

# HAMS: Layer 2 Handoff Accurate Measurement Strategy in WLANs 802.11

Francisco A. González, Jesús A. Pérez, and Victor H. Zárata, *Member, IEEE*

**Abstract**—The layer 2 handoff latency in WLANs 802.11 has traditionally been measured as the time between the first probe request message sent by the mobile station and the arrival of a reassociation response message from an access point. However, that measure does not represent the time the station remains disconnected during the handoff. Thus, the traditional way of measurement is imprecise. This paper analyzes layer 2 handoffs and experimentally shows that the mobile station may send or receive data frames during part of the handoff latency. Our proposal, called Handoff Accurate Measurement Strategy (HAMS) measures the total disconnection latency and the contribution of each handoff phase to the entire handoff latency. Our strategy is simple, sniffing-based, independent from implementations, and furthermore, it substantially improves the measurement precision compared to traditional measurement techniques.

**Index Terms**—Disconnection, Handoff, Latency, Measurement, Wireless LANs, IEEE 802.11

## I. INTRODUCTION

THE number of layers 2 and 3 handoffs in wireless local area networks (WLANs) are growing because more mobile users with handheld computers roam across the local area and because many WLANs are now divided in multiple IP subnets or VLANs. There is also a growing demand for incorporating educational applications, that show real time multimedia interactivity, to mobile devices for students and teachers in all universities. Our motivation is to study the impact handoffs may have in delay sensitive applications. Thus, there is a necessity for accurately measuring handoffs latencies [1].

Manuscript received December 24, 2004. This paper was accepted for publication in the Proceedings of the 1st IEEE International Workshop on Wireless Network Measurements (WinMee 2005), Riva del Garda, Trentino, Italy, April 3, 2005. This work was supported by the research group in Collaborative Learning Distributed Systems sponsored by the ITESM System.

F. A. González is a PhD candidate at the ITESM Cuernavaca Campus, Av. Paseo de la Reforma #182-A, Lomas de Cuernavaca, C.P. 62589, Temixco, Morelos, Mexico, phone: (52) 777-329-7163; fax: (52) 777-329-7166; e-mail: fglez@itesm.mx.

J. A. Pérez, PhD., is Associate Professor of Electronics Department at ITESM Cuernavaca Campus, Mexico (e-mail: jesus.arturo.perez@itesm.mx).

V. H. Zárata, PhD., is Director of the Electronics Department at ITESM Cuernavaca Campus, Mexico (e-mail: vzarate@itesm.mx).

In *hard* handoffs, like the ones present in 802.11 infrastructure networks, the mobile station (STA) can not sustain simultaneous communication with the new and old access point (AP). This implicates that the STA will suffer from a temporal disconnection that will impede the exchange of data packets with other stations during the handoff. Such disruption may be present during all the handoff process or just in parts of it. That is, if  $T$  is the total disconnection time and  $\Lambda$  is the total handoff signaling latency then  $T \leq \Lambda$ . We claim the handoff is a *primitive process* if and only if  $T = \Lambda$ ; however, a handoff is not always a primitive process despite having been traditionally considered so. For example, in [2] and [3] authors measure  $\Lambda$  but not  $T$ , and they implicitly consider that  $T = \Lambda$ . We argue that our measurement strategy (HAMS) is precise because it can measure both  $T$  and  $\Lambda$ . In fact, we experimentally show that  $T < \Lambda$  and that there is data exchange during part of the handoff latency.

In addition, what really affects the applications performance is  $T$  and not  $\Lambda$ , because the longer the disconnection time, the more probable is to have lost, duplicated, or delayed packets. Particularly, real time interactive applications have strict quality of service requirements, as it is shown in [4], e.g., end-to-end delay lower than 300 ms, delay variance or jitter lower than 50 ms, and a lost packets percentage inferior to 1%.

## II. THE HANDOFF PROCESS

During the handoff process exist signaling in the wireless part between STA and new AP, as well as, in the wired part among APs through the distribution system (DS). For long time, the IEEE 802.11 standard [5] just considered the handoff signaling in the wireless part, letting to manufacturers the communication between APs through the backbone wired network. Hence, *transparent roaming* was only possible between wireless products of the same manufacturer, who developed proprietary protocols for inter access points communications. The Wi-Fi (Wireless Fidelity) alliance, emerged to solve interoperability issues in 802.11 networks. Wi-Fi promotes the usage of IAPP (Inter Access Point Protocol) by providing a common protocol that allow mobile users to roam transparently among different manufacturers APs. Recently, the 802.11 working group adopted the IAPP protocol into a new standard [6].

Fig. 1 shows the main elements involved in a layer 2 handoff: the STA, the old AP, the new AP, and the DS. It can be observed that basic service sets (BSS1 and BSS2) must

belong to the same extended service set (ESS1). In the same way, radio channels of each cell (CHX, CHY) shall be non mutually interfering channels.

