Experimental Approach: Two-stage Spectrum Sensing Using GNU Radio and USRP to Detect Primary User's Signal*

[Extended Abstract][†]

Yanxiao Zhao
South Dakota School of Mines
and Technology
South Dakota, USA
yanx-
iao.zhao@sdsmt.edu

Guodong Wang
South Dakota School of Mines
and Technology
South Dakota, USA
guodong.wang@sdsmt.edu

Jems Pradhan
South Dakota School of Mines
and Technology
South Dakota, USA
jems.prad-
han@mines.sdsmt.edu

Jun Huang
Chongqing University of Posts
and Telecommunications
China
jhuang@cqupt.edu.cn

ABSTRACT

Spectrum sensing plays a critical role in improving spectrum utilization for cognitive radio networks. The majority of existing sensing approaches aim to detect the existence of a signal on a busy channel without differentiating whether a signal originates from a primary user or not. In this paper, we attempt to solve this challenge by an experimental approach using GNU radio and Universal Software Radio Peripheral (USRP) board. A two-stage sensing strategy is proposed to detect channel states. The first stage detects whether a channel is busy or idle by observing both the energy level and bandwidth. Once the channel is busy, we further determine the channel is occupied by a Primary User (PU) and an Secondary User (SU). From experiments, we observe that a receiver cannot successfully receive a signal if it implements different demodulation schemes with a transmitter. For example, a Binary Phase Shift Keying (BPSK) demodulator cannot detect a Quadrature Phase Shift Keying (QPSK) signal transmitted by a transmitter. Motivated

by this observation, we propose that at the second stage, PUs and SUs are negotiated to conduct different modulations. Then SUs are equipped with two demodulators that will be able to demodulate both the PUs signal and the SUs signal. Given that SU and PU perform distinct modulations, once the PU comes to its licensed channel, the SU communicating on that channel will recognize it and withdraw from the channel immediately. Extensive experiments using GNU radio and USRP boards are carried out under various scenarios to evaluate the effectiveness of the proposed approach.

CCS Concepts

•Computer systems organization → Embedded systems; Redundancy; Robotics; •Networks → Network reliability;

Keywords

Spectrum sensing, Experimental approach, GNU radio, USRP board.

* (Produces the permission block, and copyright information). For use with SIG-ALTERNATE.CLS. Supported by ACM.

[†]A full version of this paper is available as *Author's Guide to Preparing ACM SIG Proceedings Using L^AT_EX2_ε and BibTeX* at www.acm.org/eaddress.htm

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for components of this work owned by others than ACM must be honored. Abstracting with credit is permitted. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee. Request permissions from Permissions@acm.org.

SAC 2016, April 04-08, 2016, Pisa, Italy

©2016 ACM. ISBN 978-1-4503-3739-7/16/04...\$15.00

DOI: <http://dx.doi.org/10.1145/2851613.2851824>

1. INTRODUCTION

Cognitive Radio Network (CRN) is commonly recognized as a promising technology innovation to relieve the spectrum scarcity for the future wireless networks. A typical wireless CRN is composed of two types of users: *primary users* (PUs) and *secondary users* (SUs). To implement CRN technology successfully, spectrum sensing plays a critical role, in which SUs, i.e., unlicensed users, are allowed to opportunistically share channels with PUs, i.e., licensed users, as long as SUs cause no destructive interference on PUs.

Spectrum sensing has been attracting a great attention and a considerable number of papers can be found in the litera-

ture. The majority of existing spectrum sensing approaches focus on theoretical analysis with an objective to detect the existence of a signal on a channel. Two states of a channel: *idle* or *busy* are commonly adopted. That is, a channel is determined idle once no signals are detected, otherwise the channel is sensed busy. From this hypothesis, any captured signal is identified as a PU's signal and the SU that conducts sensing will not access the channel. To accurately reflect the channel status, it is essential to distinguish whether a busy channel is being used by a PU or an SU. We proposed a three-state channel model in [9], in which a channel is divided into three states: H_0 (idle), H_1 (occupied by a PU) and H_2 (occupied by an SU). From this three-state model, it is a great challenge how to differentiate H_1 from H_2 when a channel is occupied.

