Understanding Handoffs in Large IEEE 802.11 Wireless Networks

Ramya Raghavendra[†], Elizabeth M. Belding[†], Konstantina Papagiannaki[‡], Kevin C. Almeroth[†]
[†]Department of Computer Science, University of California, Santa Barbara
[‡]Intel Research, Pittsburgh
{ramya, ebelding, almeroth}@cs.ucsb.edu, dina.papagiannaki@intel.com

ABSTRACT

As the utility of wireless technology grows, wireless networks are being deployed in more widely varying conditions. The monitoring of these networks continues to reveal key implementation deficiencies that need to be corrected in order to improve protocol operation and end-to-end performance. Using data we collected from the 67^{th} Internet Engineering Task Force (IETF) meeting held in November 2006, we show that under conditions of high medium utilization and packet loss, handoffs can be incorrectly initiated. Using the notion of *persistence* and *prevalence* for the association of a client to an Access Point (AP), we show that although the clients were predominantly static, the handoff rate is surprisingly high. Through the analysis of the data set, we show that unnecessary handoff events not only increase the amount of management traffic in the network, but also severely impact client performance.

Categories and Subject Descriptors: C.2.2 [Computer - Communication Networks]: Network Protocols; C.2.3 [Computer - Communication Networks]: Network Operations
General Terms: Experimentation, Management, Measurement, Performance.
Keywords: Handoff, Wireless networks, Congestion, IEEE 802.11.

1. INTRODUCTION

IEEE 802.11-based WLANs have experienced rapid growth in recent years as a chief means of providing Internet connectivity to users. Large WLAN deployments are popular in locations such as conferences, university campuses, hotels, and airports. These networks are characterized by a large number of access points (APs) that are densely deployed to support network usage by many simultaneous users. Dense AP deployment helps ensure that the overall user demand is met and network coverage is provided, especially if users are mobile.

The main factor constraining performance in IEEE 802.11 WLANs is the limited number of orthogonal channels, three in the case of 802.11b/g. In order to provide good wireless coverage and sustain high transmission rates, it is commonly the case that a large WLAN deployment has several APs within range of each other. Due to the limitation in the number of orthogonal channels, multiple APs within interference range are often configured to transmit on the same channel. Large WLAN deployments are hence likely to suffer from high interference. This is particularly true when WLANs need to support flash crowds, which are defined as a sudden surge in the number of users attempting to connect to and access the WLAN [1]. Increased interference and load gives rise to several problems such as intermittent connectivity, low throughput and high loss, resulting in an unreliable network and sometimes a complete breakdown.

Congestion is detrimental to the performance of large wireless networks, as it leads to missed transmission opportunities and inefficient medium utilization. More importantly, increased loss may incorrectly lead clients to initiate a handoff in search of a better AP in their vicinity. As congestion increases, the rate of handoff increases, even in the absence of mobility. We show that the majority of these handoffs are unnecessary and are actually detrimental, leading to lower client throughput.

To investigate the prevalence of the these problems in WLANs, we collected traces from the 67^{th} Internet Engineering Task Force (IETF) meeting held in November 2006. The network consisted of about 55 APs on both 802.11a and 802.11g networks, and was used by more than 1200 users over a span of five days. We collected both the 802.11a and 802.11g traces for four of the five days, resulting in, to the best of our knowledge, the most comprehensive trace of a large conference WLAN to date.

We believe that the problems identified in this trace are not unique to the IETF network. These problems can occur in any wireless network, particularly large networks that are deployed to support many simultaneous users. Recent studies have identified implementation deficiencies in frame retransmissions, frame sizes and rate adaptation in congested networks [2, 3, 4]. Our study continues to identify deficiencies in 802.11 protocol implementations. These insights will be useful in designing systems and protocols that are more adaptive to network conditions. We believe that through protocol improvement and better implementations, the ability of large scale networks to handle high loads can be significantly enhanced.

