Reducing MAC Layer Handoff Latency in IEEE 802.11 Wireless LANs

Sangho Shin
Andrea G. Forte
Columbia University
{ss2020,andreaf}@cs.columbia.edu

Anshuman Singh Rawat
New York University
asr245@nyu.edu

Henning Schulzrinne
Columbia University
hgs@cs.columbia.edu

ABSTRACT

With the growth of IEEE 802.11-based wireless LANs, VoIP and similar applications are now commonly used over wireless networks. Mobile station performs a handoff whenever it moves out of the range of one access point (AP) and tries to connect to a different one. This takes a few hundred milliseconds, causing interruptions in VoIP sessions. We developed a new handoff procedure which reduces the MAC layer handoff latency, in most cases, to a level where VoIP communication becomes seamless. This new handoff procedure reduces the discovery phase using a selective scanning algorithm and a caching mechanism.

Categories and Subject Descriptors

C.2.1 [**Computer System Organization**]: Computer- Communication Networks

General Terms

Measurement, Performance, Experimentation

Keywords

IEEE 802.11, Fast Handoff, Selective scanning

1. INTRODUCTION

IEEE 802.11-based wireless LANs have seen a very fast growth in the last few years and Voice over IP (VoIP) is one of the most promising services to be used in mobile devices over wireless networks. One of the main problems in VoIP communication is the handoff latency introduced when moving from one Access Point (AP) to another. As we will show below, the amount of time needed for the handoff in the 802.11 environment is too large for seamless VoIP communications. We were able to reduce the handoff latency using a modified handoff procedure, with modifications being limited to mobile devices and compatible with standard 802.11 behaviour.

MobiWac'04, October 1, 2004, Philadelphia, Pennsylvania, USA.

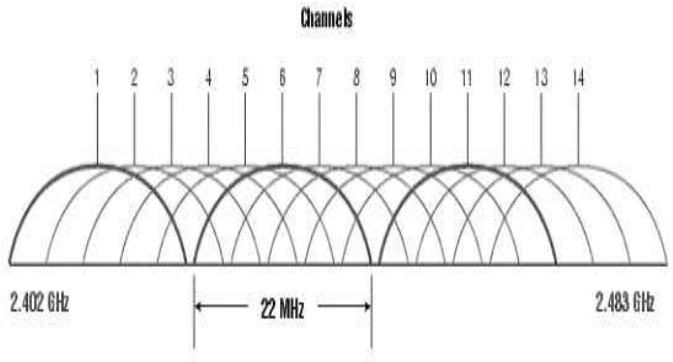

Figure 1: Channel frequency distribution in IEEE 802.11b

Below, first we discuss in brief work done in this particular area, followed by a brief description of how we tackled the problem. Then, in section 3, we describe the IEEE 802.11 architecture focusing on the management frames and the handoff process; then we will shortly describe the HostAP driver and how we modified it in order to implement our new algorithm. In section 5, we illustrate how we were able to reduce the total handoff latency to an average value of 129 ms by using a selective scanning procedure and to an average of 3 ms by using a caching mechanism. In section 7 and 8, we show the environment of the experiments and the measurement results.

2. RELATED WORK

A lot of work has been done to reduce the handoff latency when roaming between different subnets and many new schemes for mobile IP and route optimization have been proposed.

In this paper, we focused on reducing handoff latency at MAC layer. As we will describe in Section 4, MAC layer handoff latency can be divided into three components: probe delay, authentication delay and association delay.

Arunesh et. al. in [3] focused on reducing the reassociation delay. The reassociation delay is reduced by using a caching mechanism on the AP side. This caching mechanism is based on the IAPP protocol in order to exchange the client context information between neighboring APs. The cache in the AP is built using the information contained in an IAPP Move-Notify message or in the reassociation request sent to

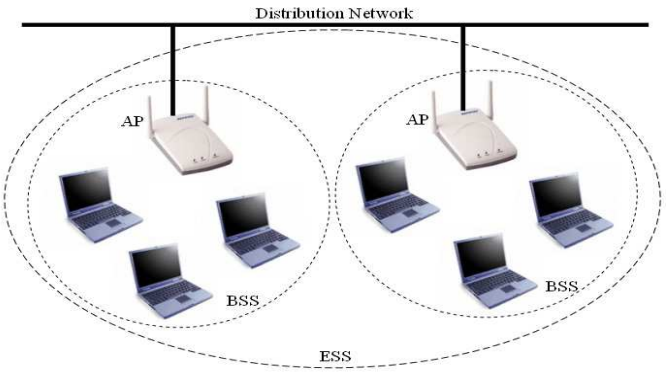

Figure 2: IEEE 802.11 architecture

the AP by the client. By exchanging the client context information with the old AP, the new AP does not require the client to send its context information in order to reassociate, hence reducing the reassociation delay.

Sangheun et. al. in [11] and Park et. al. in [12] focused on the IEEE 802.1x authentication process. This process is perfomed after the STA has already associated to a new AP. The IEEE 802.1x authentication delay is reduced by using the Frequent Handoff Region (FHR) selection algorithm.