In this paper, we are motivated to solve the above mentioned challenge, i.e, how to detect whether a busy channel is being used by a PU or an SU. We primarily focus on experimental investigation of spectrum sensing using a GNU Radio and Universal Software Radio Peripherals (USRP). A few papers can be found that carry out spectrum sensing using GNU radio and USRP boards [3, 5, 8]. [2] studies spectrum sensing using the energy detection approach and it successfully detects a signal at 890.5 MHz and distinguishes it from the unwanted signal with very low energy at same frequency. [3] performs spectrum sensing using the GNU Radio and USRP and it performs spectrum sensing using the COV (Covariance) and MME(Maximum to Minimum Eigen Value Method). The vulnerable effects of unwanted signal uncertainty in energy detection is mentioned. In our previous work [8],[7], an approach termed Energy and Bandwidth Spectrum Sensing (EBSS), in which both the energy level and bandwidth of the received signal are taken into account. In the above-mentioned papers, the objective is to detect the two states of the channel: idle and busy. They all fail to further determine whether a PU or an SU is occupying the channel once it is busy.

In our paper, an experimental approach is proposed which is capable of detecting whether a busy channel is being occupied by a PU or an SU. We have conducted extensive experiments using GNU radio and USRP boards and find an intriguing observation. That is, a receiver cannot successfully receive a signal if it implements a mismatching demodulation scheme with its transmitter. For example, a Binary Phase Shift Keying (BPSK) demodulator is not able to detect a transmitted Quadrature Phase Shift Keying (QPSK) signal. Motivated by this observation, we propose that PUs and SUs are negotiated to conduct different modulations. Then SUs are equipped with two demodulators that correspond to the modulations of PU and SU signals, respectively. As a result, SUs can demodulate both the PUs and SUs signals and easily make a decision on whether the channel is being used by a PU or a SU. Furthermore, when an SU is operating on a channel and the PU returns, the SU will recognize the PU signal and leave the channel immediately.

In addition, theoretical analysis is performed and will provide foundation of the proposed approach. Extensive experiments using GNU radio and USRP boards are carried out under various scenarios to evaluate the effectiveness of the proposed approach.

The rest of the paper is organized as follows. In Section 2, the proposed Energy, Bandwidth and Modulation Spectrum Sensing (EBMSS) technology is proposed. In Section 3, theoretical analysis is derived. Experimental results are presented in Section 4 and conclusions are drawn in Section 5.

2. PROPOSED ENERGY, BANDWIDTH AND MODULATION SENSING APPROACH

To effectively distinguish a channel state from the above-mentioned three states: H_0 (idle), H_1 (occupied by a PU) and H_2 (occupied by an SU), we propose a two-stage detection procedure. This approach is termed as Energy, Bandwidth and Modulation Spectrum Sensing which considers several factors including energy, bandwidth and modulation. In the first stage, an improved energy detection termed Energy and Bandwidth Spectrum Sensing (EBSS) is utilized [8],[7]. Extensive experiments are conducted in a lab environment and they demonstrate that the bandwidth of unwanted signal is usually narrow and around 10KHz. From this observation, we improve the accuracy of the energy detection by factoring an additional parameter, i.e., bandwidth. That is, both the energy level and bandwidth of the received signal are taken into account while making a decision on a channel's state. Specifically, a channel is interpreted busy (H_1 or H_2) [9] when two conditions hold simultaneously: 1) the received energy amplitude exceeds the energy threshold and 2) the bandwidth of the received signal is wider than the bandwidth threshold. Otherwise the channel is sensed as idle (H_0). Mathematically, the first-stage sensing results can be represented as:

$$(r > \lambda_E) \text{ AND } (b > \lambda_B) = \begin{cases} \text{False,} & \text{if } H_0 \\ \text{True,} & \text{if } H_1 \text{ or } H_2 \end{cases} \quad (1)$$

where r is the received energy amplitude at an SU; λ_E is the pre-defined energy threshold; b is the bandwidth of the received signal; λ_B is the pre-defined bandwidth threshold; "AND" represents a logic operation.

However, when the channel is considered occupied (H_1 or H_2), it is not clear whether the PU or an SU is using the channel. The received signal is further analyzed by the second stage based on a modulation scheme. The second stage will make a final decision of H_1 or H_2 .

