Mobile Networks and Applications 8, 643–653, 2003

Analysis and Evaluation of Mobile IPv6 Handovers over Wireless LAN

NICOLAS MONTAVONT and THOMAS NOËL
LSIIT-ULP, Bld Sebastien Brant, 67400 Illkirch, France

Abstract. In this paper, we analyze the IPv6 handover over wireless LANs. Mobile IPv6 is designed to manage mobile nodes movements between wireless IPv6 networks. Nevertheless, a mobile node cannot receive IP packets on its new point of attachment until the handover completes. Therefore, a number of extensions to Mobile IPv6 have been proposed to reduce the handover latency and the number of lost packets. We focus on Fast Mobile IPv6 which is an extension of Mobile IPv6 that allows the use of L2 triggers to anticipate the handover. We compare the handover latency in four specific cases: basic Mobile IPv6, the forwarding method of Mobile IPv6, the Anticipated method, and the Tunnel-Based Handover. The results of the handover latency are calculated with the L2 properties of IEEE 802.11b. In particular, we take into account the L2 handover for different configurations of the wireless network.

Keywords: handovers, Mobile IPv6, Fast Mobile IPv6, wireless LAN, IEEE 802.11b

1. Introduction

Mobile IPv6 [5] is designed to manage mobile nodes movements between wireless IPv6 networks. The protocol provides an unbroken connectivity to IPv6 mobile nodes when they move from one wireless point of attachment to another in a different subnet. Mobile IPv6 (MIPv6) set up a messages exchange to notify the correspondent(s) of a mobile node about its new localization by a binding between the mobile node addresses.

Nevertheless, the mobile node cannot receive IP packets on its new point of attachment until the handover finishes. This time includes the new prefix discovery on the new subnet, the new Care-of establishment, and the time needed to notify the correspondents and the home agent about the new localization of the mobile node. This time is called the handover latency.

Actually, the handover latency can be too long regarding real time multimedia applications. In most cases, the impact of the handover latency strongly degrades the IP stream of the mobile node. Therefore, there are many extensions to MIPv6 and new protocols proposed to improve the IP connectivity of mobile nodes. The aim of these proposals is to reduce the latency and the number of packets lost due to the handover between one point of attachment to another [2] and to reduce the signaling load on the MIPv6 home agent and on the correspondent nodes [9,10]. In this article, we focus on one of them called Fast Mobile IPv6 [2].

Fast Mobile IPv6 (FMIPv6) allows the mobile nodes to create a new valid Care of address before the movement to the new wireless acess point. If the protocol successfully completes, the layer 3 (L3) handover latency only becomes the layer 2 (L2) handover latency.

The aims of this paper is to compare the time needed by these two protocols to move the flow of a mobile node from one access network to another. We are going to consider many cases per protocol to have a good overview of these solutions and to find out which cases still introduce problems. Our measurements are based on wireless IEEE 802.11b LAN. We first tested the IEEE 802.11b in order to evaluate the useful throughput offered and to estimate the L2 handover latency. Then we used these results to calculate in a theoretical manner the handover latency involved in MIPv6 and FMIPv6.

In section 2 we present MIPv6 [5] and its extension FMIPv6 [2]. Then, in the following section, we expose the IEEE 802.11b and the tests we made. In the next section, these tests will be useful to evaluate the handover latency in MIPv6 and FMIPv6 in different cases. Finally, we give some concluding remarks in the last section.

2. Mobile IPv6 and Fast Mobile IPv6

In this section, we remind the handover procedure as it is defined in MIPv6 and in FMIPv6. We consider that most of the terms in [7] are assimilated. When a mobile node performs a handover, we call the current access router (AR) the “old AR” and we call the AR where the mobile node is going to the “new AR”.

2.1. Mobile IPv6

Mobile IPv6 [5] is designed to manage mobile nodes movements between wireless IPv6 networks. A mobile node has a home address in its home network. When it remains in its home network, it communicates with this home address like another IPv6 node with its correspondents. When the mobile node moves to a new point of attachment in another subnet, packets sent by its correspondent(s) will continue to reach its home network. Moreover, it cannot use its home address any more to send packets in the new subnet. Therefore it needs to acquire a new valid Care-of address in the visiting subnet.

Then, it informs its home agent and its correspondent(s) about the binding between its home address and its new Care-of address. On the other hand, the home address always identifies the communication, even if the mobile node is in a visited network.

2.1.1. The handover procedure

A mobile node detects that it has moved to a new subnet by analysing the *Router Advertisement* sent by the AR [8]. Indeed, the AR periodically sends *Router Advertisement* every 0.05 to 1.5 s [5]. The mobile node can detect the change of AR by the prefix contained in the *Router Advertisement* or if it does not receive a *Router Advertisement* at the frequency indicated in the *Router Advertisement* (Advertisement Interval Option [5]) sent by the old AR. In the last case, the mobile node should request a *Router Advertisement* by sending a *Router Sollicitation*. This accelerates the new Care-of address establishment since the mobile node does not have to wait for the new *Router Advertisement*.

Next, the mobile node needs to create a new Care-of address. As it is specified in IPv6 [5], the mobile node first needs to verify the uniqueness of its link-local address on the new link. The mobile node performs Duplication Address Detection (DAD) on its link-local address. Then, it may use either stateless [11] or stateful [1] Address Autoconfiguration to form its new Care-of address. Once it forms its new Care-of address, it may perform an DAD on it. However, an DAD takes quite a long time with respect to the handover latency. Actually, to perform DAD the mobile node should send one or several *Neighbor Solicitation* to its new address and wait for a response for at least one second. This implies an important additional time on the handover latency. For this reason, the mobile node should perform DAD in parallel with its communication, or should choose not to perform it.

Once the mobile node has a new valid Care-of address, it must inform its home agent and its correspondent(s) about it. The mobile node sends a *Binding Update* (*BU*) which indicates the binding between its home address and its new Care-of address. A *Binding Update* is a destination option in a IPv6 packet. The mobile node can request an acknowledgement by setting a specific bit in its message (this bit must be set in the *Binding Update* destinated to the Home Agent). The Home Agent and maybe a correspondent replies with a *Binding Acknowledge* to the mobile node. All the steps of this algorithm is described in figure 1.

2.1.2. Handover enhancement

MIPv6 already provides some enhancements to the handover procedure. In some cases, an access point can be attached to several AR. A mobile node must choose one of them because it can only have one default AR. But the mobile node can form a Care-of address for its default router (the primary Care-of Address) and other Care-of addresses based on the other AR. Then, when its default AR becomes unreachable, the mobile node can use a new default AR for which it already has a Care-of address if it is possible.

Otherwise, the packets sent by the correspondent nodes are lost until the *Binding Update* reaches them. To reduce the number of packets lost during this time, the mobile node can request the forwarding of packets from its old subnet to its new AR. To do so, a Home Agent must be present on the old link. The mobile node has to send a *Binding Update* to a Home Agent on its old link with its old Care-of address in the home address field and with its new Care-of address in the Care-of address field. Then, the Home Agent on the old link intercepts the packets intended to the mobile node and forwards them to the current localization of the mobile node (see figure 2).

Otherwise, some extensions to MIPv6 are proposed to minimize the signalization load and to accelerate the time to advertise the correspondents. One of them namely Hierarchical Mobile IPv6 [10] proposes this kind of enhancement by allowing a mobile node to register locally. Once the mobile node enters a new domain and advertises its Home Agent and its correspondents, all further movements in the domain are hidden from the rest of the Internet. Nevertheless, we do not consider this solution in our measurements since the handover latency is the same as MIPv6 apart from the time required by the *Binding Update* to reach the correspondent nodes. On the contrary, when a mobile node has many correspondents, in MIPv6 the mobile node must send a *Binding Update* to each of them while in Hierarchical MIPv6, the mobile node only sends one BU to the Mobility Anchor Point of the domain. Nonetheless, in our calculation we do not consider a mobile node which has many correspondents. This can be the subject of later studies.

