ANALYSIS OF A GEOLOCATION-BASED FMIPv6 EXTENSION FOR NEXT GENERATION WIRELESS LANS

Julien Montavont [1], Emil Ivov [1], Thomas Noel [1] and Karine Guillouard [2]
[1]LSIIT UMR CNRS 7005
Louis Pasteur University Strasbourg, France
{montavontj,Ivov,Thomas.Noel}@dpt-info.u-strasbg.fr

[2]France Telecom - 4 rue Clos Courtel, BP 91226
F-35512 Cesson Sevigne Cedex, France
karine.guillouard@orange-ftgroup.com

ABSTRACT

Innovation in wireless technologies is changing the Internet and the way users connect. It is now possible to communicate while on the move. However, the standard procedures that enable user mobility across networks do not match the requirements of real-time communications in terms of delay and packet loss. The FMIPv6 protocol, lately accepted as standard for managing seamless mobility, addresses most of the problems related to handover latency. Yet, certain issues specific to wireless LAN, such as Access Point Discovery still prevent FMIPv6 from making the entire roaming procedure seamless for Wi-Fi networks. In this article, we present an extension of the FMIPv6 protocol that addresses these problems. Our proposal uses the geographical position of the devices in order to anticipate their moves and make them attach to the wireless access points that best fit their location and expected trajectory. We also present an evaluation of our work based on the implementation of the proposal.

Keywords: Next Internet Generation, Network Mobility, wireless LANs, Fast Handovers, Geolocation.

1 INTRODUCTION

IP version 4 (IPv4) [7], the protocol used over the Internet for data delivery between hosts, is now nearly twenty years old. Even though it has been efficient during the past years, issues related to address shortage and route maintenance are beginning to appear. In the same time, the increasing popularity and improving characteristics of wireless technologies foster the appearance of new use cases involving mobility and raise the demand for non-interrupted Internet connectivity. The new version of the Internet Protocol (IPv6) [6] is trying to resolve these issues by extending the address space from 2^{32} to 2^{128} Internet addresses. It also defines a method for adding new options or extensions to the IP header. The Mobile IPv6 (MIPv6) [2] protocol, which is the Internet Engineering Task Force (IETF) standard for managing IPv6 mobility, uses this extension mechanism. The protocol allows Mobile Nodes (MN) to roam among IPv6 subnets without having to interrupt their communication with remote hosts. However, this protocol still suffers various limitations such as its poor support (or lack thereof) for rapid and seamless handovers. As a result, the mechanisms introduced by the MIPv6 protocol may cause user-perceptible connection loss and breaks, that degrade the quality of time-sensitive communication. During the last few years, there have been many optimizations that address the handover latency related to the MIPv6 mechanisms. Among these is the Fast Handovers for Mobile IPv6 (FMIPv6) [3] protocol which has lately been standardized by the IETF community. Many previous works and evaluations of this protocol, including some of our own, have shown that FMIPv6 may be very efficient for achieving seamless handover. However, as FMIPv6 remains a layer 3 only solution (i.e. with no link layer dependencies), it leaves unresolved various issues related to handovers in wireless LANs such as the discovery of candidate Access Points (AP). During this part of the FMIPv6 procedure, an MN would discover APs available in the vicinity. For wireless LANs this may introduce significant delays and/or cuts in the ongoing communication of the MN. In addition, the proposed method does not provide MNs with a way to choose their next APs according to their location, or available resources. In this document we present an

FMIPv6 extension that enhances the discovery of candidate APs in wireless LANs. We use geolocation information in order to anticipate the trajectory of MNs and select their next APs accordingly. This way MNs would obtain the parameters of their next APs (and the layer 3 parameters of the IPv6 subnet behind them) without having to interrupt their ongoing communications. Do notice that our method could be easily extended to other wireless technologies.

Performance evaluation of network mobility protocols or optimizations available in related literature is often based on theoretical studies, and simulations. We do believe, however, that many of the reasons why handover latency occurs are closely related to implementations and operating system specifics that are most often ignored in simulators or theoretical studies. Furthermore, simulation models tend to over simplify the wireless link and ignore the effects of interference and the complexity of propagation effects. These are the reasons why in this article, we have completed an entirely empirical study based on real experiments that evaluate our FMIPv6 extension. This analysis uses the new FMIPv6 Open Source Implementation Suite [21] for the GNU/Linux operating systems.

The rest of this document is organized as follow. First, we describe the mobility mechanisms introduced by the MIPv6 and the FMIPv6 protocols and provide a brief overview of the layer 2 handover management in wireless LANs. Section 3 describes our geolocation based FMIPv6 extension followed by Section 4 where we present the testbed that we have set up and used for experiments. All our measurement results are presented in Section 5, followed by a conclusion in Section 6.

2 EXISTING STANDARDS FOR MOBILITY MANAGEMENT

This Section provides an overview of the mechanisms and protocols related to the support of handovers in IPv6 wireless LANs.

2.1 IEEE 802.11

The first version of the IEEE 802.11 standard [1] was released in 1997 and describes wireless LANs as they are currently known. Since, the IEEE has been constantly improving this technology (also known as Wi-Fi), its throughput, reliability and security. Today, the IEEE 802.11 networks are very popular and are one of the most popular ways for connecting to the Internet.

Given the relatively limited coverage area of 802.11 access points, roaming Mobile Nodes are likely to often switch from one AP to another. The procedure that a node would go through during such reconnections (referred to as layer 2 handover) is defined by the IEEE 802.11 standard and consists in three major steps: discovery, authentication and association. These steps are illustrated in Fig. 1.