In the second stage, experiments are conducted and we vary the modulation schemes implemented by the PU's and the SU's. In the following description, Tx and Rx denote "Transmitter" and "Receiver", respectively. An interesting finding is observed as below:

- Tx1 sends signals at frequency f_1 using modulation scheme 1. Rx1 is set up to receive signals at the same frequency, but adopting a mismatching demodulation scheme 2. It turns out Rx 1 receives a False signal and then stops receiving any signal. Then, Rx 1 is set up using a matching demodulation scheme 1, it is able to receive signals successfully. This demonstrates that a receiver cannot receive signals if the transmitter adopts a different modulation scheme at the same frequency. For example, a receiver with BPSK demodulator is not

capable of detecting signals sent from a transmitter with QPSK modulator, even when both transmitter and receiver are operating at the same frequency.

Motivated by the above observation, a novel approach is proposed at the second stage. First, PUs and SUs are assumed operating different modulation schemes. In this paper, we make an assumption that PU transmitters perform QPSK while SU transmitters adopt BPSK. Each SU is equipped with two demodulators that are able to detect BPSK and QPSK separately. Therefore, when a channel is busy, either occupied by a PU or an SU, the SU that performs sensing simply observe which demodulator receives signals successfully. For example, if the BPSK demodulator receives signal successfully, this implies the channel is being used by an SU, i.e., channel state is H_2 . If the QPSK demodulator succeeds in detecting signals, we can perceive that the channel is being occupied by a PU, i.e., channel state is H_1 .

3. MODULATION IN EBMSS

In this section, we will mathematically prove the effectiveness of our proposed approach. The generation of BPSK and QPSK signals are introduced first, then we will verify that a QPSK signal can not be correctly demodulated by a BPSK demodulator, and vice versa.

3.1 BPSK and QPSK Signal

BPSK uses individual bits to switch the phase of the carrier signal with constant amplitude between π radians or 180 degrees apart. The modulator switches the phases to one of the two possible values, 0 or 180 degrees, during each bit interval. The modulator output can be mathematically represented by Eq. (2):

$$S_{BPSK}(t) = m(t)\cos(2\pi f_c t + \theta), \quad (2)$$

where $m(t)$ is the bipolar baseband signal, f_c is the carrier frequency and θ is the phase of the unmodulated carrier.

Figure 1: Block diagram of QPSK modulation

Different from BPSK, the block diagram of a QPSK generator is depicted in Fig. 1. QPSK uses two bits to represent each symbol which might take one of the four values 00,01,10 or 11 and has a bandwidth efficiency twice that of BPSK. The phase of the carrier takes one of the four possible equally spaced values, such as 0, $\pi/2$, π and $3\pi/2$, where each value of phase corresponds to a unique pair of message bits. Ideally, the phases are 90 degrees apart. The QPSK signal for

these set of symbol can be mathematically represented by Eq. (3):

$$S_{QPSK}(t) = A_c m_I(t)\cos(2\pi f_c t) + A_c m_Q(t)\sin(2\pi f_c t), \quad (3)$$

where, A_c is the carrier amplitude, $m_I(t)$ and $m_Q(t)$ are the demultiplexed data stream of message signal $m(t)$ as shown in Figure 1.

3.2 BPSK Demodulator fails to demodulate QPSK Signal

In this subsection, we will verify that a QPSK signal cannot be demodulated by a BPSK demodulator. Before giving the verification, we will first present how the BPSK signal is demodulated by the BPSK receiver.

BPSK implements coherent or synchronous detection which requires information of phase and the frequency of the carrier at the receiver. The received BPSK signal which is represented by Eq. (2) should be demodulated to extract the message signal $m(t)$. BPSK demodulation with carrier recover circuit is represented by the block diagram shown in Fig. 2.

Figure 2: Block diagram of BPSK carrier recovery circuit

As shown in Fig. 2, the received signal is first passed through the Square Law device to generate a dc signal and an amplitude varying sinusoid of twice the carrier frequency represented by Eq. (4).

$$S_{BPSK}(t) = m(t)^2 \left[\frac{1}{2} + \frac{\cos 2(\omega_c t + \theta)}{2} \right] \quad (4)$$

The signal represented by Eq. (4) is then passed through the Bandpass Filter whose center frequency is tuned to $2\omega_c$. Therefore, the output of the Bandpass filter is $\cos 2(\omega_c t + \theta)$. This signal is passed through the Frequency Divider to recreate the waveform $\cos(\omega_c t + \theta)$. The received signal is then multiplied with the incoming signal. The output of the multiplier is represented by Eq. (5).

$$S_{BPSK}(t) = m(t)\cos^2(\omega_c t + \theta) = m(t) \left[\frac{1}{2} + \frac{\cos 2(\omega_c t + \theta)}{2} \right] \quad (5)$$

The signal represented by Eq. (5) is then passed through the Integrate and Dump Circuit which forms the Low Pass Filter Segment of BPSK Detector. This removes the higher

frequency and leaves the desired message signal only. A bit synchronizer is used to facilitate sampling of the integrator output precisely at the end of each bit period. Depending upon whether the integrator output is above or below a certain threshold, the decision circuit decides that the received signal is binary 1 or 0.