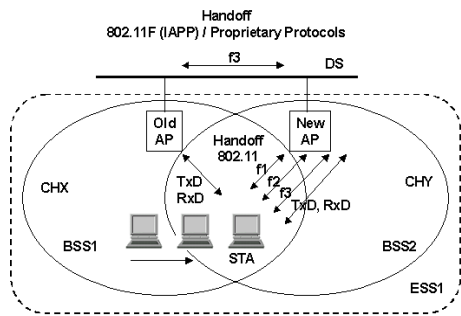


Fig. 1. Involved elements in a layer 2 handoff.

In general, a layer 2 handoff process can be explained as follows: initially, the STA transmits and receives data by using old AP. When STA moves towards BSS2 and detects a low signal strength from packets coming from old AP, it will start to explore other channels to *discover* new APs candidates for reconnection. By detecting a compatible new AP, the STA will attempt a *reauthentication* with that AP. If new AP accepts the STA authentication, then the STA will request a transfer association from old AP to new AP. After STA submits a *reassociation* request to the new AP, the STA waits for response at CHY. If reassociation request is successful then STA will continue exchanging data but now through the new AP in channel Y. In summary, three phases or logical steps can be identified for the layer 2 handoff process: (f1) discovery phase, (f2) reauthentication phase, and (f3) reassociation phase. Now, these phases will be explained.

#### A. Phase 1: Discovery

The discovery process can be *passive* or *active*. Passive discovery is not appropriate for fast handoffs. In fact, many vendors have preferred to deploy only the active discovery [7]. In active discovery, for each channel to scan, the STA sends a *Probe Request* and waits for a *Probe Response* from every reachable AP. The STA creates a report of all discovered APs and their characteristics. Then, the STA selects the *more adequate AP* to initiate next handoff phase. As it is shown in [8], several parameters control the discovery process: *BSSType*, *BSSID*, *SSID*, *ScanType*, *ChannelList*, *ProbeDelay*, *MinChannelTime*, and *MaxChannelTime*.

In active discovery, the number of channels selected for *ChannelList* defines two kinds of scans. The full-scan that sweeps all usable channels and the short-scan that sweeps only a subset of the channel spectrum. Most mobile stations use the following procedure for full or short scans:

**Procedure:** Full or short scan in active discovery.

- 1: **For each** channel in *ChannelList* **do**,
- 2: Tune the STA in channel to probe.
- 3: STA waits for (channel activity detection) **or** (*ProbeDelay* timer expiration).
- 4: **If** *ProbeDelay* expires, **then** channel is empty, probe the next channel.

- 5: **If** channel activity is detected **then** ...
- 6: STA get access to wireless medium.
- 7: STA broadcasts a *Probe Request* frame.
- 8: STA waits *MinChannelTime* sensing the channel.
- 9: **If** STA does not detects activity **then** probe next channel (not enough activity).
- 10: **If** STA detects traffic **or** *Probe Response* **then** ...
- 11: STA waits *MaxChannelTime* sensing the channel.
- 12: **do** process any received *Probe Response*.
- 13: **Until** *MaxChannelTime* expires, **then** probe next channel.

Fig. 2 illustrates the above procedure where N channels from *ChannelList* are elected to be probed.

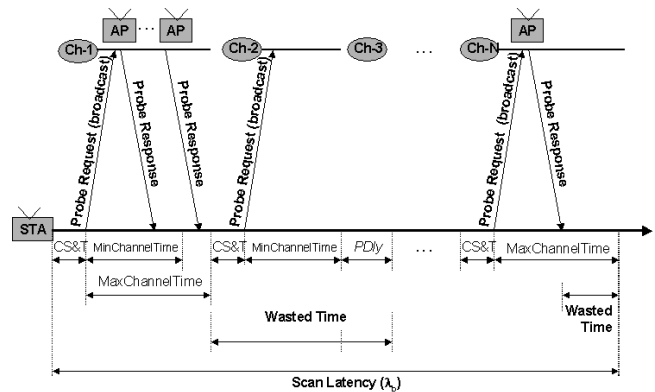


Fig. 2. Active discovery example in WLANs 802.11.

The CS&T (channel switch and transmission) latency is the time elapsed since the STA changes to the probe channel until the probe request frame is sent (lines 1-7). In channel 1, STA detects activity during *ProbeDelay* and broadcasts a probe request. The STA waits *MinChannelTime* for an answer. On reception, STA extends the sensing interval until *MaxChannelTime* to wait for more answers. As the example shows, a second probe response is received from another AP on time. In channel 2, the STA detects activity during *ProbeDelay* and broadcasts a probe request. However, during *MinChannelTime* the STA does not detect enough activity and decides to probe next channel. In channel 3, the STA does not detect any activity during *ProbeDelay* (*PDly*) and goes to the next channel. In channel N, the STA broadcasts its probe request and after receiving a probe response it keeps waiting unnecessarily because there is just one AP in the channel. Wasted times during an active discovery cycle, are examples of unnecessary delays that could be eliminated if STA had a previous knowledge of the ESS topology.