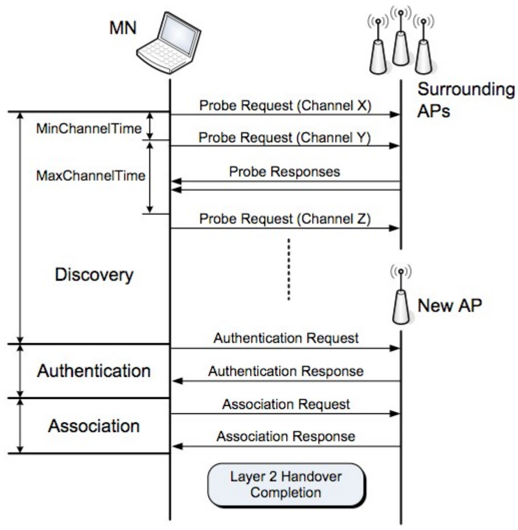

Figure 1: Standard IEEE 802.11 handover

Once an MN is required to attach to a new AP, it would first have to discover the surrounding APs and select the one that best suits its need. To discover surrounding APs, an MN would perform either passive or active (or both) scanning. The active scanning consists in broadcasting Probe Requests and listening for responses. In passive scanning, the MN just listens to the beacon frames sent periodically (approximately every 100ms) by APs. The standard defines the MinChannelTime and MaxChannelTime parameters which are respectively the minimum and the maximum amount of time that an MN has to scan (either actively or passively) a 802.11 radio channel. If an MN does not detect any APs on a specific radio channel during MinChannelTime, it switches its channel and starts scanning the new one. If at least one AP is detected, the MN remains on the radio channel for MaxChannelTime in order to detect any other APs that might be using it. After scanning all (or a subset of the) 802.11 radio channels, the MN selects its new AP and starts an authentication process. Note that the IEEE 802.11 standard does not define any numerical values for MinChannelTime or MaxChannelTime and therefore they may vary from one hardware manufacturer to another.

The second part of the layer 2 handover consists in an exchange of Authentication Request / Response frames between the MN and the new AP. The MN sends its identity to the AP which may accept or reject its request. Upon successful authentication, the MN starts the association process and completes the layer 2 handover. It is important to note that an MN is not able to communicate while performing a layer 2 handover.

According to results presented in [9], the layer 2 handover would generally take between 58.7ms and 396.7ms to complete. Approximately 90% of this time is taken by the discovery part [9]. According to [10], delays or cuts above 150ms cannot be compensated by jitter buffers and would generally cause user perceptible quality degradation.

2.2 Mobile IPv6

After attaching to the new AP an MN might in some cases be able to directly reestablish communication. Often however, the new AP would not belong to the same IPv6 subnet as the previous one. In such cases the MN would have to update its IPv6 address and default router, and make sure that flows initiated from its previous network location would be properly redirected to its current subnet. This is commonly handled by the Mobile IPv6 protocol.

The Mobile IPv6 (MIPv6) [2] protocol is an IETF standard that allows managing the mobility of IPv6 nodes. MIPv6 allows MNs to remain reachable at a primary IP address while roaming through different IPv6 networks. The protocol adopts the notion of a dedicated node, called a Home Agent (HA). The HA keeps up-to-date bindings between a primary Home Address (HoA, an address which belongs to the same IPv6 subnet as the HA itself) and a Care-of Address (CoA, an address valid only for the current network location of the MN). The HA acts as a relay station intercepting and forwarding all traffic bound for the MN to its current location (i.e. to its CoA).

In a wireless environment, once an MN roams to an AP that turns out to be on a new IPv6 subnet, the MN has to acquire a new CoA and then update its binding to the HA. These procedures are referred to as layer 3 handover. The discovery of the properties of an IPv6 subnet (also known as movement detection) is based on the reception of Router Advertisements that the local Access Router (AR) periodically broadcasts or sends in response to a Router Solicitation. Upon reception of a Router Advertisement, the MN can determine whether it has moved to a new IPv6 subnet in which case the MN would configure a new locally valid CoA. Most often it would do so through the IPv6 stateless autoconfiguration mechanism [4]. Next, the MN would inform the HA about its new location by sending its new CoA in a Binding Update (BU) message. When a corresponding Binding Acknowledgement (BACK) with a successful status code is received, the layer 3 handover is complete. This procedure is illustrated in Fig. 2.

Each stage of the layer 3 handover may introduce significant delays in the overall connection loss time during a handover. First, the minimal allowed delay between two consecutive Router Advertisements is between 0.03 and 0.07 seconds [2]. Therefore, in many cases, an MN would have to wait for 0.07 seconds before detecting layer 3 subnet change. In addition, after configuring its new IPv6 address and before actually being able to use it an MN needs to perform Duplicate Address Detection (DAD) in order to verify the uniqueness of this address. This detection may take several seconds to complete (approx. 1.5s for RFC default values) [4], [5]. Finally, the delay necessary for updating the binding with the HA depends on the Round Trip Time (RTT) between the MN and the HA.

Considering all of the above, total connection loss time during a handover would often be longer than 1 second [11], [12] which would probably be unacceptable for any kind of communication, and even more so for real-time traffic.

