An Experimental Approach to Spectrum Sensing in Cognitive Radio Networks with Off-the-Shelf IEEE 802.11 Devices

Hyoil Kim[†], Carlos Cordeiro[‡], Kiran Challapali[‡], and Kang G. Shin[†]

[†]Real-Time Computing Laboratory, EECS Department, University of Michigan, Ann Arbor, MI 48109–2121
Email: {hyoilkim,kgshin}@eecs.umich.edu

[‡]Philips Research North America, Briarcliff Manor, NY 10510
Email: {Carlos.Cordeiro,Kiran.Challapali}@philips.com

***Abstract*— Spectrum sensing is essential to the realization of spectrum agility in cognitive radio (CR) networks. Although fundamental tradeoffs and theoretical limits associated with spectrum sensing have been studied extensively, there have been very few experimental studies focused on building a spectrum "sensor" with commercial off-the-shelf devices. We have therefore built a prototype of CR-based sensor implementation with off-the-shelf IEEE 802.11 devices.[1] In particular, we have explored issues in implementing a spectrum sensor, mostly at the MAC layer, as well as the difficulty in implanting sensing functions into industrial network interfaces. Our experimental results demonstrate the feasibility of building a spectrum sensor and the construction of an incumbent-detection mechanism with off-the-shelf devices. We have also identified technical difficulties, such as device-dependency in determining the detection threshold, in-band signal jamming between secondary devices, and adjacent channel interference due to out-of-band signal emission. This experimental experience has led us to suggest a sensor design guideline for commercial wireless interfaces which can also facilitate other CR-related research.**

I. Introduction

Cognitive radios (CRs) are considered essential to the realization of *spectrum agility* for the new FCC's dynamic spectrum access policy [1]. A CR has to be aware of, and adaptive to, its surrounding environment by dynamic selection of various protocols/algorithms. Among the necessary CR features, it is crucial to effectively identify *spectrum holes*, promptly detect legacy incumbents and protect them from the harmful interferences caused by CR users. For this, *spectrum sensing* is recognized as a key requirement. Although many previous studies have addressed limitations and technical difficulties in realizing a spectrum sensor in CR networks, there have been much fewer attempts to build a real sensor with commercially-available devices and address the practical issues of spectrum sensing.

To remedy this deficiency, we have built a sensor prototype with off-the-shelf radio devices, especially WLAN cards with built-in Atheros chipset. With this prototype, we can (experimentally) explore important sensing issues, mostly in the MAC-layer, and assess/verify key ideas of spectrum sensing with a slight modification to the Atheros device driver. We can also uncover practical issues and difficulties in sensor implementation. Based on this experience, we develop a guideline for developing a CR sensor, which will benefit those who want to design a sensor testbed or commercial sensors.

There have been a limited number of publications on the implementation of cognitive radios [2], [3], [4] which describe development of testbed platforms with FPGAs. Harada [2] introduced a Software Defined Radios (SDRs) prototype that can reconfigure itself to operate on different protocols, without any actual CR implemetation. Mishra *et al.* [3] demonstrated a multi-purpose CR testbed built on Berkeley Emulation Engine 2 (BEE2), without considering the details of sensing issues. DeGroot *et al.* [4] showed their feature detector design for TV bands, with emphasis on the physical (PHY) layer. On the other hand, Doerr *et al.* [5] developed a virtual-SDR system using an Atheros platform by eliminating dependency on 802.11 in the chipset. They also implemented MultiMAC, an adaptive MAC framework, which can be used for CR research. We also use an off-the-shelf WLAN device, but focus on sensor design as well as on various practical issues associated with the implementation of spectum sensing.

The rest of the paper is organized as follows. Section II describes the general (mostly in the MAC layer) issues of spectrum sensing. Section III presents our prototype of spectrum sensor and its design details. Section IV proposes guidelines for sensor development. Finally, the paper concludes with Section V.

II. Spectrum Sensing

The key components of spectrum sensing and their issues are introduced in this section. Section III will describe our sensor implementation that addresses these issues. We first introduce assumptions and terminologies used throughout the paper.

[1]Linksys WPC55AG (Dual-Band Wireless A+G Notebook Adapter) cards which are built with Atheros chipsets (AR5212).

1-4244-0667-6/07/$25.00 ©2007 IEEE

This full text paper was peer reviewed at the direction of IEEE Communications Society subject matter experts for publication in the IEEE CCNC 2007 proceedings.