In [2], it is shown how the discovery phase (scanning time) is the most time consuming part of the handoff process, taking over 90% of the total handoff delay, while (re)association time contributes only a few milliseconds.

Our work follows a novel approach and reduces the total handoff latency by reducing the scanning time. This is achieved by using a selective scanning algorithm and a caching mechanism. This caching data structure is maintained at the client side and no changes are required in the existing network infrastructure or the IEEE 802.11 standard unlike in [3]. All the required changes are done on the client side wireless card driver.

In [5], they also propose a selective scanning algorithm. However, their proposition relies on the use of neighbor graphs. This approach requires changes in the network infrastructure and use of IAPP. The scanning delay is defined as "the duration taken from the first Probe Request message to the last Probe Response message". This definition does not take into consideration the time needed by the client to process the received probe responses. This processing time represents a significant part of the scanning delay and increases significantly with the number of probe responses received. In our work and in [2], the time required for processing the probe responses received by the client is taken into consideration.

3. IEEE 802.11 STANDARDS

There are currently three IEEE 802.11 standards: 802.11a, 802.11b and 802.11g. The 802.11a standard operates in the 5 GHz ISM band, and it uses a total of 32 channels of which only 8 do not overlap. The 802.11b and 802.11g standards both operate in the 2.4 GHz ISM band and use 11 of the 14 possible channels. Of these 11 channels, only three do not overlap. While 802.11b can operate up to a maximum rate of 11 Mbit/sec, the 802.11g and 802.11a standards can operate up to a maximum rate of 54 Mbit/sec. The 802.11g standard is backwards-compatible with the 802.11b standard while the 802.11a standard, because of the different ISM band, is not compatible with the other two.

We will focus our attention on the IEEE 802.11b standard even though most of the concepts and notions described here are still valid for 802.11a and 802.11g. As we said earlier, the 802.11b operates in the 2.4 GHz ISM band. Its 14 channels are distributed over the range from 2.402 GHz to 2.483 GHz (see figure 1), each channel being 22 MHz wide. In US, only the first 11 channels are used. Of these 11 channels, only channels 1, 6 and 11 do not overlap. So, in a well configured wireless network, all or most of the APs will operate on channel 1, 6 and 11. Also, to avoid co-channel interference, two adjacent APs should never be on the same channel.

3.1 The IEEE 802.11 Wireless LAN architecture

The 802.11 architecture is comprised of several components and services that interact to provide station mobility to the higher layers of the network stack. We outline the following components as described in [8].

Wireless LAN station: The station (STA) is the most basic component of the wireless network. A station is any device that contains the functionality of the 802.11 protocol: medium access control (MAC), physical layer (PHY), and a connection to the wireless media. Typically, the 802.11 functions are implemented in the hardware and software of a network interface card (NIC). A station could be a laptop PC, handheld device, or an Access Point (AP). All stations support the 802.11 station services of authentication, deauthentication, privacy, and data delivery.

Basic Service Set (BSS): Basic Service Set (BSS) is the basic building block of an 802.11 wireless LAN. The BSS consists of a group of any number of stations.

Service Set Identifier (SSID): A service set identifier (SSID) is a unique label that distinguishes one WLAN from another. So all APs and STAs attempting to become a part of a specific WLAN must use the same SSID. Wireless STAs use the SSID to establish and maintain connectivity with APs.

3.2 IEEE 802.11 Management Frames

The IEEE 802.11 management frames enable stations to establish and maintain communications. The following are common IEEE 802.11 management frame subtypes, with the description quoted from [6]:

"*Authentication frame*: The 802.11 authentication is a process whereby the access point either accepts or rejects the identity of a STA. The STA begins the process by sending an authentication frame containing its identity to the access point. With open system authentication (the default), the STA sends only one authentication frame, and the access point responds with an authentication frame as a response indicating acceptance (or rejection).

Association request frame: 802.11 association enables the access point to allocate resources for and synchronize with a STA. A STA begins the association process by sending an association request to an access point. This frame carries information about the STA (e.g., supported data rates) and the SSID of the network it wishes to associate with. After receiving the association request, the access point considers associating with the STA, and (if accepted) reserves memory space and establishes an association ID for the STA.

Association response frame: An access point sends an association response frame containing an acceptance or rejection notice to the STA requesting association. If the access point accepts the STA, the frame includes information regarding the association, such as association ID and supported data rates. If the outcome of the association is positive, the STA can utilize the access point to communicate with other STAs on the network and systems on the distribution (i.e. Ethernet) side of the access point.

Reassociation request frame: If a STA roams away from the currently associated access point and finds another access point having a stronger beacon signal, the STA will send a reassociation frame to the new access point. The new access point then coordinates the forwarding of data frames that may still be in the buffer of the previous access point waiting for transmission to the STA.

Reassociation response frame: An access point sends a reassociation response frame containing an acceptance or rejection notice to the STA requesting reassociation. Similar to the association process, the frame includes information regarding the association, such as association ID and supported data rates.