2.2. Fast Mobile IPv6

Fast Mobile IPv6 aims to minimize the MIPv6 handover latency [2]. It sets up services for the mobile node on the new AR before the movement of the mobile node. These services can be the new Care-of address establishment ("Anticipated Handover") or the setting up of a bidirectionnal tunnel between an anchor AR and the new AR ("Tunnel-Based Handover").

The services establishment on the new AR, before the mobile node moves, implies an anticipation of the mobile node movement. This anticipation is done by the L2 triggers [6]. A L2 trigger is an information based on the link layer protocol, below the IP protocol, in order to begin the L3 handover before the L2 handover ends. It contains information on the L2 connection and on the link layer identification of the different entities (the link layer address of the mobile node for example). In the scope of this article, we distinguish three trigger types according to the entity which receives the trigger: the handover controller's anticipation (the mobile node for example), a source trigger (information collected by the old AR) and a target trigger (information collected by the new AR). Although these triggers depend on the underlying information, they must be independent from the technology used.

However, the anticipation can be erroneous or imprecise and precautions must be taken. One of them is that the mo-

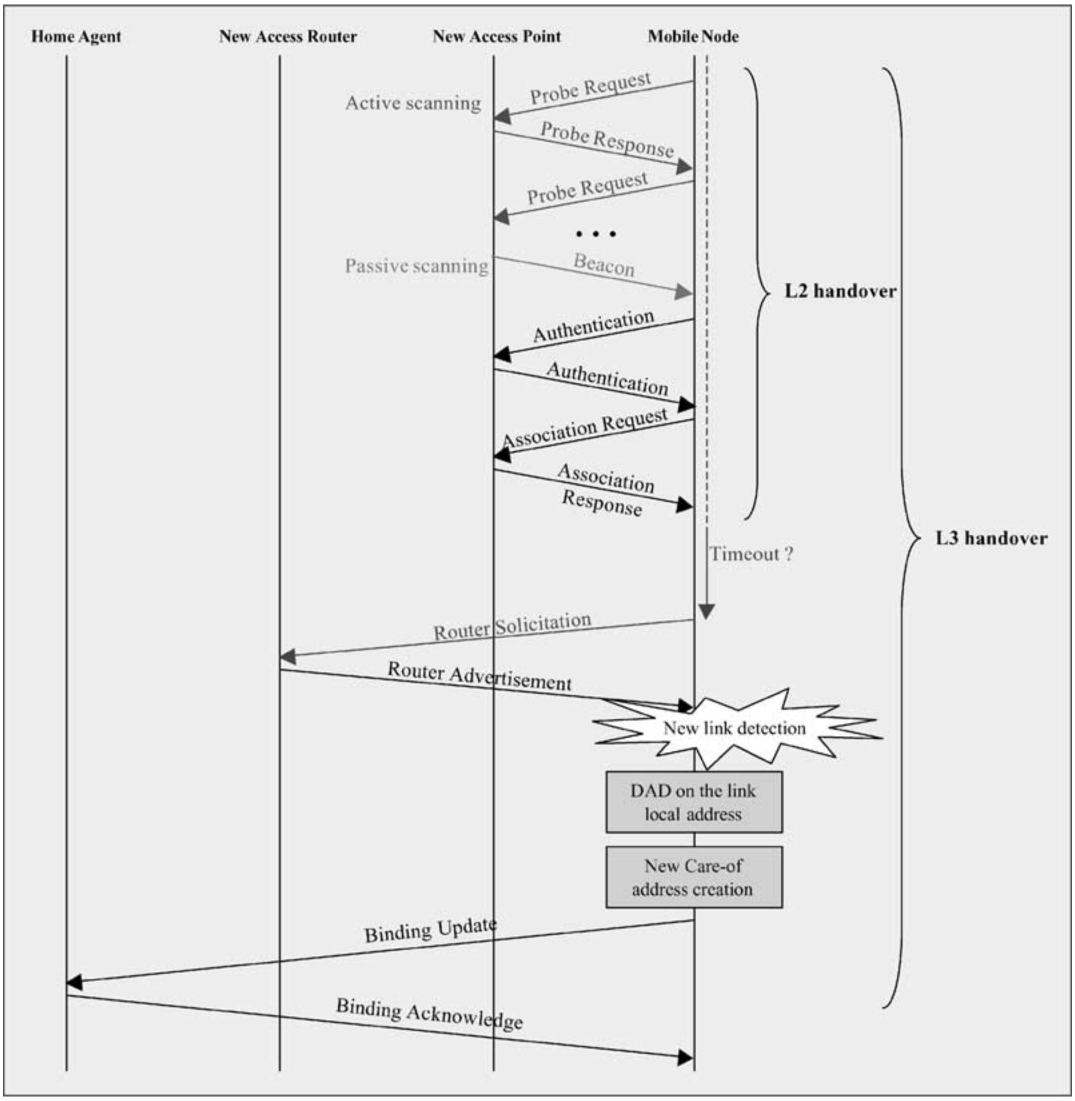


Figure 1. The L2 handover and the L3 handover.

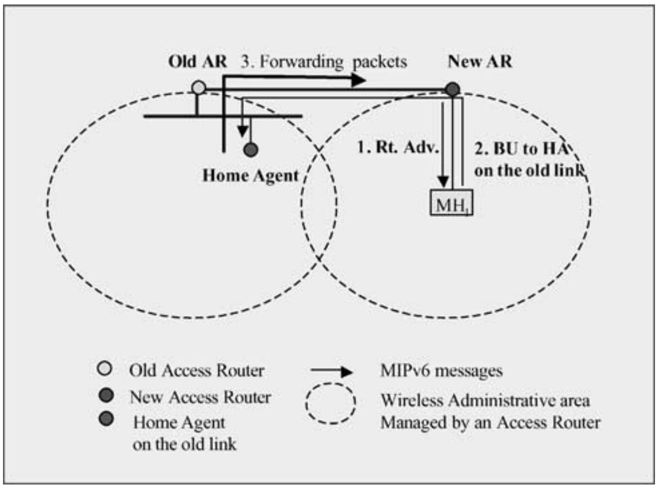

Old AR
3. Forwarding packets
New AR
Home Agent
1. Rt. Adv.
2. BU to HA on the old link
MH
Old Access Router
New Access Router
Home Agent on the old link
MIPv6 messages
Wireless Administrative area Managed by an Access Router

Figure 2. Forwarding by a Home Agent on the old link.

bile node should not use its newly formed Care-of address until it receives an acknowledgment for it [2]. Moreover, the two methods in FMIPv6 allow to chain the AR to forward the packets if the mobile node moves rapidly from several ARs. However we do not consider this case in our evaluation because we calculate the handover latency for one movement.

The protocol describes a framework as well for the mobile-controlled handover as for the network-controlled handover with only a small difference in the messages order. In the case of the network-controlled handover, a specific entity of the network decides when the mobile node needs to move to a new point of attachment. This entity can be the current AR offering the connectivity to the mobile node or a dedicated equipement in the subnet which manages the mobile node movements. In the following subsection, we describe the two methods defined in the protocol.

2.2.1. Anticipated Handover

The new AR has been found by anticipation as described above. Two cases can be distinguished according to the entity which control the handover. In the following, only the case where the handover is accepted by the new AR is considered, and we admit that the new AR address is known by the old AR. This is achieved by a beforehand exchange between the neighboring AR.