2. RELATED WORK

Studies have been conducted that evaluate the performance of 802.11 handoff mechanisms. Mishra *et al.* performed an empirical analysis of handoffs using cards from several vendors and identified that the probe mechanism is the main cause of handoff latency [5], and that this latency is significant enough to deteriorate application performance. Several improvements have been suggested to address this issue of latency and perform faster handoffs [6, 7, 8]. Recent studies have also shown that the current AP selection and triggering mechanisms are sub-optimal. Mhatre *et al.* have shown that the use of long term trends in signals instead of instantaneous sig-

IMC'07, October 24-26, 2007, San Diego, California, USA.

nal strength measurements results in better handoff decisions [9]. Potential bandwidth available after the handoff [10] and the quality of the AP's connection to the Internet [11] have been suggested as better AP selection mechanisms than signal strength.

The above handoff studies are conducted on experimental testbeds in controlled conditions, and do not analyze the protocol behavior in real settings. We believe that understanding how handoff mechanisms operate in a real network is essential for improving existing algorithms. In our work, we show that current handoff mechanisms do not differentiate losses based on congestion and result in unnecessary handoffs. We believe that the insights gained from this work will help in the design and implementation of better handoff techniques for large WLANs.

3. DATA COLLECTION: METHODOLOGY AND ANALYSIS

The IETF network consisted of 55 Cisco and D-Link Access Points (APs), spread across the East and West Towers of the hotel. The conference rooms were in the West Tower and featured 38 AP devices. Each device was equipped with one 802.11a and one 802.11g radio. Thus, the network comprised of 76 APs in total. We focused our monitoring efforts on a subset of these APs to capture client behavior during the daily sessions. The APs on the 802.11g network were configured on three orthogonal channels, 1, 6, and 11, and the APs on the 802.11a network were configured on four orthogonal channels, 36, 40, 44, and 48. The APs did not support load balancing, transmission power control, or dynamic channel assignment.

We used the *vicinity sniffing* technique to collect MAC layer traces[12, 4]. This is a technique in which a set of wireless devices, known as sniffers, are deployed to passively monitor the packets in the wireless medium. A total of 12 sniffers were deployed in the conference rooms at various locations, based on the number of users in the rooms. The sniffers were placed directly underneath the APs to maximize the likelihood of all packets being captured. The sniffers were IBM R32 and T40 ThinkPad laptops running linux 2.6 kernel. Each sniffer was equipped with an atheros 802.11a/b/g PCMCIA card. The radios were configured in the monitor mode to capture all packets. In this mode, we are able to capture all MAC layer frames, including control and management frames. In addition, the prism header information, which contains send rate, received signal strength, and noise level, was also recorded for each packet. Thus, the snap-length of the captured frames was set to 250 bytes. Packets were captured using the *tethereal* utility.

The meetings were held in two separate sessions, the day and the late evening sessions, called the *Plenary* sessions. We monitored the network during both the day and plenary sessions using different sniffer configurations. Over 140 gigabytes of uncompressed wireless network traces were collected during the week. With a goal of analyzing network behavior under conditions of high load and network activity, we focus on the 802.11g network during the Plenary II session held on November 10^{th} between 17:00 hrs and 19:30 hrs. During Plenary II, eight sniffers monitored the APs on the 802.11g network and four monitored the 802.11a network. There were three times as many users on the 802.11g network as there were on the 802.11a network, and hence the effects of heavy network usage were more pronounced.

The use of eight sniffers enabled us to gather an extensive trace of network activity. Each AP in the plenary room had a sniffer directly underneath it, and thus the sniffers were able to capture all of the AP activity on the wireless side. This placement enables us to perform the kind of handoff analysis that follows. Previous studies have collected data at a single vantage point and analyzed client performance in terms of throughout, rate adaptation, and retransmissions [3, 4]. While some initial efforts exist to analyze handoff behavior in wireless networks[1], to the best of our knowledge this is the first attempt to capture wireless data from the entire network's perspective and perform handoff analysis for a network of this scale.