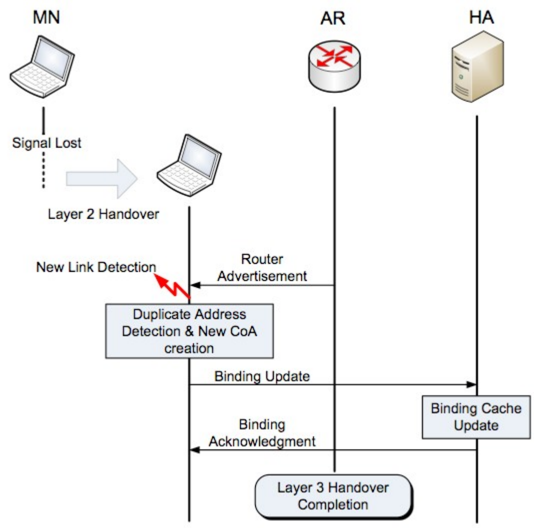

Figure 2: Layer 3 handover managed by the MIPv6 protocol

2.3 Fast Handovers for Mobile IPv6

The Fast Handovers for Mobile IPv6 (FMIPv6) [3] protocol is one of the most promising solutions that the IETF proposes in order to reduce the duration of the layer 3 handover and minimize the number of lost packets. The idea lying behind this protocol is to provide the MN with all properties of the IPv6 subnet it is going to move to, before it has actually done so. Moreover, FMIPv6 makes it possible for the next AR (the one the MN is moving to) to buffer all MN bound packets that arrive while the MN is disconnected because of the handover.

FMIPv6 defines a way for an MN to request from its current AR all layer 3 parameters of the IPv6 subnets behind neighboring APs. It also defines semantics that allow the optimization of the handover itself. If an MN is able to detect (e.g. through the use of link layer information) the need of a handover it could send a Fast Binding Update (FBU) to it's current AR. This message contains MN's current CoA and the AR that the MN is planning to switch to (referred to as NAR for Next Access Router). At that point the PAR (previously referred to as the current AR) sends to the NAR a Handover Initiate (HI) message containing the identity of the MN (link layer address, current CoA and, if known, desired next CoA). The NAR confirms (or rejects) the handover with a Handover Acknowledge (HACK) message that may provide further NAR specific details. Upon HACK reception, PAR sends a Fast Binding Acknowledgement (FBACK) back to the MN which (in this particular case) receives it on PAR's link. The MN is then ready to actually switch links. Once on NAR's link it sends a Fast Neighbor Advertisement (FNA) message which is supposed to update respective neighbor cache entries on the NAR so that it could stop buffering MN's packets and complete handover signaling.

The FMIPv6 protocol also defines a reactive handover scenario which basically represents the case where an MN could not anticipate a handover so it was able to only react once it was already in progress (hence the name). In that case the FBU is sent from NAR's link after layer 2 handover has completed and is usually encapsulated in the FNA. NAR then forwards that FBU to PAR, the HI/HACK message exchange follows as in the predictive case and PAR starts tunneling packets. Both FMIPv6 predictive and reactive modes are illustrated in Fig. 3.

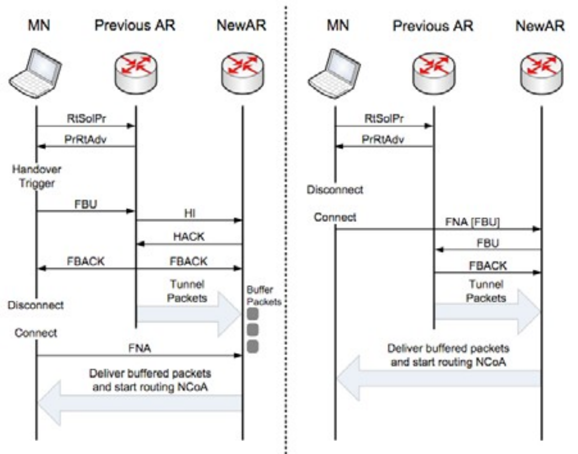

Figure 3: FMIPv6 protocol operation: Predictive mode (left) and Reactive mode (right)

Previous performance evaluations of FMIPv6, including some of our own, have shown that FMIPv6 is very efficient regarding the duration of connection disruption and the number of packets lost due to a handover. Our previous analysis has shown that FMIPv6 allows handover to remain transparent to users with no packet loss even when using real-time applications such as video streaming or conferencing [8]. Although we have noticed small delays on the reception of the buffered packets, these delays have no impact on the perception of the users. However, FMIPv6 is conceived as a layer 3 solution only and there is no mechanism designed to provide or efficiently discover the layer 2 parameters of surrounding APs (such as operating channels, Service Set Identifiers, etc.). The solution proposed by the IETF suggests that MNs periodically perform partial or complete scanning procedures in order to discover candidate APs for pending handovers [13]. However, in the case of Wi-Fi, such periodic scans may have a significant negative impact. Fig. 4 presents the results of a preliminary analysis of the mechanism presented in [13]. This study was performed with a wireless LAN card that supports IEEE 802.11b/g standards. The card is managed by the MADWiFi driver [14]. As we can see, a complete scanning procedure performed to discover the candidate APs takes, in this particular case, 1368ms to complete. As a result, the MN has lost 69 packets during this phase, which is unacceptable regarding the quality of an ongoing media flow and makes the seamless handover pointless.

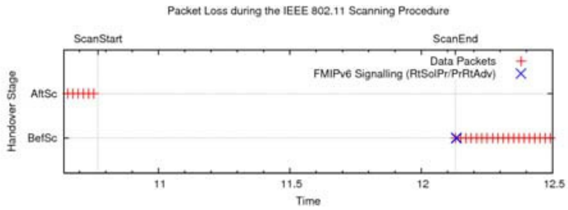

Figure 4: Packet loss and latency during a scanning for discovery of candidate access points

As we have mentioned earlier the seamless handover problem over wireless LANs has been addressed by a significant number of papers. Many of these provide optimization techniques that reduce the time necessary for a scan to complete. Some of them use geolocation information during the handover which we find especially well suited for assisting FMIPv6 and resolving the candidate AP discovery problem.

