A Characterization of Wireless NIC Active Scanning Algorithms

Vaibhav Gupta
Department of Computer Science
Georgia State University
Atlanta, GA, USA

Raheem Beyah
Department of Computer Science
Georgia State University
Atlanta, GA, USA

Cherita Corbett
Sandia National Laboratories*
Livermore, CA, USA

Abstract - **In this paper we characterize the proprietary Active Scanning algorithms of several wireless network interface cards (WNICs) and driver combinations. We believe our experiments are the first of their kind to observe the complete scanning process as the WNICs probe all the channels in the 2.4GHz spectrum. We discuss the 1) channel probe order; 2) correlation of channel popularity during active scanning and access point (AP) channel deployment popularity; 3) number of Probe Request Frames (PRFs) sent on each channel across WNICs; 4) amount of time spent on each channel across WNICs (dwell time); and 5) variation in scanning algorithms. The knowledge gained from profiling WNICs is of significant importance to numerous disciplines. It enables us to understand different implementations (hardware and software) of Active Scanning. The same knowledge can help lay a foundation for implementing Active Scanning in network simulators. It is generically considered in only one of the popular simulators. Finally, the results from our work can also radically influence research in link-layer handovers, effective deployment of Access Points (APs), securing wireless networks, etc.**

Index Terms - IEEE 802.11 Active Scanning, Wireless Network Interface Card, Host Association.

I. Introduction

With the advent of IEEE 802.11 standards, it has become easier to access a network without requiring wired Ethernet as a connection medium. The popularity of wireless networking has risen to a point where nearly 70 million 802.11 enabled devices were sold worldwide in the second quarter of 2006 [1]. The essential hardware to enable wireless communication is the WNIC. It is our attempt to characterize WNICs based on certain parameters for the reasons described in section III.

To characterize a WNIC, we focus on the Active Scanning algorithm, which is part of the IEEE 802.11 MAC Layer functions. The IEEE 802.11 MAC Layer is responsible for managing and maintaining communication between various network devices. It coordinates access to a shared radio channel and utilizes standardized protocols to facilitate communication between these devices. We focus on the parameters which can characterize the active scanning algorithm. These parameters include the channel on which the 1st PRF is sent when scanning starts, the total number of PRFs sent on all channels, the bursty nature of a WNIC, the dwell time, etc. Examining these parameters for each WNIC gives us a wealth of information which helps us to characterize all the WNICs used in our experiments. We provide statistical results for this characterization.

We passively listen on all the channels of the 2.4GHz spectrum (11 for USA). Thus, not introducing any additional traffic load on the network, helping to keep our observations unbiased.

The remainder of the paper is organized as follows. Section II mentions the relevant background work done in this field. In Section III we explain the motivation behind conducting this research. It discusses the open problems and the benefits of our work. Section IV highlights the general algorithm used for Active Scanning as described in IEEE 802.11 standards. We then describe the experimental setup and the choice of hardware in Section V. The analysis of our experiments is presented in Section VI and we later use these results to distinguish between three different WNICs in Section VII. We conclude the paper in Section VIII, mentioning the scope of our future work.

II. Related Work

Many attempts have been made to improve or create new active scanning algorithms [2, 3, 4]. The focus has been to reduce the scanning delays by introducing more efficient algorithms. As a result, more effort has been put in introducing newer algorithms rather than understanding the characteristics of the existing algorithms.

Also, on previous occasions it has been shown that different WNICs exhibit peculiar characteristics based on the active scanning algorithm used [5, 6]. The focus was on finding the periodicity of the wireless traffic caused by the active scanning algorithm for distinguishing WNICs.

In this paper we attempt to characterize parameters that have previously been ignored. A critical aspect of our work is that we examine the entire IEEE 802.11b/g spectrum at a given period. This allows us to characterize the active scanning

process of WNICs more precisely than the previous attempts, which only observed selective channels of the spectrum.

