentication |
| Average Layer 2 handover delay | 35 ms |
| Mobility (Mobile Node) | 18 kmph |
| Mobility (Background Nodes) | 0 kmph |
| Distance between the access routers | 200 m |
| Connection of the access router | T3 connection |

agent advertisements from either a HA or a FA. If a mobile node does not receive an AA within the lifetime of the last AA, it will know that it has lost its network layer connection. Table 2 gives an overview of the limits, within which the AA sending interval may be configured [10]. This interval has a maximum and a minimum value, which themselves have upper and lower limits.

**Table 2.** Agent Advertisement interval limits

| | Lower bound | Upper bound | Default |
|---|---|---|---|
| Max value | 4 s | 1800 s | 600 s |
| Min value | 3 s | Max value | 0.75·Max value |

It is easy to see that the minimum interval of 3 s by far exceeds the maximum acceptable one way delay for voice conversations which is according to the ITU-T G.114 specification 400 ms [19]. Furthermore, the corresponding AA lifetime is longer than 9 seconds. This leads to a mean waiting time of more than 7.5 s, for the old AA lifetime to expire after the handover.

Thus, simulations have been made in order to examine, how tweaking Mobile IPv4 AA interval parameters improve the situation. Fig. 9 shows the handover time in dependence on the AA transmitting interval in a foreign agent care-of-address scenario, where a MN moves from its home network to a foreign network. The AA interval is reduced beneath the recommended lower bound of 3 s in steps of 100 ms. Please note that the marked out AA interval applies for both routers, the HA and the FA, equally.

Clearly, the total handover time decreases linearly with decreasing intervals between two consecutive AAs. The step-shaped nature of the graph relies on the fact that the lifetime variable is discrete. The original standard defines the AA lifetime as a 16 Bit unsigned integer, counting the seconds until expiration. If we consider an AA interval of 600 ms with a corresponding AA lifetime of at least 1.8 s, the AA lifetime is truncated to 1 s because only integer values are accepted. This is also the reason why shorter

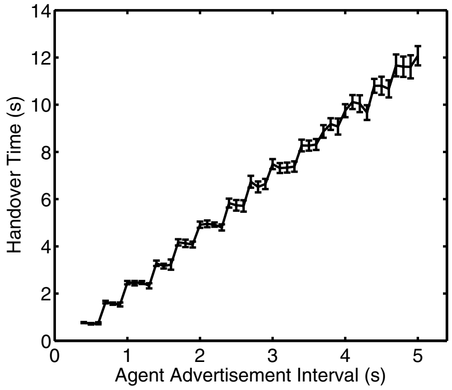

**Fig. 9.** Mobile IPv4 handover time with reduced AA transmitting intervals

intervals than 400 ms could not be evaluated. An AA interval of 300 ms leads to an AA lifetime of 0.9 seconds, effectively resulting in a lifetime of zero seconds.

The best handover performance can of course be achieved with an AA interval of 400 ms but the average handover time of 750 ms is still not sufficient for real-time traffic if we need to perform a large number of handovers. When using Mobile IPv6 the agent advertisements are replaced by so called router advertisements. The router advertisements are defined in size of milliseconds and the lower bound for these intervals is set to 30 ms. However, such a small router advertisement interval leads to a too large overhead. In our next simulation study, we want to evaluate the impact of the router advertisement interval and the duplicate address detection on the Mobile IPv6 handover performance.

### 4.2 Duplicate Address Detection

As examined in Section 2, duplicate address detection has a very negative impact on the network layer handover performance. When a MN has formed a new care-of-address using the subnet prefix information it has received with a router advertisement, it has to check whether the generated IP address is already assigned to a node in this subnet. This is done by multicasting a special neighbor solicitation message and actively waiting for a reply. After a configurable timeout, the *Neighbor Solicitation Retransmission Interval* (NSRI), the MN stops waiting for responses and starts sending one or more binding updates.

