IMPROVING FAST AND SMOOTH HANDOFF IN IEEE 802.11 WIRELESS NETWORKS

Deepak Y. Bhadane*

Akhilesh A. Waoo**

P.S.Patheja***

ABSTRACT

IEEE 802.11 Wireless LANs are increasingly being used in real environments for broad-band access. Such large scale IEEE 802.11 WLAN implies the need for client station support from one Access Point to another. The client stations (STA) can move freely, but because of the short range of their Access Points (APs), they usually need to reassociate with different APs and communicate through them. When changing APs, a client station starts a process known as a handoff that can take up to few seconds, which is too long for real-time applications such as Voice over IP (VoIP).Various solutions have been proposed to change or improve the client behavior when doing a handoff. The delay incurred in scanning for APs across channels contributes to 90% of the total handoff delay. In this paper, the Fast Scan scheme is proposed which reduces the scanning delay by using a client-based database. The net handoff delay is reduced for IEEE 802.11b networks. The proposed schemes do not need any changes in the infrastructure (access points) and require only a single radio and a small cache memory at the client side.

Keywords: *Wireless Local Area Networks (WLAN), IEEE802.11, Access Points, VoIP.*

*BIST, Bhopal, Madhya Pradesh.

**Assistant Professor, Department of M. Tech., BIST, Bhopal, Madhya Pradesh.

***HOD, Department of M.Tech., BIST, Bhopal, Madhya Pradesh.

I. INTRODUCTION

The IEEE 802.11 wireless LAN (WLAN) technology has spread rapidly [3], as it is cheap, and allows anytime, anywhere access to network data. As bandwidth of WLANs has grown, multimedia over WLAN has begun to look feasible. The IEEE 802.11n standard now offers a bandwidth of 100 Mbps which is sufficient for high-quality multimedia. Mobility is a natural consequence of wireless technology especially when used for applications such as voice communication. However, mobility with multimedia communication requires fast seamless transfer (i.e. *handoff)* of the wireless device's connection from one access point to the other.

A Wi-Fi network has access points (AP) to which stations get associated. Data transfer between stations take place through the AP. An AP and its associated mobile stations form a basic service set (BSS). A handoff occurs when a *station* (STA) moves beyond the radio range of its *access point* (AP), and enters another BSS. Management frame exchange takes place between the STA and the AP during the handoff procedure. Consequently, the handoff process incurs some latency, during which the STA is unable to send or receive traffic.

In this context, we propose to get rid of mobility management in mobile stations and put it entirely inside the network of interconnected access points [2]. To do so we simply change to our point of view: we propose to consider stations as being fixed; conversely, the access point to which a station is connected is now mobile. Of course, physically this is not the case, and we introduce the concept of *virtual access point*, which is a mobile entity within the infrastructure network. Every mobile station is therefore associated with its own virtual access point when it connects to the network, the latter moving along with its client. In this way we totally get rid of the problems introduced earlier, while being fully compatible with legacy clients, without any neither hardware nor software modification. We will show how we could easily implement this concept using a packet manipulation framework called *PacMap*. Using this lightweight framework for rapid prototyping, we have developed a first implementation in Python to test the concept on a simple scenario, and then natively for improved performance. A first round of experiments with these prototypes gave some insight on performances and limitations of the proposed solution. Finally, taking a look at related work on mobility in WiFi networks, we will conclude and present future work.

In infrastructure mode - the most common form of deployments - if a mobile station (STA) wishes to send or receive data [7], it needs to associate with an Access Point (AP). The AP and its associated clients form a Basic Service Set (BSS). A set of BSSs form an Extended Service Set (ESS). IEEE 802.11 usually follows the Distributed Co-ordination function

(DCF), which uses CSMA/CA with a random backoff algorithm. All data transfers between mobile stations or a client and server in the backbone (Internet) is facilitated through the AP. While this mode has the advantages of minimal configuration and low cost, there are some issues which limit the use of WLANs. Enhanced FastScan builds on the initial idea, and further uses direction and relative position of the client with respect to the current AP to divide the current BSS area into different sub-sectors. So far the most popular AP scan strategy is active scan the client actively sends a probe request and waits a period of time on the channel to receive all probe responses issued by APs.