III. Motivation

Network simulators like OPNET [7], NS-2 [8], GTNeTs [9], etc. do not take active scanning into consideration. The only simulation tool we noticed that takes active scanning into consideration is QualNet [10]. However, we did not find parameters which were WNIC specific that could be introduced into any simulated environment. This results in the inability to distinguish the active scanning algorithm of one WNIC from another, which neglects the dynamic behavior of active scanning that changes with each implementation. Our work helps by laying guidelines to the parameters and their values which should be added to simulation to accurately depict the behavior of a specific type of WNIC.

Additionally, the research community has been focused on reducing the link-layer handover delays of hosts between APs, which typically ranges from 300-550ms [11]. Without a thorough understanding of how a WNIC behaves while scanning for APs, it is difficult to introduce an effective scheme which can reduce these handover delays. Almost 90% of the time in a handover process is spent scanning for wireless networks [4, 11]. Reducing these active scanning delays is necessary for improving the quality of service, namely for seamless audio and video connectivity.

The same knowledge can also help in efficient deployment of APs in a network. With the knowledge of how different active scanning algorithms work, APs can be deployed on the channels on which the majority of WNICs start scanning (still considering spectrum interference), thereby reducing the initial association time and unnecessary probes.

Another important encouraging factor is the promising use of our work in wireless network security. Profiling WNICs during active scanning can be useful to network administrators for detecting unauthorized WNICs types. Techniques like MAC address spoofing and password phishing are known to easily circumvent security policies. But it is difficult to change the signature of a WNIC. Such a profiling of wireless hardware has applications in both military and civilian use.

IV. Active Scanning

The IEEE 802.11 standard specifies the essentials of all the services a WNIC should implement. However, some of the features have been left vaguely specified for a WNIC manufacturer to implement. It is this set of features which we profile to characterize a WNIC. Our characterization method is generally similar to existing fingerprinting techniques. Tools like Nmap, P0f, etc. can be used to remotely fingerprint an operating system using its TCP/IP stack. Also, fingerprinting denial of service attacks, Bluetooth devices, network worms, etc. have also been researched extensively.

A. Scanning

Scanning for wireless networks is an important function of the IEEE 802.11 MAC protocol. The wireless node attempts to search for available wireless networks and then attempts to associate with them. The IEEE 802.11 standard [13] defines two types of scanning techniques: passive scanning and active scanning. In passive scanning mode, the WNIC listens on one channel at a time for beacon frames from APs. It records the corresponding signal strength and other relevant information about the AP. Using this information, the WNIC then chooses which AP to associate with. In the case of active scanning, PRFs are transmitted on all the channels. The responses received from APs in the form of PRFs are then subsequently processed by the WNIC. Active scanning is the default scanning technique for a WNIC, which enables it to implore an immediate response from an AP, without waiting for the beacon frames to be sent by the AP.

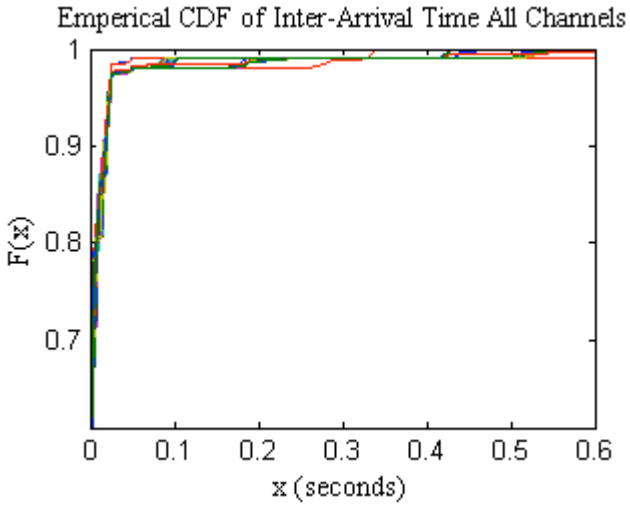

FIGURE 1. CDF OF INTER-ARRIVAL TIME FOR INTEL (ALL CHANNELS, 100 TRIALS, INTERVAL 10^{-2} SECONDS).