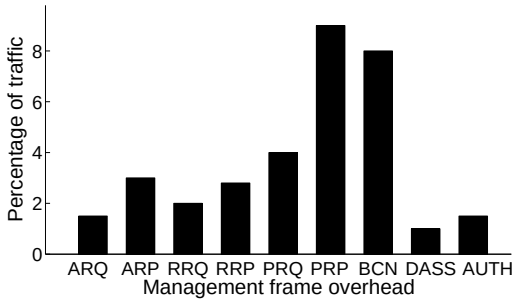

Figure 1: Breakdown of management traffic as a percentage of total traffic. ARQ:Association Request, ARP: Association Reply, RRQ: Reassociation Request, RRP: Reassociation Reply, PRQ:Probe Request, PRP: Probe Reply, BCN: Beacon, DASS: Disassociation, AUTH: Authentication.

4. TRAFFIC ANALYSIS

We begin with an analysis of the overhead of management frame traffic. The IEEE 802.11 standard defines three frame types: 1) Management; 2) Control; and 3) Data frames. Management frames enable the stations (clients and APs) to establish and maintain connections. Figure 1 shows the percentages of each management frame subtype as recorded by the sniffers, averaged over all three channels. The x-axis in the graph stands for each of the management frame subtypes, as defined by the 802.11 standard, and the y-axis shows the percentage of frames of each subtype. A high percentage of the total frames, nearly 40%, were management frames. This high percentage of management traffic has also been reported in previous studies [3].

To further analyze the effect of this management frame overhead on the clients and APs, we calculate a metric called *frame overhead.* Frame overhead is defined as the number of overhead frames transmitted by a client or AP per frame of data. Frame overhead is computed as the ratio of number of management frames to the number of data frames transmitted in every 1 second interval. For a client, the overhead consists of probe, association and reassociation requests. For an AP, the overhead frames are the corresponding response frames. This metric is useful as it gives a sense of how many overhead frames a station transmits before obtaining the opportunity to transmit a data frame. Each overhead frame transmission implies a missed data transmission opportunity for a node in the network.

The frame overhead for each client is shown in Figure 2 and for each AP in Figure 3. Each value on the x-axis represents a single station (client or AP). The y-axis shows frame overhead for each of the three frame types. The clients and APs are arranged in descending order of frame overhead for the purpose of clarity. As we can see, the frame overhead for majority of the clients is over

[1]http://www1.cs.columbia.edu/ andreaf/new/ietf.html

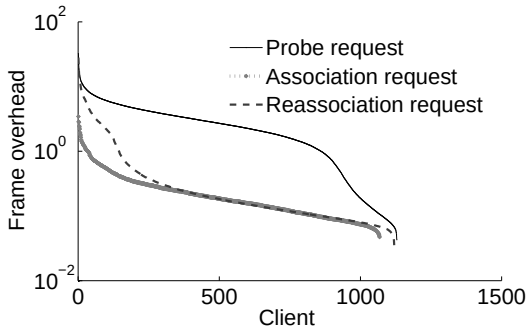

Figure 2: Frame overhead per client.

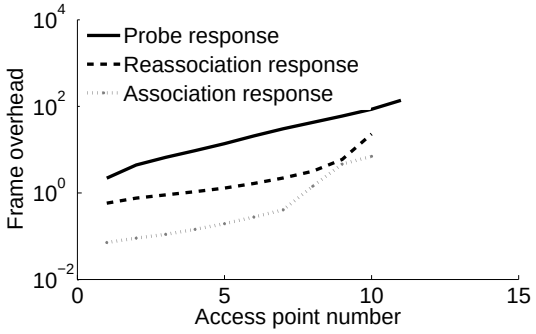

Figure 3: Frame overhead per AP.

one. This implies that majority of stations must transmit multiple overhead frames before transmitting a single data frame.