However, if the QPSK signal passes through the BPSK demodulator, the situation will be totally different. Eq. (3) represents the QPSK signal. When this signal passes through the BPSK demodulator it first passes through the Square Law device as shown in Fig. 2. Then the signal can be depicted by Eq. (6)

$$S_{QPSK}(t) = A_c^2[\cos^2(2\pi f_c t)m_I^2(t)] - 2A_c\cos(2\pi f_c t)m_I(t) \times A_c\sin(2\pi f_c t)m_Q(t) + A_c^2[\sin^2(2\pi f_c t)m_Q^2(t)] \quad (6)$$

The signal represented by Eq. (6) is then passed through the Bandpass Filter with center frequency $2\omega_c$, so the output of the Bandpass Filter is $\cos 2(\omega_c t + \theta)$. When this signal passes through the frequency divider, $\cos(\omega_c t)$ is generated. The received signal is then multiplied with the incoming signal. The output of the multiplier is represented by Eq. (7).

$$S(t) = A_c m_I(t) \cos^2(\omega_c t) = A_c m_I(t) \left[\frac{1}{2} + \frac{\cos 2(\omega_c t)}{2} \right] \quad (7)$$

When the signal represented by Eq. (7) passes through the Low Pass Filter only $m_I(t)$ is regenerated which is not the desired message signal.

Based on the mathematical equations, we conclude that if a QPSK signal demodulated by a BPSK demodulator, the receiver will not be able to obtain the appropriate signal as the phase of the incoming signals do not match with that of the receiver. The result is the same if the demodulator is QPSK and the received signal is BPSK as two bits are transmitted in a single modulation symbol in QPSK while BPSK uses one bit. So, the demodulator will not be able to recognize the incoming BPSK signal. Therefore, the transmitter and receiver must use the same modulation technique for a successful communication.

The above analysis verifies the feasibility of our proposed approach, that is, equipping SUs with two different demodulators for BPSK and QPSK. One of them is used to demodulate the PU signal (QPSK) and the other for SU signal (BPSK). Once a channel is busy, the SU that performs sensing is able to further detect the signal is from a PU or an SU.

4. EXPERIMENTAL RESULTS

In this section, we conduct extensive experiments in a lab environment. Signals are transmitted and received using several USRP N200 boards which serve as transmitters or receivers. The set up of experiments is described first, followed by various experiments and results.

4.1 Experiment Setup

The experiments are performed using the USRP N200 boards and GNU Radio software. GNU Radio is a free and open source software that includes various signal processing blocks

to implement software radios. Software radio technology enables many waveforms to be processed by a single hardware platform by simply changing its programming [6]. USRP board is a hardware platform for software radios [4][1]. The experiment is set up in a lab environment as shown in Fig. 3.

Figure 3: Experimental setup using USRP boards and GNU radio in a lab environment

4.2 Experiments and Results

We evaluate the transmission with varied frequencies, modulations and demodulation schemes. For signals of PU and SU, QPSK and BPSK are assumed, respectively. We observe signals transmitted and received in the form of packets. There are different parameters in the experimental results where “True” represents the successful reception of transmitted packets and “False” represents the failure to receive the transmitted packets. Other parameters keep the count of the transmitted packets, received packet and the acknowledged packets.

In the first experiment, we set up an SU transmitter and an SU receiver at the same frequency with matching modulation and demodulation schemes. In the first scenario, one signal is transmitted at frequency 2.47 GHz adopting BPSK modulation. A SU receiver is set up at the same frequency to receive the signal using BPSK demodulator. The received signal in the form of packets are shown in Fig. 4. It shows successful receptions of all the transmitted packets. From

