Spectrum Sensing with WLAN Access Points

Ryan T. Jacobs, Jason B. Coder
Communications Technology Laboratory
National Institute of Standards and Technology
325 Broadway St., Boulder, CO 80305
Ryan.Jacobs@nist.gov

Vivian M. Musser
Department of Electrical and Computer Engineering
University of Maryland
2410 A.V. Williams Bldg., College Park, MD 20742

***Abstract*—With wireless communication becoming increasingly common in simple everyday devices, the available spectrum is quickly filling up and the risk of interference is increasing. This interference could be a slight nuisance or a disruption to critical services. To better understand the quantity and type of traffic in congested environments, a potential spectrum sensing solution in the ISM bands is discussed. By using a commercially available wireless access point we may be able to monitor the spectrum within range of the access point. If the electromagnetic environment is better understood, device manufacturers should be better able to test their products before deployment, ensuring they can still perform in a crowded electromagnetic environment.**

I. Introduction

The use of spectrum sharing technologies and methods is growing at a rapid rate. As new methods and technologies are developed and deployed, device manufacturers need to be able to characterize new and existing devices to ensure they will perform in a congested RF environment. One component of this characterization involves understanding what activity is taking place in the electromagnetic environment of interest. A better understanding of the environment leads to a characterization test that is more appropriate and realistic.

One example of a popular, uncoordinated spectrum sharing scenario is the 2.4 GHz ISM band. As this band (2.4 GHz -2.5 GHz) is loosely regulated in the U.S., there are many different protocols and devices that make use of this band. Two of the largest occupants are IEEE 802.11 and IEEE 802.15 wireless devices. As new 802.11 and 802.15 standards are developed, understanding how they perform (i.e., send/receive data) in this crowded environment is crucial.

But without an understanding of the actual electromagnetic activity in the ISM band, the characterization test these devices undergo represent estimates, at best. For example, in-field measurements of the ISM band may show that at 2450 MHz, there is consistently a high level of traffic. This information can be fed back into the device development and measurement standards efforts which would recommend an appropriate amount of testing that corresponds to the actual usage seen in the field.

Accomplishing the task of understanding what's happening in the ISM band may sound simple, but considering the amount of traffic and its widespread geographic use this is a daunting task. One option would be to deploy high-end instrumentation that is capable of taking very detailed measurements, but this is not practical for measurements outside of a laboratory setting. However, most buildings have several wireless access points (WAPs) that make up their 802.11 network. These networks facilitate the 802.11 traffic, perform Clear Channel Assessments (CCA), can detect other wireless networks, and measure the noise level in the environment. These data are collected by WAPs for use in selecting the best channel to use with connected clients. With some modification and automation, we show that we can acquire the spectrum data from the WAP and process it for spectrum occupancy information. We also discuss some of the challenges associated with using a WAP network as a spectrum sensor.

II. Information Available From the Access Point

Here, our goal was to examine how much spectrum information we could acquire from the WAP. For the WAP tested, there are two modes that are of interest: access point mode and scanner mode [1, pg. 4-10].

When in access point mode, the WAP allows wireless devices to connect to it for access to the network. While in this mode, the 802.11 channel can be set manually or automatically via a CCA. By manually selecting the 802.11 channel, the WAP is still able to perform CCAs, but does not take any action based on their results. When preforming CCAs, the WAP is able to detect wireless devices utilizing 802.11 a/b/g/n/ac. We can also retrieve the RF power level in the channel, as measured by the WAP. Here, we refer to this as noise power because this is a simple power measurement, without regard for what device is generating the power, or what protocol is being used.

The other WAP mode of interest is the scanner mode. This mode will allow the WAP to be dedicated to scanning for traffic in its frequency band and RF spectrum. To use Scanner mode, there must be more than one WAP on the network. For this study only one WAP was used so it was not possible to put the WAP into scanner mode.

III. Measurement Setup

Figure 1 shows the measurement setup. For the WAP to be used, a Layer 2 managed switch and WAP controller are required. The managed switch provides the main interface into the network, a Layer 2 switch does switching only (based on the MAC address). This is where the WAP, WAP controller and computer are connected to the wired network. The WAP controller is used to provide the command line interface to the

U.S. Government work, not subject to U.S. copyright.
U.S. Government work not protected by U.S. copyright

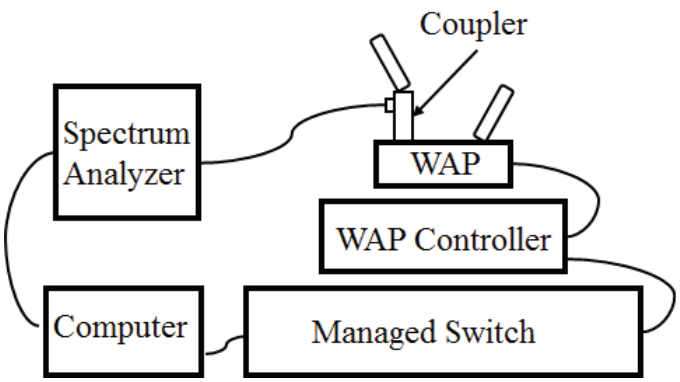

Figure 1: Block diagram for WAP measurement setup.

