Implementation and evaluation of an IEEE802.11 assisted mobile IP handover scheme

Reference:
De Cleyn Peter, Blondia Christian, Moerman I..- *Implementation and evaluation of an IEEE802.11 assisted mobile IP handover scheme*
Proceedings of the 9th European Conference on Networks and Optical Communications (NOC2004), Session on Mobile Networks, Eindhoven, The Netherlands, June 29-July 1, 2004 - s.l., 2004, p. 245-252
Handle: http://hdl.handle.net/10067/505830151162165141

Implementation and evaluation of an IEEE802.11 assisted Mobile IP handover scheme[1]

P. De Cleyn, C. Blondia
University of Antwerp - Belgium

I. Moerman
Ghent University/IMEC - Belgium

Abstract

This paper describes the design and the implementation of a smooth handoff scheme using IEEE802.11 triggers. The scheme is based on the idea of Post-Registration, a Layer 3 low latency handoff scheme proposed by the IETF. In order to avoid packet loss during Layer 2 handover (i.e. while the mobile node is searching for a new access point) and during the Mobile IP registration process, packets are buffered at the old Foreign Agent. As soon as the new access point is known, a tunnel is built between the old and the new Foreign Agent and packets are forwarded through the tunnel towards the new access point. The mobile node can then perform its Mobile IP registration without losing any packets. The implementation details of the mechanism are described. Experimental results show that the handoff is smooth (i.e. zero packets are lost) and the delay induced by the buffering and the forwarding scheme is assessed.

1. Introduction

While various micro-mobility solutions exist to minimize the registration latency introduced by Mobile IP [3] (such as Regional Registrations[9]), L2 handover latency has been kept out of scope. To tackle this problem, the IETF has proposed Low Latency

[1] This work was supported by the by BELSPO Belgium under project IAP P5/11 MOTION (Mobile Multimedia Communication Systems and Networks), by IWT under project 020152 – End-to-end QoS in IP based Mobile Networks and by the 6th Framework Program Network of excellence Euro-NGI.

Handoffs in Mobile IPv4 [4] that use L2 information: pre- and post-registration. Using pre-registration, a mobile node will try to register with its new foreign agent (nFA) before a L2 handoff occurs. Post-registration postpones MIP registration till after an L2 handoff. Traffic for the MN will continue to arrive at the oFA, and will be tunnelled towards the nFA for delivery. Both approaches make use of L2 events (triggers) in order to schedule the necessary control messages.

When using IEEE 802.11 as link layer, its functionality does not provide the necessary L2 triggers in order to implement the proposed solutions. When a mobile station moves towards a new AP, it will disconnect from its old access point (oAP) and scan for other APs in range. Based on the results of these scans, it will choose its next AP. There is thus no possibility for the MN to use pre-registration as the MN does not know in advance where to go and once a new AP selected, it is no longer connected with its oAP. The same remarks can be made with regard to post-registration. A MN should remain connected with its oFA while selecting its nAP and it should signal the oFA when disconnecting definitely from its oFA. IEEE 802.11 is neither capable of communication with two APs nor can it signal its leave from a certain AP.

Although the in [4] proposed solutions do optimize latency problems [5][6], packet loss can not be ruled out without a buffering scheme. In the following paragraphs, we will show that the combination of the limited L2 triggers in 802.11 and a buffering mechanism can minimize Mobile IP registration delay and avoid packet loss.

2. Architecture and protocol

2.1 Reference network

The reference network is illustrated in Figure 1. In order to optimize the exchange of information between L2 and L3 agents, the 802.11 AP and MIPv4 FA functionalities are combined within one access router. In the following discussion, we will use the terms AP and FA to indicate the specific service offered by the same router and we assume that information between both functionalities can be exchanged. The old and new access routers are part of a different subnet and are connected to an internet using a gateway router. The Corresponding Node (CN) and the Home Agent (HA) are also connected to this internet. In the tests, the CN sends Constant Bit Rate (CBR) traffic towards the MN.