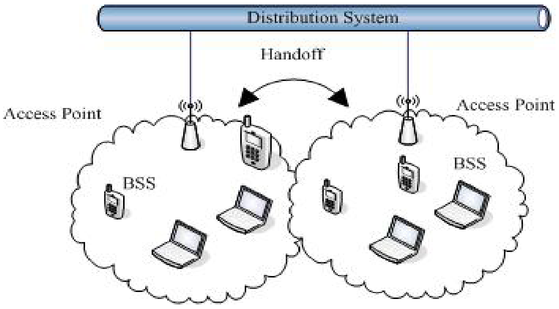

Figure 1: The Handoff Scenario

A typical handoff scenario in a IEEE 802.11 WLAN is shown in Figure 1.The handoff process is essentially divided into three phases - scanning, re-authentication and re-association. Scanning of channels for APs can be done in two ways - passive and active - according to the IEEE 802.11 standard. Passive scanning which involves the reception of beacon frames by the client in each channel usually takes up to a second to complete and hence is not favored in time-critical situations like a handoff. Active scanning involves active determination of each channel status by sending probes; this process can be completed within 250ms in a typical IEEE 802.11b deployment. Once the best AP is identified, the station authenticates and re-associates with the new AP. The default IEEE 802.11 handoff mechanism involving scanning of all channels provides, at best, a handoff delay of 300ms.The proposed Fast Scan strategy reduces the latency by i) reducing both the number of channels to scan and ii) the number of APs to scan in each channel, by utilizing a client database. The database stores information about the neighboring best APs and their corresponding channels, for each entry of the current AP. The client uses the database to select a subset of all the system channels and sends a unicast probe request only to the best AP for each channel in the subset. With the help of this information, broadcast probing is avoided and the client only needs to wait for a single probe response. As a result, the latency is reduced.

The remainder of this paper is organized as follows. Section II gives the background & related work, section III presents design of Handoff procedure, section IV gives implementation & finally, Section V concludes the whole paper.

II. BACKGROUNDS AND RELATED WORK

The basic handoff process in IEEE 802.11 consists of three phases - Scanning, Authentication and Re-Association. First, the mobile station has to determine that it is moving out of range of the AP and initiates handoff. This is usually done through monitoring the signal-to-noise ratio (or received signal strength) and detecting a downward crossing of a pre-defined handoff threshold; the channel scanning phase then starts. Velayos et al. [3] suggest for example, that three consecutive transmission failures is enough to trigger a handoff. Handoff can also be detected through missed beacons, if the station is not sending or receive any data packets. In passive scanning, the station listens for beacon messages on every channel. Thus the mobile node can create a candidate set of APs prioritized by the received signal strength indicator (RSSI) and select the strongest AP. But passive scanning is usually not favored during a handoff scenario, as the station has to wait for at least one Beacon Interval (usually 100ms) to get most or all of the beacons in that channel.

A. The Handoff Process in 802.11

As is said before, connection switch among different APs in a wireless network is essential to keep an on-going session alive. Simple as it may sound; a disruption of com-munication is likely to happen before a successful handoff. It’s largely due to ‘the improvident nature’ of 802.11 standards. That is to say, the STA (mobile station) doesn’t bother to prepare for any possible deterioration of connection quality, a parameter which often measured in RSSI. Only when the connection quality becomes substantially poor will the STA start to scan and search for other prospective APs to get connected. This process of AP scan and reconnection turns out to be intolerably slow, i.e. may take as much as 200-300ms or even longer, which is way too long for delay sensitive services such as VoIP, which sees incoming voice packets every 20ms.On careful analysis [3], [4], one finds out that the delay caused by reconnection, which can be further broken down to authentication and (re)association, is quite constant, since they are actually bandies of no more than 10 messages. 80% to 90% of the delay goes to the scan phase.

B. *MadWiFi Device Driver*

Our proposed mechanisms were implemented in the Mad-WiFi driver [3], which is a Linux kernel device driver for wireless LAN chipsets from Atheros Communications. The MadWiFi code consists of four main modules: net80211 stack, the Atheros specific ‘ath’ part, Hardware Abstraction Layer (HAL) and rate algorithms for selecting the best transmission rates. Our modifications have been in the net80211 module. We now discuss how a potential AP is extracted from the scan cache. We use two main parameters: RSSI threshold and hysteresis.

C. Related Work

Apart from solutions several layer-2 handoff mechanisms for WLAN have been proposed in recent papers [1], [2], [3], [4], [7]. We describe some of the important solutions briefly and compare them. In Sync Scan [7], clients passively scan the channel by switching its current working channels. A beacon broadcast arrangement is done for time synchronization. For a short time after this beacon, the AP does not send any data to the clients which avoid loss of data frames which are destined to the client. By periodic switching to each channel all nearby access points can be discovered and thus eliminating the need of discovery of APs at the time of handoff. In [1], the authors propose an algorithm in which an AP informs the client about its neighbour list and the client scans only those channels which are in that list. In Multiscan a dual radio wireless network card is used. One radio is used for packet transmission while the other radio is used for background scanning and pre-associating with alternate APs.