The number of channels to scan is the main contributing factor to discovery latency. Therefore, a short-scan is preferred to a full-scan for fast handoffs. However, the active discovery procedure may exhibit variable latencies due to the varying number of channels to scan and the variable time the STA stands on each channel (*ProbeDelay*, *MinChannelTime*, or *MaxChannelTime*). The scan latency ( $\lambda_b$ ) is delimited by  $N*ProbeDelay \leq \lambda_b \leq N*(MaxChannelTime+ProbeDelay)$ .

The handoff algorithm called *relative signal strength with*

*hysteresis and threshold (RSSHT)*, used by many manufacturers, describes the conditions to start handoffs. Fig. 3 depicts typical signal-to-noise ratio (SNR) changes between old AP and new AP according to the STA movement.

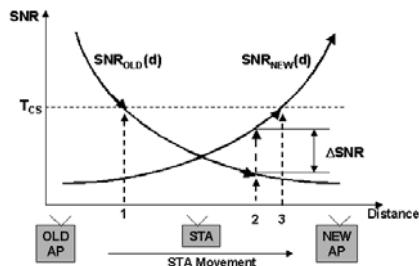


Fig. 3. Decision points during layer 2 handoff process.

As the STA moves from old AP to new AP, the SNR from old AP decreases while SNR from new AP increases. While  $SNR(d) \geq T_{CS}$  (Cell Search Threshold) a handoff is not required (normal state). As soon as  $SNR_{OLD}(d) < T_{CS}$  (position 1) the STA enters the discovery state and initiates an active discovery. While the SNR value keeps lower than  $T_{CS}$ , the STA will achieve a short-scan active discovery for every 2 seconds (ORiNOCO Systems). After scan latency, a critical comparison is made by the STA at some moment during the trip to new AP. If  $|SNR_{NEW}(d) - SNR_{OLD}(d)| > \Delta SNR$  (hysteresis threshold), the STA will definitively change its association from old to new AP (position 2). After reassociation, the STA may keep standing in the discovery state or it may pass directly to a normal operation state (position 3), depending on the values for  $T_{CS}$  and  $\Delta SNR$ . In any case,  $\Delta SNR$  avoids the ping-pong effect in handoffs [9].

The conditions to initiate a handoff or criteria for selecting the *best* new discovered AP, are not specified in the IEEE 802.11 standard. Therefore, companies defined their own conditions and criteria that resulted in incompatibilities or extremely slow handoffs between different vendors products. However, most Wi-Fi products use only active short-scans and the RSSHT algorithm to control layer 2 handoffs.

*B. Phase 2: Reauthentication*

In this second phase, the STA authenticates with the *best* discovered AP of phase 1. Authentication is a necessary prerequisite to association. However, *IEEE 802.11 standard neither requires that authentication must immediately precede to association nor the authentication must immediately follow a channel scan cycle*. For this reason, some vendors have implemented *preauthentication schemes*, e.g., *discovery with preauthentication* [8] and *IAPP based preauthentication* [10]. In the first scheme, the STA authenticates with the new AP immediately after the scan cycle finishes, getting anticipate the moment of reassociation. The second scheme is accomplished even with greater anticipation; it is performed as soon as the STA associates with the first AP in the ESS. In that moment, IAPP sends through the DS, authentication information to all APs in the ESS, thus, when reassociation is required, the STA is already authenticated with any AP. IAPP

based preauthentication is achieved even before STA enters to the discovery state, thus, it does not contribute to handoff latency.

*C. Phase 3: Reassociation*

Reassociation is the process for transferring associations from one AP to another. Once the STA authenticates with the new AP, the reassociation can be started. According to [8], reassociation process is a six step process (Fig. 4.).

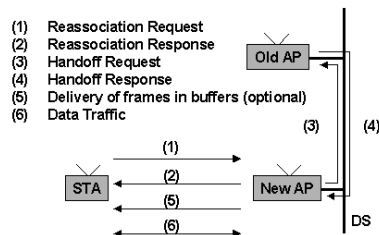


Fig. 4. Steps in the reassociation process.