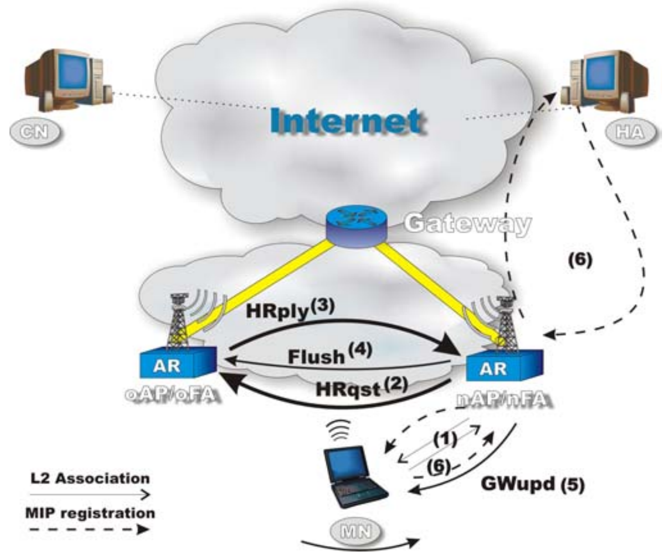

Figure 1: Reference Network

Handoff mechanism

802.11 uses a hard handoff mechanism [7]. Once the mobile station decides that the link quality has dropped such that switching towards a new AP becomes necessary, it disconnects from its current AP and starts a scanning phase. Scanning can either be active, with the station sending probes to discover new access points, or passive, using the beacons broadcast by the APs to learn about other APs. Based on the received information from the APs, a new AP is selected and authentication and association messages are exchanged. Once the association is achieved, L2 connection is re-established. Research [1] has shown that this handoff cycle can take up to 500 ms. In this period of time, multiple packets can get lost.

In order to avoid packet loss due to L2 disconnection, incoming packets for the MN should be buffered at the oFA. As this agent and its AP counterpart are unaware of the exact moment when a MN disconnects, the oFA should continuously buffer packets for the MN in a circular buffer. Once the L2 connection with the new FA is established, the oFA is notified and a BET (bidirectional tunnel) [4] between oFA and nFA is constructed. The content of the buffer in the oFA will be flushed into the BET and newly incoming packets also will be tunnelled towards the nFA. While no MIP registration is performed yet, the MN is already capable of communicating via the BET and thus the registration delay is shortened and thanks to the buffering mechanism, no packets will get lost during the L2 handoff.

2.2 Detailed description

We start our discussion of the developed protocol with the MN sending a MIP registration request (*regreq*) to the oFA to perform its first MIP registration in the foreign domain. A successful MIP registration triggers the buffer process at the FA to intercept all incoming traffic from the CN towards the MN and to copy these packets into a circular buffer before making a routing decision. Once copied, the packets are forwarded towards the MN. When the MN disconnects from the oAP, the oFA continues to buffer packets and to forward them on the airlink, as it is unaware of the departure of the MN. After being successful associated (Figure 1 (1)) with the nAP, the MAC address of the MN is known to the nAP and signalled to the FA service. The nFA, who knows the oFA's address using an exchange mechanism outside the scope of this paper, will send a Handoff Request message (*HRqst* (2)) [4] towards the oFA. This message will contain the L2 address of the MN which will enable the oFA to lookup the binding for the MN in its binding table. Using the MN's home address and the HA address from this binding entry, the oFA, now aware of the handoff of the MN, will stop forwarding packets on the airlink and will construct its endpoint of the tunnel between oFA and nFA. Once this tunnel endpoint is activated, the oFA will send the nFA a successful Handoff Reply (*HRply* (3))[4], containing the home address and HA address of the MN. Using the IP addresses in the *HRply* message, the nFA is now able to configure its own buffer and to activate its tunnel endpoint. Once the nFA is finished configuring the tunnel endpoint, its buffer and routing tables, it signals the oFA using, a flush message (*Flush* (4)), to flush the contents of the buffer towards the nFA. From this moment on, all incoming packets for the MN coming from the oFA will also be buffered at the nFA and forwarded over the nAP's airlink: L3 connectivity towards the MN is established.

In order for the MN to send traffic upstream in the network, it has to adapt its routing tables and ARP caches to the new situation. It needs to choose the nFA as its default gateway, but as only a L2 association is performed yet, it is unaware of the nFA's IP address. The nFA will thus have to send a Gateway Update (*GWupd* (5)) message, containing its IP address. Using the received IP address and the MAC address obtained during the association the MN can create an ARP entry for the nFA in the ARP table and a default gateway rule in its routing tables. L3 connection is now fully restored and traffic to and from the MN will be possible. The MN can now decide to perform a MIP registration (6) of its new location or refresh its current binding with the oFA and HA using standard MIP mechanisms.