The following are the guidelines described in the IEEE 802.11 MAC Layer standard for active scanning [13].
For each channel to be scanned:

a) Wait until the ProbeDelay time has expired or a PHYRxStart.indication has been received.
b) Perform the Basic Access procedure to determine it may transmit.
c) Send a PRF with the broadcast destination, SSID and broadcast BSSID.
d) Clear and start a ProbeTimer.
e) If PHYCCA.indication (busy) has not been detected before the ProbeTimer reaches MinChannelTime, then clear Network Allocation Vector (NAV) and scan the next channel, else when ProbeTimer reaches MaxChannelTime, process all received probe responses;
f) Clear NAV and scan the next channel.

ProbeDelay is the delay to be used prior to transmitting a PRF on a new channel. MinChannelTime is the minimum amount of time to be spent on each channel. MaxChannelTime is the maximum amount of time to be spent on each channel.

B. Parameters for Distinction

As noticed in Section IV-A, the active scanning procedure is not thoroughly defined in the IEEE 802.11 standards, resulting

TABLE 1. WNICS PROFILED AND THE DRIVERS USED.

WNIC	Driver
Airlink AWLC4030	Madwifi ver. 0.9.2.
D-Link Air DWL-650	Madwifi ver. 0.9.2.
Intel PRO/Wireless 2915ABG	IPW2200 ver. 1.1.2.
Linksys WPC11	Prism2_cs
Linksys WPC11	Host AP ver. 0.4.9
Cisco Aironet 350	Airo_cs
Lucent Orinoco Gold PC24E-H-FC	Orinoco_cs

in WNIC manufacturers implementing proprietary active scanning algorithms. The parameters that can vary depending on the WNIC include:

a) Channel on which the 1st PRF is sent.
b) ProbeDelay, MinChannelTime, MaxChannelTime.
c) Number of PRFs transmitted per channel (Burstiness).
d) Delays between PRFs on the same channel.
e) Frequency of channels probed (Number of Probes sent on a channel).
f) Order of channels probed.

These parameters help govern the performance of any active scanning algorithm. We focus our research on the channels on which the 1st PRF is sent, number of PRFs sent on a channel, bursts of PRFs and the dwell time on each channel. We also include an initial analysis of several other parameters.

V. EXPERIMENTATION

In the following section, we describe the hardware and the drivers used to capture the wireless traffic. The testbed was verified to be interference free on the 2.4GHz spectrum.

A. Experimental Setup

For the experiments, 6 Lenovo 3000 C100 laptops running Fedora Core 4, kernel ver. 2.6.11-1.1369 with 512 MB RAM were used. The internal WNIC, Intel PRO/Wireless 2915ABG, was used for sniffing the channels.

The driver and the firmware used for the internal card were ipw2200 ver. 1.1.2 and ver. 3.0 respectively. To obtain additional information, the *radiotap* [14] header was enabled to capture extra header details about each packet, such as the channel number. The crontab command in conjunction with the Network Time Protocol (NTP) was used to synchronize the traffic capture process. Captures were done using the tcpdump utility.

B. Experimental Problems

Our initial attempt was to use an external WNIC along with the internal WNIC to capture traffic over the entire spectrum of 11 channels simultaneously using the 6 laptops. We were able to use an Airlink AWLC4030 and the D-Link DWL-650 using the Madwifi ver. 0.9.2 driver [15] in conjunction with the the internal Intel 2915 using its default IPW2200 ver. 1.1.2. driver. But we observed that the two external WNICs using the Madwifi driver only captured one third or even fewer frames compared to the internal Intel 2915 WNIC. One theory for this