In [2], a client measures the signal strength of received beacon of all the APs operating on the current, and the overlapping channels. Depending on the long term and short term trends in these signals received from the different APs, handoff decision is taken. The schemes proposed above have some disadvantages. Most need code modification at the APs. They are also not available as open source implementations. Some solutions require multiple wireless cards. This motivated us to build an open source handoff solution which improves on some of the features of previous papers, and presents some new features that improve handoff efficiency. Specifically, we improve the neighbor list mechanism so that no AP-side code modification is required, and add background scanning with *preauthentication* to further reduce handoff latency.

III. DESIGN OF A FAST HANDOFF SOLUTION

Existing implementations check the RSSI of the packets received from the currently associated AP. A handoff procedure is triggered when this RSSI falls below a certain threshold. This procedure consists of the following phases: 1) Probe phase, in which all 802.11 channels are scanned, meaning that a probe is sent, and the RSSI and other information is noted from the response. The AP with the best RSSI is selected as the new AP to associate to. 2) Authentication phase. 3) Reassociation phase, after which the data transfer begins. A station can reduce the probe delay if the list of potential APs and their operating channels is known beforehand. In that case, at the time of handoff, a station can reduce the number of channels to be scanned by scanning only these known channels. Our proposed solution rests on three main mechanisms for reducing total handoff latency: background scan, server based restricted channel set and preauthentication with no modifications at the AP.

A. Protocol details

In this section [1], we describe the Multichannel Virtual Access Point protocol in detail.

Figure 2 presents the following steps:

1) A station (STA) is associated with *APi* on channel *i*. STA starts moving and *APi* detects that the signal of STA is less than a threshold *Threshold*.
2) *APi* sends to its neighbor APs (*APj_=i*) a **Scan Request** message through the DS.
3) All *APj_=i* switch to channel *i* and listen to STA packets for a short period of time.
4) If *APj* successfully listens to STA packets, *APj* sends a **Scan Response** message to *APi* through the DS.
5) *APi* receives the **Scan Response** messages and chooses the AP with the best signal, if better than its own.
6) *APi* sends a **Station Move** message to the chosen *APk* through the DS. *APk* is listening to channel *k*.2
7) *APk* receives the **Station Move** message and starts sending the beacons for STA.
8) *APi* sends beacons to the STA with the Channel Switch Announcement (CSA) element to force the STA to switch to channel *k*.
9) STA receives the beacons with the CSA element and switches to channel *k.*
10) STA has changed AP and channel without losing connectivity. From the STA perspective; it is still connected to the same VAP.

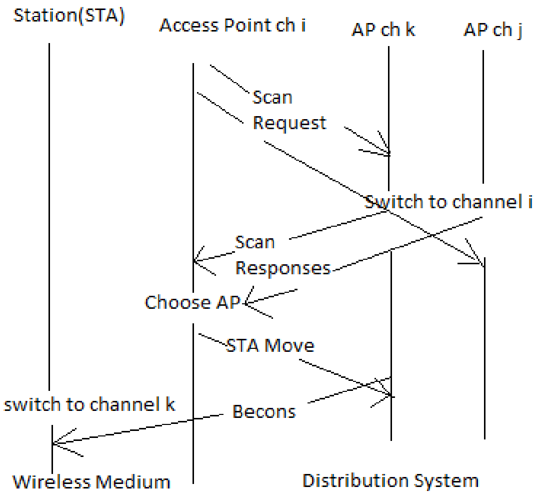

Figure 2: Multichannel VAP protocol

IV. IMPLEMENTATION

We provide fast & smooth Handoff in IEEE 802.11 WLAN that is to reduce the time required by handoff procedure using tool PACMAP [1]: PACket MAniPulation framework. PACMAP is a framework for controlling and manipulating 802.11 frames. It is a user-space frame monitor and injector that allows for fast prototyping of modifications or customization of the IEEE 802.11 MAC protocol (management and data functions).At the same time, MadWifi makes it possible to inject packets and send them over the wireless medium. A TAP3 interface emulates an Ethernet device and handles Ethernet frames. PACMAP uses a TAP interface.

The CSA element is sent in the beacon only when the new AP is chosen. In our implementation, the current AP sends 3 consecutive beacons, with an interval of 100 ms between them, decrementing in each beacon the value of Channel Switch Count. When this value reaches 0, 300 ms after the first CSA announcement, the AP deletes the station from the associated client list and stops sending beacons for the station.

