This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE INFOCOM 2009 proceedings.

D-Scan: Enabling Fast and Smooth Handoffs in AP-dense 802.11 Wireless Networks

Jin Teng, Changqing Xu
Shanghai Jiao Tong University
Shanghai, China
{kenteng, cqxu}@sjtu.edu.cn

Weijia Jia
City University of Hong Kong
Hong Kong SAR, China
wei.jia@cityu.edu.hk

Dong Xuan
The Ohio State University
Columbus, Ohio, USA
xuan@cse.ohio-state.edu

***Abstract*—802.11 wireless networks have gained ever greater popularity nowadays. Apart from static wireless connections, people begin to expect more user-friendly features from this kind of networks, such as support for seamless roaming. In this paper, we study the handoff process in large AP-dense 802.11 networks, which is one of the most common forms of WiFi under usage. A series of field experiments are carried out and some critical handoff parameters are evaluated. With some newly discovered features, i.e. differentiated probe response time and rich AP information hidden in wireless traffic, we have managed to significantly improve the essential process of AP scan, a bottleneck towards fast and smooth handoffs. The solution is collectively called D-Scan (Scan in AP-Dense 802.11 networks). Real experiments are conducted to show the superiority of our solution.**

I. INTRODUCTION

802.11-based wireless networks, also called WiFi comercially, have seen spectacular growth in recent years [1]. As 802.11 networks go large-scale and even city wide, a lot of challenges occur. One of them is service continuity in clients' roaming. So far the handoff process in 802.11 networks incurs a large delay at the magnitude of several hundreds of milliseconds, which is intolerable to delay-sensitive applications like VoIP.

Besides, as the scale and density of 802.11 wireless networks grow dramatically, a typical WiFi wireless network nowadays comprises hundreds or even thousands of APs covering an area up to several square kilometers. A client in WiFi service area is likely to receive signals from more than 10 APs most of the time [2,3]. Many of them are accessible to the clients, since they may be APs deployed by the same institution, open government proxies and voluntary individuals or shops. So the wireless service, including handoff support, faces an unprecedented contentious and chaotic wireless environment.

A lot of researches have been dedicated to improving the handoff performance in 802.11 networks [4-10]. Some consensus has been reached: the search for candidate APs, or AP scan, is the main contributor to the great delay [4,5]. 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. By amortizing this scan into background activities before actual handoff, which we call background pre-scan, the delay can be made satisfactorily low for most applications [10]. However it is generally agreed that long background pre-scan will heavily interfere with normal traffic [11,12]. So in order to enable frequent and timely pre-scans, it's desirable to finish scanning a channel in as little time as possible.

The probe waiting time is a major part of the scanning time. Though in a light-loaded and AP-sparse 802.11 network, many researches have tried to give an appropriate value for this time, e.g. [4,5] set it around 11ms, yet no serious study of this time is conducted in a large AP-dense 802.11 network. After extensive field surveys, we find the probing time for each channel can be intolerable in an AP-dense network, i.e. generally it takes over 50ms to guarantee the reception of all the responses. As a result, the client is supposed to spend much more time on pre-scanning to learn about nearby APs than was considered before.

To curtail this prolonged scanning time, we introduce two inspiring discoveries, namely differentiated probe response time and rich AP information hidden in wireless traffic. Then we work out a solution in an effort we collectively call D-Scan. In the first step, a correlation between response arrival time and AP signal quality has been established that APs of better quality statistically respond faster. Hence, by ignoring late arriving responses, which are likely to be from bad handoff AP candidates, we can safely shorten this 50ms to 30ms or less. In the second step, we progress to introduce eavesdropping to assist active probing, since much useful information about nearby APs can be extracted from MAC headers of passing wireless packets. With the help of an elaborated scheme to sniff APs out of wireless traffic, we have managed to bring the MaxChannelTime further down to less than 10ms, which may satisfy the needs of most delay-sensitive applications.