This high overhead is detrimental to network performance, particularly in networks with high numbers of users. As the number of users simultaneously accessing the network increases, the probability of medium access for each individual client decreases. Given that each client needs to send several management frames before sending a single data frame, the probability of user sending out a data frame further decreases. In a network with a large number of users, the amount of management traffic increases proportionately, with each user sending probes and hearing responses from multiple APs. The probability of user gaining access to the medium for data transmissions is even lower. We show in section 5 that the users were predominantly static in the plenary session and did not need to aggressively search for new APs. Therefore, it is critical to have a protocol that allows each user to transmit useful frames in a congested network, instead of transmitting a large number of management frames.

5. HANDOFF ANALYSIS

A *handoff* occurs when a client moves beyond the radio range of one AP, and into the range of another AP. When a client moves and loses connectivity to its AP, it starts gathering information on the APs present in the vicinity by broadcasting probe messages. The client can receive responses from multiple APs, and based on some implementation-dependent policy, it sends a reassociation request to one of the APs. The AP responds with either a success or a failure. On a successful response, the client is associated with the new AP, and the pre-handoff AP exchanges client-specific context information with this new AP. This process is called a Layer 2 (L2) handoff.

Even when clients are not moving, neighbor discovery is performed frequently to check whether an AP with a higher signal strength is available, thus attempting to improve performance. When a client wishes to associate with a different AP, a handoff process is initiated. Handoff trigger is the first stage of handoff wherein a client identifies the need to look for another AP. The implementation of this mechanism is left to the vendors, however it is usually a reaction to one or more of the following: 1) consecutive missed beacons[1]; 2) unacknowledged packets [6]; or 3) beacon frame loss or quality degradation [9]. As a result of frequent probing and implementations that use packet loss information to trigger handoffs, we expect a high rate of handoffs in a congested network. In this section, we analyze the duration and frequency of these associations and the handoff behavior of the clients.

[1]http://ipw2200.sourceforge.net

5.1 Trace Analysis

To explore the handoff behavior observed in our traces, we investigate the number and frequency of handoffs and the nature of handoffs between different channels. Most importantly, we investigate whether the handoff resulted in a performance improvement to the clients.

The number of handoffs on each channel observed during the plenary is summarized in Table 1. We observe a total of nearly 1800 handoffs during the three hours of the plenary, which is unexpected since we visually observed client mobility to be minimal during the session. To better understand the client handoff behavior and validate our anecdotal observation of low client mobility, we compute the length and frequency of client-AP associations. We define two metrics for this computation: *Prevalence* and *Persistence*. Prevalence and persistence of Internet routes was previously studied by Paxson [13]. We define these terms in the context of client-AP associations, and compute values of these metrics for the IETF traces.

Channel 1	Channel 6	Channel 11
614	586	627

Table 1: Number of handoffs during the plenary session.

5.2 Prevalence

Adapting the notion of prevalence as defined by Paxson [13], we define prevalence of clients as follows: "Given that we observe a client c associated with an AP A, what is the probability of observing c associated with A in the future?" Prevalence has specific implications on client mobility. If a client is predominantly static, the prevalence of a client-AP association pair is high, we call this AP as the *dominant* AP. On the other hand, evenly distributed prevalence values indicate that there was no single dominant AP, and that the users were mobile. In a well functioning network characterized by clients with low mobility, we expect the majority of the client-AP associations to have high prevalence values indicating that clients did not bounce back and forth between APs.

We compute prevalence values at a fine granularity of one second and a coarse granularity of one minute. Let n_s be the total number of 1 second intervals in the trace. At each 1 second interval, we check whether a client has sent at least one data packet to the AP. If it has, then it is still connected to the AP, else it has either roamed or become inactive. We consider the client to have reconnected to the AP when we see a data packet from that client again. Let k_s be the total number of 1 second intervals in which the client was

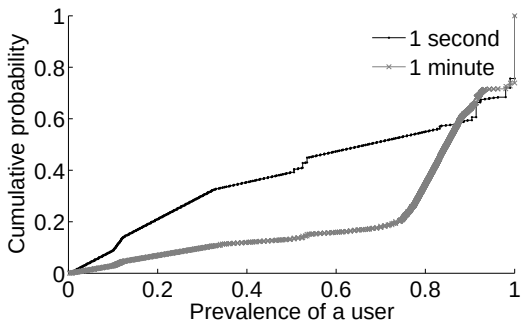

Figure 4: Client prevalence on an AP, given as the cumulative distribution of the probability of a client being associated with an AP.