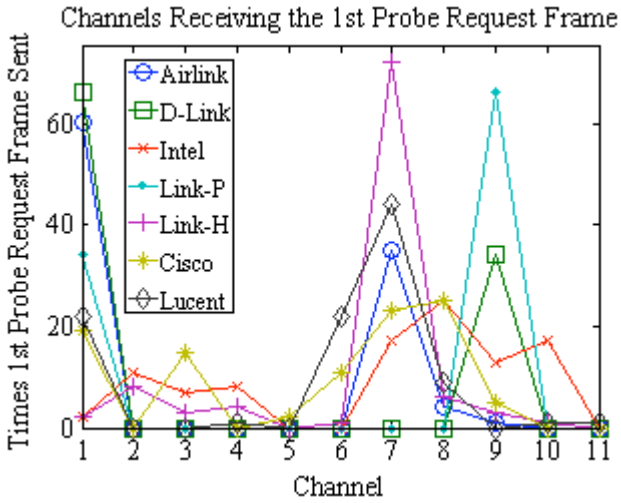

FIGURE 2. CHANNELS RECEIVING THE 1ST PRF (ALL CHANNELS - 100 TRIALS).

could be that the Hardware Abstraction Layer [15], which is part of the Madwifi driver, down samples the number of PRFs. As a result of the poor performance of the Airlink and D-Link WNICs, we decided to only use the internal Intel 2915 WNIC. Our experiments were divided into two blocks. We first conducted 100 trials for channels 1-6 and then 100 trials for channels 7-11 for each of the WNICs. We then merged these files successively, removing the difference in the timestamps from when these two sets of experiments were started. Thus, we were able to examine the activity on all 11 channels for each WNIC for a given period. The wealth of information resulting from examining the entire 2.4GHz spectrum is far better than examining selective channels at a time.

C. Integrity of the Results

To ensure that the capture files were merged properly, we plotted the Cumulative Distribution Function (CDF), Figure 1, showing the inter-packet arrival time for Intel PRO/Wireless 2915ABG WNIC for each trial. We notice that there is a significant overlap between trials in the CDF plot. This shows that each trial followed a similar pattern and our approach of merging the files preserved the integrity of the experimental data. The small variation seen in the plot is a result of cyclic pseudo-random changes in the variables (section IV.B.) associated with active scanning. We further verified our results by plotting the CDF for PRF-Arrival Rate. We did both types of CDF plots for all the WNICs profiled. The integrity of the experiments for the other WNICs was consistent.

D. WNICs Profiled

The WNICs profiled and the drivers used by them are shown in Table 1. For ease of discussion, throughout the paper we will address these WNICs as Airlink, D-Link, Intel, Link-P, Link-H, Cisco and Lucent respectively. All the WNICs were external (PCMICIA) except the Intel, which was an internal WNIC.

As it can be observed in Table 1, we performed two sets of experiments for Linksys WPC11 using two different drivers.

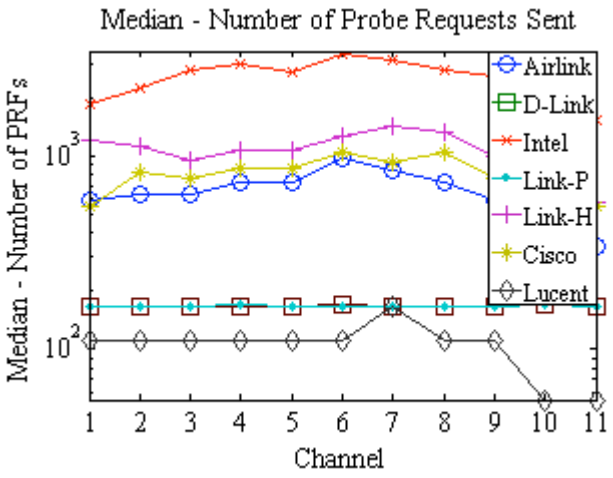

FIGURE 3. MEDIAN - NUMBER OF PRFS (ALL CHANNELS - 100 TRIALS - LOG SCALE).