3 FMIPv6 ASSISTED BY GEOLOCATION INFORMATION

The goal of the proposed solution is to provide an optimized method for discovering candidate APs and remove the delay inherent to the standard procedure (i.e. periodically performing complete or partial scanning [13]). Following result from some previous work [8], we decided to extend the FMIPv6 mechanisms in a way that would allow taking into account the geographical position of an MN in order to anticipate its trajectory and choose its next AP accordingly. This way, based on its position, velocity and direction, an MN would be able to request from its current AR the parameters of the AP it is most likely to switch to. We also define several ICMPv6 options that an AR could use with a PrRtAdv message in order to send L2 connection parameters to an MN so that it won't need to discover them through a scan. The actual handover (i.e. the way FBU, FBAck, HI, and HAck messages are exchanged) remains unchanged and follows the procedure defined by FMIPv6.

Our FMIPv6 extension requires MNs to be able to determine their geographical coordinates using a generic geolocation system. In order to do this, existing geolocation systems generally use triangulation based on radio signal strength as "seen" by fixed or mobile nodes with a known location. There are three major kinds of geolocation systems: mobile-based, mobile-assisted and network-based [16], [17]. We consider that for assisting mobility using a geolocation system in wireless LAN, it is best to use a mobile-based solution such as the GPS System or the wireless LAN infrastructure itself as suggested by [18]. This is the approach we have adopted for our experiments. In all tests scenarios MNs use a mobile-based geolocation system, i.e. each MN is aware of its own position.

3.1 Database extension for Access Routers

In order to support our new candidate AP detection mechanism, we had to extend FMIPv6 routers. As previously mentioned, FMIPv6 defines the semantics that allow sending to an MN the properties of IPv6 subnets behind the surrounding APs before it has actually engaged in a handover. For this purpose, every AR manages a database that maps APs to IPv6 subnets, including the layer 3 parameters of these IPv6 subnets. We have extended this database to include some extra layer 2 parameters related to APs. In addition to the link layer addresses (already stored in the database), the APs are registered together with their operating channel, Service Set Identifier (SSID), radio range, and position (either with relative or geodesic coordinates). As this information does not change often, the database is populated manually.

3.2 Mobility Cache

In addition to the database described in the previous section, every AR also monitors the MNs currently connected to its subnet and keeps their last known status in a so called Mobility Cache. Every record in this cache contains the link layer address of the corresponding MN, its last coordinates, the link layer address of its current AP, and a context. A context is a collection of layer 2 and 3 data related to the APs that the MN may move to. Section 3.3 describes the way we create such contexts.

The Mobility Cache of an AR is dynamically updated by RtSolPr messages. In FMIPv6, an MN would generally send an RtSolPr message to its current AR when it needs to resolve one or more Access Point Identifier (generally the link layer address) to subnet specific information (see Section 2.3). We have slightly extended the purpose of RtSolPr-s and in our solution an MN would also use them to periodically update its geographic position with its AR. For this reason, we have defined a new ICMPv6 option, called Position Information Option, that allows the MN to also send its coordinates inside the RtSolPr. It contains the coordinates of the MN and the identifier of its current AP (i.e. the link layer address).

In order to limit the signaling overhead that may be generated by frequent transmissions of RtSolPr, the MN would only be sending periodic updates if the signal quality of its radio connection with the AP has fallen below a certain level. We define a first signal quality threshold S_a corresponding to an average quality. Whenever the signal quality drops below S_a, the MN would start sending the results of its position checks to the AR which would update its Mobility Cache. The AR would then try to determine if the MN would soon have to perform a handover. This assessment is based on the AP range parameter R, that we store in the extended AR database. R corresponds to the maximum distance between the AP and an MN that still allows for a relatively good signal quality. As long as the distance D between the MN and its AP is shorter than R, we assume that the MN is still well covered by its current AP. Otherwise (i.e. when $R < D$), the AR would try to select a new AP for the MN according to its trajectory. The combination of signal quality and distance allows ARs to overcome temporary signal degradations or geolocation errors which may disturb the algorithm behavior when taken separately. According to the results presented in [19], we have set S_a between [-75dBm;-78dBm] and R to the half of the maximum range of the corresponding AP.

3.3 Next Access Point determination

As previously mentioned, the selection of the next APs is based on the trajectory of the MNs. To do this, we determine a trajectory by applying a linear interpolation on the two last known positions of the MN. This gives us the following parametric representation:

$$\begin{aligned} x(t) &= O_x + t \times U_x \\ y(t) &= O_y + t \times U_y \end{aligned} \quad (1)$$

where O_x and O_y are the coordinates a point, and U_x and U_y the coordinates of the director vector $\vec{U}$ of a line that passes through that point. Let (x_0, y_0) and (x_1, y_1) be the two last known positions of an MN. The equation of the trajectory would then be:

$$\begin{aligned} x(t) &= x_1 + t \times (x_1 - x_0) \\ y(t) &= y_1 + t \times (y_1 - y_0) \end{aligned} \quad (2)$$

We assume that the coverage area of an AP is a circle. Let us denote the radius of this circle as G

and let (a,b) be the coordinates of its center (the geographical position of the AP). The equation of the boundary of its coverage area would then be:

$$G^2 = (x-a)^2 + (y-b)^2 \quad (3)$$

Then, if we replace x and y in Eq. (3) by Eq. (2), we obtain a polynomial equation of second degree:

$$At^2 + Bt + C = 0 \quad (4)$$

in which:

$$A = \left\|\vec{U}\right\|^2$$
$$B = 2 \times \overrightarrow{MO}.\vec{U} \quad (5)$$
$$C = \left\|\overrightarrow{MO}\right\|^2 - G^2$$

where $\vec{U}$ is the line's director vector for the MN's trajectory, O is a point of the MN's trajectory, and M is the center of the circle defined by Eq. (3).