FMIPv6 sets up the new Care-of address allocation before the mobile node moves to the new AR. According to the handover control, the old AR sends a *Proxy Router Advertisement* (step 2b in figure 3) which can be unsolicited or in reply to a *Router Solicitation for Proxy* (step 2a) from a mobile node. This *Proxy Router Advertisement* contains a new Care-of address that the mobile node will be able to use at the new AR. In the stateful address configuration [1], the old AR must request the new Care-of address to the new AR. This is done by a *Handover Initiate* (step 1a). The new AR replies with a *Handover Acknowledgement* (step 1b) which contains a new Care-of address for the new subnet. In this case, the old AR sends the *Proxy Router Advertisement* after receiving the *Handover Acknowledgement*. Moreover, the new AR registers the mobile node in its neighboring cache to defend the new Care-of address.

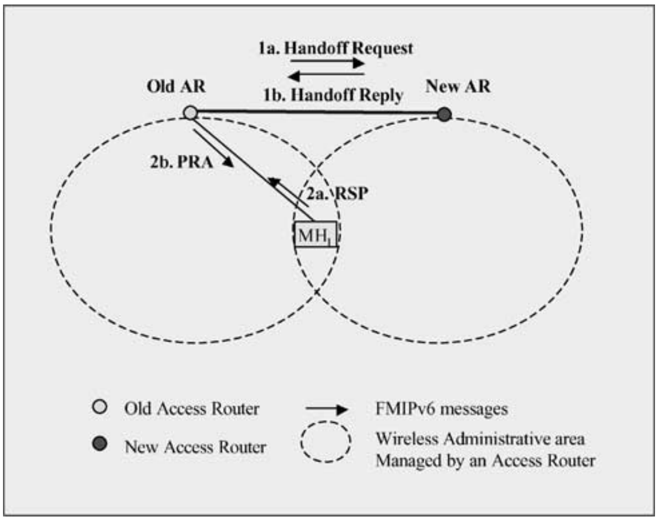


Figure 3. Anticipated Handover Initiation.

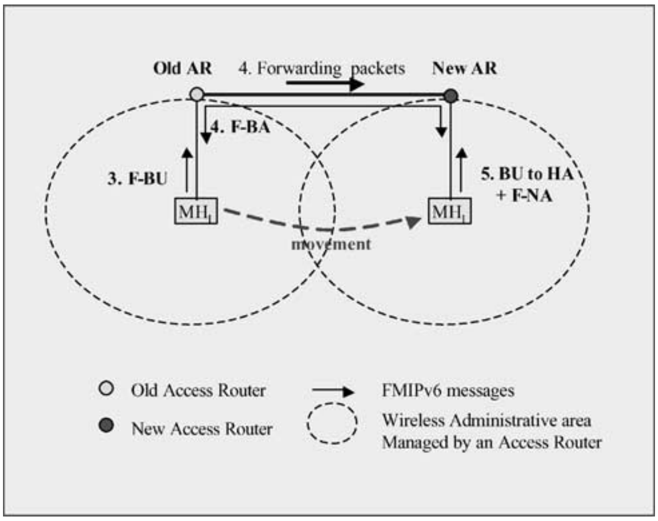


Figure 4. Anticipated Handover Registration.

The transition to IPv6 allows some more flexibility in the fast handover protocol: IPv6 allows stateless address configuration [11]. Therefore, the old AR can immediately send the *Proxy Router Advertisement* (step 2b) to the mobile node with a new Care-of address or a network prefix for the new subnet without waiting for the *Handover Acknowledgement*. In the mean time, as it sends the *Proxy Router Advertisement*, the old AR sends a *Handover Initiate* (step 1a) to the new AR in order to request the validation of the new Care-of address (Duplication Address Detection) and to inform the new AR about the arrival of the mobile node. The result of the validation of the new Care-of address is sent by the new AR in a *Handover Acknowledgement* (step 1b).

In order to indicate its departure, the mobile node sends a *Fast-Binding Update* (step 3 in figure 4) to the old AR just before moving. This message triggers the packets forwarding between the AR: upon the receipt of the *Fast-Binding Update*, the old AR sets up a temporary tunnel towards the new AR. Then, the old AR sends a *Fast Binding Acknowledgement* (step 4) to both the mobile node old Care-of address and through the tunnel made. The receipt of the *Fast Binding Acknowledgement* points out the mobile node that it can use the new Care-of address as the source address in its future packets.

When the mobile node establishes the connection with the new AR, it immediately sends a *Fast-Neighbor Advertisement* (step 5) if it does not receive the *Fast-Binding Acknowledgement* to inform the new AR from its arrival. Otherwise, if the mobile node still received the *Fast-Binding Acknowledgement* in its old subnet, it only sends a *Neighbor Advertisement*. The new AR checks in its neighboring cache if it has a mapping for this mobile node. If the entry for the mobile node has not expired, the new AR forwards the packets destinated to the new Care-of address of the mobile node to it.

On the other hand, as soon as the mobile node receives an acknowledgement for the new Care-of address, it registers it with its home agent and its correspondents. To do so, it sends a *Binding Update* (step 5), as required in MIPv6 [5].

Nevertheless, according to the mobility pattern and the movement speed, a lot of cases can take place. For example, the mobile node cannot always keep the connection with the old AR during all the procedure; sometimes, the mobile disconnects as soon as it receives the *Proxy Router Advertisement*. In this case, it can send the *Fast-Binding Update* under the new AR. Several special cases like this can occur and we evaluate this protocol in most of them in 4th section.

2.2.2. *Tunnel-Based Handover*

The Tunnel-Based Handover is the establishment of a bidirectional tunnel between the old and the new AR for the mobile node. The mobile node attaches to a new AR, but it only performs a L2 handover, i.e. the mobile node continues to use its old Care-of address in the new network. Moreover, the mobile node does not need to exchange any packet: only the two AR communicate together in order to set up the bidirectional tunnel from the L2 events.

The two basic L2 triggers needed are the L2 handover start and the L2 handover end. If the AR receives a source trigger or a target trigger, the time to set up the bi-directional tunnel is shorter because they know in advance that the mobile node begins or ends a L2 handover.

First an AR (the old one or the new one) receives a L2 trigger (step 1 in figure 5) about the movement of the mobile node. This trigger must contain the L2 address of the mobile node and the IP address of the other AR. Then the receiving AR sends a *Handover Initiate* (step 2) to request a tunnel between him and the other AR. This *Handover Initiate* contains the L2 address of the mobile node and the lifetime of the tunnel. If it is the old AR which sends the *Handover Initiate*, it must add the old Care-of address and the home address of the mobile node.

At the reception of the *Handover Initiate*, the AR replies with a *Handover Acknowledgement* (step 3 in figure 5). If this message is sent by the old AR, it must include the old Care-of address and the home address of the mobile node because the new AR does not know this information in this instance. Finally, when the old AR detects that it lost its connection with the mobile node (Link Down) (step 4), it begins the forwarding. On the other hand, when the new AR detects that it has a connection with the mobile node (Link Up) (step 5), it begins to forward the packets to the mobile node and forwards the out coming packets.

2.3. IEEE 802.11b: practical analysis

The IEEE 802.11b [3], mainly developped in the USA, aims to manage wireless communications. IEEE 802.11b is the wireless equivalent of the well-known IEEE 802.3 [4] (i.e. Ethernet). This is the most used protocol in Wireless LAN and several products are already available. To ensure interoperability among different vendors products, the specification defines a radio propagation model interface, an encoding and modulation method, and a MAC layer.