This great improvement in waiting time results from the underlying philosophy that adverse networking conditions can be turned into favorable ones. To be concrete, the busy wireless traffic itself, which delays or even blocks exchanges of probe packets, can acquaint us with the wireless environment. So no matter whether the network is crowded or not, there are ways for clients to speedily gain access to the information they need.

We have implemented a prototype of D-Scan on commercial 802.11 Network Interface Cards (NICs) and tested it in real large AP-dense networks. Results prove that the proposed solution can actually lead to fast and smooth handoffs.

In summary, we claim the contributions as follows:

- The handoff performance is evaluated in large-scale AP-dense 802.11 networks through a series of field experiments. And the probe waiting time, i.e. MaxChannelTime, is scientifically and systematically evaluated in the course.

The work is partially supported by China National 863 Project No. 2007AA01Z224, Hong Kong SAR Competitive Earmarked Research Grant– GRF Grant No. 9041350 (CityU 114908), CityU Applied R & D Centre (ARD(Ctr)) grant No. 9681001, the US National Science Foundation (NSF) CAREER Award CCF 0546668 and the US Army Research Office (ARO) grant No. AMSRD-ACC-R50521-CI.

- To the best of our knowledge, we are the first to identify the correlation between probe response arrival time and AP signal quality, which helps to greatly reduce active probing time.
- We give out an elaborated scheme of eavesdropping to extract AP information from wireless traffic and thereby further bring down the active probing time to a satisfactory level at 6ms.
- D-Scan, an AP-scan solution which makes full use of high AP density and heavy traffic load, is proposed and evaluated in real large AP-dense 802.11 networks.

The remainder of this paper is organized as follows. Section II gives the background to the question we are addressing. Section III presents our discoveries of some new features in a large-scale AP-dense 802.11 network. Section IV explains our optimizing efforts of the pre-scan process. Some parameters settings of the solution and its general performance are also evaluated in Section IV. Finally, Section V concludes the whole paper.

II. Preliminaries

The large handoff delay in 802.11 networks is attributable to 'the improvident nature' of the 802.11 standards. That is to say, the STA (mobile station) does not bother to prepare for any possible deterioration of the connection quality, a parameter which is often measured in RSSI (Received Signal Strength). 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.

On careful analysis [4,5], 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.

The AP scan strategies can be divided into active and passive ones. During an active scan, the STA broadcasts a probe request packet, asking all the APs on that channel to impart its existence and capabilities with a probe response packet. Active scan is normally speedy but unreliable, since probe packets may get lost or greatly delayed in wireless 'traffic jam'. While for a passive scan, the STA listens passively for the beacons, which bear all the necessary information about an AP and are broadcast by all APs at a certain interval, normally around 100-200ms. Though this kind of scan is reliable, its cost is the long waiting time for beacons, which is prohibitive to many services. So in practice, active scans are the preferred method.

In active scans (Fig. 1), two parameters, MinChannelTime and MaxChannelTime, are important:

- MinChannelTime represents the arrival time of the first probe response. So a client must listen for this period of time to decide whether there's ANY AP on this channel. It's recommended to be set as 4-7ms by [4].
- MaxChannelTime is the estimated time to collect ALL probe responses. It's supposed to be at the magnitude of tens of milliseconds and all packets arriving later, which was deemed quite impossible in light-loaded and AP-sparse 802.11 networks, will be discarded.