pk = True	pktno = 467	n_rcvd = 112	n_right = 100
pk = True	pktno = 468	n_rcvd = 113	n_right = 101
pk = True	pktno = 469	n_rcvd = 114	n_right = 102
pk = True	pktno = 470	n_rcvd = 115	n_right = 103
pk = True	pktno = 471	n_rcvd = 116	n_right = 104
pk = True	pktno = 472	n_rcvd = 117	n_right = 105
pk = True	pktno = 473	n_rcvd = 118	n_right = 106
pk = True	pktno = 474	n_rcvd = 119	n_right = 107
pk = True	pktno = 475	n_rcvd = 120	n_right = 108
pk = True	pktno = 476	n_rcvd = 121	n_right = 109
pk = True	pktno = 477	n_rcvd = 122	n_right = 110
pk = True	pktno = 478	n_rcvd = 123	n_right = 111
pk = True	pktno = 479	n_rcvd = 124	n_right = 112
pk = True	pktno = 480	n_rcvd = 125	n_right = 113
pk = True	pktno = 481	n_rcvd = 126	n_right = 114
pk = True	pktno = 482	n_rcvd = 127	n_right = 115
pk = True	pktno = 483	n_rcvd = 128	n_right = 116
pk = True	pktno = 484	n_rcvd = 129	n_right = 117
pk = True	pktno = 485	n_rcvd = 130	n_right = 118
pk = True	pktno = 486	n_rcvd = 131	n_right = 119
pk = True	pktno = 487	n_rcvd = 132	n_right = 120
pk = True	pktno = 488	n_rcvd = 133	n_right = 121
pk = True	pktno = 489	n_rcvd = 134	n_right = 122

Figure 4: A SU receiver (USRP N200) receiving BPSK signals at 2.47 GHz

the above experiment, we conclude that successful transmissions are achieved if both transmitter and receiver communicate at the same frequency with matching modulation and demodulation schemes.

In the second experiment, we investigate simultaneous communications between a PU and an SU at two close frequencies and observe the interference to each other. At first, a signal is transmitted at 2.47 GHz by a SU transmitter using BPSK modulation, and the transmitted packets are successfully recovered at the SU receiver which is programmed to receive 2.47 GHz signal using BPSK demodulation. While the successful transmission is going on, another PU transmitter at 2.47001 GHz which uses QPSK modulation, is turned on. The communication results are shown in Fig. 5. All transmitted packets at the receiver of 2.47 GHz are successfully recovered. This experiment suggests that there is no interference if two signals are transmitted using different modulations even when their frequencies are considered close to each other. Therefore, if PUs and SUs operate using different modulations, there will be no interference between them even when the frequencies are extremely close to each other.

```
ok = True pktno = 227 n_rcvd = 125 n_right = 119
ok = True pktno = 228 n_rcvd = 126 n_right = 120
ok = True pktno = 229 n_rcvd = 127 n_right = 121
ok = True pktno = 230 n_rcvd = 128 n_right = 122
ok = True pktno = 231 n_rcvd = 129 n_right = 123
ok = True pktno = 232 n_rcvd = 130 n_right = 124
ok = True pktno = 233 n_rcvd = 131 n_right = 125
ok = True pktno = 234 n_rcvd = 132 n_right = 126
ok = True pktno = 235 n_rcvd = 133 n_right = 127
ok = True pktno = 236 n_rcvd = 134 n_right = 128
ok = True pktno = 237 n_rcvd = 135 n_right = 129
ok = True pktno = 238 n_rcvd = 136 n_right = 130
ok = True pktno = 239 n_rcvd = 137 n_right = 131
ok = True pktno = 240 n_rcvd = 138 n_right = 132
ok = True pktno = 241 n_rcvd = 139 n_right = 133
ok = True pktno = 242 n_rcvd = 140 n_right = 134
ok = True pktno = 243 n_rcvd = 141 n_right = 135
ok = True pktno = 244 n_rcvd = 142 n_right = 136
ok = True pktno = 245 n_rcvd = 143 n_right = 137
ok = True pktno = 246 n_rcvd = 144 n_right = 138
ok = True pktno = 247 n_rcvd = 145 n_right = 139
ok = True pktno = 248 n_rcvd = 146 n_right = 140
ok = True pktno = 249 n_rcvd = 147 n_right = 141
ok = True pktno = 250 n_rcvd = 148 n_right = 142
ok = True pktno = 251 n_rcvd = 149 n_right = 143
ok = True pktno = 252 n_rcvd = 150 n_right = 144
ok = True pktno = 253 n_rcvd = 151 n_right = 145
```

Figure 5: SU receiving signals at 2.47 GHz modulated using BPSK when PU sending signals at 2.47001 GHz using QPSK

In the next experiment, we set up two SU transmitters and one SU receiver, all of which communicate at the same frequency. We attempt to evaluate interferences among them. Initially, when we set up one SU transmitter operating at 2.45 GHz using BPSK modulation and a SU receiver which also works at 2.45 GHz using BPSK demodulator, the communication is successful. Then, we turn on another SU transmitter at the same frequency 2.45 GHz using the same modulation scheme BPSK, a great amount of interferences are observed, as shown in Fig. 6. This experiment demonstrates that if multiple SUs are operating at the same frequency, severe interference are generated. Therefore, SUs have to be appropriately coordinated to operate on a certain frequency.