In order to select a new AP for an MN, the AR will resolve Eq. (4) for every AP that is geographically adjacent to the current one (i.e. the zones covered by both APs intersect). When the discriminant is negative, the Eq. (4) has no real roots, this means that the MN is probably not headed for the coverage area of the AP. If the discriminant is zero, the Eq. (4) has exactly one root, this means that the trajectory of the MN is tangent to the coverage area of the corresponding AP. Finally, if the discriminant is positive, the Eq. (4) has two distinct roots, this would mean that the MN seems to be moving right into the zone covered by the corresponding AP. When resolving Eq. (4), the AR will create a list of adjacent APs sorted in ascending order by the value of t. This way the first AP of the list would be the one that is likely to cover the MN for the longest distance according to its trajectory. Once the handover begins, the MN will try to connect to the first AP in the list. If it is not reachable it will go on with the second, and so on (see Section 3.4). As the selection of the next AP consumes resources on the AR, we try to maintain the AP list as long as possible. If a context is already set for the current association of the MN, the AR would check if the first AP of the list is still a valid target for the pending handover. If this is no longer the case, the AR has to select a new one as described previously.

Once the context is calculated, the AR would send it to the MN using a PrRtAdv message. We have also defined a new option for PrRtAdv, that we call the Access Point Information Option. It allows transporting the SSID and the radio channel of an AP. Do notice that FMIPv6 already defines options to provide in PrRtAdv all other parameters necessary for the handover (link layer address of AP, new IPv6 prefix, new AR's link layer and IP address). The way options are ordered in PrRtAdv-s has to follow the AP order in the list (i.e. the first options are related to the first AP of the list). Upon reception, the MN will save the context until it starts a handover or until a new context is received.

3.4 Handover Management

This section describes the handover process when initiated by MNs. Note that FMIPv6 also defines a mechanism for an AR to initiate a handover - a network-initiated handover [3], initially previewed for purposes like load sharing. We have defined a second signal quality threshold S_w, which corresponds to the lowest acceptable signal level. Once the signal quality drops under S_w, the MN would start the handover process. Layer 3 handover is carried out exactly as described in FMIPv6. If a context is set, the MN begins an FMIPv6 predictive handover by sending an FBU to its current AR including the parameters related to the first AP of the context. Once the MN receives the corresponding FBACK, it starts the layer 2 handover by switching its radio channel to that of the new AP and sends a Probe Request to its SSID. Upon reception of a Probe Response from the destination AP (identified by its link layer address), the MN moves directly to the authentication stage. If the authentication is successful, the MN goes through the association stage and completes the layer 2 handover. As a result, in case of a successful anticipation the delay of the layer 2 handover is significantly reduced , as the MN does not have to scan several channels to discover its next AP and neither does it have to wait for MinChannelTime or MaxChannelTime before completing the handover process.

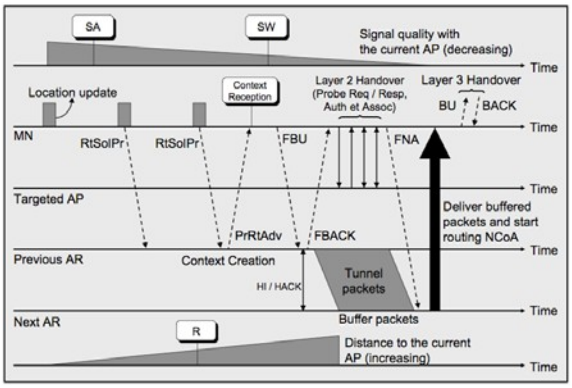

Figure 5: Protocol overview when the anticipation is successful

The rest of the handover follows the FMIPv6 specifications. During the layer 2 handover, the data packets sent to the MN are forwarded by the

Previous AR (PAR) to the Next AR (NAR) which buffers them. After associating with its new AP, the MN sends an FNA to the NAR so that it would deliver all buffered packets and start routing the New CoA (NCoA) of the MN. Finally, the MN sends a BU to update its binding with the HA. Fig. 5 illustrates the entire procedure.

If the MN does not receive a Probe Response from the targeted AP, this could either mean that there was a collision on the wireless link, or that the AP was out of range. The latter may occur as a result of a wrongful projection of the MN trajectory (e.g. due to geolocation errors or change of the direction of the MN). As the probability for an AP to fall out of range is quite high, we have decided to limit the time the MN waits for a Probe Response from an AP to 5ms. After 5ms, the MN considers that the target AP is not reachable and tries the next one in the AP list and so on.

When a layer 2 handover completes, and the AP that the MN has attached to was the second one it tried (i.e. the attempt to connect to the first one has failed) two cases may occur. If the new AP is connected to the same IPv6 subnet as the first one it tried, no further considerations are necessary and the MN can pursue the handover process as defined in the case of a successful anticipation. Otherwise, the MN would find itself in a situation where its packets are being tunneled to and buffered by a different router (referred to as AAR for Anticipated Access Router in the following) and not the NAR. In this case the MN would perform a specific reactive handover by sending to AAR an FNA which contains the FBU corresponding to its current location. As a result, two tunnels will be set up simultaneously, the first one from PAR to AAR, and the second one from AAR to the actual NAR. Upon reception of data packets addressed to the MN, the NAR delivers them directly to the MN. Finally, the MN updates its binding to the HA. This case is referred to as enhanced reactive mode.

4 EXPERIMENTATION

4.1 The Testbed

In order to evaluate the performance of our proposal, we implemented it and set up a testbed composed of two APs, one HA, two ARs, one MN and one correspondent node. The testbed contains three IPv6 subnets. The top AR provides IPv6 Internet connectivity to the rest of the testbed and is also configured as a HA. Each AP is connected to a different IPv6 subnet and AR. Fig. 7 illustrates the testbed.