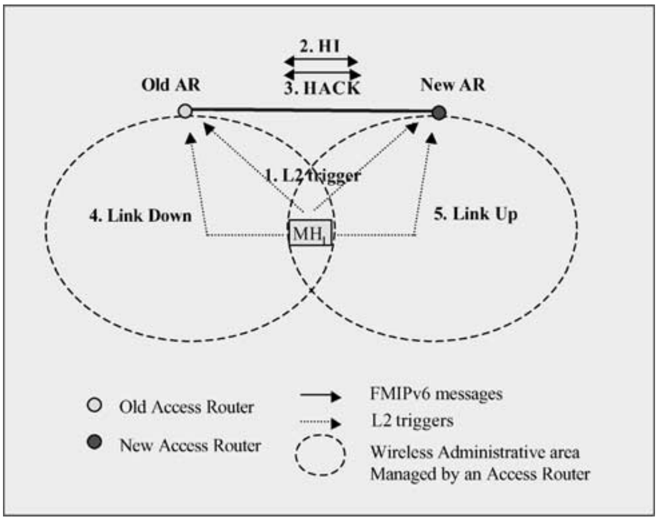


Figure 5. Tunnel-Based Handover.

We mainly focus on IEEE 802.11b in order to have an overview of the real mobile node possibilities over wireless LAN. In particular, it is interesting to evaluate the delay required to move between access points (L2 handover), the offered throughput with respect to the number of users and the triggers really available. In subsection 2.3.1 we first outline IEEE 802.11b: the topology, the medium access, the backoff algorithm, and the roaming. Then we give the results of the tests we made to evaluate the observed useful bandwidth per user and the handover latency between two access points.

2.3.1. Overview of IEEE 802.11b

IEEE 802.11b enables two operational modes. The first one is the ad hoc mode where there is no central point. The stations communicate directly if they can hear each other. The second is the infrastructure mode, where all the communications occur via an access point. An access point is a dedicated equipment which has at least one wireless interface and one wired interface. It is a bridge between the wired network and the wireless LAN. The communications occur within the cover area of the access point. One or more mobile nodes connected to an access point are called a BSS (Basic Service Set) and several BSS connected together through an Ethernet link under the same subnet are called an ESS (Extended Service Set). The basic topology is illustrated in figure 6.

When several mobile nodes are connected to an access point, they must share the channel access. IEEE 802.11b defines two access methods: the basic protocol DCF (Distributed Coordination Function) which is a CSMA/CA MAC protocol, and PCF (Point Coordination Function) where a point coordinator determines which mobile node is given the right to transmit.

The DCF protocol defines two methods. The first is a basic access mechanism where the destination node immediately replies with a positive acknowledgement upon a successful packet reception (see figure 7). When a mobile node wants to transmit, it senses the channel to determine whether another mobile node is transmitting. If the channel is idle, the mobile node waits for a Distributed InterFrame Space (DIFS) and be-

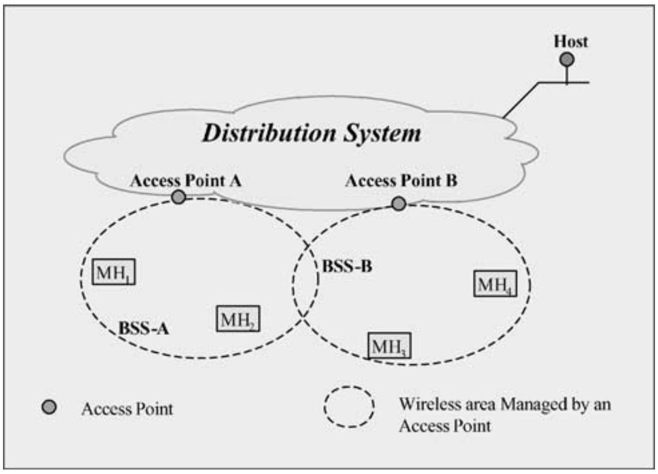


Figure 6. IEEE 802.11b topology.

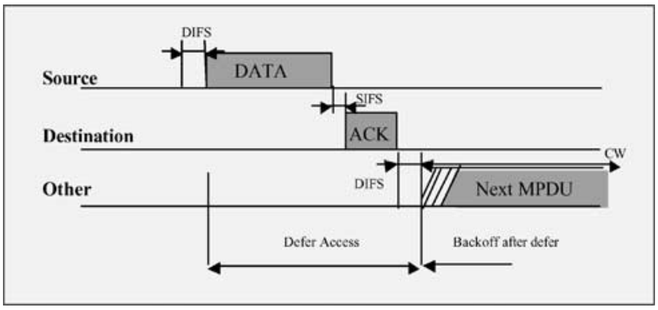


Figure 7. Basic mechanism in DCF.

gins its transmission. Upon the reception of the frame, the destination node waits for a Short InterFrame Space (SIFS) before sending the ACK. The acknowledgement is necessary to inform the transmitting node that the transmission was successful because a mobile node cannot listen to its own transmission on the radio interface.

Otherwise, if the channel is busy when the mobile node senses the channel, it must defer its transmission (the line "other" in figure 7). Then the mobile node performs a backoff algorithm to determine the time to wait before it can resume channel sensing. The backoff algorithm consists in choosing a random number called the backoff timer within an interval that increases with the number of collisions. The mobile node only decreases the backoff timer when the channel is idle. When the backoff timer reaches zero, the mobile node can sense the channel to transmit.

The second mechanism of the DCF protocol is the RTS/CTS (Request To Send/Clear To Send) system. In this mechanism, before transmitting a packet, a mobile node exchanges RTS/CTS frames with the destination to reserve the channel. To do so, the transmitting node sends a RTS to the destination node to notify all the nodes in the BSS about the transmission. The destination node replies with a CTS to acknowledge the transmission. If a collision occurs, the transmitting node performs the backoff algorithm. This mechanism allows a transmitting node to detect a collision faster than with the basic access mechanism. The RTS/CTS are indeed short frames when compared to the data frames, and the collision only occurs on the RTS/CTS frames. Therefore the collision detection is faster. However, without collision, this mechanism delays data transmission since it requires the transmission of two additional frames with respect to the basic mechanism.

When a mobile node enters in a new BSS, after an idle mode or after moving, it needs to synchronize itself with the access point. To do so, the mobile node has two possibilities: the passive scanning where it waits for a signalization frame periodically sent by the access point, or the active scanning where the mobile node sends a *Probe Request* frame to solicit a *Probe Response* frame. Once the mobile node is synchronized with the access point, it enters into an authentication procedure. If the authentication is successful, the mobile node starts an association process where the access point informs the mobile node about the transmission parameters in the BSS (e.g., the data rate and the transmission power). Once the association completes, the mobile node can communicate via the new access point. The roaming process also known as L2 handover is illustrated in figure 1.

When cover areas of different access points share a common cover zone, the mobile node can roam between the access points. A mobile node associates itself with the access point which offers the best signal or which has the minimum load among the access points. The time needed to roam between two access points is evaluated in the following subsection.

2.3.2. Performance evaluation

In this subsection we present the measurements we obtained with IEEE 802.11b. We used up to six mobile nodes and two access points. First, we present the throughput we measured with respect to the number of users and the different raw bandwidths with the basic mechanism of the DCF. Next, we present the handover latency for an idle mobile node, a low-transmitting mobile node and a fast-transmitting mobile node for different raw bandwidths.

2.3.2.1. The useful bandwidth in IEEE 802.11b We configure the access point to offer 1, 2, 5.5 and 11 Mb/s, respectively. Then, for each raw bandwidth, we measured the throughput per mobile node for an increasing number of users. The results are presented in the figure 8 where each curve represents the throughput for a given raw bandwidth in Bytes.