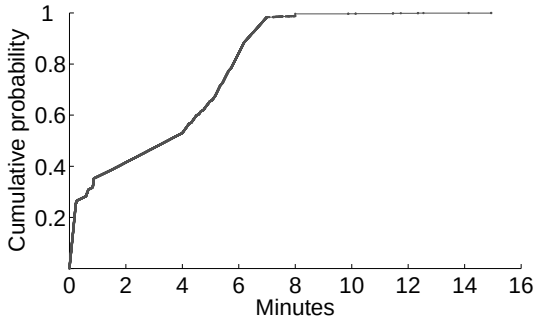

Figure 5: Client persistence on AP, given as the cumulative distribution of client-AP association duration.

active. The prevalence of the client on the AP is given by

$$\pi_s = k_s/n_s \quad (1)$$

The prevalence values at 1 second granularity are shown in Figure 4. The prevalence values at one second granularity are evenly distributed, which indicates that at a fine granularity, not all clients were highly prevalent on the dominant AP. About 40% of the clients had only a 50% chance of being associated with their dominant AP.

Prevalence at a granularity of 1 minute is calculated similarly. If n_m is the total number of 1 minute intervals in the traces, and k_m is the number of intervals in which a client was active, the prevalence is given by

$$\pi_m = k_m/n_m \quad (2)$$

From Figure 4, we see that the majority of clients are more prevalent on the dominant AP on a 1 minute granularity. Only about 30% of the clients had prevalence of 80% or less on the dominant AP. The remaining 70% of the clients were prevalent on the dominant AP over 80% of the time. These results indicate that clients were frequently found associating with the same AP, implying that mobility in the network was low. Even though multiple APs on the same channel were within the range of a client, we can observe that a client tends to be prevalent on one AP, the dominant AP. Most clients use signal strength to select an AP for association. Consequently, the dominant AP is most likely the AP closest to the client. The lower prevalence at a higher granularity of time implies one of two things: i) the clients were sending data frames infrequently; or ii) the clients were bouncing back and forth between APs within short intervals. However, trace analysis shows that there was at most one second interval between two data packets. Hence, we believe that frequent switching of clients between APs contributed significantly to the lower prevalence rates at one second intervals.

5.3 Persistence

We define the persistence of a client as follows: "Given that a client is associated with a particular AP, how long before the client changes its association to another AP?" Thus, persistence is the length of time a client remains associated with an AP. A low persistence value indicates that the clients did not remain connected to an AP for a long time. In a well-functioning network characterized by clients with low mobility, we expect clients to have high persistence values. That is, clients stay connected to an AP for long periods while they are static, and only infrequently change APs during movement.

We calculate the persistence of clients on the dominant AP. The dominant AP for a client is the AP on which the client has high prevalence. An association length is calculated as the time elapsed between the first and the last data frame observed from the client. This computation also takes into account the null data packets, which are data packets that are sent to keep the client-AP association alive. The persistence is computed for one second time interval; if no data frame has been observed for up to one second, we assume the session has ended. The one second interval for this computation is based on the observed rate at which null data packets are transmitted by the clients to keep the session alive. Analysis of the traces reveals that null data packets are transmitted at a high frequency, with at most an interval of one second between two successive frames. Furthermore, if we observe a data frame from a client at second s_1 and do not observe a frame in the subsequent second s_2, we make a "best guess" that the disassociation occurred halfway between these two time intervals.