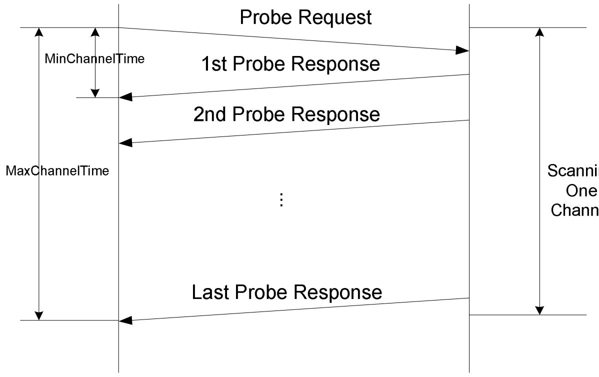


Figure 1. Active Scan

III. Our Discoveries

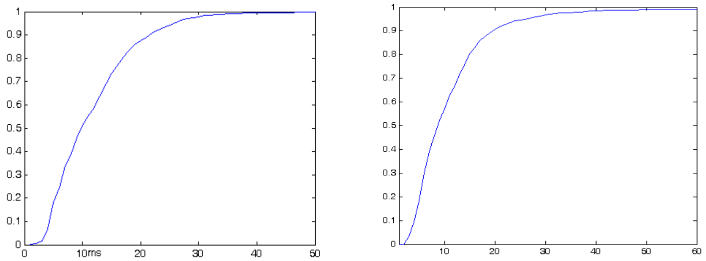
We collect performance data in various spots of Hong Kong under coverage of large AP-dense 802.11 wireless LANs, including universities, streets and malls.

All the following data and implementations are based on a Compaq 6520s notebook and an IBM T60. Both of them are equipped with an Intel Pro/Wireless 3945 NIC, one of the most popular commercial wireless NICs. In order to fully control the 3495 NIC, we deploy our testbed on Ubuntu 7.10. A wireless NIC driver named ipwraw [14] is also employed. All data reported hereafter, unless stated otherwise, are measured in Hong Kong, especially in City University, the whole campus of which is densely covered by 802.11 networks [15]. The data were all taken in August, 2008 and the whole measurement lasts for about 3 weeks.

A. A Pertinent MaxChannelTime in Large AP-Dense 802.11 Network

In ideal lab environments, the MaxChannelTime has been carefully evaluated. MaxChannelTime at 11ms [4,5] shows quite good performance. However, no real evaluation of this value under AP-dense network has been given before. So we set hands to conduct surveys of this kind of networks with real notebooks and NICs.

Our data from the field measurements in this kind of networks show that the collection time of probe responses is so long that they can be definitely perceived by human users.



(A) Concourse, City University HK

(B) In Apliu Street

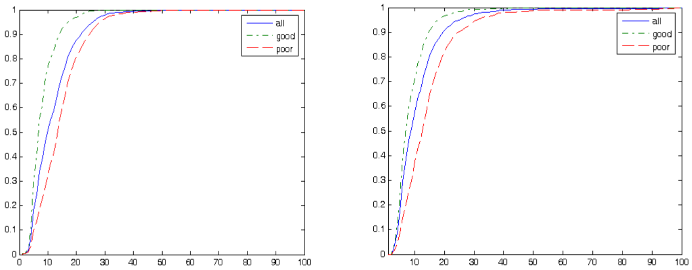
Figure 2. Cumulative Density of Arrival Time of Probe Responses in Large AP-Dense 802.11 networks

Figure 2 shows the cumulative density of the probe response arrival time. From this figure, we can see that only about 40% of all probe responses return within 11ms, the ideal time set for AP-sparse networks. Meanwhile it takes 50ms for 98% of the responses to return and around 30ms for 95% of the responses to return.

This discovery is a discouraging one. It implies that if we do not change our current pre-scan strategy, we will spend 50ms each to scan over 15 channels for all networks belonging to the 802.11 family (at least 3 non-overlapping channels for 802.11b/g and 13 orthogonal channels for 802.11a). Then we are to see a full frequency scan last over 500ms. It's a time gap large enough to be perceptible by human users.

B. The Relationship between RSSI and Probe Response Time

We observe that in AP-dense 802.11 networks, APs with stronger RSSI tend to respond faster. From statistical analysis, we find that the AP with the best quality stands a chance of 48.7% to respond first, and a chance of 90.2% to be among the first three responders. The average probe response time from the AP with the highest RSSI is 6.054ms, with a standard deviation of 1.58ms.