A secondary network is assumed to be a single-hop ad-hoc wireless network. The network is allowed to occupy at most one channel at a time, and this is possible only if all secondary users (SUs) are guaranteed not to cause harmful interference with the channel's primary users (PUs).

We will use the following terms throughout the paper. *Home channel* is defined as the channel which is currently being utilized by the secondary network. On the other hand, a *foreign channel* refers to any of the other channels that are not currently being utilized but may possibly be used later. *In-band sensing* implies sensing on the home channel, whereas *out-of-band sensing* means sensing on a foreign channel.

A. Incumbent Detection

Incumbent detection is one of the most critical tasks of sensing. Its purpose is to protect PUs against harmful interference from SUs by promptly detecting PUs' presence. As soon as PUs are detected in the home channel, the secondary network has to vacate/switch its home channel. For example, the IEEE 802.22[2] [6] standard for unlicensed operation in the TV bands regulates that PUs (in the IEEE 802.22 case, TV signals and FCC Part 74 devices) should be detected within 2 seconds from their appearance [7].

From the physical (PHY) layer's perspective, PU signal detection can be classified [8] as: *matched filter*, *energy detection*, *feature detection*. Among these, energy and feature detection schemes have thus far received most of the attention. Although energy detection is simpler and faster than feature detection, the former cannot distinguish SUs from PUs. To solve this problem, 802.22 introduced the concept of *quiet period*. During a quiet period, SUs are not allowed to transmit so that only PU signals can be present. Hence, it is preferred to perform incumbent-detection within a quiet period.

In this paper, we address the two main issues of incumbent detection: (i) how to implant PHY detection in commercial 802.11 devices, and (ii) how to set up an incumbent detection threshold.

B. Channel-Switching

This is the procedure a secondary network uses to switch its home channel. There are two types of channel-switching: *mandatory* and *voluntary*. Mandatory switching is triggered by in-band incumbent detection, whereas voluntary switching is performed if the QoS requirements of the secondary network cannot be met by the current home channel. *Backup channels* are a set of foreign channels prepared in-advance to expedite the channel-switching process [6]. The secondary network proactively measures foreign channels to find candidate home channels, which may have to be sensed again at channel-switching time in order to validate its availability.

C. Secondary Traffic Characterization

Secondary traffic characterization is another function of sensing, whose purpose is to characterize and estimate the quality of a channel by observing a secondary network's traffic pattern. The link quality helps prioritize backup channels so that a secondary network can select its new home channel. In this paper, *channel utilization*, a portion of time in which the channel is being utilized by its SUs, is used as a metric of the link quality.

D. Scheduling Sensing

Sensing resembles a channel sampling process in that each measurement is performed for a bounded amount of time on a specific channel. Depending on the purpose of sensing, there could be four types of sensing: in-band/out-of-band incumbent detection, and in-band/out-of-band secondary traffic measurement. This, in turn, requires the development of a sensing schedule so that each sensing type could be scheduled multiple times. Scheduling sensing must consider the priority of sensing types, as well as sensing constraints. For example, incumbent detection should be done only during a quiet period.

III. Sensor Prototype with Atheros Platform

The objective of our prototyping is to test key ideas of spectrum sensing in a real wireless environment and to highlight difficulties in implementing a sensor device. Since it is illegal to utilize a licensed spectrum for testing purposes, we have chosen UNII bands as our testbed environment. Hence, SUs are implemented with IEEE 802.11a WLAN cards, Linksys WPC55AG (Dual-Band Wireless A+G Notebook Adapter) built with Atheros chipsets. For our purpose, any of the thirteen 802.11a channels are treated as licensed channels and can thus be occupied by a PU signal. In our testbed, a primary signal is generated by Rohde&Schwarz signal generator. This signal generator can transmit a sine-wave signal with controllable center frequency. It is assumed that PUs follow a different PHY encoding scheme from SUs. In the current prototype, the effect of fading and shadowing is not considered.

Atheros supports an open source Linux device driver, called *MadWifi* [9]. Most of the PHY and MAC functions are implemented in the Atheros chipset, and HAL (Hardware Abstraction Layer) acts as a gateway between Atheros and MadWifi. We implement the spectrum sensor by adding sensing features to MadWifi. The sensor operates in the monitor mode to overhear all signal activities in the air.