Figure 5 shows the cumulative distribution of persistence values of the users present during the plenary session. The Figure captures values for all client-AP pairs observed in the traces. The x-axis represents the length of associations in minutes and the y-axis represents the cumulative percentage of associations. About 40% of the associations were under two minutes and 90% of associations were under seven minutes. This indicates that clients remained connected to APs for fairly short periods of time.

5.4 Discussion

In a network with dense AP deployment and a large number of users connected to the network simultaneously, the number of handoffs is high inspite of low mobility. The reason for this behavior lies in the handoff mechanisms. Handoff triggering mechanisms rely on packet loss information to detect when a client has moved away from its AP. This loss can consist of either consecutive beacon frame losses or unacknowledged data packets. In our traces, we found that the number of beacons received by a client, called *beacon reception rate*, influences the number of handoffs, as shown in Figure 6. Beacon reception rate is computed as the average percentage of beacons received by the sniffer from each AP within range. Sniffers are physically close to the APs and have a higher probability of beacon reception than the clients. Hence, this graph provides an upper bound on the number of beacons that a client could have received. The graph is a time series plot of the percentage of beacons the sniffer received from all the APs in one second, and the corresponding number of handoffs that occurred. The beacons were sent at 100ms intervals, implying that the snif-

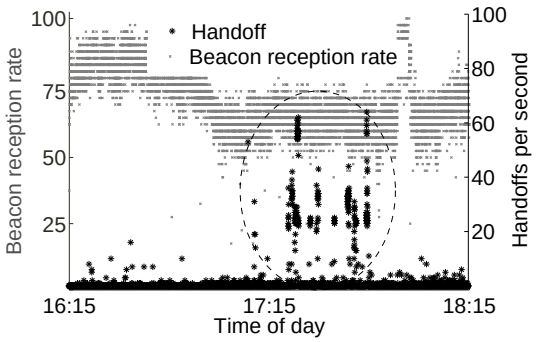

Figure 6: Comparison of utilization and number of handoffs across all channels.

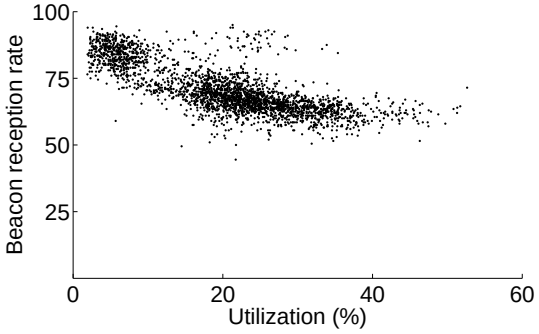

Figure 7: Scatter plot of beacon reception rate vs utilization. The correlation coefficient is -0.65.

fer should receive 10 such beacons per second from each AP in its range. The graph shows a sharp increase in the number of handoffs when the beacon reception decreases.

Using beacon frame loss as a handoff trigger is incorrect and problematic in a congested environment. At high utilization levels, the beacon loss increases, i.e. the beacon reception rate decreases, for two reasons. First, the packet loss rate increases, resulting in missed beacon packets. Second, certain AP implementations are known to not queue beacon packets, and broadcast beacons at the specified beacon interval only if the send queue is empty[1]. Figure 7 illustrates this effect. When the medium is utilized over 50%, the sniffer received beacons only slightly more than 50% of the time.

The use of packet loss information as a handoff trigger has adverse effects in a congested network. Missed beacons initiate a client to commence roaming, wherein a client actively probes the medium and waits for responses from APs. This not only results in high probe traffic in the wireless medium, but also results in unwanted handoffs. We analyzed the nature of handoffs between channels and the results are summarized in Table 2.

As indicated by Table 2, 76% of the handoffs occur between APs on the same channel (found by summing along the diagonal). About 85% of the handoffs to the same channel and 58% of the total handoffs were to the same AP from which the client disconnected. This can be reasoned as follows: a handoff is triggered due to packet loss, as we have seen earlier. On a trigger, the client scans the medium and obtains information on all the available APs. Currently implemented AP selection mechanisms typically select the AP from which the client receives the strongest signal, without any knowledge of the load on the AP or on the channel. For clients that are predominantly stationary, the AP with the strongest signal strength will be, with a very high probability, the AP from which the client disconnected.