(A) Concourse, City University HK

(B) In Apliu Street

Figure 3. Cumulative Density of Arrival Time of Probe Response with Respect to AP's Signal Quality

Figure 3 demonstrates this phenomenon in another perspective. Blue lines (solid) show the cumulative density of the arrival time of probe responses from ALL APs. Green lines (dash-dot) only count responses from APs with good RSSI, which we define here as showing a RSSI greater than -75 dBm. And the Red lines (dash) represent APs with poor RSSI, i.e. weaker than -75dBm. A blue line can be distinctively split into a green one and a red one. That is to say, a shorter response arrival time can be observed for APs with good RSSI.

We find two reasons to explain this phenomenon:

First, poor RSSI leads to high transmission error rate. So a response packet must be sent more times to get received correctly.

Second, RSSI is greatly correlated with distance between client and AP. APs with stronger RSSI are generally closer to the client. Then these APs will receive probe requests from the client a little bit earlier than their counterparts, resulting in their advantage in competing for the wireless channel.

Say AP A is 50m closer to the client than AP B, then it will finish receiving the probe request 0.2 microseconds earlier than AP B and therefore enters the channel contention process 0.2 microseconds earlier than AP B. Moreover, every AP will arrange probe response to be sent first after having heard a probe request. So ideally no other packets will be transmitted after the probe request. Then after a period of DIFS, AP A will determine the channel clear and send the response before AP B. Even if other packets intervene after the probe request, AP A will enter the backoff phase earlier than AP B. Then AP A will make a statistically faster response than AP B. Figure 4 illustrates the mechanism.

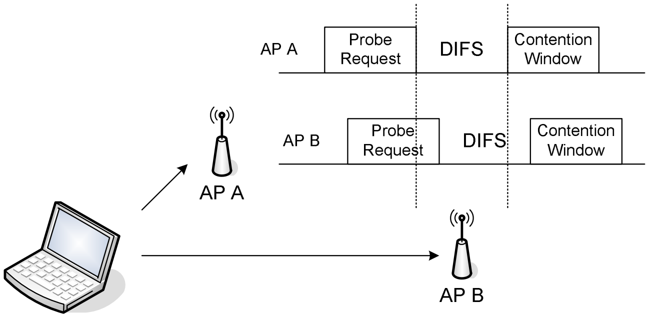


Figure 4. Contention to Respond between APs at Different Distance

C. Eavesdropping to Acquire Information of Nearby APs

There's actually a treasure of AP information in the wireless traffic. Figure 5 illustrates the wireless traffic and the fields of interest for capturing. MAC header information can be safely and surely acquired, so they are depicted with solid lines, while we must try our luck to get other information such as SSID or IP/Domain, since they are only contained in certain types of unencrypted packets, so they are given in dashed lines.

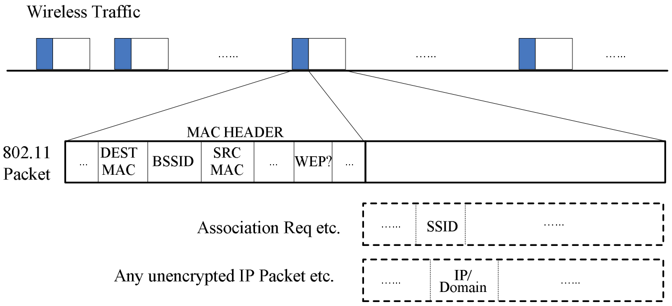


Figure 5. Wireless Traffic and Fields of Interest for Eavesdropping

Certain packets can only be sent by APs, e.g. such management frames as association responses or disauthentications. We may also identify data packets distributed by or heading for APs. This is done by reading the To_DS and From_DS fields in the MAC header. The To_DS field shows whether the packet is heading outside the BSS (Basic Service Set), e.g. to the Internet, while the From_DS reveals that the packet is from outside the BSS. They are indicators of whether a device is acting as a router between inside the BSS and the outside distribution system. Needless to say, the routing device in an infrastructure 802.11 network is nothing other than an AP. So by analyzing the MAC headers in these AP-related packets, we can learn the existence, MAC addresses and other valuable information about nearby APs.