A. Inter-AP messages

Inter-AP communication takes place over the DS as an Ethernet wired network commonly interconnects APs in current deployments. Messages are sent over reliable TCP connections between APs[1]. The Inter-AP messages contain the following information:

- **Scan Request**: station MAC address, station IP address, BSSID, station channel.
- **Scan Response**: station MAC address, station IP address, station Received Signal Strength Indicator (RSSI), new AP channel.

- **Station Move**: station MAC address, station IP address, CSA count, Beacon interval.

We have implemented Inter-AP communication using TCP sockets between the AP Ethernet interfaces. Each AP listens on a specific port and sends messages to other APs through these sockets.

B. Channel Switch Announcement

An AP uses the CSA element as described in the IEEE 802.11 standard to advertise that it is switching to a new channel. It contains the following fields:

- **Channel Switch Count**: number of beacons to listen to before channel switch. This value decreases in each consecutive beacon.
- **Channel Switch Mode**: indicates any restrictions on transmission before the channel switch..

Each station associates with its own VAP and receives a custom beacon, so the channel switch only applies to the station that changes APs. As the MadWifi driver implements the CSA element, stations can use this solution without client side modification. The CSA element is sent in the beacon only when the new AP is chosen.

V. RESULTS

In this paper, the FastScan scheme is proposed which reduces the scanning delay by using a client-based database. The Handoff delay is reduced to as low as 20ms for IEEE 802.11b networks, well under the 50ms voice threshold. A better scheme Enhanced FastScan is also proposed which uses the direction and relative position of the client with respect to the current AP. This scheme satisfies voice constraints for IEEE 802.11a networks and provides precise Handoffs in IEEE 802.11b networks (avoiding wrong Handoffs). To facilitate WLAN simulations for future research, a full-featured multi-channel IEEE 802.11 infrastructure mode model was implemented on top of the existing model. These Handoff schemes were analyzed using null authentication. If secure authentication schemes like IEEE 802.1X and WEP are used, the authentication delay can last up to a second. Future research in Handoff optimization can be directed towards reducing authentication delay in secure IEEE 802.11 networks.

VI. CONCLUSION

We have presented Multichannel VAPs, a new solution using the VAP scheme for multichannel WLANs, where the client changes AP without disrupting its current communications. The advantage of Multichannel VAPs is low latency of handoffs, which is required for multimedia applications such as VoIP.

We have designed and implemented a fast handoff mechanism for IEEE 802.11 WLANs, to reduce the latency incurred due to handoff at layer-2 in such a way that requirements of multimedia traffic are met. Our proposed fast handoff solution rests on three main mechanisms for reducing the handoff latency: The solution was implemented in an open source Linux device driver, MadWiFi, and the solution requires only client side modification. In the paper, we have not studied the effect of speed of mobility on the handoff latency.

ACKNOWLEDGEMENT

I express my sincere gratitude and acknowledgement towards P.S.Patheja sir and Akhilesh A. Waoo sir who guided me. It was their constant support & inspiration without which my efforts would have taken this shape. I sincerely thank them for this & seek them support for all my future endeavors.

REFERENCES

1. Maria Eugenia Berezin, Franck Rousseau, Andrzej Duda,” Multichannel Virtual Access Points for Seamless Handoffs in IEEE 802.11 Wireless Networks”, in IEEE 2011.
2. Y. Grunenberger and F. Rousseau, “Virtual Access Points for Transparent Mobility in Wireless LANs”, in *WCNC*, 2010.
3. Yogesh Ashok Powar and Varsha Apte, “Improving the IEEE 802.11 MAC Layer Handoff Latency to Support Multimedia Traffic”, in proceedings of the WCNC 2009.
4. Xi Chen and Daji Qiao,”HaND: Fast Handoff with Null Dwell Time for IEEE 802.11 Networks”, in proceedings of the IEEE INFOCOM 2010.
5. J. Teng, C. Xu, W. Jia, and D. Xuan, “D-Scan: Enabling Fast and Smooth Handoffs in AP-dense 802.11 Wireless Networks,” in *INFOCOM*, 2009.
6. G. Athanasiou, T. Korakis& L.Tassiulas,”Cooperative Handoff in Wireless Networks”, in IEEE 2008.
7. H. Velayos and G. Karlsson,” Techniques to reduce the IEEE 802.11b handoff time”, in *IEEE International Conference on Communications*, volume 7, pages 3844–3848 Vol.7, 2004.