	Channel 1	Channel 6	Channel 11
Channel 1	33%	7%	2%
Channel 6	2%	24%	6%
Channel 11	4%	3 %	19%

Table 2: Percentage of handoffs between different channels for each channel pair. The row value indicates the channel before handoff. The column value indicates the channel after handoff.

[1]http://hostap.epitest.fi

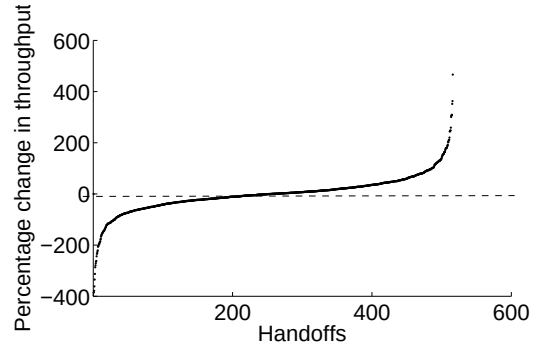

Figure 8: Percentage change in throughout after handoff over a period of 30s. The x-axis represents each handoff event ordered by throughput improvement.

Reassociation with the same AP is wasteful; not only does it result in MAC overhead, but it also causes application performance deterioration. Handoffs to APs on the same channel can be beneficial only if the new AP is less loaded than the AP to which the client was previously connected. However, connecting to APs with lower signal strength is likely to result in lowered data rates. Further, if the network around the client is congested, switching to a different AP on the same channel is not beneficial since the client continues to see a similar level of congestion.

Switching to an AP on a different channel can be beneficial if the new channel is less congested and can offer better throughput to the clients. However, we observed in the traces that the congestion levels of the channels at a given point in time are comparable. Further, the AP selection mechanisms do not make the handoff decicion based on whether a throughput improvement will be obtained after switching to a new AP. As a result, we do not expect the user to have obtained significant gains from the handoff.

To determine whether the handoffs were beneficial, we compute the percentage change in throughput immediately before and after a handoff, for each handoff between two different APs. To calculate the percentage throughput improvement of the client, we consider the throughput obtained by the client 30 seconds before and after the handoff and plot the difference. These values are plotted in Figure 8, where the handoffs events are ordered in the ascending order of the throughput improvement. The x-axis represents individual handoff events and the y-axis represents the percentage

improvement in throughput as a result of the handoff. The graph indicates that about 50% of the handoffs had a negative impact on the throughput. While 50% of the handoffs resulted in an increase in throughput, 20% of these handoffs resulted in less than a 10% increase in throughput. These results indicate that a significant portion of the handoffs were not beneficial, and may even have been detrimental. Reduction in useless handoffs will reduce the amount of management traffic, leading to greater transmission opportunities for nodes with data packets and an increase in efficient medium utilization.

In general, a mechanism that reacts to packet loss will result in incorrect handoffs in a network that has a high loss rate. We saw in Section 4 that there is high management frame overhead due to the current association mechanisms. We also saw that up to 70% of the handoffs either resulted in throughput degradation, or insignificant throughput improvement. This result is not surprising, given that the current handoff mechanisms do not take into account the expected throughput improvement while making handoff decisions. Handoff mechanisms that take into account signal strength trends [9] are necessary to mitigate the high overhead and the resulting incorrect handoffs.

6. CONCLUSION

Analysis of real world deployments are critical to identify deficiencies in the 802.11 protocol and its implementations. For this reason, we collected data from the 67^{th} Internet Engineering Task Force (IETF) meeting held in November 2006 in San Diego CA. Through the analysis of these traces, we show that clients have short association times with the APs. This is a consequence of the current mechanisms that trigger a handoff under conditions of high medium utilization and packet loss rate, even in the absence of client mobility. We analyze the traffic to understand when handoffs occur and whether the handoffs were beneficial or should have been avoided.