Disassociation frame: A station sends a disassociation frame to another station if it wishes to terminate the association. For example, a STA that is shut down gracefully can send a disassociation frame to alert the access point that the STA is powering off. The access point can then relinquish memory allocations and remove the STA from the association table.

Beacon frame: The access point periodically sends a beacon frame to announce its presence and relay information, such as timestamp, SSID and other parameters regarding the access point, to STAs that are within range.

Probe request frame: A station sends a probe request frame when it needs to obtain information from another station. For example, a STA would send a probe request to determine which access points are within range.

Probe response frame: A station will respond with a probe response frame, containing capability information, supported data rates, etc., after it receives a probe request frame."

4. HANDOFF PROCEDURE WITH ACTIVE SCANNING

Handoff is a procedure executed when a mobile node moves from the coverage area of one AP to the coverage area of another AP. The handoff process involves a sequence of messages being exchanged between the mobile node and the participating APs. This sequence of messages can be divided into three types: probe, authentication and association, which will be described later in detail. The transfer from the old AP to the new AP results in state information being transferred from the former to the latter, consisting of authentication, authorization and accounting information. This can be achieved by an Inter Access Point Protocol (IAPP) that is currently under draft in IEEE 802.11f, or by a proprietary protocol, specific to a vendor.

4.1 Steps during Handoff

The handoff process can be divided into two logical steps: discovery and reauthentication [2].

Discovery: The discovery process involves the handoff initiation phase and the scanning phase. When the STA is moving away from the AP it is currently associated with, the signal strength and the signal-to-noise ratio of the signal from the AP decrease. This causes the STA to initiate a handoff. Now, the STA needs to find other APs that it can connect to. This is done by the MAC layer scanning function.

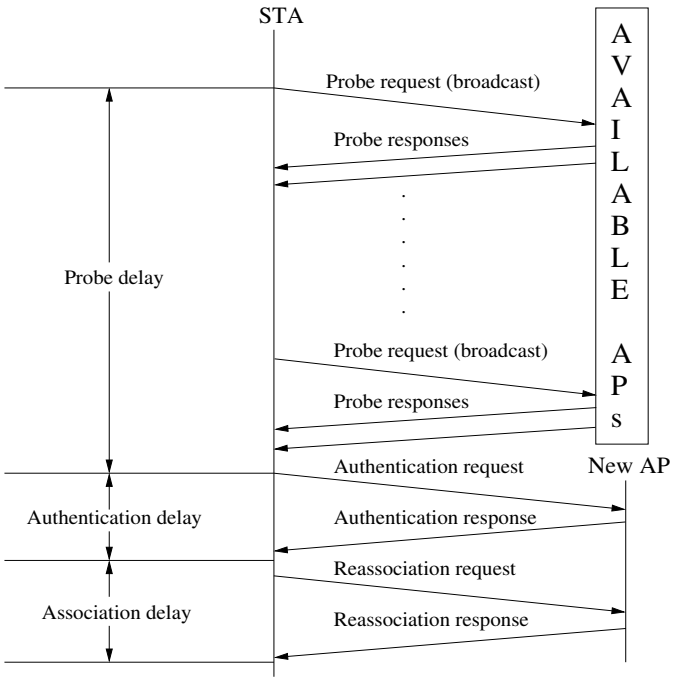

Figure 3: Handoff process using active scanning [2]

Scanning can be accomplished either in passive or active mode. In passive scan mode, the STA listens to the wireless medium for beacon frames. Beacon frames provide a combination of timing and advertising information to the STAs. Using the information obtained from beacon frames the STA can elect to join an AP. During this scanning mode the STA listens to each channel of the physical medium to try and locate an AP.

Active scanning involves transmission of probe request frames by the STA in the wireless medium and processing of the received probe responses from the APs. The basic procedure of the active scan mode includes the following steps as explained in [7]:

1. Using the normal channel access procedure, Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA), gain control of wireless medium.
2. Transmit a probe request frame which contains the broadcast address as destination.
3. Start a probe timer.
4. Listen for probe responses.
5. If no response has been received by minChannelTime, scan next channel.
6. If one or more responses are received by minChannelTime, stop accepting probe responses at maxChannelTime and process all received responses.[1]
7. Move to next channel and repeat the above steps.

After all channels have been scanned, all information re-

[1]minChannelTime and maxChannelTime values are device dependent.

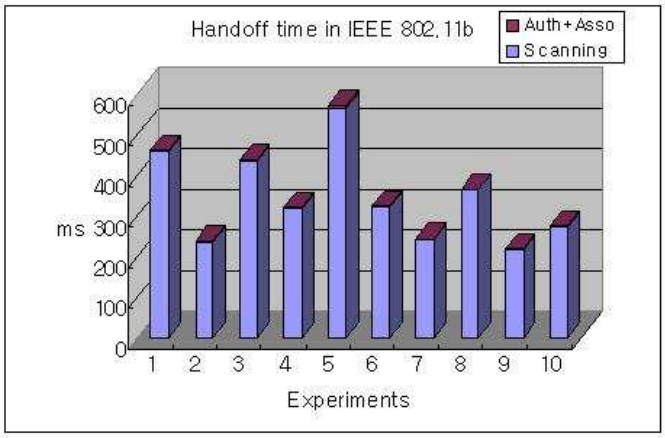

Figure 4: Handoff time in IEEE 802.11b

ceived from probe responses are processed so that the STA can select which AP to join next.