For a single user, the observed throughput is much smaller than the raw bandwidth: 682 KB/s for 11 Mb/s, 420 KB/s for 5.5 Mb/s, 182 KB/s for 2 Mb/s and 95.5 KB/s for 1 Mb/s. On the other hand, the raw bandwidth usage is proportionally better for the low rate: the ratio between the throughput and the raw bandwidth increases when the raw bandwidth decreases. This result is shown in table 1 where the ratio is calculated as follows:

$$\text{ratio} = \frac{\text{throughput} \times 8 \times 1000}{\text{bandwidth}}.$$

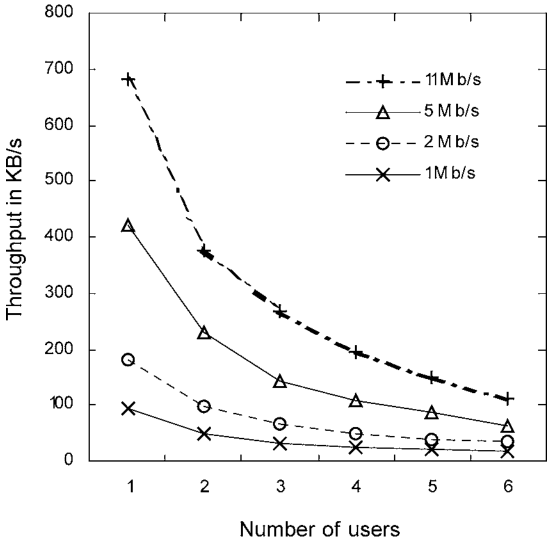


Figure 8. Achieved throughput per mobile node.

Table 1
Ratio between the throughput and the raw bandwidth for a single user

Raw bandwidth	1 Mb/s	2 Mb/s	5.5 Mb/s	11 Mb/s
Ratio	0.496	0.610	0.728	0.764

Moreover, when the number of users increases, the throughput per user strongly decreases: for 11 Mb/s, the throughput is reduced from 682 KB/s down to 110.1 KB/s and for 1 MB/s the throughput is reduced from 95.5 KB/s down to 16.7 KB/s. Therefore from the above results, we can conclude that the number of users is quite restricted per access point. We can presume that from 30 active users on an access point, the throughput on a mobile node is too limited to receive or transmit multimedia traffic like video or voice over IP.

2.3.2.2. The IEEE 802.11b handover latency As explained above, a mobile node can roam between adjacent access points. We measured the handover latency in IEEE 802.11b, i.e. the time needed for a mobile node to attach to a new access point. The mobile node detects that it moves to a new access point by the beacon sent by the access point. The beacon interval used in the tests is 100 ms, which is the default in the specification [3]. The first set of tests considers a single mobile node which roams between two access points with no other mobile nodes connected to the same access point. The results obtained with the four raw bandwidths are presented in figure 9.

We notice on figure 9 that the handover latency is bounded between 0.144 and 0.177 s whatever the bandwidth, and the average handover latency is 0.158 s. The handover latency is shorter for an idle node than for an active node for all the raw bandwidths except for a bandwidth of 1 Mb/s. Moreover, for all the raw bandwidths, the handover latency is shorter for a low-transmitting mobile node than for a fast-transmitting mobile node. Furthermore, the handover latency is longer for low bandwidth than for high bandwidth: for 1 and 2 Mb/s, the average handover latency is 0.165 s and it is equal to 0.152 s for 5.5 and 11 Mb/s.

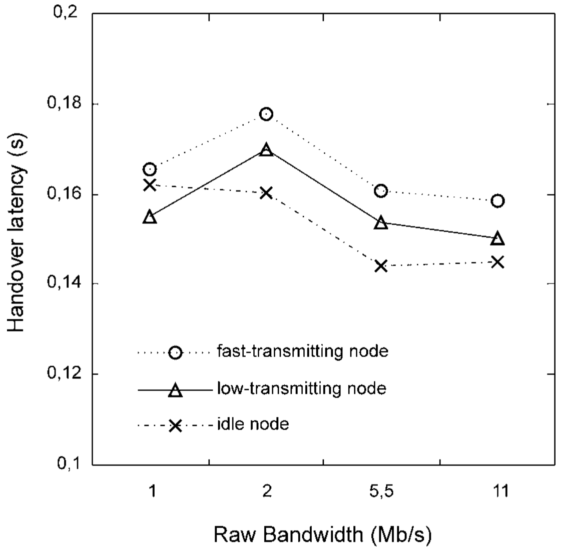


Figure 9. Handover latency in IEEE 802.11b for a single mobile node.

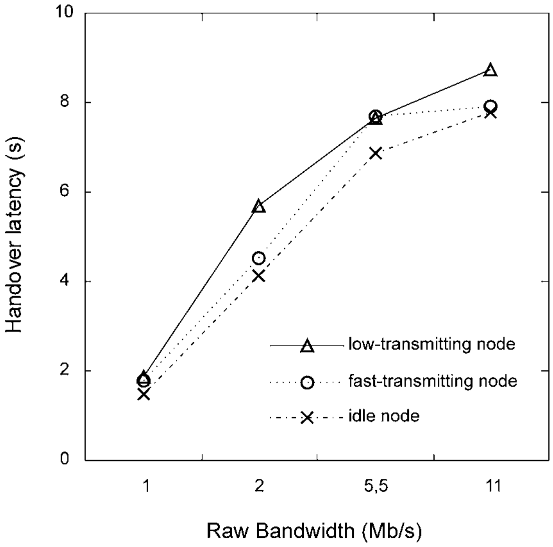


Figure 10. Handover latency in IEEE 802.11b for six users.

This handover latency has been measured in the optimal case, where the user is alone. The curves in figure 10 represent the handover latency when there are five users in addition to the roaming node.

The handover latency measured when there are six users are much longer than the latency observed with a single user: the average value is 5.511 s, the minimum is 1.490 s and the maximum goes up to 8.729 s. This average handover latency is more than 30 times greater than the one measured for a single user. The handover latency is shorter for an idle node whatever the raw bandwidth. On the contrary, the handover latency of a low-transmitting node is longer than the handover latency of a fast-transmitting node. For example, for 11 Mb/s, the handover latency is 7.796 s for an idle node, 7.897 s for a fast-transmitting node and 8.729 s for a low-transmitting node. These handover latencies are very long and totally incompatible with real time multimedia applications.

As soon as the access point manages the communications of several mobile nodes, the access to the channel is delayed. If we increase the beacon interval, the mobile node will detect the new access point earlier. However the beacons sent use the throughput and this can delay the authentication and association procedures.

3. MIPv6 and FMIPv6 evaluation

In this section, we compare the handover latency in MIPv6 with the handover latency in FMIPv6 over Wireless LAN IEEE 802.11b. For MIPv6, we consider basic MIPv6 and the forwarding from a Home Agent in the old subnet (see section 1). For FMIPv6, we evaluate the Anticipated Handover in two different cases and also determine the Tunnel-Based Handover in a single case. We then show the variation of the handover latency in FMIPv6 with different bandwidths.

3.1. Hypothesis

In all the following tests, we determine the time during which the mobile node cannot send or receive packets. We do not focus on the number of lost packets, or on the time needed to complete the different protocols, but we do rather concentrate on the disruption time in the mobile node communications. In all the cases, we use the L2 handover latency over IEEE 802.11b that we found in the second section and we do not consider the time required for messages processing (e.g., the time to process a *Binding Update*).