A. Implementation of Incumbent Detection

Energy detection is the only PHY-layer detection scheme supported by 802.11. Even so, a key difficulty in implementing incumbent detection with the Atheros platform is that energy detection mechanism is hidden in the hardware. For this reason, we developed our incumbent detection method based on counting PHY/CRC errors. A PHY error is reported from Atheros to MadWifi if a packet/signal without an 802.11 PHY preamble is observed, which happens when the emulated PU signal is present since it is a pure sine-wave. On the other hand, a CRC error is indicated by Atheros if a legitimate 802.11 SU packet has an incorrect CRC checksum. This occurs if a SU packet is interfered with by PUs. Therefore, PHY/CRC errors could be a strong indicator of existence of incumbents.

[2]The first international standard of CR networks in TV bands.

There is, however, a drawback in this approach. Due to the uncertainty of wireless spectrum, PHY/CRC errors could occur even in the absence of PUs. Hence, we need to define a principled incumbent detection threshold in terms of the number of PHY/CRC errors. In our prototype, we have determined this threshold experimentally since the mechanism of Atheros for detecting/reporting errors is not known.

Our experiments are set up as follows. A PU, Rohde&Schwarz signal generator, transmits a sine-wave signal for D(ms) with the frequency of 5.18GHz, which is the center frequency of 802.11a channel 36. The sensor, operating at channel 36, overhears the signal L(inches) away from the PU signal source. L and D are testing parameters to see the difference in the number of observed PHY/CRC errors at the sensor. As L decreases, the Receive Signal Strength Indicator (RSSI) of the observed PU signal increases. RSSI values of +33 and +39 are tested, where RSSI +33 corresponds to -62dBm in Atheros,[3] which is the energy detection threshold in IEEE 802.11a for a signal without a PHY preamble. In other words, RSSI +33 is the minimum signal strength above which energy detection scheme works properly in Atheros.

Figure 1 shows the plot of the total number of PHY/CRC errors observed during D(ms). For the given L and D, the experiment is repeated 100 times and the average number of errors is computed. Figure 2 illustrates the average time interval (in milliseconds) between errors. As shown in Figure 1, the longer observation time, the more errors observed. Furthermore, a stronger signal tends to incur more errors.[4] This suggests that the plot of RSSI +33 in Figure 1 can be used as a lower bound for the detection threshold. However, it should be noted that the number of errors does not increase linearly with D. One plausible explanation is that Atheros tries to interpret the unpacketized sine-wave signal into a sequence of packets, and reports a PHY error for every virtually-recognized packet. As the signal duration D increases, Atheros seems to adapt and enlarge the time-length of a virtual packet, resulting in less frequent error reports, as clearly shown in Figure 2.

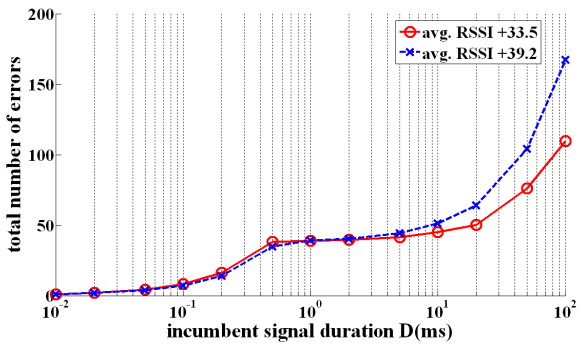

Fig. 1. Number of PHY/CRC errors during the observation period D(ms)

[3]The conversion formula is given as RSSI - 95 (dBm) [10].

[4]Although the plot of RSSI +39.2 shows a slight degradation for some D$\leq$1(ms), it is negligible, considering the apparent increase over the plot of RSSI +33.5 for D$\geq$1(ms).

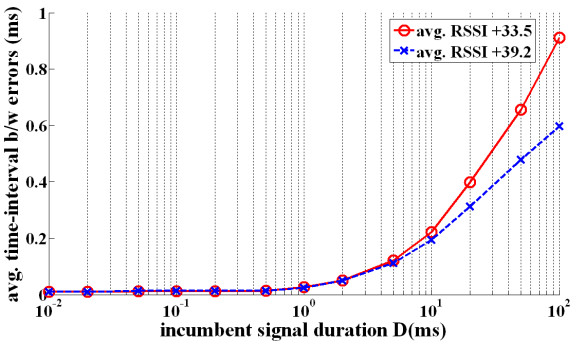

Fig. 2. Time-Interval between errors (ms)

Based on this study, we define the rules to set up the detection threshold. First, the graph of RSSI +33 becomes a reference to determine the threshold. Second, given that incumbent detection is performed in a quiet period of D(ms), a reference number of errors is obtained from the graph of RSSI +33 corresponding to D in the x-axis. For example, if the quiet period is 2(ms), the corresponding number of errors is given as 39.61(errors). Third, the detection threshold can be set as one-fourth of the reference, 9.9(errors) in the current example, to enhance the detection probability. Then, in case a sensor detects more than 9.9 errors during the quiet period of 2(ms), the channel is considered as occupied by its PUs.