We further extend our experiment in which two transmitters (one is for PU and another one is for SU) as well as one SU receiver operate at the same frequency. The PU transmitter and the SU transmitter adopt different modulations schemes, i.e., QPSK and BPSK. The SU receiver

```
ok = False pktno = 279 n_rcvd = 58 n_right = 0
ok = False pktno = 280 n_rcvd = 59 n_right = 0
ok = False pktno = 281 n_rcvd = 60 n_right = 0
ok = False pktno = 283 n_rcvd = 61 n_right = 0
ok = False pktno = 285 n_rcvd = 62 n_right = 0
ok = False pktno = 287 n_rcvd = 63 n_right = 0
ok = False pktno = 293 n_rcvd = 64 n_right = 0
ok = False pktno = 296 n_rcvd = 65 n_right = 0
ok = True pktno = 297 n_rcvd = 66 n_right = 1
ok = False pktno = 298 n_rcvd = 67 n_right = 1
ok = False pktno = 299 n_rcvd = 68 n_right = 1
ok = False pktno = 300 n_rcvd = 69 n_right = 1
ok = False pktno = 302 n_rcvd = 70 n_right = 1
ok = False pktno = 303 n_rcvd = 71 n_right = 1
ok = False pktno = 309 n_rcvd = 72 n_right = 1
ok = False pktno = 311 n_rcvd = 73 n_right = 1
ok = False pktno = 314 n_rcvd = 74 n_right = 1
ok = False pktno = 317 n_rcvd = 75 n_right = 1
ok = False pktno = 319 n_rcvd = 76 n_right = 1
ok = True pktno = 320 n_rcvd = 77 n_right = 2
ok = True pktno = 321 n_rcvd = 78 n_right = 3
ok = False pktno = 322 n_rcvd = 79 n_right = 3
ok = False pktno = 323 n_rcvd = 80 n_right = 3
ok = False pktno = 463 n_rcvd = 81 n_right = 3
ok = False pktno = 326 n_rcvd = 82 n_right = 3
ok = False pktno = 331 n_rcvd = 83 n_right = 3
ok = False pktno = 336 n_rcvd = 84 n_right = 3
```

Figure 6: An SU receiver receiving BPSK signals at 2.45 GHz when there is another SU transmitter at 2.45 GHz using BPSK

adopts BPSK demodulation scheme. At first, one SU transmitter send signals at 2.47 GHz using BPSK modulation. All the data packets transmitted are received successfully by the SU receiver programmed at 2.47 GHz using BPSK demodulation. Afterwards, we turn off the SU transmitter, once we turn on the PU transmitter at the same frequency, i.e, 2.47 GHz, which adopts QPSK. The results are posted in Fig. 7, from which we observe that the SU receiver gets a FALSE packet and the communication automatically terminates. This experiment indicates that the receiver will

```
ok = True pktno = 140 n_rcvd = 73 n_right = 73
ok = True pktno = 147 n_rcvd = 74 n_right = 74
ok = True pktno = 148 n_rcvd = 75 n_right = 75
ok = True pktno = 149 n_rcvd = 76 n_right = 76
ok = True pktno = 150 n_rcvd = 77 n_right = 77
ok = True pktno = 151 n_rcvd = 78 n_right = 78
ok = True pktno = 152 n_rcvd = 79 n_right = 79
ok = True pktno = 153 n_rcvd = 80 n_right = 80
ok = True pktno = 154 n_rcvd = 81 n_right = 81
ok = True pktno = 155 n_rcvd = 82 n_right = 82
ok = True pktno = 156 n_rcvd = 83 n_right = 83
ok = True pktno = 157 n_rcvd = 84 n_right = 84
ok = True pktno = 158 n_rcvd = 85 n_right = 85
ok = True pktno = 159 n_rcvd = 86 n_right = 86
ok = True pktno = 160 n_rcvd = 87 n_right = 87
ok = True pktno = 161 n_rcvd = 88 n_right = 88
ok = True pktno = 162 n_rcvd = 89 n_right = 89
ok = True pktno = 163 n_rcvd = 90 n_right = 90
ok = True pktno = 164 n_rcvd = 91 n_right = 91
ok = True pktno = 165 n_rcvd = 92 n_right = 92
ok = True pktno = 166 n_rcvd = 93 n_right = 93
ok = True pktno = 167 n_rcvd = 94 n_right = 94
ok = True pktno = 168 n_rcvd = 95 n_right = 95
ok = True pktno = 169 n_rcvd = 96 n_right = 96
ok = True pktno = 170 n_rcvd = 97 n_right = 97
ok = True pktno = 171 n_rcvd = 98 n_right = 98
ok = True pktno = 172 n_rcvd = 99 n_right = 99
ok = True pktno = 173 n_rcvd = 100 n_right = 100
ok = True pktno = 174 n_rcvd = 101 n_right = 101
ok = False pktno = 175 n_rcvd = 102 n_right = 101
ok = False pktno = 176 n_rcvd = 103 n_right = 101
SD Error!
An unexpected exception was caught in a task loop
The task-loop will now exit, things may not work.
```