WAP. The controller enables us to control the WAP's radios, transmit power levels, and set the IP address of the WAP. It is also used to setup and configure how the WAP can be accessed by network administrators (e.g., TELNET, SSH, Serial, SNMP, etc.). For our experiments, we communicated with the controller and WAP via TELNET. We chose TELNET because we could easily write scripts to access the controller and WAP, and acquire data. In addition to collecting RF data with the WAP, a spectrum analyzer was also connected to one of the WAP's antennas via a directional coupler. By collecting data from the spectrum analyzer and WAP at the same time, we can compare the data sets collected by each to see how similar they are.

IV. Measured Data

After verifying the measurement setup with known signals, we acquired data over a 48 hour period. Figure 2 shows a cumulative plot of the measured noise power over the 48 hour period for each of the 11 standard 802.11 channels. These data were recorded in an office environment over a weekend. Thus, we would not expect to see a significant amount of activity.

Figure 3 shows a comparison between the recorded WAP data and a spectrum analyzer. Since the spectrum analyzer takes data once every second and the WAP only updates once every 60 seconds, the data collected from the spectrum analyzer are condensed into smaller "blocks" to make it match the update

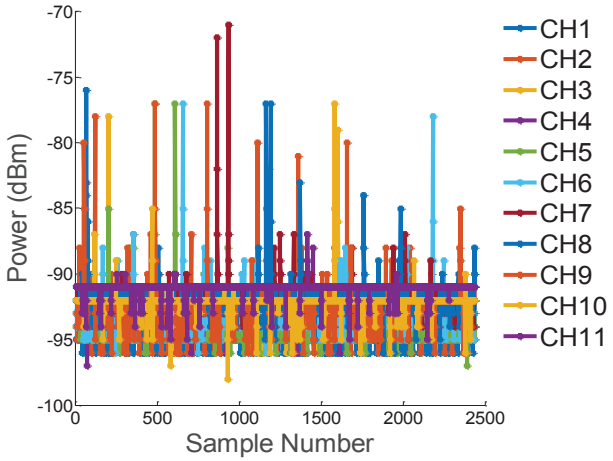

Figure 2: Recorded spectrum noise from the WAP

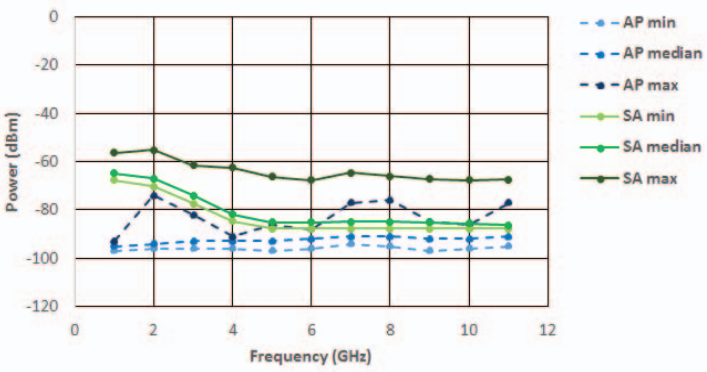

Figure 3: Spectrum analyzer vs. Wireless access point

frequency of the WAP. This is done by taking every 60 samples of spectrum analyzer data and finding the peak value for each frequency. By doing this, we are able to directly compare the data from the WAP to the recorded data from the spectrum analyzer. As seen from Figure 3, there is not much correlation between the spectrum analyzer and the WAP. There are two likely reasons why the signals do not have better correlation. The first reason could be that because the signals appear so infrequently, the WAP either does not see them because it is scanning across the channel, or because the RF detector on the WAP, based on an average (or average-like) detection and does not register a signal of shorter duration. The offset between the WAP and spectrum analyzer data may be the result of different amounts of loss in the RF cabling and RF circuitry present inside the WAP.

V. Future Work and Conclusions

The data shown in Section IV indicate that we can get general spectrum occupancy data from a WAP, though the accuracy of the data may be an issue. Also, the granularity of the data acquired from the WAP (in terms of frequency) may not be enough to draw conclusions about what traffic is traversing the environment. The WAP likely has the hardware to provide data with increased granularity, the current firmware does not provide access to it. Additional capabilities may be possible with the use of the "scanner mode" discussed earlier. Future work may involve setting up a larger test network to examine a WAP with scanner mode enabled.

In addition to the characterization performed here, additional work needs to be done to show how well the WAP (in any mode) responds to signals other than the 802.11 standard. For example, how well does the WAP respond to 802.15 signals, or other non-standard "pulse-type" signals frequently seen in the ISM bands. Here, we have shown some preliminary measurements investigating how feasible it is to use a WAP as a spectrum sensor for the purpose to better understanding the traffic in the crowded ISM bands. The data indicate that more work needs to be done to ensure that the WAP is capable of making RF measurements with an accuracy appropriate for spectrum sensing.

References

[1] Cisco Systems, Inc., "Cisco Aironet Access Points Configuration Guide for Cisco IOS Software," Cisco IOS Release 15.2(4)JB3a, 6-1. Accessed September 21, 2015.