Different kinds of 802.11 packets contains different information of AP. Table I lists the information we can extract from each type of wireless packets. Ticks in brackets mean that the information may be acquired, but not for sure. For instance, a probe request may carry the SSID, but it's not absolutely necessary. And since ACKs only bear the destination MAC address, AP information can only be inferred in a communication context.

TABLE I. AP INFORMATION CONTAINED IN WIRELESS PACKETS

AP Information	Exist	MAC	WEP	SSID	RSSI
Beacon	✓	✓	✓	✓	✓
Probe Response	✓	✓	✓	✓	✓
Probe Request		✓		(✓)	
(Re)association Request		✓	✓	✓	
(Re)association Response	✓	✓			✓
Authentication Response	✓	✓	✓		✓
Disauthentication	✓	✓			✓
ACK from AP	(✓)	(✓)			(✓)
ACK to AP	(✓)	(✓)			
Data from AP	✓	✓	✓		✓
Data to AP		✓	✓		

From Table I, we observe that we have not too many means to get the SSID information. But it's compensated by the fact that once an SSID is correlated with an AP MAC, it's done once for all, for it is very much probable that the SSID will not change over a long period of time.

One thing to concern us is that this kind of information acquisition is susceptible to legal and security problems. However, we still regard it as justified for the following two reasons: Firstly, the information contained in the wireless MAC header is essentially not considered confidential. Any wireless NIC should be able to obtain such information so as to decide whether it should receive the packet or not. And we can find in almost all networking textbooks that SSID should not be used as a security measure, which it is not supposed to be capable of. So the information acquisition on the MAC layer is totally lawful. Secondly, since handoffs should be transparent to users, the data collected to assist MAC-layer handoff don't need to be exposed to the user. That is to say, the information is encapsulated in the kernel and cannot be seen from without.

IV. D-SCAN AND ITS PERFORMANCE

Based on the abovementioned discoveries of large AP-dense 802.11 wireless networks, we set hands to design a new pre-scan strategy, which we call D-Scan (Scan in AP-Dense 802.11 networks). We first examine the core process of scanning a single channel and then present the D-Scan algorithm in its entirety. All data reported hereafter, unless stated otherwise, are measured in the concourse of City University of Hong Kong.

A. Speedy Scan of a Single Channel

When changed to a certain channel, the client stays tuned all the time. If eavesdropping is applied, it will gather much information of nearby APs after a period of time, e.g. during the waiting time for probe responses. In an area densely covered by 802.11 APs, the client is likely to overhear more wireless traffic and is more ready for eavesdropping.

Moreover, based on our second discovery, we may expect APs of better link quality to respond first. So we may cut short the waiting time by intentionally ignoring all late arriving responses. One conservative method to cut waiting time is to listen for 30ms and manage to receive 95% of all probe responses. It's safer, but 30ms still seems too long for some delay-sensitive applications. Another radical method is to set listening time within 10ms, hoping to capture 1 or 2 APs of best link quality, since we know from our survey that APs with best quality show an average response time of around 6ms. This approach is fast enough to satisfy most applications. And eavesdropping may help us acquire AP information if the wireless channel is congested. It will be shown that this radical method turns out to work tolerably well.

The performance of this kind of speedy scan and the following handoff under different MaxChannelTime is evaluated here. Both the conservative method of 30ms and the radical one at 6ms are tested. A middle one, i.e. 15ms is also tested. The scan is conducted at a certain interval until the actual handoff takes place. The RSSI of the newly associated AP is obtained from the response packets during the reassociation process.

TABLE II. PERFORMANCE COMPARISON OF SCANNING A SINGLE CHANNEL WITH DIFFERENT MAXCHANNELTIME

MaxChannelTime	30ms	15ms	6ms
Percentage of Response Received	100%	81.9%	36.7%
Percentage of Capturing the Best AP	100%	89%	100%
Avg. difference of Handoff AP RSSI and the highest	-0.5dB	-4dB	0dB

Three tests for each time length are performed. We have observed in Table II a decreasing reception percentage of incoming probe responses. However, the probability of capturing the best AP stays quite constant and the final handoff APs are almost the best ones. That is to say, though we capture only a small fraction of all probe responses with 6ms' waiting time, yet we are still able to pick out the best AP on a specific channel. So MaxChannelTime=6ms shows as good performance as 30ms and 15ms.