The reassociation phase begins when STA switches to the new channel to issue a reassociation request to the new AP. The station’s request includes the current BSSID. New AP verifies the existence of a previous association between STA and old AP. If such association does not exist, the new AP deauthenticates the STA and the process ends. If previous association exist, then the new AP must *locally decide* if grants or not permission for reassociation, notifying to the STA with a reassociation response. Although 802.11 standard does not specify what factors shall be considered to take that decision, most AP manufacturers consider aspects like the number of stations already associated to the new AP, the size of free buffers in the AP, and current traffic load in the BSS. If permission is granted, the response message carries a success code and a value identifying the new association (AID), otherwise, the response message just carries the status code indicating the reason for denying permission. Next steps are part of IAPP. The new AP sends a *Handoff Request* to the old AP. Then, old AP dissociates the STA from its associations table, update the new STA’s association, and send any temporarily buffered packet to the new AP. Old AP returns a *Handoff Response* and transfer any buffered frames to the new AP if they exist, so they can be delivered to the mobile station. Finally, the new AP begins processing frames for the recent associated STA.

III. HANDOFF ACCURATE MEASUREMENT STRATEGY

In [2], authors measure handoff latency as *the elapsed time since the STA broadcast the first Probe Request frame until it receives a Reassociation Response from the new AP*. However, that measurement technique has several drawbacks: (1) It can be a rather complex task to determine the moment when the STA broadcast the first probe request frame. The reason is that sniffers only capture packets from one channel at a time, and the first channel the STA will probe is unknown to the user. (2) With APs based on IAPP, the handoff latency is lightly extended until the new AP receives a handoff

response from the old AP. (3) The technique does not provide a method to measure  $T$ , it measures  $\Lambda$  and implicitly consider that  $T = \Lambda$ . (4) The technique does not provide information about how much time during a handoff, the STA is able to send or receive data packets or even to count those data packets. Our measurement strategy (HAMS) provides a solution to drawbacks (2), (3), and (4); for drawback (1), HAMS assumes that the first channel the STA will probe in the scan cycle is the channel assigned to the new AP. Next, we will explain the parameters to measure and how will they be measured.

### A. Handoff Parameters to Measure

Measuring with *sniffers* the latency of each handoff phase ( $\lambda_{f1}$ ,  $\lambda_{f2}$ , and  $\lambda_{f3}$ ) requires to identify the signaling frames that precisely separates one phase from the other. Figures 5a and 5b, illustrates the events in time that delimit each handoff phase. Fig. 5a follows the traditional handoff model of three phases, while Fig. 5b illustrates the new handoff model of two phases, which uses IAPP preauthentication, where  $\lambda_{f2} = 0$ .

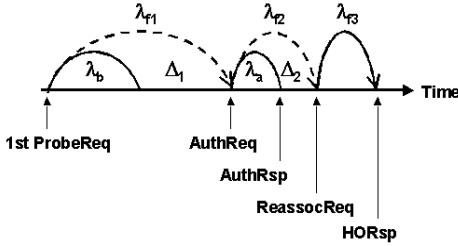


Fig. 5a. A 3-phase handoff in a timeline.

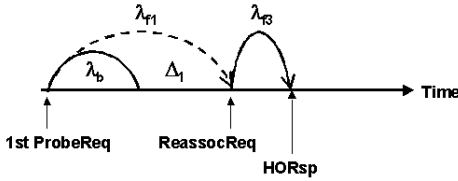


Fig. 5b. A 2-phase handoff in a timeline.

The dashed arcs indicate that during  $\Delta_1$  in  $\lambda_{f1}$  or  $\Delta_2$  in  $\lambda_{f2}$ , data communications are possible if either  $\Delta_1$  or  $\Delta_2$  are slot times greater than the transmission time of a single data packet and their acknowledgement. On the other hand, the solid arcs in  $\lambda_b$  (scan latency),  $\lambda_a$  (authentication algorithm latency), and  $\lambda_{f3}$  (reassociation latency) indicate they are primitive processes, that is, the STA is unable to establish any communication during those processes. The STA remains disconnected during all that time. The following expressions relate the handoff parameters to measure. Relations 1 to 6 hold for a 3-phase handoff model; relations 7 to 12 are the counterpart for a 2-phase handoff model:

$$\begin{aligned}
 \Lambda &= \lambda_{f1} + \lambda_{f2} + \lambda_{f3} & (1) \quad \Lambda &= \lambda_{f1} + \lambda_{f3} & (7) \\
 \lambda_{f1} &= \lambda_b + \Delta_1 & (2) \quad \lambda_{f1} &= \lambda_b + \Delta_1 & (8) \\
 \lambda_{f2} &= \lambda_a + \Delta_2 & (3) \quad \lambda_{f2} &= 0 & (9) \\
 \Lambda &= (\lambda_b + \Delta_1) + (\lambda_a + \Delta_2) + \lambda_{f3} & (4) \quad \Lambda &= (\lambda_b + \Delta_1) + \lambda_{f3} & (10) \\
 T &= \lambda_b + \lambda_a + \lambda_{f3} & (5) \quad T &= \lambda_b + \lambda_{f3} & (11) \\
 \Lambda &= T + (\Delta_1 + \Delta_2) & (6) \quad \Lambda &= T + \Delta_1 & (12)
 \end{aligned}$$

Other authors that follow a measurement strategy similar to the traditional [2], are Velayos in [3] and De Cleyn in [11]. Therefore, their results are affected by the same drawbacks explained at the beginning of this section, mainly, they measure  $\Lambda$  but no the other handoff parameters showed above.