The impact of the NSRI and the router advertisement interval on the handover performance is shown in Fig. 10. The NSRI is set to 1000 ms and 500 ms. The scenario is a standard Mobile IPv6 scenario without route optimization, where the MN leaves its home network and enters another subnet. The router advertisement interval applies equally to the old and the new access router.

Here, three things can be seen. First, similar to Mobile IPv4, there is a linear behavior between the router advertisement interval and the network layer handover performance.

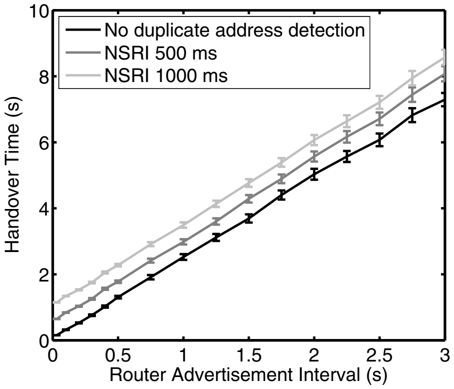

**Fig. 10.** Impact of different duplicate address detection settings on Mobile IPv6

The smaller the interval, the shorter the handover time. Second, without duplicate address detection, handover latencies in the magnitude of 200 ms seem achievable using extreme router advertisement interval settings. Finally, the value of the NSRI adds a constant delay to the network layer handover. Please note that with a value of 3 seconds, the maximum router advertisement interval in this figure is the minimum router advertisement interval of nodes not supporting Mobile IPv6.

### 4.3 Mobility Detection Factor

In the previous scenario, the router advertisement lifetime is set to 3 times the router advertisement interval. However, in Mobile IPv6, the lifetime of a router advertisement can be varied and is calculated by multiplying the value contained in the advertisement interval option by the MN specific *Mobility Detection Factor* (MDF). Thus, the time a MN has to wait until old RAs expire, may not only be reduced by increasing the transmitting frequency of the RAs. It may also be shortened, by simply setting the MDF to a lower value.

This is simulated in the next graph. Fig. 11 shows the results of three simulations. Each is based on a standard IPv6 scenario, using the same router advertisement intervals at both routers. The MN moves from its home network to another subnet. Route optimization and duplicate address detection are not supported. The simulations differ only in the value used for the MDF.

The gray curves, plotted beneath the simulation result graphs illustrate the functions: $y = 0.5 \cdot x$, $y = 1.5 \cdot x$, and $y = 2.5 \cdot x$. It can easily be seen that the result graphs are good approximations of those functions. This is because the time, at which a handover occurs, is uniformly distributed between the sending of two router advertisements. Thus, in the average, the handover takes place right in the middle of two RAs. Consequently, when using an MDF of 2 for example, the MN has to wait for another one and a half router advertisement intervals before it may drop its old access router. Of

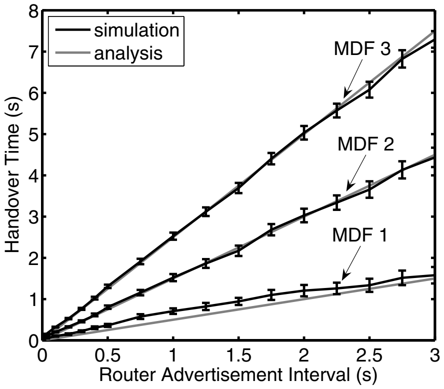

**Fig. 11.** Effect of the Mobile IPv6 Mobility Detection Factor

course, analog considerations apply for the mobility detection factors 1 and 3. However, although lowering the MDF visibly reduces the network layer handover latency, concurrently the risk increases of disconnecting from the old access point too early. Thus, adjustments to the MDF have to be taken seriously. An MDF of 2 is a good trade off between handover performance and loss probability of router advertisements. However, the MDF might also be adapted according to the network conditions. If we have a high packet loss rate, the MDF has to be increased.