2.3 *Implementation details*

The testbed used to obtain the experimental results discussed in the following chapter was constructed as defined above using of the shelf PCs. On every node, a Linux Mandrake 9.1 distribution was installed using the 2.4.21-0.13mdk kernel. One access router is equipped with three Linksys WPC11 pcmcia cards. The first one is used to deliver access point functionality using the HostAP drivers [11] in master mode and the other two cards are set up in monitor mode in order to capture L2 management frames from the used channels. The second AR is equipped with only one WLAN card to provide the AP functionality. The MN is equipped with only one WPC11 card in managed mode. The HostAP drivers support the Wireless Extensions mechanism [12] of the Linux kernel which makes it possible to interrupt the MIP software for L2 events, in particular at the event of an association of a new MN. The MIP functionality was realised with HUT Mobile IP [2] adapted to support the described messaging scheme. Both access routers serve a different subnet and APs use different BSSIDs and radio channels.

The buffers were implemented as a separate application in user space. The netfilter mechanism [10] was used to divert the incoming packets from the MN towards this application.

3. Experimental Results

In this section we discuss the results obtained from the scheme and the platform described in the previous section. The test results were obtained by sending CBR traffic from the CN towards the MN. The ping command was used for this purpose as it allows us to monitor the packets using the available sequence numbers. The echo packets are also independent of each other, so loss or duplication of a packet does not influence other packets. 100 packets of 64 bytes were transmitted every 50 ms and for all of them a reply was received. During this period, a handoff was forced by changing the BSSID at the MN. Also a MIP handover was triggered due to this L2 handoff, as the nFA serves a different subnet. No packets were lost during the two handovers or in the period between them thanks to a 12 packet large circular buffer at the oFA.

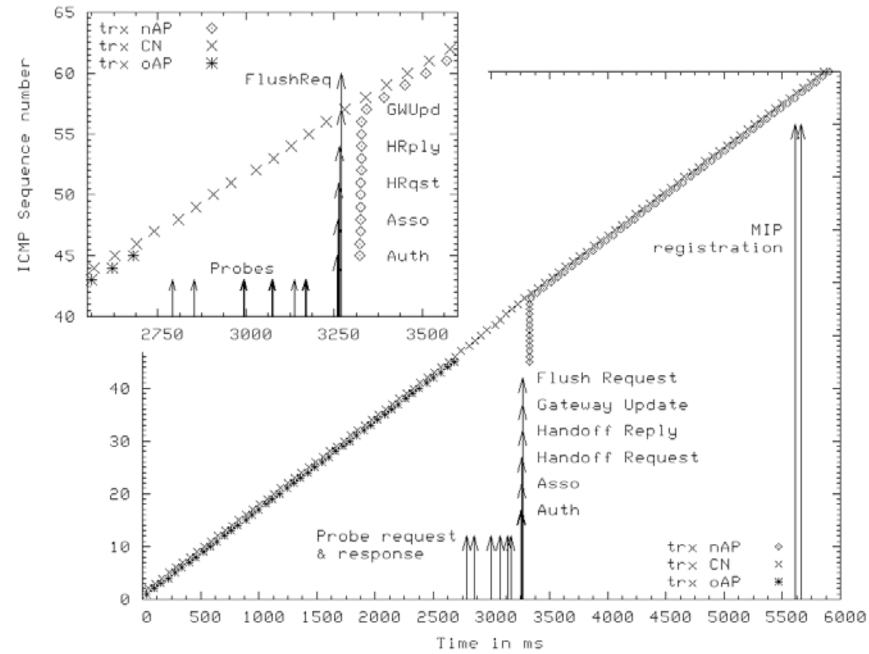

Figure 2: Sequence graph of transmitted ICMP echo requests

In Figure 2 we see that echo requests up to 45 are being delivered to the MN by the oAP. The MN then disconnects from its current AP and starts scanning for a more suitable AP. The probe requests and responses to and from the nFA are indicated with arrows on the graph. After authentication and association, the handoff messages are triggered, the BET is constructed and the buffer at the oFA is flushed. In the detailed graph, we can clearly see the flushed requests (45 to 56). From these packets, only request 45 had already been transmitted by the oAP. Without our buffering scheme, all other requests would have been lost due to L2 handoff. Furthermore we see that 2.3 seconds after connection was restored, MIP registration started. Packets transmitted before this instance are still delivered to the oFA and tunnelled to the nFA. If no BET was used, this would correspond to an additional loss of 39 packets. It is clear that the discussed scheme avoids packet loss at the expense of possible packet duplication. Buffer dimensioning should thus be studied in order to optimize this handoff solution.