### B. Measurement Strategy

Once identified the parameters to measure, the next step is to show up an experimental strategy of measurement. Basically, our testbed consists of two co-located IEEE 802.11b [12] APs belonging to the same ESS and connected to an Ethernet hub, thus STAs can perform layer 2 handoffs between APs. The handoff phenomenon will be observed and monitored simultaneously from two reference points. For this reason, our measurement strategy requires two *sniffers*; one is a *wired sniffer* placed in the DS and the other is a *wireless sniffer* permanently tuned in the channel used by the new AP. The mobile station (STA-M) moves from old to new BSS being followed in every moment by the *wireless sniffer*. The STA-M sends a continue flow of voice or data packets to a fixed station (STA-C) placed in the DS.

Handoff parameters like  $\Lambda$ ,  $\lambda_{f1}$ ,  $\lambda_{f2}$ ,  $\lambda_{f3}$ ,  $\lambda_a$ , and  $\Delta_2$ , can be easily measured with *sniffers* because we have identified 802.11 signaling frames that delimit their duration. However, in order to measure the total or accumulated disconnection time ( $T$ ), as well as the total or accumulated time for data communication during handoff ( $\Delta_1 + \Delta_2$ ), it is necessary to measure either  $\Delta_1$  or  $\lambda_b$ .

The measurement of  $\lambda_b$  directly with a *wireless sniffer* is particularly difficult because of the following reasons: the STA-M is changing from one channel to another, the time spent on each channel is variable, and the sequence and number of channels to scan is only known by the card firmware. Moreover, we found that it is easier to measure  $\Delta_1$  and then obtaining  $\lambda_b$  from expressions (2 or 8). In order to measure  $\Delta_1$  we need to *map*  $\lambda_{f1}$  into the wired capture handoff file. We can make a good approximation of  $\Delta_1$  by counting the time of data packets received or transmitted during  $\lambda_{f1}$ . If the mapping is correct, surely those data packets were sent after  $\lambda_b$  and before  $\lambda_{f3}$ . Fig. 6 illustrates this idea.

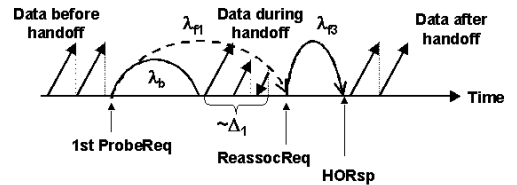


Fig. 6. Data packets exchanged during the handoff.

Another issue is on how can we map  $\lambda_{f1}$  into the wired capture handoff file. In order to do that, it is necessary a synchronization method between the wireless and the wired capture. Synchronization of sniffers is another hard topic, however, during the first handoff occurs an event that is equally registered in both *sniffers*. Such event occurs in phase

3, just before the new AP contacts the old AP for the IAPP handoff request. The new AP does not know the Ethernet MAC Address of the old AP, so it broadcast an ARP Request *simultaneously* through both, the wired and wireless media. Using such packet as a common reference it is possible to make a correct mapping of the whole handoff process in the wired capture file. Clearing the ARP cache in the new AP before the handoff initiates, forces the new AP to generate the ARP Request.

A final remark about  $\Delta_1$  and  $\Delta_2$  is that they represent variable wait times that the handoff process takes before deciding to initiate the next handoff phase. These parameters are not defined in the standard. Some conditions that may impact on its values are the STA's velocity, the hysteresis threshold ( $\Delta SNR$ ), the traffic load in the new BSS, the number of associated STAs in the new AP, or the preauthentication scheme.

#### IV. EXPERIMENT DESIGN

To experimentally analyze the handoff process and to measure its latency, Lucent/Proxim access points models AP-1000 and AP-2000 were used. APs and mobile stations used Orinoco Silver Cards 802.11b. A laptop IBM ThinkPad R30 was used as mobile station (STA-M). We used the analyzers AiroPeek and EtherPeek from WildPackets to capture wireless or wired packets respectively. The *wireless sniffer* was also a laptop TPR30 always moving near the STA-M. The *wired sniffer* was a desktop Dell computer directly connected to the DS. The distribution system was implemented with a 10/100 Ethernet hub connecting besides a fixed station (STA-C) that was in permanent communication with the mobile station. That communication consisted of a file transfer using TFTP or a voice conference using Microsoft NetMeeting (VoIP). Fig. 7 depicts the testbed implemented.