A critical issue in the mobility is to execute the duplicated address detection (DAD) when the mobile node acquires a new Care-of address. Performing DAD indeed generates too much delays in the handover latency. Considering that the probability of address duplication on the same link is extremely low, the mobile node could choose not to perform DAD. Moreover, FMIPv6 allows the use of the old Care-of address during the DAD execution to minimize the impact of the DAD.

3.1.1. MIPv6

The handover latency in basic MIPv6 is the time needed to detect that the new access point is on a new subnet, in addition to the round trip time to reach a correspondent. The way it is defined in MIPv6 [5], the recommended *Router Advertisement* interval is between 0.05 and 1.5 s. We then consider three cases: an optimal case where the mobile node receives the *Router Advertisement* immediately after the L2 connection, an average case where the mobile node receives it after 50 ms, and a worst case where the mobile node receives it after 1500 ms. This L3 handover latency must be added to the L2 handover latency to derive the total disruption time.

In the forwarding case, where the mobile node requests a Home Agent on its old link to forward all packets from and to the mobile node, the handover latency is calculated like the basic case except for the round trip time. The mobile node only needs to send a *BU* to its old subnet instead of sending it to a correspondent somewhere in the Internet. The three detection cases (immediately after the L2 connection, with a 50 ms or 1500 ms delay) are also considered.

3.1.2. FMIPv6

All the results for FMIPv6 are based on stateless address configuration. However, with stateful address configuration, if the mobile node can remain in the old subnet during the time the new AR performs DHCPv6 [1] for it, the disruption time will be the same as in the case of stateless address configuration.

We consider two cases in the Anticipated Handover for FMIPv6. First, we evaluate the best case where the mobile node has enough time to send the F-BU and the F-BACK while it is still connected to the old AR. We also suppose that the new AR detects the L2 connection of the mobile node through the L2 triggers. Consequently, the new AR starts forwarding the packets tunneled by the old AR. Second, we consider the worst case where once the Anticipated Handover is initiated, the mobile node disconnects from the old AR and begins the L2 handover. The initiation is done by the transmission of the *Router Solicitation for Proxy* in the mobile controlled handover, or by the reception of an unsolicited *Proxy Router Advertisement* in the network controlled handover.

In the Tunnel-Based Handover, the two AR establish a bidirectional tunnel for the mobile node without any interaction with it. We consider that the new AR receives a L2 trigger when the mobile node begins its L2 handover (the first *Probe Request* sent by the mobile node). During the time the mobile node performs the L2 handover, the two AR set up the tunnel.

3.2. Comparison

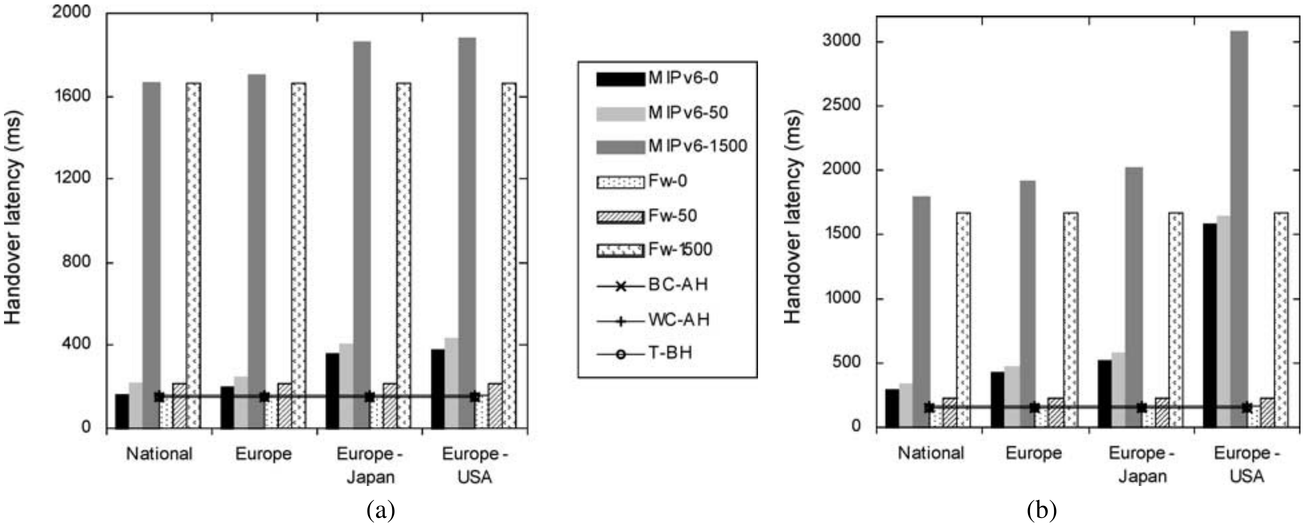
First we are going to analyze the handover latency for FMIPv6 and MIPv6 when the mobile node is the only node within the access point cell. The results for a bandwidth of 11 Mb/s are presented in figure 11. In this figure, “Fw” means the forwarding method of MIPv6, “BC-AH” and “WC-AH” means the best and the worst case in Anticipated Handover, and “T-BH” means Tunnel-Base Handover.

The handover latency measured for a single node is comprised between 151 ms for the Tunnel-Based Handover up to 1877 ms for the minimum value in the worst case in MIPv6 (figure 11(a)) and up to 3084 ms for the maximum value in the same case (figure 11(b)). We can also see that the results obtained with FMIPv6 are always better than those obtained with MIPv6. The handover latency in FMIPv6 is always around 160 ms whatever the localization of the correspondent since the mobile node only deals with the local AR. The forwarding method in MIPv6 is also constant whatever the localization of the correspondent since the mobile node does not send messages to it. In fact, the handover latency when the mobile node immediately receives the new *Router Advertisement* is similar to the worst case in the Anticipated Handover. This is due to the fact that in the Anticipated Handover, the mobile node needs to send a F-BU to the old AR through the new AR before the old AR forwards packets. This mode of operation is very close to the Forwarding MIPv6 algorithm. But in Anticipated Handover, the mobile node has a new valid Care-of address after the procedure, while in forwarding MIPv6 the mobile node has not even started to acquire a new Care-of address.

We can also notice that the minimum value observed in the best case of MIPv6 for a national correspondent is close to the handover latency observed in FMIPv6 (see figure 11(a)): 163 ms for MIPv6 compared to 152 ms. Actually, the minimum time to notify a national correspondent can be very short, especially if the correspondent is within the same domain as the mobile node. This time can be close to the round trip time between the old and the new AR. Nevertheless, handover latency induced in MIPv6 increases with the distance between the mobile node and its correspondent.