Figure 7: USRP N200 receiving signals at 2.47 GHz modulated using BPSK when there is another transmitter at 2.47 GHz using QPSK

not be able to receive the signals, if the modulation and demodulation schemes do not match. So, whenever a receiver designed to receive a signal using QPSK receives a BPSK signal or vice versa, it goes into dilemma and cannot recover the packets.

Next, two receivers and one transmitter are involved. One pair of transmitter and receiver are viewed for a SU transmission. The second receiver serves as an PU. For SU's signal, it is transmitted at 2.49 GHz frequency using BPSK modulation. This signal is received by the SU receiver programmed to the same frequency using BPSK demodulator. Now, when the PU receiver is set up to receive signals at 2.49 GHz using QPSK demodulator, it fails to receive any

packets while the PU communication is continuing successfully. Fig. 8 shows the error at the receiver which is trying to receive signals at 2.49 GHz using QPSK. The same results are found when signals are transmitted and received using QPSK at 2.49 GHz. Once, again when we turn on another SU receiver designed to receive signals at 2.49 GHz using BPSK, it fails to receive any packets, without causing any interference to previous successful communication.

```

 UHD Warning:
 The hardware does not support the requested RX sample rate:
 Target sample rate: 0.100000 MSps
 Actual sample rate: 0.195312 MSps

 Symbol Rate: 50000.000000
 Requested sps: 2.000000
 Given sample rate: 195312.500000
 Actual sps for rate: 3.906250

 Requested sample rate: 100000.000000
 Actual sample rate: 300200.000000
 Warning: Failed to enable realtime scheduling.

 UHD Error:
 An unexpected exception was caught in a task loop.
 The task loop will now exit, things may not work.
 Error: Invalid argument

```

Figure 8: USRP N200 failing to receive signals at 2.49 GHz using QPSK when there is a transmitter at 2.49 GHz using BPSK