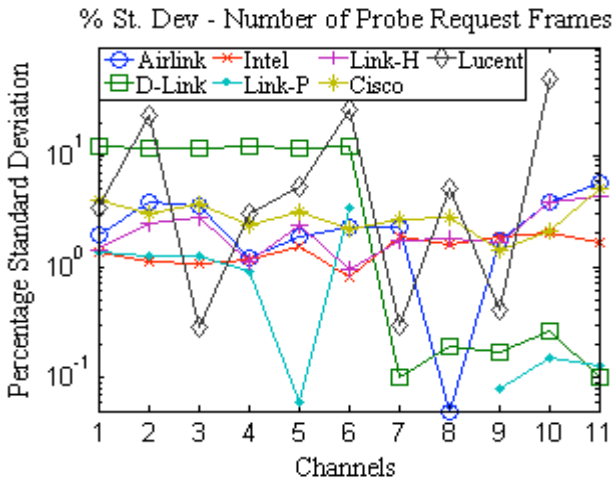

FIGURE 4. PERCENTAGE STANDARD DEVIATION OF NUMBER OF PRFS (LOG SCALE).

Also, experiments for Airlink and D-Link used the same Madwifi driver. Both of these WNICs use different chipsets made by the same manufacturer, Atheros. Our goal with these sets of experiments was to examine two scenarios: 1) the effect of change in drivers on the same hardware; and 2) the effect of change in hardware (even when having a common manufacturer but different chipsets) keeping the same driver. The goal was to understand how different permutations of hardware and software configurations affect the behavior of the active scanning process.

VI. ANALYSIS

In this section we provide the results from our experiments, focusing on: a) the channels on which the 1st PRFs are sent; b) the number of PRFs sent including the burstiness; and c) the dwell time on each channel for every WNIC.

A. Channels Receiving the First Probe Request Frame

Contrary to the belief widely held [3, 16, 17], active scanning does not always start from Channel 1 (see Figure 2). Summarizing the 100 trials for Channel 1: Airlink sent the 1st PRF on Channel 1 in 60 trials; D-Link in 66 trials; Link-P, Cisco and Lucent between 19 to 34 trials; and Intel and Link-H in only 2 trials. Channel 6 only received 1st PRF from Link-H, Cisco and Lucent WNICs. The least favored channel for the 1st PRF was Channel 11 where none of the WNICs except a single trial where Lucent sent the 1st PRF on Channel 11. Cisco was the only card that sent its 1st PRF on Channel 5 (2 trials). Similar behavior was seen on Channels 2, 3, 4, and 10. There was no single channel that received the majority of 1st PRF from all the WNICs. However, the combination of Channels 1, 7 and 9 received nearly 75 percent of the 1st PRFs. If an AP is set to one of these channels, it will reduce the scanning delays during the initial connection.

Our results contradict the assumption that scanning starts at Channel 1. Another observation was that scanning was not sequential in nature. That is, the active scanning algorithms we monitored do not probe the channels in an increasing order. Also, depending on the active scanning algorithm, one or more PRFs can be sent when a WNIC is probing a channel.

In a wireless network, APs are preferred to be setup on Channels 1, 6 and 11, often called the three non-overlapping channels because they theoretically have minimum interference with each other. Our analysis illustrates that configuring APs to operate on these channels will increase the time required for scanning and associating with an AP. Channel 6 received very few 1st PRFs and Channel 11 received only a single 1st PRF from Lucent, among all the WNICs we characterized during the 100 Trials. Thus, to decrease the active scanning delays and the network traffic due to these management frames, the active scanning algorithm should start probing on the channels where APs are most likely to be deployed. Selective active scanning is a proposed solution for implementing such a technique [3, 18, 19].

B. Number of Probe Request Frames

Examining the number of PRFs sent on each channel is another parameter which can help characterize the scanning behavior of WNICs. Figure 3 displays the median number of PRFs on each channel. Figure 4 shows the percentage of standard deviation in the number of PRFs for all trials. The standard deviation plot reveals that the number of PRFs sent across different trials is stable. All WNICs (except Lucent and D-Link) had less than 3% standard deviation across all trials for all channels. For channels where D-Link and Lucent exceeded 3% standard deviation, the number of PRFs fluctuated between two distinct values. For example, on channels 1 through 6, D-Link fluctuated between 111 or 168 PRFs per trial, yet 75-84% of the trials sent 168 PRFs on these channels.