Our analysis shows that handoff mechanisms should be adaptive to congestion losses. Use of packet loss information to trigger handoffs results in a high rate of handoffs, even in the absence of mobility. In the IETF network, a significant fraction of these handoffs were to the same AP, and thus unnecessary. Further, many of the handoffs that occurred to other APs impacted the clients negatively. Schemes that use signal strength trends to detect disconnection, and schemes that incorporate network information such as load in conjunction with loss are needed to avoid unnecessary handoffs.

Acknowledgments

This work is supported in part by NSF NeTS Award CNS-0435527, NSF CRI Award CNS-0454329, and a grant from Intel Corporation. We thank Jim Martin (Netzwert AG) and the IETF 67 NOC team, and Amit Jardosh from UC Santa Barbara for assisting us in the collection of the data used in this paper. We also thank the anonymous reviewers and our shepherd Rocky Chang for their valuable feedback.

7. REFERENCES

[1] A. P. Jardosh, K. Mittal, K. N. Ramachandran, E. M. Belding, and K. C. Almeroth, "IQU: practical queue-based user association management for wlans," in *Proceedings of MobiCom*, Sept. 2006, pp. 158–169.

[2] A. P. Jardosh, K. N. Ramachandran, K. C. Almeroth, and E. M. Belding-Royer, "Understanding Link-Layer Behavior in Highly Congested IEEE 802.11b Wireless Networks," in *Proceedings of EWIND*, Philadelphia, PA, Aug. 2005, pp. 11–16.

[3] M. Rodrig, C. Reis, R. Mahajan, D. Wetherall, and J. Zahorjan, "Measurement-based characterization of 802.11 in a hotspot setting," in *Proceedings of EWIND*, Aug. 2005, pp. 5–10.

[4] A. P. Jardosh, K. N. Ramachandran, K. C. Almeroth, and E. M. Belding-Royer, "Understanding congestion in ieee 802.11b wireless networks," in *Proceedings of IMC*, Oct. 2005.

[5] A. Mishra, M. Shin, and W. A. Arbaugh, "An empirical analysis of the IEEE 802.11 MAC layer handoff process," *ACM SIGCOMM Computer Communication Review*, vol. 33, no. 2, pp. 93–102, Apr. 2003.

[6] H. Velayos and G. Karlsson, "Techniques to reduce IEEE 802.11b handoff time," in *Proceedings of ICC*, Paris, France, June 2004.

[7] H.-S. Kim, S.-H. Park, C.-S. Park, J.-W. Kim, and S.-J. Ko, "Selective Channel Scanning for Fast Handoff in Wireless LAN using Neighbor Graph," in *Proceedings of ITC-CSCC*, Sendai/Matsusima, July 2004, pp. 303–316.

[8] I. Ramani and S. Savage, "SyncScan: Practical Fast Handoff for 802.11 Infrastructure Network," in *Proceedings of IEEE Infocom*, Miami, FL, Mar. 2005.

[9] V. Mhatre and K. Papagiannaki, "Using smart triggers for improved user performance in 802.11 wireless networks," in *Proceedings of MobiSys*, June 2006, pp. 246–259.

[10] S. Vasudevan, K. Papagiannaki, C. Diot, J. Kurose, and D. Towsley, "Improved access point selection," in *Proceedings of IMC*, Oct. 2005.

[11] A. J. Nicholson, Y. Chawathe, M. Y. Chen, B. D. Noble, and D. Wetherall, "Improved access point selection," in *Proceedings of MobiSys*, June 2006, pp. 233–245.

[12] J. Yeo, M. Youssef, and A. Agrawala, "A framework for wireless LAN monitoring and its applications," in *Proceedings of WiSe*, Philadelphia, PA, Oct. 2004, pp. 70–79.

[13] V. Paxson, "End-to-end routing behavior in the Internet," in *Proceedings of SIGCOMM*, 1996, pp. 25–38.