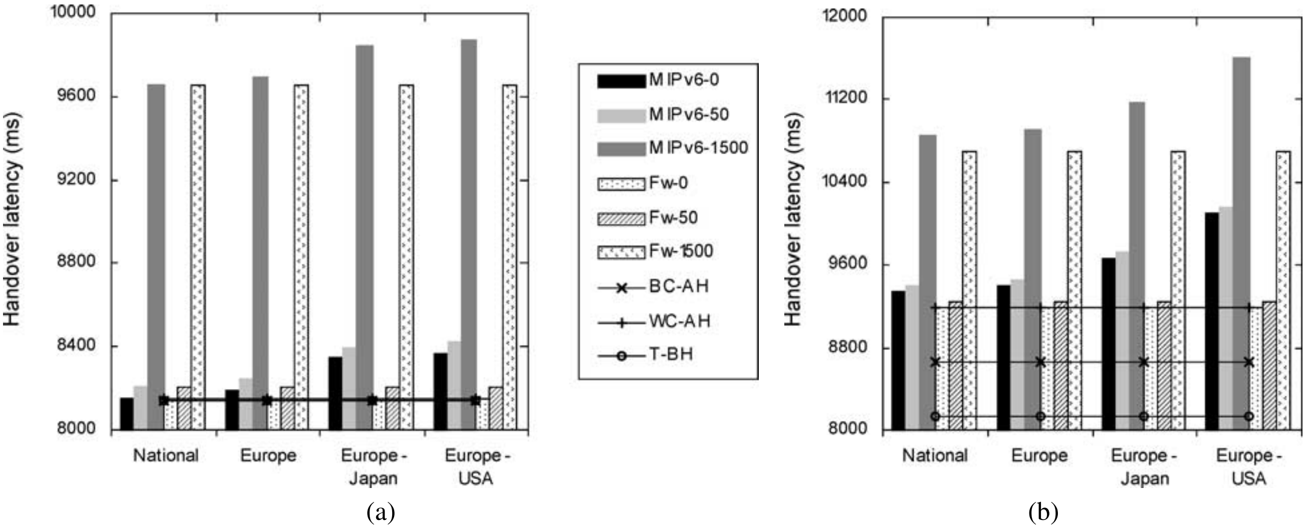
We only show these results for a single user because the results with other bandwidths are similar.

In the next two figures (figures 12 and 13) we analyze the variation of the handover latency in an average case where the



(a) (b)

Figure 11. (a) Minimum and (b) maximum L3 handover latency for a single user at 11 Mb/s.



(a) (b)

Figure 12. (a) Minimum and (b) maximum L3 handover latency for six users at 1 Mb/s.

mobile node shares the available bandwidth with five other nodes. The results for a bandwidth of 1 and 11 Mb/s are also presented in figures 12 and 13.

First we can see an important difference in the handover latency in comparison to the previous case. In figure 12(a), the handover latency is comprised between 1723 ms for the Tunnel-Based Handover (compared to 151 ms for a single user) and 3517 ms for the worst case in MIPv6 (compared to 1877 ms for a single user). The maximum handoff latency is over 11600 ms for the maximum value in the worst case in MIPv6 (figure 13(b)). This is due to the results we observed in the IEEE 802.11b section. When several nodes share an access point cell, the L2 handover latency is very important and can reach up to 8 s. Furthermore, the time needed to send a packet over the wireless interface is much more important than when the mobile node is alone in the access point cell.

In this situation, the difference between the cases of FMIPv6 becomes more important, especially when considering the maximum values (figures 12(b) and 13(b)). Once more, this comes from the difficulty to have access to the shared channel. Each message sent over the air causes a significant delay in the handover latency. Therefore, the disruption time becomes more important with the number of packets sent over the wireless interface. For instance, for a bandwidth of 1 Mb/s (see figure 12(b)), the handover latency takes 1723 ms in Tunnel-Based Handover, 4478 ms in the best case of Anticipated Handover and 7244 ms in the worst case of Anticipated Handover. This is due to the fact that the Tunnel-Based Handover does not require the mobile node to send packets, and the worst case of Anticipated Handover requires more messages from the mobile node than from the best case. In conclusion, the limitation of the mobile node interaction in the protocol procedure optimizes the mobile node L3 handovers.

However, the Tunnel-Based Handover defers the new Care-of address creation and allocation while once the Anticipated Handover completes, the mobile node has a new valid Care-of address. The handover latency in Tunnel-Based

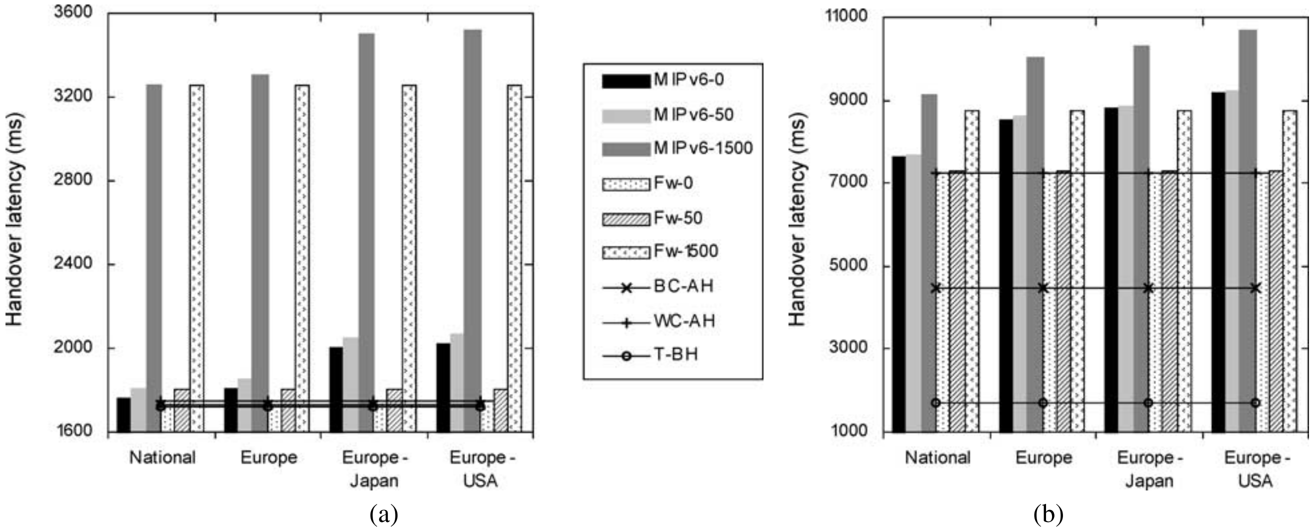


Figure 13. (a) Minimum and (b) maximum L3 handover latency for six users at 11 Mb/s.

Handover is thus lower but requires network resources for the forwarding.

Otherwise, we can still see that the handover latency in the best case of the forwarding method in MIPv6 remains equivalent to the latency in the worst case of the Anticipated Handover (see figures 12 and 13).

Therefore, even with multiple users under the same access point, the handover latency involved in FMIPv6 is shorter than in MIPv6. However, the disruption times we found are not suitable for real time applications, except when the user is alone and uses FMIPv6. Moreover, if we realize these tests over another wireless LAN which uses a separated control channel, the L2 handover latency and the time to access the channel will certainly be better (because the data frames do not interact with the control channel). This will be the subject of later studies.

3.3. The FMIPv6 handover latency

It can be interesting to evaluate in details the impact of the bandwidth on the handover latency in FMIPv6 more. To be more complete, we consider an average case in Anticipated Handover where the mobile node managed to send the F-BU before beginning the L2 handover but where it has not received the F-BACK when it establishes the L2 connection with the new AR.

We first compare the three cases of the Anticipated Handover and the Tunnel-Based Handover for a single user according to different bandwidths. The figure 14 represents the observed L3 handover latency. The handover latency is comprised between 151 ms for the Tunnel-Based Handover up to 186 ms for the worst case of the Anticipated Handover. The handover latency in Tunnel-Based Handover is always shorter than the Anticipated Handover. Since the L2 handover latency tends to reduce with the bandwidth increasing (see section 2), the L3 handover latency also reduces when the bandwidth increases. In all these cases, FMIPv6 gives good results because it does not introduce much more delay to the L2 handover latency, even in the worst case.