Concluding the results from the duplicate address detection, the router advertisements, and the mobility detection factor, the possibilities to accelerate the network layer handover in Mobile IPv6 are better than the ones in Mobile IPv4. Simulation results show that when using extreme parameter values like a router advertisement interval of 30 ms, network layer handover latencies in the area of 150 ms are not impossible. Thus, fast Mobile IPv6 might be able to support real-time interactive communication in some very special cases. However, it is not designed to do so.

Furthermore, we strongly recommend to deploy some means of overcoming the extreme delay caused by duplicate address detection. Such a means may be *"Optimistic Duplicate Address Detection for IPv6"* [20]. If no such mechanism is used, the standard Mobile IPv6 network layer handover takes at least one second because the default value for the neighbor solicitation retransmission interval is one second.

### 4.4 Fast Mobile IPv6

Especially designed for reducing network layer handover latencies, Fast Mobile IPv6 constitutes a very promising solution if we want to support real-time traffic. In our implementation, we use three triggers to further accelerate the protocol operation. For the next simulation scenarios, we turned the duplicate address detection off, since the amount of MNs in the subnet is quite manageable.

The goal of the Fast Mobile IPv6 scenarios is not only to see the performance gain compared to the normal Mobile IPv6 scenarios, but also to see the impact of background traffic on the handover latency. Therefore, we use an increasing number of VoIP clients. We discovered that a wireless LAN cell using the IEEE 802.11g standard is able to manage 22 VoIP clients that are all communicating with respective VoIP correspondents using the traffic model described in Section 3. Those 22 clients include the moving MN.

We simulate all three possible movements with up to 21 clients generating background traffic. Those three movements are from the home network to a foreign network, from one foreign network to another, and from a foreign network back to the home network. Thereby, we do not measure the duration of the previous wireless LAN scan for two reasons. First, the scan takes longer then the whole Fast Mobile IPv6 protocol operation. Second, in Fast Mobile IPv6, the wireless LAN scan does not extend the duration of the IP connectivity loss. This is because after the scan, the MN has connectivity again in order to handle the pre-handover communication. Thus, the network layer handover related IP connectivity loss begins with the initialization of the actual link layer handover.

Fig. 12, Fig. 13, and Fig. 14 respectively illustrate two parts of a Fast Mobile IPv6 handover. The IP connection loss is the time in which the MN can not send nor receive IP packets and knows that it has no connection. The overall protocol activity time without route optimization begins as soon as the wireless LAN module tells Fast Mobile IPv6 about the forthcoming handover. Thus, it includes all pre-handover protocol operations and ends when the binding acknowledgment message from the MNs home agent is received. On the x-axis, the number of wireless LAN clients generating real-time VoIP traffic in the background is applied. The y-axis measures the time in milliseconds.

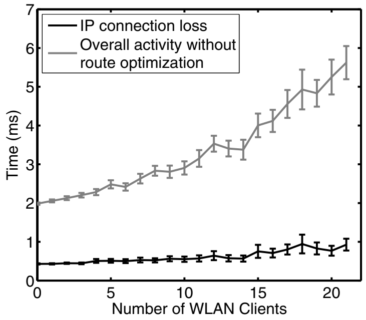

**Fig. 12.** Fast Mobile IPv6 moving from the home network to a foreign network

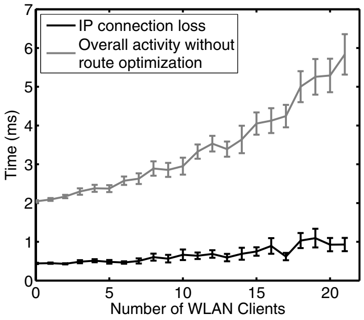

**Fig. 13.** Fast Mobile IPv6 moving from one foreign network to another

The three handover behaviors are almost identical which is different to normal Mobile IPv4 or Mobile IPv6 scenarios where the handover delay differs caused by tunneling redirections or tunnel removals. The time of the IP connection loss is quite independent of the amount of clients in the cell. It has the magnitude of 1 ms and thus, it is not much longer than the wireless LAN reassociation procedure. However, the overall protocol activity may take up to 6 ms when many clients are present.