For all WNICs, we observed that channel 6 received the maximum or close to the maximum number of PRFs, asserting the inclination of finding an AP on channel 6, though it received very few number of 1st PRFs. While most of the WNICs sent a different number of probes per channel, two WNICs, D-Link and Link-P probed all channels equally. Lucent probed Channels 1-6, 8 and 9 equally, sending 111

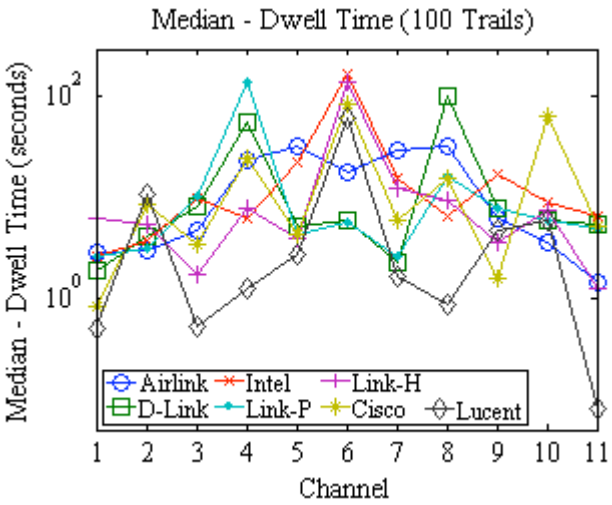

FIGURE 5. MEDIAN DWELL TIME FOR PRFS (LOG SCALE).

PRFs. Channel 7 received 168 frames and Channels 10 and 11 each received 55 PRFs. The scanning algorithm of the Intel WNIC was much more aggressive than the other WNICs, sending 2.5 times more PRFs than the second highest WNIC, Link-P. Compared to the WNIC sending the least number of PRFs (Lucent) on Channel 6, Intel sent nearly 25 times more. The Intel WNIC also exhibited another unique behavior. While measuring the number of PRFs sent per channel we noticed that Intel repeatedly sent a burst of 2 to 6 successive PRFs on a single channel. Whereas, the other WNICs typically sent a single PRF (occasionally two PRFs) per channel. Another interesting observation was that the Intel WNIC in more than 70 trials sent bursts of PRFs ranging from 2 to 19 when sending the first PRFs. For experiments where we varied the device driver for the same WNIC, we observed distinctive behavior. When the Linksys WNIC is used with the Host AP driver (Link-H), the WNIC behaves more aggressively sending 2 to 6 times more PRFs per channel. When the Linksys WNIC is used with the Prism driver (Link-P), the WNIC sends an equal number of PRFs across all channels. From this scenario we can infer that the scanning algorithm is implemented in the driver software.

When comparing Airlink and D-Link, which are two brands of WNICs with chipsets from the same manufacturer (Atheros) that used the same driver (MadWifi), we also noted distinctive behavior. The Airlink WNIC sent 4 to 8 times more PRFs per channel, while D-Link sent a constant number of PRFs across all channels. The differences could be attributed to the fact that the chipset of each WNIC are different versions or the WNIC vendor imposed their own limitations on the scanning process. Additional testing is needed to pinpoint the contributing factor of how the hardware influences the scanning algorithm.

We also noticed an unexpected observation between two WNICs. The D-Link and Link-P WNICs behave almost identically, sending a constant number of PRFs across all channels, despite the fact that the WNICs are based on two different chipsets and used different drivers. This unique observation warrants further investigation as part of our future work to explain this behavior.

TABLE 2. VARIOUS STATISTICAL CHARACTERISTICS OF INTEL, LINK-P AND LUCENT WNICS.