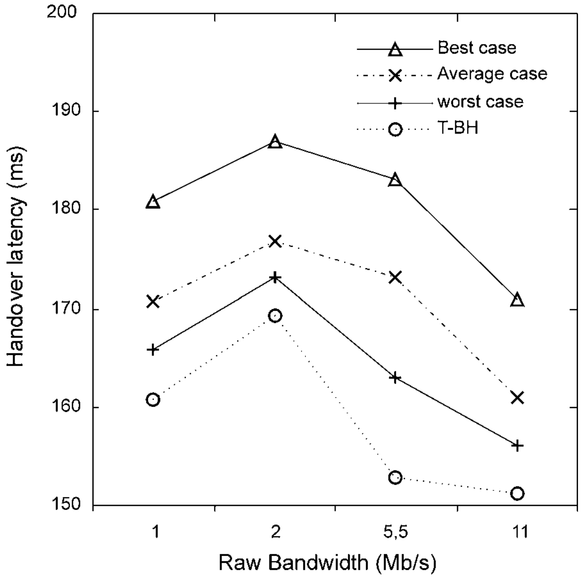


Figure 14. L3 handover latency in FMIPv6 for a single user.

Figure 15 shows the FMIPv6 handover latency for different bandwidths, when the mobile node shares an access point cell with five other wireless nodes. The results are totally different from the single mobile node case. First, the handover latency increases with the bandwidth. This is due to the L2 handover we observed in IEEE 802.11b in section 2. Second, the difference between the cases is more important: with a bandwidth of 1 Mb/s, the handover latency in Tunnel-Based Handover is 1723 ms while in the average case of the Anticipated Handover it is 7235 ms, i.e. almost four times in addition. Already with six users, the access to the channel is much deferred as we saw in the above comparison. However, the differences between the cases decreases for higher bandwidths. For a bandwidth of 11 Mb/s, the difference between the latency in Tunnel-Based Handover and the latency in the

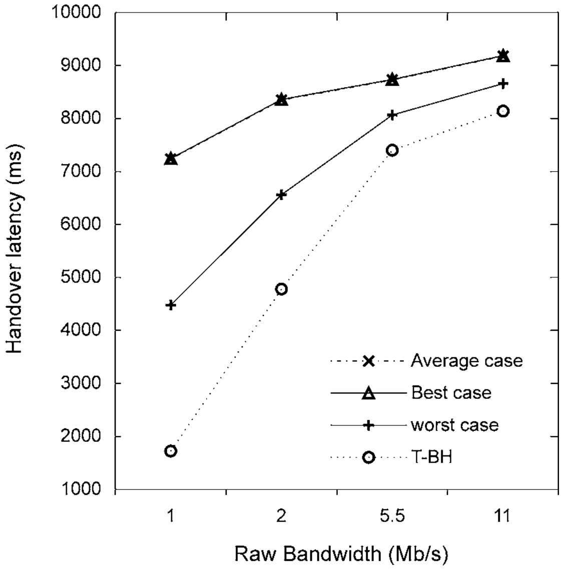


Figure 15. L3 handover latency in FMIPv6 for six users.

worst case of Anticipated Handover is 1047 ms. Future Wireless LAN specifications offering better bandwidth could still reduce the impact of the channel access.

4. Conclusion

This paper aims to analyze and evaluate the L3 handover latency over wireless LAN. We compared the handover latency in Mobile IPv6 with the handover latency in the two methods of Fast Mobile IPv6, namely the Anticipated Handover and the Tunnel-Based Handover. To calculate the disruption time, we used measures made over IEEE 802.11b.

The first observation we made was that the L2 handover latency over IEEE 802.11b can be very important. When there are several users connected to an access point, the L2 handover strongly increases and the available throughput for a mobile node becomes very restricted.

The comparison between MIPv6 and FMIPv6 showed us that FMIPv6 offers shorter disruption times. However, the optimal cases in MIPv6 are close to the times with FMIPv6. Apart from the L2 limits, MIPv6 is restricted by the time needed to detect the new network prefix, and by the localization of the correspondents. Furthermore, we did not take into account the time to perform DAD, which, if it is completed, increases the disruption time.

Otherwise, in FMIPv6 we saw that the Tunnel-Based Handover introduces less latency than the Anticipated Handover, especially when there are several users connected to the wireless access point. This is due to the fact that the mobile node does not need to interact with the AR. With an important load of the access point, each message sent over the wireless interface is greatly delayed. However, in the Tunnel-Based Handover, the mobile node must continue to use its old Care-of address while in the Anticipated Handover, the mobile node has a new Care-of address.

The most of these results introduces unacceptable delays for real time applications. In particular in FMIPv6, the principal overhead is due to the L2 properties. It will be interesting to realize the same tests over a different technology that deploys a dedicated control channel to accelerate the control messages transmission. In our future work, we plan to evaluate more protocols to analyze problems like the “ping-pong” effect and the handover between different access technologies.

References

[1] J. Bound, M. Carney, C. Perkins and R. Droms, Dynamic Host Configuration Protocol for IPv6 (DHCPv6), Internet Engineering Task Force (IETF) draft-ietf-dhc-dhcpv6-20.txt (October 2001).

[2] G. Dommety, A. Yegin, C. Perkins, G. Tsirtsis, K. El-Malki and M. Khalil, Fast handovers for mobile IPv6, Internet Engineering Task Force (IETF) draft-ietf-mobileip-fast-mipv6-02.txt (July 2001).

[3] IEEE 802.11b: IEEE Std 802.11-1999.

[4] IEEE 802.3: IEEE Std 802.3ad-2000.

[5] D. Johnson and C. Perkins, Mobility support in IPv6, Internet Engineering Task Force (IETF) draft-ietf-mobileip-ipv6-15.txt (July 2001).

[6] J. Kempf, D. Funato, K. El-Malki, Y. Gwon, M. Petterson, P. Roberts, H. Soliman, A. Takeshita and A. Yegin, Supported optimized handover for IP mobility – requirements for underlying systems, Internet Engineering Task Force (IETF) draft-manyfolks-l2-mobilereq-01.txt (November 2001).

[7] J. Manner, M. Kojo, T. Suihko, P. Eardley, D. Wisely, R. Hancock and N. Georganopoulos, Mobility related terminology, Internet Engineering Task Force (IETF) draft-manner-seamoby-terms-01.txt (March 2001).

[8] T. Narten, E. Nordmark and W. Simpson, Neighbor discovery for IP version 6, Internet Engineering Task Force (IETF) RFC 2461 (December 1998).

[9] Z. Shelby, D. Gatzounas, A. Campbell and C.-Y. Wan, Cellular IPv6, Internet Engineering Task Force (IETF) draft-shelby-seamoby-cellularipv6-00.txt (November 2000).

[10] H. Soliman, C. Castelluccia, K. El-Malki and L. Bellier, Hierarchical MIPv6 mobility management, Internet Engineering Task Force (IETF) draft-ietf-mobileip-hmipv6-05.txt (July 2001).

[11] S. Thomson and T. Narten, IPv6 stateless address autoconfiguration, Internet Engineering Task Force (IETF) RFC 2462 (December 1998).

Nicolas Montavont received his B.Sc. (1998) and his M.Sc. (2001) in computer science from the Universities of Lyon and Strasbourg (France), respectively. Currently, he is studying toward a Ph.D. within the Network Research Team at LSIIT laboratory. His research work has included IP mobility, multiple interfaces management and wireless LAN architectures.
E-mail: montavont@dpt-info.u-strasbg.fr

Thomas Nöel is assistant professor at the Louis Pasteur University, Strasbourg – France. He is member of the network research team of the LSIIT Laboratory. He received his M.Sc. in 1995 and Ph.D. in computer science in 1998. His research interests include network architectures, protocols and more especially wireless IP networks and multicast routing protocols for mobile IP nodes.
E-mail: Thomas.Noel@dpt-info.u-strasbg.fr