B. Implementation of Secondary Traffic Characterization

Secondary traffic characterization is to estimate the quality of a channel, and in particular, channel utilization for our testbed. The channel utilization is estimated as follows. First, the sensor overhears the secondary traffic and estimates the air-time of each packet. With the packet length L(bits) and data rate R(Mbps), the air-time is estimated as L/R(ms). Second, channel utilization is estimated from a history of packet observations, by accumulating air-times and dividing it by the total sensing time. *Moving window* can also be employed to discard obsolete observations.

For each secondary traffic characterization measurement, we recommend to use a sensing duration of 16(ms). This recommendation is to ensure that at least one complete packet will be observed in case there is consistent data traffic. In the worst case, the observation could start right after the PHY preamble of the largest packet has been transmitted, followed by the worst-case contention, as shown in Figure 3. The maximum air-time of a packet, obtained from the maximum payload size and minimum data rate (6Mbps), is 3.15(ms), and the worst-case contention time, resulting from CW_{max}, is 9.24(ms). Based on this, the sensing duration is derived as $2 \cdot 3.15 + 9.24 = 15.54$(ms).

C. Priority-based scheduling of sensing

There are two constraints in scheduling sensing: (i) incumbent detection should be scheduled during a quiet period, and (ii) the sensing priority depends on the type of sensing. In our prototype, we set the sensing priority as:

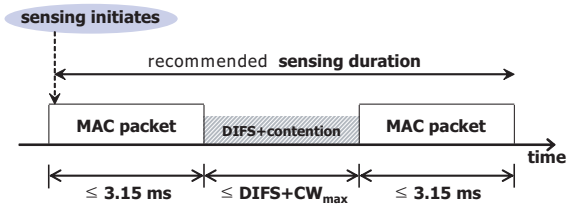

Fig. 3. The worst-case scenario in sensing secondary traffic

- highest priority for in-band incumbent detection,
- 2nd priority for out-of-band incumbent detection,
- 3rd priority for out-of-band secondary traffic measurement, and
- lowest priority for in-band secondary traffic measurement.

First, incumbent detection has priority over secondary traffic measurement since the former is key to incumbent protection. Second, in-band incumbent detection has priority over out-of-band incumbent detection because PUs in the home channel should be protected first. Finally, out-of-band secondary traffic measurement should be given priority over in-band secondary traffic measurement, since the former is necessary for mandatory switching, whereas the latter only supports voluntary switching, which is less critical than mandatory switching.

We propose a priority-based scheduling algorithm for sensing. A prioritized scheduling queue is allocated to each type of sensing, and a queue entry indicates a sensing request on a certain channel issued by the secondary network. The algorithm searches four queues according to their priorities, and the sensing requests in the queue with the highest priority are always scheduled first. If a request for incumbent detection is received, a quiet period has to be scheduled first by the network and the sensing is performed during the period. For out-of-band sensing, it is preferable to schedule multiple foreign channels' visits in a round-robin fashion.

IV. Guidelines for Sensor Implementation

Based on the results of our extensive experiments with off-the-shelf IEEE 802.11 devices, we suggest a practical guideline for the implementation of spectrum sensors in CR networks.

A. Incumbent Detection

In case the sensor exploits energy detection, the duty cycle of PU signals should be considered because the incumbent detection threshold is susceptible to the duty cycle. For example, the plot of error rate derived from our experiments in Section III would be different if the sine-wave signal were pulse-modulated to have some ON/OFF patterns with a duty cycle less than 100(%). Therefore, the detection threshold has to be chosen by considering the characteristics of the PU signal, such as duty cycle, ON/OFF pattern, etc.

B. Secondary Traffic Measurement

Secondary traffic measurement plays an important role in preparing back-up channels. Although channel utilization has been used as a metric of the link quality, it is preferable to have a multi-dimensional vector to describe channel characteristics. For instance, parameters such as the expected interference temperature level at the primary receiver, path loss, wireless link errors, link-layer delay, or holding time by the SU can be considered [8].