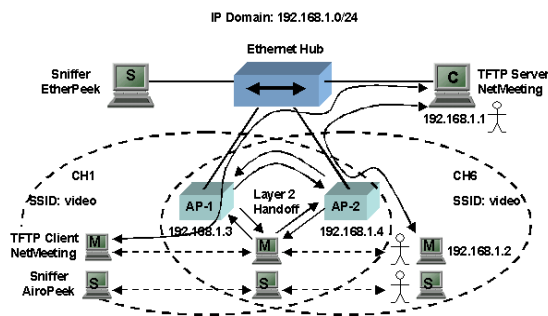


Fig. 7. Testbed implemented to measure handoffs.

The experiment ran as follows: one person with STA-M initially associated to AP-2 in channel 6, starts a voice over IP conference with other person located at STA-C. Such conversation will be sustained during all the test. STA-M and wireless sniffer are carried walking from AP-2 to AP-1 and coming back from AP-1 to AP-2. The trip is 20 meters in length around the hallways of the laboratory. On each round trip, two handoffs are displayed, one for each direction. The test is over when STA-M comes back to AP-2. The wireless

sniffer monitors permanently channel 1 in one way (from AP-2 to AP-1) and changes to permanently monitor channel 6 in the other way (from AP-1 to AP-2). The wired sniffer captures all Ethernet traffic in the DS. The same procedure was replicated for files transfer using TFTP from STA-M to STA-C. The file size was chosen so that the transfer lasts at least the time of a round trip (~2 minutes). The next section presents the obtained results.

#### V. RESULTS AND ANALYSIS

The main result is that users do not perceive any interruption in the audio conference, and files are correctly transferred in presence of layer 2 handoffs. However that result was obtained only if both APs are from the same model, that is, two AP-1000 or two AP-2000. When the testbed included one AP-1000 and one AP-2000, the reassociation from mobile station was not possible. The reason is that those AP's models use different roaming protocols. The AP-1000 model use a proprietary protocol from Lucent known as *WaveAround*, while the AP-2000 model use the IAPP protocol. In consequence, adjacent APs must use the same roaming protocol.

Besides, AP-2000 uses IAPP based preauthentication while AP-1000 does not use a preauthentication scheme. Thus, with the AP-2000 there is no exchange of authentication frames during a handoff, however, using the AP-1000 there is an explicit exchange of authentication frames between STA and AP just before requesting the reassociation. The APs in the experiment were configured to accept open authentication. Using both AP-1000 in the experiment, the reauthentication phase latency was around 1.5 ms, representing a minimum increment to the total handoff latencies. The *WaveAround* protocol uses a two-way message exchange like IAPP, so the measure strategy of  $\lambda_{r3}$  is similarly applied.

Packet	Source	Destination	Protocol	Data...	Ch...	Relative Time
576	AP2000-1-WIRELESS	Ethernet Broadcast	802.11 Beacon		11.0	1 20.889286
577	STA-M	Ethernet Broadcast	802.11 Probe Req		2.0	1 20.895987
578	AP2000-1-WIRELESS	STA-M	802.11 Probe Rsp		11.0	1 20.895489
579	AP2000-1-WIRELESS	AP2000-1-WIRELESS	802.11 Ack		11.0	1 20.896683
580	STA-M	AP2000-1-WIRELESS	802.11 Reassoc Req		2.0	1 20.940172
581	AP2000-1-WIRELESS	STA-M	802.11 Ack		2.0	1 20.940409
582	AP2000-1-WIRELESS	STA-M	802.11 Reassoc Rsp		11.0	1 20.940708
583	AP2000-1-WIRELESS	AP2000-1-WIRELESS	802.11 Ack		11.0	1 20.940911
584	AP2000-1-ETHERNET	Ethernet Broadcast	ARP Request		11.0	1 20.942129
585	STA-M	STA-C	IP UDP		11.0	1 20.948905
586	STA-M	STA-M	802.11 Ack		11.0	1 20.949086
587	STA-C	STA-M	IP UDP		11.0	1 20.960389
588	AP2000-1-WIRELESS	STA-M	802.11 Ack		11.0	1 20.960562
589	STA-C	STA-M	IP UDP		11.0	1 20.964319
590	AP2000-1-WIRELESS	STA-M	802.11 Ack		11.0	1 20.964499
591	STA-M	STA-C	IP UDP		11.0	1 20.976051
592	STA-M	STA-M	802.11 Ack		11.0	1 20.976229

Fig. 7. Wireless capture handoff (CH6 to CH1).