All network entities are running the GNU/Linux operating system, except for the APs which are 802.11b Cisco AP 1200 devices. The HA is running the new MIPv6 daemon for the GNU/Linux operating system (MIPL [20]). The MN and the ARs are running a modified version of the FMIPv6 Open Source Implementation Suite (fmipv6.org [21]). The modifications are related to our protocol specifics. In order to modify the behavior of the MN's wireless LAN device, we have used a 3com 802.11 a/b/g PCMCIA wireless card managed by the MADWiFi driver [14].

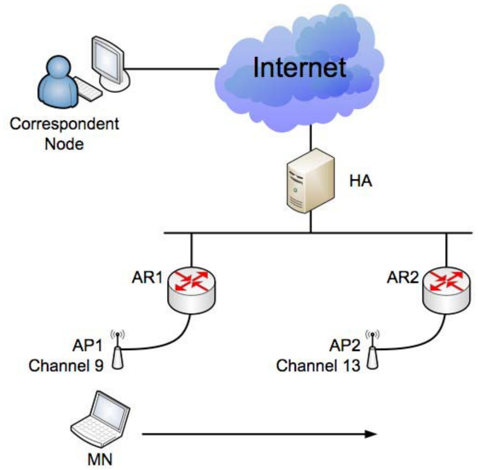

Figure 7: Testeb used in the experiments

Concerning the geolocation system, the MN is equipped with a GPS device. We have chosen GPS for its ease of use and installation. Other systems with similar (or better) characteristics, such as [18], could also be used. As the experiments take place in an indoor environment, we first recorded GPS output generated by a moving MN in an open area. We then used the recorded GPS positions while performing the real experiments inside. The position and range of the APs are derived from indoor measurements and are configured statically in all ARs.

4.2 Evaluation Scenario

For the evaluation of our proposal we have defined the following scenario: the MN would move from AP1 to AP2 (see Fig. 7). While the MN is moving, a correspondent node sends a video stream to it using the well known VideoLAN application [22]. Data is encapsulated and sent in Real-time Transport Protocol (RTP) [23] packets, with an average length of approximately 1336 bytes and sent every 30ms.

5 PERFORMANCE EVALUATION

Results presented in this section are obtained by running the network analyzer tool Wireshark [24] on the MN. Additional wireless sniffers are also used to collect the results. The evaluation scenario was run 10 times.

Fig. 8 presents one significant run illustrating the entire handover procedure. When the signal quality of the MN is below the S_a threshold, it starts sending periodic RtSolPr messages to its AR in order to update its status and position. Upon reception of the fourth RtSolPr, the AR detects that the distance between the MN and its current AP is greater than the R threshold. Therefore, the AR calculates a new context and sends it to the MN using PrRtAdv. The reception of a new RtSolPr request (e.g. between seconds 9.5 and 12) does not initiate the calculation of a new context because the previous one remains valid until the actual handover occurs. Once the signal quality of the MN drops below S_w, the MN starts a predictive handover as described in the FMIPv6 specifications. The MN has thus obtained the parameters of the candidate APs (i.e. the context) without loosing a single data packet. Executing the standard scanning procedure [13] MN would have been scanning several 802.11 channels in order to discover candidate APs, which, as we have already mentioned, would have caused significant loss of data packets. In addition, regarding the time at which the scanning occurs, there is no guarantee that the set of candidate APs discovered during the last scan would still be pertinent (i.e. still in the radio coverage of the MN) when the MN actually begins its handover. Furthermore, by sorting the list of candidate APs according to the length of the trajectory segment that they are expected to cover, our solution also reduces the number of performed handovers.

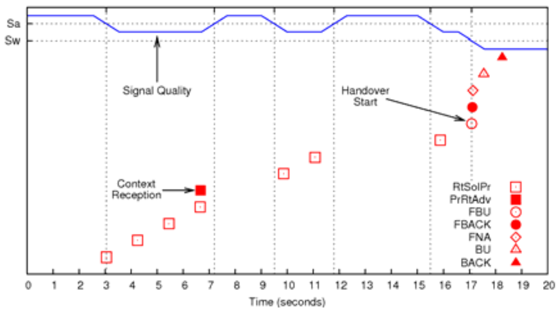

Figure 8: Candidate access points discovery followed by an FMIPv6 predictive handover

Fig. 9 presents the complete handover procedure. Each dot represents the reception or the transmission of a packet by the MN at the time indicated on the X-axis. As previously mentioned, the MN moves while receiving a video stream (data packets are sent every 30ms). Once its signal quality drops below the S_w threshold, the MN starts the FMIPv6 procedure by sending a FBU to its current AR including the parameters of the NAR, i.e. the AR related to the first AP of the context. Then, it takes approximately 25.8ms for the current AR to get handover confirmation from the NAR (HI/HACK exchange) and to send the FBACK back to both MN and NAR. Upon reception of FBACK, the current AR starts tunneling data packets to the NAR while the MN starts the layer 2 handover procedure. As we can see, the MN completes the layer 2 handover in 20.4ms on average. This time is significantly reduced in comparison to the standard layer 2 handover latency which may vary between 58.7ms and 396.7ms according to the results described in [9]. Compared to the method defined in the IEEE 802.11 standard [1] in which MNs have to scan several 802.11 channels to detect surrounding APs, our scheme allows the MN to directly send Probe Requests over the radio channel of the pre-selected AP. When a Probe Response is received from the pre-selected AP, the MN proceeds with authentication and completes the layer 2 handover with the association stage. Do notice that the size of the NAR's buffer is limited and therefore such layer 2 optimization is necessary to avoid buffer overflow and packet loss. Simply augmenting the buffer size would not resolve this problem as real-time communications would still suffer the delays accumulated while packets were being buffered.