Channel	1	2	3	4	5	6	7	8	9	10	11
1st PRF Sent											
Intel	2	11	7	8	0	0	17	25	13	17	0
Link - P	34	0	0	0	0	0	0	0	66	0	0
Lucent	22	0	0	1	0	22	44	9	0	1	1
Median Number of PRF											
Intel	1845	2234	2816	2962	2720	3350	3157	2817	2622	2331	1553
Link - P	168	168	168	169	168	168	168	168	168	169	168
Lucent	111	112	111	111	111	111	168	111	111	55	55
Median Dwell Time (seconds)											
Intel	2.65	3.85	9.79	6.30	23	167	15.3	6.66	17.1	9.14	6.42
Link - P	2.62	3.16	10.5	143	4.44	5.77	2.59	16.5	8.00	5.99	4.97
Lucent	0.51	10.6	0.53	1.26	2.78	62.4	1.66	0.86	4.69	5.92	0.08

The statistics regarding the number of PRFs varied greatly across the set of WNICs we analyzed. Some WNICs were more aggressive in the number of probes sent. Some WNICs exhibited a steady scanning algorithm probing different channels equally, while other scanning algorithms favored certain channels. The analysis also illustrated the impact that the hardware and driver software combination has on the number of PRFs.

C. Dwell Time

Next we measured the dwell time, which is the amount of time spent by a WNIC on each channel. Channel dwell time is calculated by subtracting the arrival time of the first PRF on a particular channel from the arrival time of the first PRF on the subsequent channel probed. Figure 5 shows the median dwell time for all the WNICs on each of the channels.

An interesting observation was that the dwell time varied for each channel and each WNIC, i.e., the MinChannelTime was found to be channel specific. Another observation was that the majority of the WNICs spent a substantial amount of time scanning on Channel 6 (reflected by the peaks on Channel 6 in Figure 5). We found that a generally heightened dwell time was due to either of the following two reasons: 1) there were a larger number of PRFs on a particular channel, thereby increasing the dwell time; or 2) the WNIC actually dwelled longer on a particular channel before scanning the next channel. For example, Intel had a high dwell time on Channel 6, even though it sent almost the same number of PRFs as on Channel 7. The dwell time on Channel 6 was close to 11 times more than that on Channel 7.

VII. Distinguishing Between WNICs Using Probe Request Statistics

In this section we discuss how some of the parameters obtained from characterizing active scanning algorithms can be used to distinguish WNICs. We randomly chose three WNICs (Intel, Link-P and Lucent) and used the parameters in Table 2 to distinguish them.

The comparison shows that the channel on which the 1st PRF is sent by the three WNICs to be very distinctive. If an intrusion detection system (IDS) is sniffing on all the channels, if can clearly ascertain which among the three WNICs has started scanning for APs. This parameter can help distinguish between WNICs. However, as previous work has shown [5,6], such a distinction is hard to achieve if sniffing is limited to a few channels.

However, there are some channels which receive the 1st PRF for two or more WNICs. In this case, we can look at the number of PRF sent on those channels. Clearly the median values for the number of PRFs sent by Intel on all channels is larger than Link-P or Lucent. Also, the values for Link-P are always larger than that for Lucent. Therefore, setting thresholds on the number of PRFs could help distinguish between WNICs. To more precisely distinguish between NICs each card can have a profile consisting of probabilities associated with the active scanning variables. Due to limitations of space, more comparisons could not be shown. However, these set of examples illustrate how an IDS could identify a WNIC by analyzing the behavior of a WNIC during active scanning.

VIII. Conclusion and Future Work

Our findings have shown that scanning does not always start on channel 1, is not sequential, and contains a significant amount of variation depending on the WNIC chipset and software used. Also, we showed that there is no correlation between the channels where access points are commonly deployed (1, 6, and 11), and the channels that are favored by the scanning algorithms. We further find that the number of Probe Request Frames (PRFs) sent per WNIC and on each channel were unique with Channel 6 being the most popular for the majority of the WNICs. Intel sent the most probes overall and showed a bursty nature. Finally, we showed that the dwell time for each WNIC is channel, WNIC and driver specific. Some WNICs had a significantly higher dwell time on particular channels because they sent more PRFs on that channel or because the WNIC waited for a longer length of time on a particular channel before probing the next channel.