Reauthentication: The reauthentication process involves authentication and reassociation to the new AP as well as transfer of the STA's credentials from the old AP to the new AP. Authentication is a process by which the AP either accepts or rejects the identity of the STA. The STA begins the process by sending the authentication frame, authentication request, informing the AP of its identity; the AP responds with an authentication response, indicating acceptance or rejection. After successful authentication, the STA sends a reassociation request to the new AP which will then send a reassociation response, back to the STA, containing an acceptance or rejection notice. Figure 3, taken from [2], shows the sequence of messages expected during the handoff. As seen in Figure 3, the sequence of messages can be divided into three types:

1. **Probe messages**: Once the STA decides to look for other APs, the probing process starts. The STA starts sending out probe requests and then processes received probe responses, based on the active scanning algorithm explained above. The time involved in this probing process is called probe delay.

2. **Authentication messages**: Once the STA decides to join an AP, authentication messages are exchanged between the STA and the selected AP. The time consumed by this process is called authentication delay.

3. **Reassociation messages**: After a successful authentication, the STA sends a reassociation request and expects a reassociation response back from the AP. These messages are responsible for the reassociation delay.

5. FAST HANDOFF ALGORITHM

As described in [2] and confirmed by our experiments, the probe delay constitutes the biggest part (over 90%) of the handoff latency (Figure 4); for this reason, we focus on minimizing this delay.

In order to reduce the probe delay, we have focused our attention on two different aspects of the problem. First, we had to reduce the probe delay by improving the scanning procedure, using a selective scanning algorithm; second, we had to minimize the number of times the previous scanning procedure was needed. This second point was achieved with

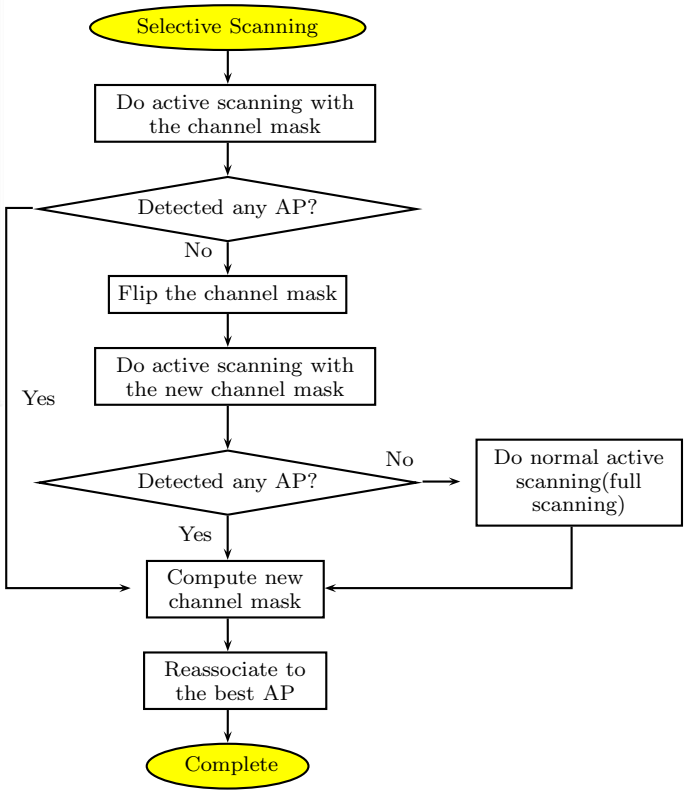

Figure 5: Selective scanning procedure

the use of a caching mechanism.

We will now describe the two algorithms.

5.1 Selective Scanning

As we described in Section 3, among the 14 possible channels that can be used according to the IEEE 802.11b standard, only 11 are used in USA and, among these 11 channels, only three do not overlap. These channels are 1, 6 and 11. The selective scanning algorithm is based on this idea. In the selective scanning, when a STA scans APs, a channel mask is built. In the next handoff, during the scanning process, this channel mask will be used. In doing so, only a well-selected subset of channels will be scanned, reducing the probe delay. In the following, we describe in detail the selective scanning algorithm.

1. When the driver is first loaded, it performs a full scan (i.e., sends out a Probe Request on all the channels, and listens to responses from APs).

2. A channel mask is set by turning on the bits for all the channels in which a Probe Response was heard as a result of step 1. In addition, bits for channel 1, 6 and 11 are also set, as these channels are more likely to be used by APs.

3. Select the best AP, i.e. the one with the strongest signal strength from among the scanned APs, and connect to that AP.