Once the layer 2 handover is complete, the MN sends an FNA to the NAR. After receiving it, the NAR, delivers all buffered packets, and starts routing the NCoA. As we can see from Fig. 9, the NAR has only buffered two data packets during the entire procedure. Although there is a delay in the reception of buffered packets, this delay remains imperceptible to the application user and the handover is completely seamless with no packet lost and no perceptible delays.

While the MN does not update its binding with the HA, the data packets are still sent to the Previous CoA (PCoA) of the MN and are therefore forwarded through the FMIPv6 tunnel between the PAR and the NAR. The lifetime of this tunnel is specified by the MN at the transmission of the FBU. During our experiments, we configured the MN to request the minimal allowed tunnel lifetime, i.e. 4 seconds according to [3]. As shown in Fig. 9, the data packets are sent to PCoA until the time 310.6ms at which the MN sends a BU to the HA. After receiving it, the HA updates the tunnel endpoints with the NCoA and sends back to the MN a BACK message with a successful status code which completes the MIPv6 signaling. Then, the following data packets are directly sent to the NCoA and thus do not use the FMIPv6 tunnel. 4 seconds later, the FMIPv6 tunnel between the PAR and NAR is removed.

Note that the procedure defined for the enhanced reactive mode (i.e. when the anticipation is not successful) is still being implemented and thus we can not yet provide results for this particular case.

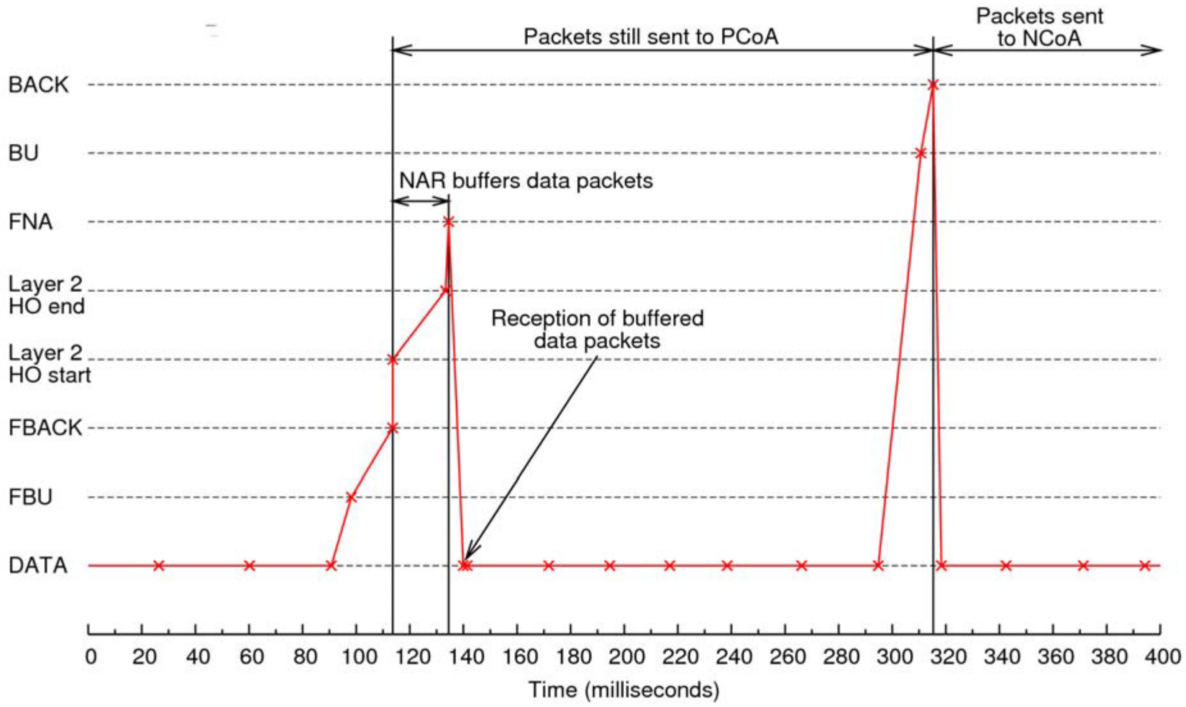

Figure 9: Impact of the Predictive FMIPv6 handovers on a video stream

6 CONCLUSIONS

The development of wireless technologies and their wide-scale deployment have allowed for new use cases and types of user behavior. Users are beginning to expect Internet connectivity to be available anywhere, and anytime. This demand is also related to the development and availability of small communicating devices supporting various wireless technologies. The pending deployment of the new version of the Internet Protocol (IPv6) [6] will allow providing globally routable addresses for all of these new devices. In an effort to guarantee uninterrupted IPv6 connectivity, the Internet Engineering Task Force (IETF) has defined the Mobile IPv6 (MIPv6) [2] protocol which enables IPv6 nodes to communicate while on the move. On the other hand, the increasing performance of wireless technologies, wireless LANs in particular, allow the transmission of broadband traffic over the air, and enables support for real-time applications such as voice calls (VoIP). Real-time communications need to satisfy a set of specific requirements regarding delay and packet loss in order to achieve guarantee acceptable transmission quality. However, the mechanisms supported in wireless LAN and proposed by MIPv6 to support mobility do not match these requirements as the time needed for a Mobile Node (MN) to roam from an Access Point (AP) to another is too long. To address this problem, the IETF has defined the Fast Handovers for Mobile IPv6 (FMIPv6) [3] protocol, which allows achieving efficient and seamless handovers. However, this protocol is a network layer only solution without any link layer dependencies, and therefore leave unresolved issues related to handovers in wireless LAN like for example the discovery of candidate APs. The FMIPv6 extension proposed in this article provides a reliable mechanism to select the next APs and obtain their link layer parameters without disturbing ongoing communications. This extension uses the geographical position of MNs to deduce their trajectories and thus anticipate their next APs. Our proposal has been implemented and tested on a GNU/Linux operating system using the new MIPv6 daemon for Linux (MIPL [20]) and the new FMIPv6 Open Source Implementation Suite (fmipv6.org [21]). To measure the impact of our mechanisms on applicative flows, the MN receives a video stream while performing handovers.