C. In-Network Interference

SUs can interfere with each other due to co-channel and adjacent-channel interference. We investigated two interference models: (i) in-band jamming, which is a kind of co-channel interference, and (ii) out-of-band signal emission, as an example of adjacent-channel interference. Experiments with 802.11 transceivers and sensors have been performed to derive guidelines to mitigate in-network interference.

1) In-band Jamming: In-band jamming is caused by a nearby strong signal which makes a SU's Automatic Gain Control (AGC) produce a very small gain. If it occurs, the observed signal cannot be processed/recognized properly. To overcome this problem, the maximum power level acceptable to a SU must be defined. An experiment with the setup shown in Figure 4 have been conducted once to determine this power level. Nodes A and B are 802.11a devices. Node A generates UDP traffic with a goodput of 34Mbps to Node B via AP. The link between Node A and AP is wireless (channel 36), whereas AP and Node B are connected via an Ethernet link. Node B also works as a sensor with its wireless interface, and it observes the wireless traffic (generated by Node A) in channel 36 for 30(seconds), d(inches) away from Node A and 72(inches) away from AP. The overheard packets are used to calculate the average RSSI of 802.11 DATA/ACK packets. Since the sensor is far away from AP, RSSI of ACK packets shows consistency at the sensor side. However, we are primarily interested in DATA packets from Node A. As shown in Table I, the observed signal strength of DATA packets increases as d decreases. At $d \leq 1$(inch), however, DATA packets are not detected, indicating that the sensor is jammed by the jamming signals. This suggests that no more than RSSI +72 should be introduced to the sensor to avoid in-band jamming, as far as Atheros is concerned.

2) Out-of-band Emission: Out-of-band (OOB) emission is caused by energy leakage from adjacent bands. This can introduce uncertainty in incumbent detection. For example, strong signal activities in foreign channels could induce unwanted additional PHY/CRC errors to be seen by a sensor, thus increasing the false-alarm probability. To observe the number of errors induced by OOB emission, we performed an experiment once with the same setting as Figure 4, with one difference: Node A and AP communicate via channel 36, and the sensor listens to one of the adjacent channels. The list of adjacent channels and the experimental results are summarized in Table II, where each measurement implies the number of errors observed during a period of 30(sec). In case the sensor performs in-band incumbent detection during a quiet period of D=2(ms), the detection threshold is set to 9.9(errors) as derived in Section III. If a maximum of 10% more unwanted errors are allowed on the threshold, the errors caused by OOB

emission should be suppressed to less than 0.99/2(errors/ms), or equivalently, less than 14850(errors) for 30(sec). In Table II, channel 40/44 with $d \leq 6$ and channel 48 with $d = 3$ cannot meet the requirement. Therefore, the guideline for solving the OOB emission issue in Atheros is: (i) any two WLAN cards (or nodes) should be placed with enough distance between them, or (ii) the maximum transmission power should be regulated, so that out-of-band emission will not cause too many PHY/CRC errors.

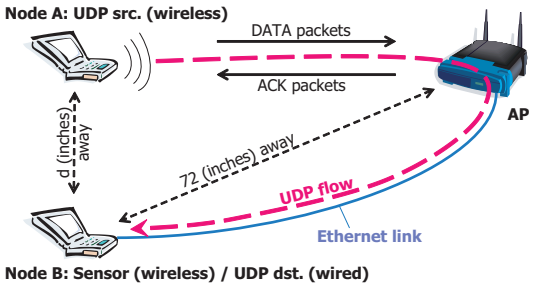

Fig. 4. The experimental setup of in-network interference test

d (inches)	24	12	6	3	1	0 (contact)
min/max RSSI of DATA packets	+49/ +52	+61/ +65	+62/ +67	+66/ +72	n/a	n/a

TABLE I

IN-BAND JAMMING TEST RESULTS

Channel \ d (inches)	24	12	6	3
40 (f_c=5.20GHz)	5576	149	87480	65944
44 (f_c=5.22GHz)	32	5307	63969	62852
48 (f_c=5.24GHz)	1	48	854	17332
52 (f_c=5.26GHz)	0	2	14	45
56 (f_c=5.28GHz)	0	0	0	0

TABLE II

OUT-OF-BAND EMISSION TEST RESULTS

D. Single-interface vs. Multi-interface Secondary Devices

One of the design issues of a secondary device is to decide how many wireless interfaces should be built into a SU. In other words, we want to analyze if it is worth having a separate and independent sensing interface in addition to the communication interface. Here we investigate the tradeoffs between single-interface and double-interface architectures.