B. D-Scan Algorithm

Here we present the entire D-scan algorithm (Fig. 6). It's an extension of the above core process and is triggered by the link quality of the currently associated AP. We perform a regular detection of the link quality of the current AP every 200ms. If the current link quality of the associated AP is poor enough to need a handoff, i.e. RSSI<HANDOFF_THRESHOLD, then an actual handoff process will be enforced. If it is lower than a certain threshold (SCAN_ THRESHOLD), the NIC begins to perform the back-ground pre-scan. The scan will try to find 3 APs with enough RSSI (>-75dBm), since one AP candidate is not safe. If we cannot find 3 good APs on the current channel, we switch to the next channel to scan until the whole frequency has been searched. In an AP-dense environment, 3 APs with good RSSI are not very difficult to find.

For the scan process, the current working channel is first scanned with the MaxChannelTime set as 6ms. If not enough APs with good RSSI are detected on the current channel, we jump to other channels to scan. The scan frequency can be set as done in [10]. But because of high efficiency brought about by eavesdropping, the scan intensity can be somewhat relaxed. We will show that pre-scanning every 2 second is enough for a good handoff. As for other crucial parameters here, SCAN_ THRESHOLD ought to be much larger than HANDOFF_ THRESHOLD. Here we fix the latter as -85 dBm (cf. the reception sensitivity is typically -95dBm), and we set SCAN_ THRESHOLD a little bit higher at -65 dBm.

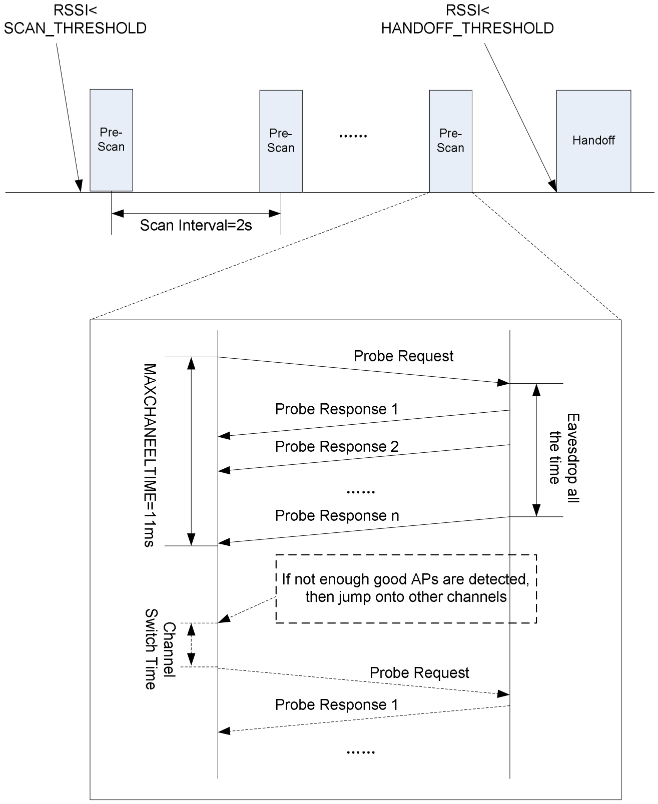


Figure 6. D-Scan Framework

We have done five tests to evaluate the performance of D-Scan (Table III). All the time starting from the point when the handoff is triggered is counted in the association time. Four of the experiments reported that the AP the client associated with has an RSSI less than 3dB lower than the highest. Their mean association time is 17.06ms with a standard deviation at 8.71ms. For comparison's sake, we have also conducted five times the traditional active probing scan with MaxChannelTime=11ms. Its mean association time is 32.37ms with a standard deviation at 24.71ms. And the average quality of the handoff AP is 5.8dB lower than the best AP. From Table III, we can figure out that D-Scan performs better than the traditional practice in both the association time and the appropriateness of AP selection. We believe this sort of advantage of D-Scan can be attributed to eavesdropping, since we are able to acquire AP information even when the probe responses or beacons are delayed greatly. On the other hand, as the pre-scan of D-Scan can be finished much faster than traditional active scan, it definitely causes much less impact on the foreground communications under the same background pre-scan intensity.