Packet	Source	Source Port	Destination	Dest. Port	Protocol	Relative Time
865	STA-C	IP-49586	STA-M	IP-49506	IP UDP	22.138121
866	STA-M	IP-49606	STA-C	IP-49586	IP UDP	22.140532
867	STA-M	IP-49606	STA-C	IP-49586	IP UDP	22.168062
868	STA-M	IP-49606	STA-C	IP-49586	IP UDP	22.193485
869	STA-C	IP-49586	STA-M	IP-49606	IP UDP	22.197355
870	STA-C	IP-49586	STA-M	IP-49606	IP UDP	22.201296
871	STA-M	IP-49606	STA-C	IP-49586	IP UDP	22.239196
872	AP2000-1-ETHERNET		Ethernet Broadcast		ARP Request	22.242007
873	AP2000-2-ETHERNET		AP2000-1-ETHERNET		ARP Response	22.242724
874	AP-1	10pp	AP-2	10pp	IP UDP	22.243296
875	AP-2	10pp	AP-1	10pp	IP UDP	22.244613
876	STA-M	IP-49606	STA-C	IP-49586	IP UDP	22.249656
877	STA-C	IP-49586	STA-M	IP-49606	IP UDP	22.259991
878	STA-C	IP-49586	STA-M	IP-49606	IP UDP	22.264042
879	STA-M	IP-49606	STA-C	IP-49586	IP UDP	22.276770

Fig. 8. Wired capture handoff (CH6 to CH1).

Figures 7 and 8 show the handoff capture files of AiroPeek

and EtherPeek, respectively, using both AP-2000.

The STA-M accomplishes the handoff in the trip from channel 6 to channel 1, while an audio conference is in course with STA-C. In both figures appear highlighted the ARP Request frame that we are using as a synchronization event. According to our previous discussion, we first measure  $\lambda_{f1}$ ,  $\lambda_{f3}$ , and then calculate  $\Lambda$ .

**$\lambda_{f1}$  Measurement:** The time between packets 577 (1<sup>st</sup> ProbeReq) and 580 (ReassocReq) corresponds to phase 1 latency. That is:  $\lambda_{f1} = 20.940172 - 20.895987 = 44.185$  ms.

**$\lambda_{f3}$  Measurement:** The reassociation phase latency is measured as the time between packets 580 (ReassocReq) and 584 (ARPreq) plus the time between packets 872 (ARPreq) and 875 (HORsp). That is:  $\lambda_{f3} = 1.957 + 2.606 = 4.563$  ms.

**$\Lambda$  Measurement:** Using (7),  $\Lambda = \lambda_{f1} + \lambda_{f3} = 48.748$  ms.

Now, we measure  $\Delta_1$  and then we obtain  $\lambda_b$  using (8). Next, using (11) we calculate T.

**$\Delta_1$  Measurement:** According to figure 7, phase 1 and handoff process initiated 46.142 ms before the ARP Request event. Now in figure 8, phase 1 and handoff process also started 46.142 ms before the ARP Request, that is at 22.195865 seconds of relative time or in a time between packets 868 and 869. According to figure 7, phase 3 initiated 1.957 ms before the ARP Request. Thus, in figure 8, phase 3 began at 22.24005 or in a time between packets 871 and 872. Therefore, packet 868 is the last packet sent by STA-M *before handoff* is initiated; packets 869, 870, and 871, were transmitted after  $\lambda_b$  and before phase 3 (*during handoff*), and packet 876 is the first packet sent by the STA-M *after handoff* is completed. We estimate  $\Delta_1$  as the time difference between packets 871 and 869, that is  $\Delta_1 = 41.841$  ms.

**$\lambda_b$  Measurement:** From (8),  $\lambda_b = \lambda_{f1} - \Delta_1 = 2.344$  ms.

**T Measurement:** From (11),  $T = \lambda_b + \lambda_{f3} = 6.907$  ms.

According to these results, the total handoff latency is divided in 90% for discovery phase and 10% for reassociation phase. However, the STA was unable to send or receive data packets just for around 14% of the total handoff latency. Almost during 86% of the total handoff process, the STA was exchanging data packets with other stations. Other related works [2], [3], and [11], imprecisely assume that the total handoff latency equals the total time during which the data traffic is interrupted. Therefore, HAMS improves the measurement precision compared to the traditional measurement techniques.

HAMS precision is subject to three clue conditions: (1) the first channel the STA scans is the one assigned to the new AP; (2) the ARP Request frame that new AP broadcast arrives simultaneously to both sniffers; and (3) HAMS is dependent on the rate of data to measure  $\Delta_1$  with accuracy. However, under our experiment, such conditions were taken in consideration; for instance, we left a continuous tone during the audio conference to guarantee a uniform flow of voice packets (3). We did not implement a switched backbone network in the DS to avoid bridging delays. We did not generate extra traffic load in the network so that the medium

access time, and transmission and propagation times can be negligible (2). The Orinoco wireless cards implement smart short scans with very short Channel-list [7], thus the scan latency measurement error is minimized (1).