4. The channel the STA connects to is removed from the channel mask by re-setting the corresponding bit, as the likelihood of an adjacent AP on the same channel of the current AP is very small. So, the final formula for computing

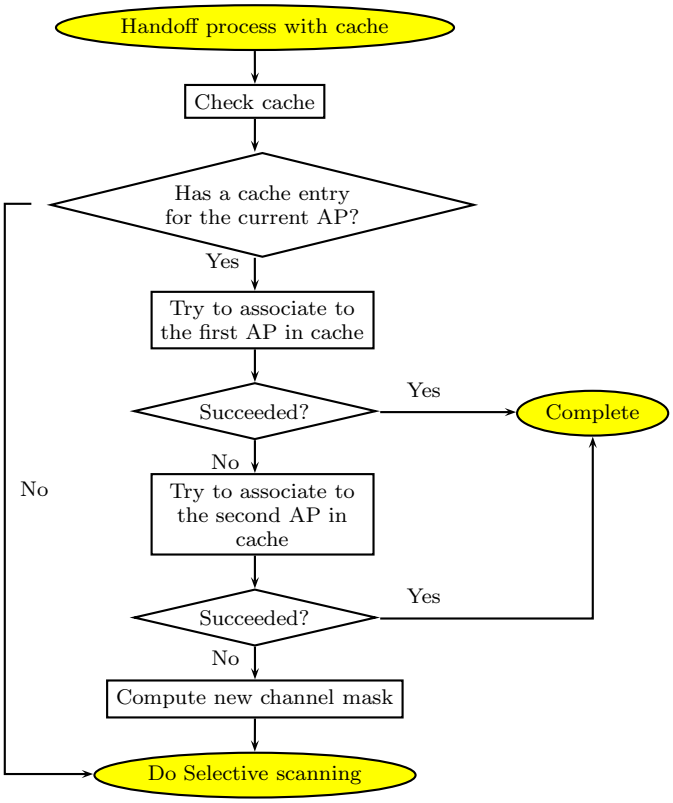

Figure 6: Caching procedure

Table 1: Cache structure

1	Key	Best AP	Second Best AP
2	MAC1 (Ch1)	MAC2 (Ch2)	MAC3 (Ch3)
:.			
10			

the new channel mask is 'scanned channels (from step 2) + 1 + 6 + 11 - the current channel'.

5. If no APs are discovered with the current channel mask, the channel mask is inverted and a new scan is done. If still no APs are discovered, a full scan, on all channels, is performed.

5.2 Caching

The selective scanning procedure described above reduced the handoff latency in our experiments (Section 7) to a value between 30% to 60% of the values obtained with the original handoff (see Figure 9), bringing the average values for the total handoff latency to 130 ms against an original handoff latency of 343 ms (see Table 2). For seamless VoIP, it is recommended that overall latency does not exceed 50 ms [1]. This further improvement was achieved by using an AP cache. The AP cache consists of a table which uses the MAC address of the current AP as the key. Corresponding to each key entry in the cache is a list of MAC addresses of APs adjacent to current one which were discovered during scanning. This list is automatically created while roaming.

Our cache has a size of ten, meaning that it could store up to ten keys and a width of two, meaning that for each key, it can store up to two adjacent APs in the list. Below we describe how the caching algorithm works:

1. When a STA associates to an AP, the AP is entered in the cache as a key. At this point, the list of AP entries, corresponding to this key, is empty.

2. When a handoff is needed, we first check the entries in cache corresponding to the current key.

3. If no entry is found (cache miss), the STA performes a scan using the selective scanning algorithm described in Section 5.1. The best two results based on signal strength are then entered in the cache with the old AP as the key.

4. If an entry is found (cache hit), we issue a command to associate to this new AP. On success, the handoff procedure is complete.

5. When the STA fails to connect to the first entry in cache, the second entry is tried and if association with the second entry fails as well, our selective scanning algorithm is used.

From the above algorithm, we can see that scanning is required only if a cache miss occurs; every time we have a cache hit, no scanning is required.

Usually, using cache, it takes less than 5 ms to associate to the new AP. But, when the STA fails to associate to the new AP, the firmware waits for a long time, up to 15 ms[2]. To reduce this time-to-failure we are using a timer. The timer expires after 6 ms, and the STA will then try to associate to the next entry in cache. In selective scanning, when the timer expires the STA performs a new selective scanning using the new channel mask.

A cache miss does not significantly affect the handoff latency. As mentioned above, when a cache miss occurs, the time-to-failure is only 6 ms. For example, if the first cache entry misses and the second one hits, the additional handoff delay is only 6 ms. When both cache entries miss, the total handoff delay is 12 ms plus selective scanning time, all of this still resulting in a significant improvement compared to the original handoff time.

6. IMPLEMENTATION

To implement our new algorithm, we had to modify the handoff procedure. Usually the handoff procedure is handled by the firmware; using the HostAP driver [10], we were able to emulate the whole handoff process in the driver.

6.1 The HostAP Driver

The HostAP driver is a Linux driver for wireless LAN cards based on Intersil's Prism2/2.5/3 802.11 chipset [10]. Wireless cards using these chipsets include the Linksys WPC11 PCMCIA card, the Linksys WMP11 PCI card, the ZoomAir 4105 PCMCIA card and the D-Link DWL-650 PCMCIA card.