1) Single-interface Architecture: The single-interface architecture is beneficial in that there is less in-network interference caused by in-band jamming and out-of-band emission. Since data transmission and sensing cannot take place at the same time [11], in-network interference is caused only by neighboring SUs, which are not likely due to their mobility and distance. On the other hand, the single-interface design introduces frequent interruptions to data transmission due to sensing. The channel switching reconfiguration delay required for out-of-band sensing induces an additional delay before data transmission can be resumed (e.g., in Atheros, it takes 5-6ms to reconfigure the operational frequency which requires the hardware to be reset).

2) Double-interface Architecture: In case there are more than one interface installed in a SU, one interface can be configured as a dedicated sensor. Because the sensor and another interface (a transceiver) operate independently, no unnecessary interruption occurs to data transmission by sensing. It is, however, recommended that in-band sensing is performed by the transceiver. It is because the transceiver could overhear in-band secondary packets as well as in-band PU signals all the time. The major drawback of this approach comes from the potential in-network interference between interfaces in the same SU. There are two solutions to mitigate the problem: (i) regulate the maximum transmission power level from a transceiver, or (ii) put two interfaces as far as possible from each other. The latter, however, may not be suitable for compact-sized SUs. In either case, the level of OOB emission may depend on the vendor of the card [12].

V. CONCLUSION

We have taken an experimental approach to implementation of a spectrum sensor in CR networks. Despite the certain limitations with a commercial wireless device, key ideas of spectrum sensing were demonstrated successfully with our sensor prototype. The guidelines developed in this paper can facilitate building testbeds as well as developing CR sensors.

The next step would be to equip a SU with this sensor and transceiver interfaces, and show the efficiency of the prototype in utilizing the spectrum opportunities.

REFERENCES

[1] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 23, no. 2, pp. 201.220, February 2005.

[2] H. Harada, "Software Defined Radio Prototype Toward Cognitive Radio Communication Systems," *in Proc. IEEE DySPAN 2005*, pp. 539-547, November 2005.

[3] S.M. Mishra, D. Cabric, C. Chang, D. Willkomm, B. van Schewick, A. Wolisz, and R.W. Brodersen, "A Real Time Cognitive Radio Testbed for Physical and Link Layer Experiments," *in Proc. IEEE DySPAN 2005*, pp. 562-567, November 2005.

[4] R.J. DeGroot, D.P. Gurney, K. Hutchinson, M.L. Johnson, S. Kuffner, A. Schooler, S.D. Silk, and E. Visotsky, "A Cognitive-Enabled Experimental System," *in Proc. IEEE DySPAN 2005*, pp. 556-561, November 2005.

[5] C. Doerr, M. Neufeld, J. Fifield, T. Weingart, D. C. Sicker, and D. Grunwald, "MultiMAC - An Adaptive MAC Framework for Dynamic Radio Networking," *in Proc. IEEE DySPAN 2005*, pp. 548-555, November 2005.

[6] IEEE 802.22 Working Group on Wireless Regional Area Networks, http://www.ieee802.org/22/.

[7] C. Cordeiro, K. Challapali, and M. Ghosh, "Cognitive PHY and MAC Layers for Dynamic Spectrum Access and Sharing of TV Bands," *First International Workshop on Technology and Policy for Accessing Spectrum (TAPAS)*, August 2006.

[8] I. F. Akyildiz, W.-Y. Lee, M. C. Vuran, and S. Mohanty, "NeXt generation/dynamic spectrum access/cognitive radio wireless networks: A survey," *Computer Networks Journal (Elsevier)*, Vol. 50, pp. 2127-2159, September 2006.

[9] *MadWifi*, http://www.madwifi.org/.

[10] J. Bardwell, "Converting Signal Strength Percentage to dBm Values,", *WildPackets, Inc.*, November 2002.

[11] S. Shankar, C. Cordeiro and K. Challapali, "Spectrum agile radios: utilization and sensing architectures," *in Proc. IEEE DySPAN 2005*, pp. 160-169, November 2005.

[12] J. Robinson, K. Papagiannaki, C. Diot, X. Guo, and L. Krishnamurthy, "Experimenting with a Multi-Radio Mesh Networking Testbed," *1st workshop on Wireless Network Measurements (WiNMee)*, April 2005.