The results presented in Section 5 have shown that our scheme allows the entire FMIPv6 procedure to remain imperceptible to users, from the discovery of candidate APs to the completion of the handover. Based on the trajectory of an MN access routers are able to select its next APs and provide the related parameters. The proposed method allows the MNs to avoid scanning prior to a handover and thus does not disturb communications. Moreover, use of our various thresholds on signal quality or geographical distance reduces the signaling overhead introduced by our additional mechanisms. The actual handover is also seamless due to the optimized layer 2 handover and the buffering of data packets defined by the FMIPv6 specification. As a result, the quality of the video stream transmission is not affected by the movement of the MN.

Encouraged by the results presented here, we plan to extend the present analysis to large scale experiments and error cases, especially to evaluate the enhanced reactive mode. We expect to be able to use Louis Pasteur University wireless LAN network deployment and design more realistic scenarios. We are also planning on evaluating our proposal using other geolocation systems, such as systems based on wireless LAN [18], and extending it to other wireless technologies in order to design a global solution for heterogeneous mobility.

7 REFERENCES

[1] IEEE Std. 1999 Edition (R2003) (ISO/IEC 8802-11), IEEE Standard Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications (1999).

[2] D. Johnson, C. Perkins, and J. Arko: Mobility Support in IPv6, Internet Engineering Task Force Request for Comments (RFC) 3775 (2004).

[3] R. Koodly (ed.): Fast Handovers for Mobile IPv6, Internet Engineering Task Force Request for Comments (RFC) 4068 (2005).

[4] S. Thomson and T. Narten: IPv6 Stateless Address Autoconfiguration, Internet Engineering Task Force Request for Comments (RFC) 2462 (1998).

[5] T. Narten, E. Nordmark, and W. Simpson: Neighbor Discovery for IP version 6 (IPv6), Internet Engineering Task Force Request for Comments (RFC) 2461 (1998).

[6] S. Deering, and R. Hinden: Internet Protocol Version 6 (IPv6) Specification, Internet Engineering Task Force Request for Comments (RFC) 2460 (1998).

[7] J. Postel: Internet Protocol, Internet Engineering Task Force Request for Comments (RFC) 791 (1981).

[8] J. Montavont, E. Ivov, and T. Noel: Analysis of Mobile IPv6 Handovers Optimizations and their Impact on Real-Time Communications, in Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC'07), pp. 3244-3249 (2007).

[9] A. Mishra, M. Shin, and W. Arbaugh: An empirical analysis of the IEEE 802.11 MAC layer handoff process, ACM SIGCOMM Computer Communication Review, Vol. 33, No. 2, pp. 93-102 (2003).

[10] International Communication Union (ITU), Transmission Systems and Media, Recommendation G.714: One-way Transmission Time (1996).

[11] N. Montavont, and T. Noel: Handover Management for Mobile Nodes in IPv6 Networks, IEEE Communication Magazine, Vol. 40, No. 8, pp. 38-43 (2002).

[12] N. Montavont, and T. Noel: Analysis and Evaluation of Mobile IPv6 Handovers over Wireless LAN, Mobile Networking and Applications (MONET), special issue on Mobile Networking through IPv6 or IPv4, Vol. 8, No. 6, pp. 643-653 (2003).

[13] P. MacCann: Mobile IPv6 Fast Handovers for 802.11 Networks, Internet Engineering Task Force Request for Comments (RFC) 4260 (2005).

[14] G. Chesson, M. Renzmann, and S. Leffler: Multiband Atheros Driver for WiFi (MADWiFi), http://madwifi.org

[15] S. Shin, A.G. Forte, A. S. Rawat, and H. Schulzrinne: Reducing MAC layer handoff latency in IEEE 802.11 wireless LANs, in Proceedings of the 2nd International Workshop on Mobility Management and Wireless Access Protocols (MobiWac'04), ACM press, pp. 19-26 (2004).

[16] S. S. Soliman, and C. E. Wheatley: Geolocation technologies and applications for third generation wireless, Wireless Communications and Mobile Computing, Vol. 2, No. 3, pp. 229-251 (2002).

[17] P. Prasithsangaree, P. Krishnamurthy, and P. K. Chrysanthis: On Indoor Position Location with Wireless LANs, in Proceedings of the 13th IEEE International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC'02), Vol. 2, pp. 720-724 (2002).

[18] Ekahau Positioning Engine for wireless LAN based navigation, http://www.ekahau.com

[19] N. Montavont, and T. Noel: Anticipated Handover over IEEE 802.11 Networks, in Proceedings of the IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob'05), Vol. 2, pp. 64-71(2005).

[20] V. Nuorvala, H. Petander, and A. Tuominen: Mobile IP for Linux (MIPL), http://mobile-ipv6.org

[21] E. Ivov, and M. Andre: The FMIPv6 Open Source Implementation Suite, http://fmipv6.org

[22] A. Cellerier and Al.: VideoLAN – VLC media player, http://www.videolan.org

[23] H. Schulzrinne, S. Casnet, R. Frederick, and V. Jacobson: RTP: A Transport Protocol for Real-Time Applications, Internet Engineering Task Force Request for Comments (RFC) 3550 (2003).

[24] G. Combs and Al.: The Network Protocol Analyser Wireshark, http://wireshark.org