The driver supports a so-called Host AP mode, i.e., it takes care of IEEE 802.11 management functions in the host computer and acts as an access point. This does not require any special firmware for the wireless LAN card. In addition to this, it has support for normal station operations in BSS and possible also in IBSS.[3]

[2]Actual values measured using Prism2/2.5/3 chipset cards. These values may vary from chipset to chipset.

[3]IBSS, also known as ad-hoc network, comprises of a set of

The HostAP driver supports a command for scanning APs, can handle the scanning results and supports a command for joining to a specific AP. It is also possible to disable the firmware handoff by switching to manual mode. By enabling this mode, we were able to control the card functionalities at the driver level and use our fast handoff procedure.

7. MEASUREMENTS

This chapter describes the hardware and software used for measuring the handoff latency and the environment in which the measurements were taken.

7.1 Experimental Setup

For the measurements, we used three laptops and one desktop. The laptops were a 1.2 GHz Intel Celeron with 256 MB of RAM running Red Hat Linux 8.0, a P-III with 256 MB of RAM running Red Hat 7.3, and another P-III with 256 MB RAM running Red Hat Linux 8.0. Linksys WPC11 version 3.0 PCMCIA wireless NICs were used in all three laptops. The desktop was an AMD Athlon XP 1700+ with 512 MB RAM running WinXP. The 0.0.4 version of the HostAP driver was used for all three wireless cards, with one of them modified to load our improved driver, and the other two cards were used for sniffing. Kismet 3.0.1 [9] was used for capturing the 802.11 management frames, and Ethereal 0.9.16 [4] was used to view the dump generated by Kismet and analyze the result.

7.2 The Environment

The experiments were conducted in the 802.11b wireless environment in the CEPSR building of Columbia University, on the 7th and the 8th floor. With only two laptops running the sniffer (Kismet), many initial runs were first conducted to get to know the wireless environment, specifically the channel numbers the APs were operating on, the handoff starting points and the next AP and channel the STA would connect to.

The environment in which the packet loss measurements were taken differed from the one above. The measurements were still taken in the CEPSR building of Columbia University, on the 7th and 8th floor, but some rogue APs were removed. This change in the environment caused a reduction of the original handoff time and consequentially a drastic reduction of the packet loss. This will be shown in section 8.2.

7.3 Experiments

After gathering sufficient information about the environment, we started taking the actual handoff measurements. One sniffer was set to always sniff on channel 1 (as the first Probe Request is always sent out on channel 1 in normal active scanning), and the other sniffer on the next channel the STA was expected to associate to. For the measurement, the system clock of the three laptops was synchronized using the Network Time Protocol (NTP). Also, to avoid multi-path delays, the wireless cards were kept as close as physically possible during the measurements.

For measuring the packet loss, in addition to the three laptops, the desktop was used as a sender and receiver. A UDP packet generator was used to send and receive data packets. Each UDP packet contained in the data field the packet sequence number to improve accuracy by linking the packet sequence number to its timestamp on all three laptops.

stations which can communicate directly with each other, via the wireless medium, in a peer-to-peer fashion.

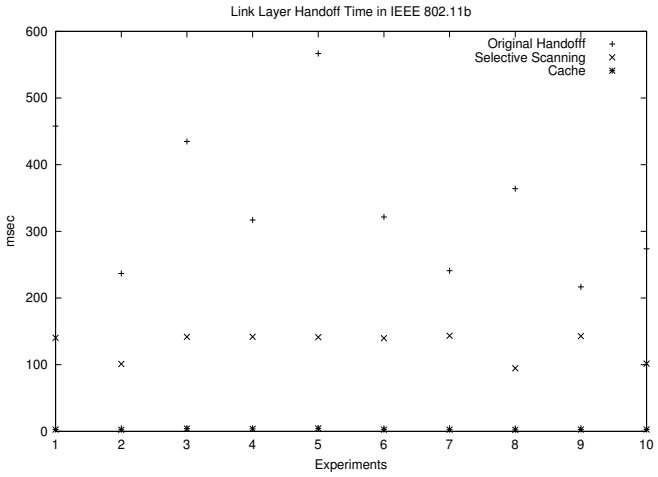

Figure 7: Link layer handoff time in 802.11b

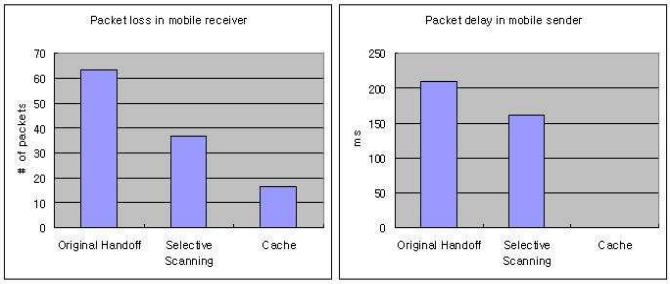

Figure 8: Packet loss and packet delay

8. MEASUREMENT RESULTS

In the following sections we present the results for the total handoff time and packet loss.