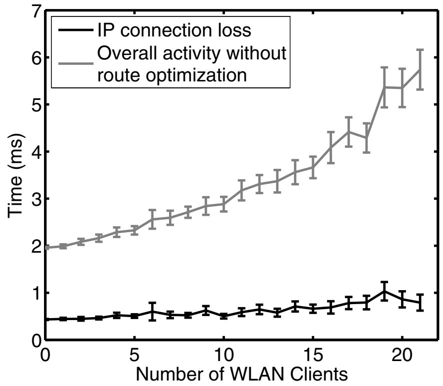

**Fig. 14.** Fast Mobile IPv6 moving from a foreign network back to the home network

### 4.5 Fast Mobile IPv6 with Route Optimization

Finally, we want to take a look at the overhead of route optimization. As described in Section 2, route optimization reduces the traffic which is normally routed over the home network by using mobility binding caches at the correspondent nodes. For this simulation scenario, we take a look at the handover delay when traversing from one foreign agent to another foreign agent. Fig. 15 shows the results of this simulation setup. In order to compare the handover latency using route optimization with the original handover latency, we also plotted the delay without route optimization. The x-axis shows again the number of VoIP wireless LAN clients at each cell which produce background traffic and the y-axis shows the handover latency. The IP connection loss is the same for both scenarios, with and without route optimization, but the overall Fast Mobile IPv6 latency differs. The overall activity with route optimization takes around 1.5 ms longer but is with less than 10 ms still faster than the scanning procedure on the link layer.

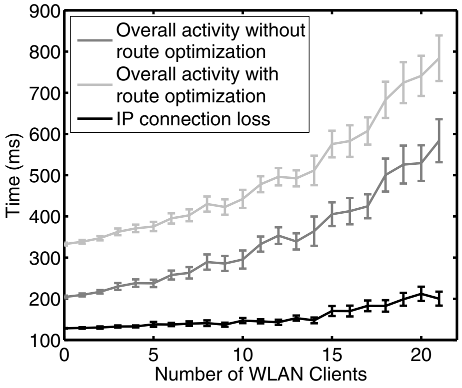

**Fig. 15.** Fast Mobile IPv6 with route optimization

The results of Fast Mobile IPv6 have shown that it is possible to support real-time traffic even when a network layer handover has to be performed. The overall handover latency consisting of link layer scanning, the Fast Mobile IPv6 messages and the reassociation on the link layer has been less than 50 ms for all simulation settings. However, a communication between the link layer and the network layer has to be managed.

## 5 Conclusion

In this paper we have shown the performance of different Mobile IP versions and their extensions. The Mobile IP handover process can be subdivided into three phases. Those are the movement detection phase, the care-of-address configuration phase, and the registration phase. Mobile IPv4 suffers from a too long movement detection latency that prevents the protocol from achieving overall handover delays smaller than six seconds. One method to reduce the movement detection latency is to reduce the agent advertisement interval to a value smaller than the one specified in the RFC. However, real-time applications requiring a specific QoS level can still not be supported.

Mobile IPv6 on the other hand has a much better design in terms of feature integration and security. However, as an extension to version 6 of the internet protocol, it inherits a major drawback. This is the duplicate address detection, which ensures that an IPv6 address is not already assigned to another node on the same subnet. Our results have shown that with the duplicate address detection turned on, real-time traffic can not be supported even if we reduce the mobility detection factor because an additional second is needed to identify the uniqueness of the IP address.

In principle, Fast Mobile IPv6 also suffers from the drawback of the duplicate address detection latency, which is surely a knockout criteria. However, the specification shows a way of how to avoid the duplicate address detection. The results of the simulation studies of Fast Mobile IPv6 without duplicate address detection have shown that the network layer handover can be performed in less than 10 ms. If we add the time needed for scanning on the link layer, the complete handover is, with less than 50 ms, still fast enough to support real-time traffic. However, the communication between the link and the network layer has to be implemented.