Previous works in [2] and [3] indicate that current implementations of MAC layer do not meet the needs for real time traffic. Furthermore, they report handoff latencies much higher than us, reaching values around 1 second. They probably are arriving to that conclusion because they are using different vendors equipment that are not interoperables or WiFi approved. Besides, in [3] the handover was forced by temporarily switching off the radio transmitter of the AP to which the station was connected, which is not a natural handover produced by the station movement. In [2], authors use the term “Probe Delay” to what we call scan latency. We changed the term so that not to confuse with the *ProbeDelay* timer used in the discovery phase.

## VI. CONCLUSION AND FUTURE WORK

This article reviews the layer 2 handoff process in WLANs 802.11. The main contribution of this paper is the development of a new strategy for measuring layer 2 handoff latencies. Our strategy, called HAMS experimentally showed to be more detailed and precise than the traditional measurement strategy defined in [2]. HAMS is considered “precise” because it differentiates between the disconnection time T and the handoff process latency  $\Lambda$ . HAMS is based on *sniffers*, so it is simple to apply and is independent from the manufacturer of wireless products. HAMS measures  $\Lambda$  and T, while traditionally only  $\Lambda$  is measured and it is incorrectly assumed that  $\Lambda = T$ . We claim that what really affects to delay sensitive applications is T and no  $\Lambda$ . Using HAMS, values for  $T = 6.907$  ms and  $\Lambda = 48.748$  ms, were obtained. That implicates that during  $\Delta_1 = 41.841$  ms, after the scan cycle and before reassociation, the mobile station exchanged 3 data packets with other stations.

In our experiment, only 802.11b technology was tested, however, the strategy can also be applied to other higher rate wireless technologies. Lucent/Orinoco/Proxim wireless products were tested, including the AP-1000 and AP-2000 access points models. Those AP models showed interoperability problems due to they use a different inter access communication protocol. In our testbed no problems were detected to voice quality or file transfer during handoffs. However, we expect increments in the values for T and  $\Lambda$  if the number of mobile stations and traffic increases.

IAPP protocol has benefited phases 2 and 3, however, it is still necessary that the Wi-Fi alliance and the 11F group extend the benefits of IAPP to discovery. IAPP will allow in the future, handoffs initiated by the APs, making unnecessary the discovery phase as it is now defined.

In the future, we are interested in using HAMS for measuring handoffs with different vendor equipment. We also plan to work in developing an accurate strategy for measuring layer 3 handoffs with Mobile IP over 802.11 networks.

## REFERENCES

- [1] E. Buenfil, "Analysis of the reassociation process in mobile IP over 802.11 networks," *Master in Computer Science Thesis*, ITESM Cuernavaca Campus, Jan. 2005. (In Spanish).
- [2] A. Mishra, M. Shin, and W. Arbaugh, "An empirical analysis of the 802.11 MAC layer handoff process," University of Maryland, Technical Report CS-TR-4395, *ACM Computer Communications Review*, 2002.
- [3] H. Velayos and G. Karlsson, "Techniques to reduce IEEE 802.11b MAC layer handover time," *Laboratory for Communication Networks*, Royal Institute of Technology, Stockholm, Sweden, Apr. 2003.
- [4] D. Miras, "A survey of network QoS needs of advanced Internet applications," *Internet2 QoS Work Group*, Nov. 2002.
- [5] IEEE 802.11, "Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications," *IEEE Standard 802.11*, Aug. 1999.
- [6] IEEE 802.11F, "Trial-use recommended practice for multi-vendor access point interoperability via an inter-access point protocol across distribution systems supporting IEEE 802.11 operation," *IEEE Standard 802.11F*, Jul. 2003.
- [7] Orinoco TB 021/A, "...roaming with ORiNOCO/IEEE 802.11," *Technical Bulletin*, Dec. 1988.
- [8] M. S. Gast, "802.11 wireless networks, the definitive guide," O'Reilly & Associates, USA, 2002, pp. 114-137.
- [9] G. P. Pollini, "Trends in handover design," *IEEE Communications Magazine*, Mar. 1996.
- [10] Orinoco TB 034/A, "...Inter Access Point Protocol (IAPP)," *Technical Bulletin*, Feb. 2000.
- [11] P. De Cleyn, N.V. den Wijngaert, L. Cerdá, and C. Blondia, "A smooth handoff scheme using IEEE 802.11 triggers—design and implementation," *Computer Networks*, vol. 45, issue 3, pp. 345-361, Elsevier, Jun. 2004.
- [12] IEEE 802.11b, "Part 11: Wireless LAN medium access control (MAC) and physical layer (PHY) specifications: higher-speed physical layer extension in the 2.4 GHz band," *IEEE Standard 802.11b*, Sept. 1999.