8.1 Handoff Time

Figure 7 and Table 2 present the results we obtained.

As can be seen, with selective scanning the handoff latency improved considerably, with an average reduction of 40%. But even this reduced time is not good enough for seamless VoIP. However, using the cache, the handoff latency time drops to a few ms, making it possible to have seamless VoIP. This huge reduction was possible because scanning, which took more than 90% of the total handoff time, was eliminated by using the cache.

8.2 Packet Loss

Table 3 present the results we obtained when the STA performing the handoff was the receiver. Table 4 present the results we obtained when the STA performing the handoff was the sender.

For measuring packet loss, UDP packets were transmitted to and from the STA, to simulate voice traffic during

Table 2: Handoff delay (ms) of 802.11b in link layer

Experiment	1	2	3	4	5	6	7	8	9	10	avg
Original handoff	457	236	434	317	566	321	241	364	216	274	343
Selective scanning	140	101	141	141	141	139	143	94	142	101	129
Caching	2	2	4	3	4	2	2	2	2	2	3

Table 3: Packet loss during handoff in mobile receiver (number of packets; 20 ms interval)

Experiment	1	2	3	4	5	6	7	8	9	10	avg
Original Handoff	36	55	32	79	37	122	134	32	69	36	63
Selective Scanning	88	24	26	19	31	28	46	26	64	18	37
Cache	16	15	14	14	16	15	23	21	15	14	16

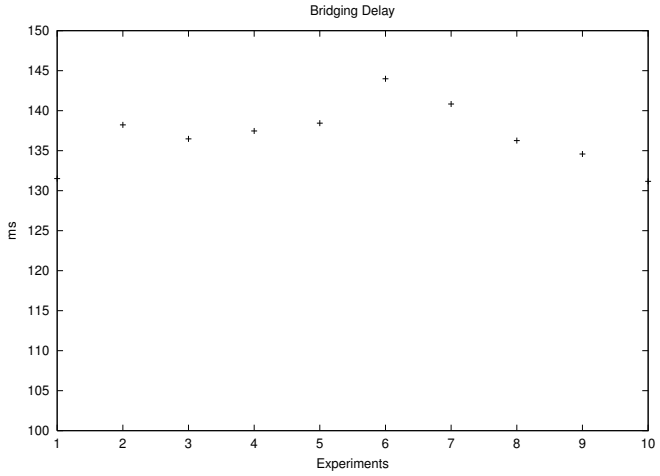

Figure 9: Bridging delay

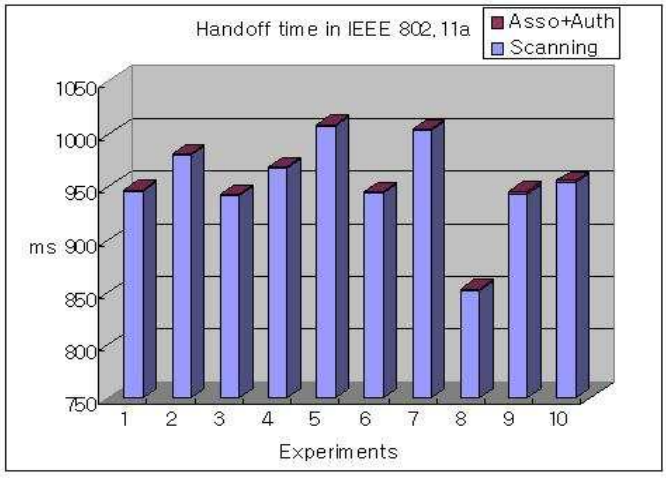

Figure 10: Handoff time in IEEE 802.11a

the handoff. Transmitting data packets adds to the handoff delay. This delay is caused by the fact that data packets are transmitted *during* the handoff process, in particular between the last probe response and the authentication request. This behaviour is only noticed when the STA performing the handoff is the sender (see Table 5). When the STA performing the handoff is the receiver, no such delay is introduced. However, a new delay is introduced. This new delay, *bridging delay* [2], is caused by the time needed for updating the MAC addresses to the ethernet switches forming the distribution system. In particular, when handoff happens and the STA associates to the new AP, the switch continues to send the packets, addressed to the STA, through the old AP which after many retries, discards them. This behaviour persists for about 140 ms[4] (see Figure 9) after which the MAC addresses have been updated and the switch starts forwarding the data packets, addressed to the STA, through the new AP. This results in an additional packet loss.

As can be seen in Figure 8, when the receiver is performing the handoff, the packet loss drops to about 60% and 40% of the value obtained with the original handoff using selective scanning and cache, respectively. When using cache, the effect of the bridging delay is particularly prominent. Table 3 shows how, even though the handoff time is only a few milliseconds, when using a cache, the packet loss is still considerable.

Figure 8 also shows the average packet delay introduced by the handoff procedure when the sender is performing the handoff. For VoIP sessions, packets exceeding a delay of 100 ms can be considered lost. Table 4 shows the packet delay when using the original handoff scheme, selective scanning and cache. Even though selective scanning reduces such a delay by about 25%, in order to achieve seamless VoIP communication, the caching mechanism is necessary.