TABLE III. COMPARISON OF D-SCAN AND TRADITIONAL ACTIVE SCAN

	D-Scan	Active Scan
Avg. Association time	17.06ms	32.37ms
Avg. difference of Handoff AP RSSI and the highest	-1.1dB	-5.8dB

V. CONCLUSION

In this paper, we show that the collection of AP responses in large AP-dense 802.11 networks is a very time-consuming process. Meanwhile, the unique features of AP scan in this kind of environment are exposed, including differentiated probe response time and rich AP information hidden in wireless traffic. With the help of these discoveries, we have proposed an ameliorated AP scan, D-Scan, where eavesdropping and shortened active probing cooperate to achieve an efficient AP pre-scan. Experiments on commercial NICs show that D-Scan works well in real large AP-dense 802.11 wireless networks and helps to effect a faster and smoother handoff.

REFERENCES

[1] RNCOS, "Wireless LAN Market (2007-2008) Report"

[2] A. Akella, G. Judd, S. Seshan et al., "Self Management in Chaotic Wireless Deployments", ACM MobiCom '05, July 2005

[3] A. Nicholson, Y. Chawathe, M. Chen et al., "Improved Access Point Selection", ACM MobiSys '06, June 2006

[4] A. Mishra, M. Shin and W. Arbaugh, "An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process", ACM SIGCOM '03, April 2003

[5] H.Velayos and G. Karlsson, "Techniques to Reduce IEEE 802.11b MAC Layer Handover Time", KunglTekniska Hogskolen, Stockholm, Sweden, Tech. Rep. TRITA-IMIT-LCN R 03:02, April 2003

[6] M. Shin, A. Mishra and W. Arbaugh, "Improving the Latency of 802.11 Handoffs Using Neighbour Graphs", in Proceedings of the ACM MobiSys Conference, June 2004

[7] P. Huang, Y. Tseng and K. Tsai, "A Fast Handoff Mechanism for IEEE 802.11 and IAPP Networks", IEEE 63rd Vehicular Technology Conference, Spring, 2006

[8] I. Ramani and S. Savage, "SyncScan: Practical Fast Handoff for 802.11 Infrastructure Networks", INFOCOM '05, March 2005

[9] V. Brik, A. Mishra and S. Banerjee, "Eliminating Handoff Latencies in 802.11 WLANs Using Multiple Radios: Applications, Experiences and Evaluation", ACM IMC, October 2005

[10] H. Wu, K. Tan and Q. Zhang, "Proactive Scan: Fast Handoff with Smart Triggers for 802.11 Wireless LAN", INFOCOM '07, May, 2007

[11] G. Singh, A. Atwal and B. Sohi, "Effect of Background Scan on Performance of Neighboring Channels in 802.11 Networks", International Journal of Communication Networks and Distributed Systems, Vol. 1, No. 1, 2008

[12] K. Kwonand and C. Lee, "A Fast Algorithm Using Intelligent Channel Scan for IEEE 802.11 WLANs", in 6th International Conference on Advanced Communication Technology, 2004

[13] Y. Liao and L Gao, "Practical Schemes for Smooth MAC Layer Handoff in 802.11Wireless Networks", WoWMoM '06, 2006

[14] http://homepages.tu-darmstadt.de/~p_larbig/wlan/

[15] http://www.cityu.edu.hk/csc/deptweb/facilities/ctnet/wlan/wlanmain.htm