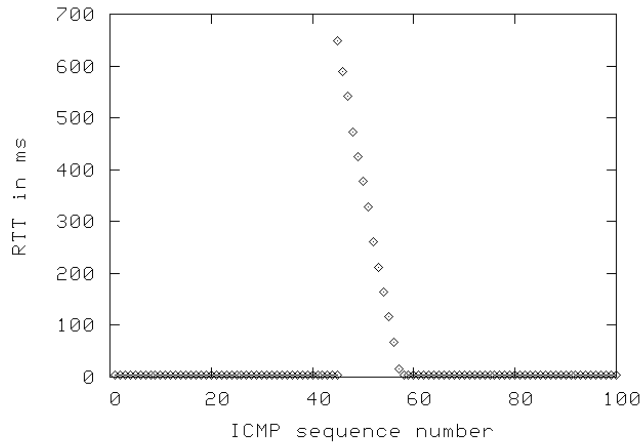

Figure 3: Delay experienced by the application

The use of buffers introduces additional delay in the network. In **Figure 3** we plot the difference in time between an outgoing echo request and its corresponding incoming reply. From the graph it is clear that the BET does not add any extra delay worth mentioning; average delay measured for packets directly delivered is 3.6 msec, while 3.7 msec in average for the tunnelled packets. As oFA and nFA only one hop from each other, this should be no surprise. In this run packets that were flushed from the buffer, do experience an additional delay up to 645 msec. We believe this amount of delay is acceptable for streaming applications, if a playout buffer is used. Interactive sessions could however notice the handover, but the effect should remain significantly smaller than without our handoff scheme.

4. Conclusions and future work

This paper shows that using L2 information from IEEE 802.11 and a buffering and tunnelling scheme, it is possible to implement a smooth handoff scenario. The first results show that no packets are lost neither during L2 handoff nor due to late L3 registration or registration delay. The study also shows that the extra delay the scheme introduces stays within an acceptable range.

Further tests will be done in order to get an insight in to the behaviour of various types of applications (video streaming, VoIP, interactive applications) during handoff. Also (dynamic) buffer dimensioning and duplicate packet elimination will be studied.

References

[1] Arunesh Mishra, Minho Shin, William Arbaugh, “An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process”, http://citeseer.nj.nec.com/541775.html.

[2] Dynamics Hierarchical Mobile IP: http://dynamics.sourceforge.net/

[3] C. Perkins, RFC 2002: IP mobility support (Oct. 1996).

[4] K. El Malki and others, “Low Latency Handoffs in Mobile IPv4”, draft-ietf-mobileip-lowlatency-handoffs-v4-04.txt (2002).

[5] O. Casals, Ll. Cerdà, G. Willems, C. Blondia, N. V. den Wijngaert, “Performance evaluation of the Post-Registration method, a low latency handoff in MIPv4”, in: Proceedings of ICC, 2003.

[6] C. Blondia, O. Casals, Ll. Cerdà, N. V. den Wijngaert, G. Willems, P. De Cleyn, “Performance Comparison of Low Latency Mobile IP Schemes”, in: Proceedings of WiOpt'03, INRIA Sophia Antipolis, France, 2003, pp. 115-124.

[7] IEEE, ANSI/IEEE Std 802.11, 1999 Edition (1999).

[8] R. Ramjee, T. La-Porta, S. Thuel, K. Varadhan, L. Salgarelli, “IP micro-mobility support using HAWAII”, Internet draft, July 2000.

[9] E. Gustafsson, A. Jonsson, and C. Perkins, “Mobile IPv4 Regional Registration,” Internet draft, work in progress, Sep. 2001.

[10] The netfilter/iptables project is the Linux 2.4.x/2.5.x firewalling subsystem, http://www.netfilter.org.

[11] Host AP driver for Intersil Prism2/2.5/3, http://hostap.epitest.fi/.

[12] Wireless extensions, http://www.hpl.hp.com/personal/Jean_Tourrilhes/Linux/Linux.Wireless.Extensions.html.

Authors’ contact addresses

P. De Cleyn and C. Blondia
University of Antwerp,
Dept. Mathematics and Computer Science,
Middelheimlaan 1, BE-2020 Antwerp – Belgium,
Tel: +32 3 2653903,
E-mail: {peter.decleyn,chris.blondia}@ua.ac.be

I. Moerman
Ghent University/IMEC,
Dept. of Information Technology,
Sint-Pietersnieuwstraat 41, BE-9000 Ghent – Belgium,
Tel: + 32 9 2649973,
E-mail: Ingrid.moerman@intec.ugent.be