As a note, the behaviour of the selective scanning algorithm is not dependent on the environment, while the original handoff performance is very much affected by it. Table 2 and Figure 7 show an environment in which rogue APs are present. Table 5 refers to a clean environment, without the presence of rogue APs. As we can see, the selective scanning behaviour is very consistent, while the original handoff performance deteriorates with the environment.

9. CONCLUSIONS AND FUTURE WORK

In this paper we described the handoff procedure and demonstrated how the handoff latency can be substantially

[4]Actual values may vary according to the environment.

Table 4: Delay during handoff in mobile sender (ms)

Experiment	1	2	3	4	5	6	7	8	9	10	avg
Original Handoff	281	229	230	210	209	227	185	174	189	168	210
Selective Scanning	185	132	147	131	204	182	164	133	151	184	161
Cache	0	0	0	0	0	0	0	0	0	0	0

Table 5: Summary of result

	Handoff time in mobile receiver (ms)	Packet loss in mobile receiver (num of packets)	Handoff time in mobile sender (ms)	Packet delay in mobile sender (num of packets)
Original Handoff	182.5	63.2	201.5	210.7
Selective Scanning	102.1	37.0	141.1	161.7
Cache	4.5	16.3	3.9	0

reduced with the use of a caching mechanism combined to a selective scanning algorithm. We demonstrated how, in the best case, we were able to reduce the handoff latency to an average value of 129 ms by only using the selective scanning algorithm and to an average value of 3.0 ms by using the caching mechanism (Table 2). This reduction in handoff latency also considerably decreased packet loss and packet delay (Table 5).

By using a dynamic channel mask (refer to selective scanning algorithm 4 and 5 in section 5.1), scanning a subset of channels can be used as a generic solution.

Another important result of our work is that by using selective scanning and caching, the probing process, the most power consuming phase in active scanning, is reduced to the minimum. This makes it possible to use the active scanning procedure also in those devices such as PDAs where power consumption is a critical issue.

With the new IEEE 802.11g standard out, we will be testing our algorithm to the new standard. The extension of our algorithm to the new 802.11g standard will only require minor adjustments, if any.

Figure 10 shows the original handoff time in IEEE 802.11a networks. As can be seen, the discovery phase is still the most time consuming phase of the handoff process. Future testing will be done in an IEEE 802.11a environment. The extension of our algorithm to this standard will also require minor adjustments such as modification of the channel mask (selective scanning), improved cache dimensioning and management.

The channel with the best signal is not necessarily the best channel to connect to because it could be much more congested than a channel with a lower signal strength. Because of this, a heuristic which considers bit rate information together with signal strength can achieve optimal performance.

A procedure in which an AP somehow knew its neighboring APs [3] and could provide that information to the STA could be used to fill the cache. This could also be combined with a positioning algorithm such as GPS or any other WiFi positioning algorithm allowing a real-time filling and refreshing of the cache, according to the STA actual position, always resulting in a cache hit.

Very critical issues are the cache size and cache management policy. A good cache policy, together with the use of AP neighboring and other heuristics, can achieve seamless VoIP sessions.

10. ACKNOWLEDGMENTS

This work was supported by grant of SIPquest Inc. Equipment was partially funded through grant CISE 02-02063 of the National Science Foundation.

11. REFERENCES

[1] General characteristics of international telephone connections and international circuits. *ITU-TG*, 114, 1998.

[2] M. S. A. Mishra and W. Arbaugh. An Empirical analysis of the IEEE 802.11 MAC Layer Handoff Process. *ACM SIGCOMM Computer Communication Review*, 33(2):93–102, April 2003.

[3] M. S. A. Mishra and W. Arbaugh. Context caching using neighbor graphs for fast handoffs in a wireless network. Technical report, University of Maryland, February 2004.

[4] G. Combs. Ethereal network protocol analyzer.

[5] H.-S. K. et. al. Selecive channel scanning for fast handoff in wireless lan using neighbor graph. Japan, July 2004. International Technical Conference on Circuits/Systems, Computer and Communications.

[6] J. Geier. Understanding 802.11 frame types. Technical report, Jupitermedia Corporation, August 2002.

[7] IEEE. *IEEE Std. 802.11, Wireless LAN Medium Access Control (MAC) and Physical (PHY) specifications: High Speed Physical Layer Extension in the 2.4 GHz Band*, 1999.

[8] A. Jain. Handoff delay for 802.11b wireless lans. Technical report, University of Kentucky, 2003.

[9] M. Kershaw. Kismet wireless network sniffer.

[10] J. Malinen. Host AP driver for intersil prism2/2.5/3.

[11] S. Park and Y. Choi. Fast inter-ap handoff using predictive-authentication scheme in a public wireless lan. Networks2002 (Joint ICN 2002 and ICWLHN 2002), August 2002.

[12] S. Park and Y. Choi. Pre-authenticated fast handoff in a public wireless lan based on ieee 802.1x mode. Singapore, October 2002. IFIP TC6 Personal Wireless Communications.