We are currently attempting to further describe the active scanning algorithm, both quantitatively and qualitatively. We plan to find an algorithm that can predict the pattern of PRFs sent on each channel and the dwell time for each WNIC on that channel. Our initial findings for certain WNICs show that the number of PRFs changed by a constant value every specific interval of time. Our hypothesis for the dwell time is that the algorithm randomly selects a MinChannelTime from a certain range and then keeps decreasing it at a pseudo fixed rate. We plan to thoroughly test and confirm our findings.

We also plan to research on the nature of active scanning of a WNIC when connected to an AP. We hope to find how frequently WNICs continue to send PRFs, and how the algorithm behaves in that scenario. We plan to use signal processing as a tool to analyze the temporal behavior of these streams of PRFs to extract the periodicity in the scanning algorithms.

References

[1] Gartner Research: Website 2006, (http://www.gartner.com/)

[2] I. Ramani and S. Savage, "SyncScan: Practical Fast Handoff for 802.11 Infrastructure Networks", *Proceedings of the IEEE INFOCOM 2005*

[3] Sangho Shin, Andrea G. Forte, Anshuman Singh Rawat and Henning Schulzrinne, "Reducing MAC Layer Handoff Latency in IEEE 802.11 Wireless LANs", *Proceedings of the 2nd International Workshop on Mobility Management and Wireless Access*, PA, USA, 2004

[4] H. Velayos and G. Karlsson, "Techniques to Reduce the IEEE 802.11b Handoff Time", *IEEE Communications*, 2004

[5] Cherita Corbett, Raheem Beyah and John Copeland, "Using Active Scanning to Identify Wireless NICs", *Proceedings of IEEE Information Assurance Workshop (IAW)*, June 2006.

[6] Jason Franklin, Damon McCoy, Parisa Tabriz, Vicentiu Neagoe, Jamie Van Randwyk and Douglas Sicker, "Passive Data Link Layer 802.11 Wireless Device Driver Fingerprinting", *Proceedings of the 15th USENIX Security Symposium*, August 2006

[7] OPNET Modeler: Network Simulator, Website 2006, *(http://www.opnet.com/)*

[8] NS-2: Network Simulator, Website 2006, *(http://www.isi.edu/nsnam/ns/)*

[9] GTNetS: Network Simulator, Website 2006, *(http://www.ece.gatech.edu/research/labs/MANIACS/GTNetS/)*

[10] QualNet: Network Simulator, Website 2006, *(http://www.scalable-networks.com/)*

[11] Arunesh Mishra, Minho Shin and William Arbaugh, "An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process", *ACM SIGCOMM Computer Communication Review*, 2003, pages 93 - 102

[12] Cherita Corbett, Raheem Beyah, and John Copeland, "A Passive Approach to Unauthorized Sensor Node Identification", *Wireless Sensor Networks and Applications*, Chapter 17, Springer, 2005.

[13] IEEE 802.11 Standards, Website 2006, *(http://standards.ieee.org/)*

[14] Radiotap Header: Radiotap header for IPW2200, Website 2006, *(http://ipw2200.sourceforge.net/)*

[15] MadWifi: Multiband Atheros Driver for WiFi, Website 2006, *(http://madwifi.org/)*

[16] Rastin Pries and Klaus Heck, "Simulative Study of the WLAN Handover Performance", *OPNETWORK 2005*, Washington D.C., USA, August 2005.

[17] Rastin Pries and Klaus Heck, "Performance Comparison of Handover Mechanisms in Wireless LAN Networks", *ATNAC 2004*, Sydney, Australia, December 2004.

[18] Sonia Waharte, Kevin Ritzenthaler and Raouf Boutaba, "Selective Active Scanning for Fast Handoff in WLAN Using Sensor Networks", *International Conference on Mobile and Wireless Communication Networks*, Paris, France, October 2004, pages 59-70.

[19] S. Speicher and C. Bunnig, "Fast MAC-Layer Scanning in IEEE 802.11 Fixed Relay Radio Access Networks", *International Conference on Mobile Communications and Learning Technologies*, 2006.

*Sandia is a multiprogram laboratory operated by Sandia Corporation, a Lockheed Martin Company, for the United States Department of Energy's National Nuclear Security Administration under Contract DE-AC04-94AL85000.