Finally, with route optimization, the traffic which is normally routed over the home network can be minimized with only a little overhead on the handover latency. In future work, we will take a look on the performance of Hierarchical Mobile IPv6 [21] and evaluate if the handover performance can further be increased.

## References

1. Valkó, A.G.: Cellular ip: A new approach to internet host mobility. SIGCOMM Comput. Commun. Rev. **29** (1999) 50–65
2. Ramjee, R., Varadhan, K., Salgarelli, L., Thuel, S.R., Wang, S.Y., Porta, T.L.: HAWAII: a domain-based approach for supporting mobility in wide-area wireless networks. IEEE/ACM Transactions on Networking (TON) **10**(3) (2002) 396–410
3. Perkins, C.E.: IP Mobility Support. RFC 2002, http://www.ietf.org/rfc/rfc2002.txt (1996)
4. Perkins, C.E.: IP Mobility Support for IPv4. RFC 3344, http://www.ietf.org/rfc/rfc3344.txt (2002)

5. Johnson, D., Perkins, C.E., Arkko, J.: Mobility Support in IPv6. RFC 3775, http://www.ietf.org/rfc/rfc3775.txt (2004)
6. Akyildiz, I.F., Xie, J., Mohanty, S.: A Survey of Mobility Management in Next-Generation All-IP-Based Wireless Systems. IEEE Wireless Communications **11** (2004) 16–28
7. Li, J., Chen, H.H.: Mobility Support for IP-Based Networks. IEEE Communications Magazine **43** (2005) 127–132
8. Kwon, D.H., Kim, Y.S., Bae, K.J., Suh, Y.J.: Access router information protocol with FMIPv6 for efficient handovers and their implementations. In: GLOBECOM 2005 - IEEE Global Telecommunications Conference, St.Louis, MO, USA (2005) 3812–3817
9. Sharma, S., Zhu, N., Chiueh, T.: Low-Latency Mobile IP Handoff for Infrastructure-Mode Wireless LANs. IEEE Journal on Selected Areas in Communications **22**(4) (2004) 643–652
10. E-Perkins, C.: Mobile IP Design Principles and Practices. Prentice Hall PTR (1998)
11. Conta, A., Deering, S.: Generic Packet Tunneling in IPv6 Specification. RFC 2473, http://www.ietf.org/rfc/rfc2473.txt (1998)
12. Deering, S., Hinden, R.: Internet Protocol Version 6 (IPv6) Specification. RFC 2460, http://www.ietf.org/rfc/rfc2460.txt (1998)
13. Johnson, D.B., Perkins, C.E.: Route Optimization in Mobile IP. Internet Draft draft-ietf-mobileip-optim-11.txt (work in progress) (2001)
14. Deering, S., Hinden, R.: Internet Protocol Version 6 Addressing Architecture. RFC 3513, http://www.ietf.org/rfc/rfc3513.txt (2003)
15. Koodli, R.: Fast Handovers for Mobile IPv6. RFC 4068, http://www.ietf.org/rfc/rfc4068.txt (2005)
16. (OPNET Modeler, OPNET University Program: http://www.opnet.com/services/university/)
17. Pries, R., Heck, K.: Simulative Study of the WLAN Handover Performance. In: OPNETWORK 2005, Washington D.C., USA (2005)
18. ITU-T Recommendation G.711: Pulse Code Modulation (PCM) of Voice Frequencies. International Telecommunication Union (1998)
19. ITU-T Recommendation G.114: One Way Transmission Time (2000)
20. Moore, N.: Optimistic Duplicate Address Detection for IPv6. Internet Draft (2005)
21. Soliman, H., Castelluccia, C., Malki, K.E., Bellier, L.: Hierarchical Mobile IPv6 Mobility Management (HMIPv6). RFC 4140, http://www.ietf.org/rfc/rfc4140.txt (2005)