At last, we simulate a scenario that a pair of PUs are transmitting signal while an SU attempts to sense the presence of the PU signal. The PU pair are programmed to operate on QPSK modulation at 2.45 GHz and the PU receiver receives the signal using QPSK demodulation successfully. An SU receiver is setup to receive signals at 2.45 GHz using QPSK demodulation. Both the PU receiver and the SU receiver receives signals successfully at 2.45 GHz at the same time. The received signals at SU are shown in Fig. 9. This experiment suggests that an SU is capable of detecting the PU's signal without disturbing PU's communications. In this case, the SU determines that the channel is occupied by the PU and leave the channel immediately.

```

k = True pktno = 109 n_rcvd = 10 n_right = 10
k = True pktno = 110 n_rcvd = 11 n_right = 11
k = True pktno = 111 n_rcvd = 12 n_right = 12
k = True pktno = 112 n_rcvd = 13 n_right = 13
k = True pktno = 113 n_rcvd = 14 n_right = 14
k = True pktno = 114 n_rcvd = 15 n_right = 15
k = True pktno = 115 n_rcvd = 16 n_right = 16
k = True pktno = 116 n_rcvd = 17 n_right = 17
k = True pktno = 117 n_rcvd = 18 n_right = 18
k = True pktno = 118 n_rcvd = 19 n_right = 19
k = True pktno = 119 n_rcvd = 20 n_right = 20
k = True pktno = 120 n_rcvd = 21 n_right = 21
k = True pktno = 121 n_rcvd = 22 n_right = 22
k = True pktno = 122 n_rcvd = 23 n_right = 23
k = True pktno = 123 n_rcvd = 24 n_right = 24
k = True pktno = 124 n_rcvd = 25 n_right = 25
k = True pktno = 125 n_rcvd = 26 n_right = 26
k = True pktno = 126 n_rcvd = 27 n_right = 27
k = True pktno = 127 n_rcvd = 28 n_right = 28
k = True pktno = 128 n_rcvd = 29 n_right = 29
k = True pktno = 129 n_rcvd = 30 n_right = 30
k = True pktno = 130 n_rcvd = 31 n_right = 31
k = True pktno = 131 n_rcvd = 32 n_right = 32
k = True pktno = 132 n_rcvd = 33 n_right = 33
k = True pktno = 133 n_rcvd = 34 n_right = 34
k = True pktno = 134 n_rcvd = 35 n_right = 35
k = True pktno = 135 n_rcvd = 36 n_right = 36
k = True pktno = 136 n_rcvd = 37 n_right = 37

```

Figure 9: USRP N200 successfully receiving signals at 2.45GHz using QPSK when there is a PU transmitter receiver pair at 2.45 GHz using QPSK

We have performed extensive experiments for a wide number of frequency from 2.4 GHz-2.5 GHz and 4.9 GHz-5.85 GHz and all the results are similar. Overall, these experimental results verify the effectiveness of our approach, that is, the PU and SU implement different modulation techniques and SUs are equipped with two different modulators, so that it can detect if the received signal is PU signal or SU signal.

5. CONCLUSION AND FUTURE WORK

In this paper, we have investigated spectrum sensing from an experimental approach using GNU radio and USRP boards.

A two-stage sensing strategy is proposed to detect channel states based on the three-state channel model. The first stage detects whether a channel is busy or not by observing both the energy level and bandwidth. Once the channel is busy, we further determine the channel is occupied by a PU and an SU. Specifically, we have proposed that PUs and SUs are negotiated to operate with different modulations. Then we also propose that SUs are equipped with two demodulators that correspond to the modulations of PU and SU signals, respectively. Even though there is no such device which implements two demodulators the proposal is supported by the experimental results of Fig.9. In this way, an SU is able to detect whether a signal is from an SU or PU. Extensive experiments have been conducted and results verify the effectiveness of the proposed approach. These results verifies the possibility of SUs being built with two demodulators and is one of the possible future works.

Acknowledgment

The research of Yanxiao Zhao is supported in part by NSF grant ECCS-1310562.

6. REFERENCES

- [1] F. Ge, C. J. Chiang, Y. M. Gottlieb, and R. Chadha. Gnu radio-based digital communications: Computational analysis of a gmsk transceiver. In *Global Telecommunications Conference (GLOBECOM 2011)*, IEEE, pages 1–6.
- [2] M. KIM and J.-i. TAKADA. Development of spectrum sensing system with gnu radio and usrp to detect emergency radios. In *IEICE Technical Report*, 2009.
- [3] A. Mate, K.-H. Lee, and I.-T. Lu. Spectrum sensing based on time covariance matrix using gnu radio and usrp for cognitive radio. In *Systems, Applications and Technology Conference (LISAT)*, pages 1–6, 2011.
- [4] G. Radio. The gnu software radio. Available from World Wide Web: <https://gnuradio.org>, 2007.
- [5] A. Sapello, A. Sethi, C. Serban, C. J. Chiang, and K. Moeltner. A software defined radio modeling framework for enabling cognitive applications. *Analog Integrated Circuits and Signal Processing*, 78(3):543–556, 2014.
- [6] D. C. Tucker and G. A. Tagliarini. Prototyping with gnu radio and the usrp-where to begin. In *Southeastcon, 2009. SOUTHEASTCON'09. IEEE*, pages 50–54.
- [7] Y. Zhao, J. Pradhan, J. Huang, Y. Luo, and L. Pu. Joint energy-and-bandwidth spectrum sensing with gnu radio and usrp. *ACM SIGAPP Applied Computing Review*, 14(4):40–49, 2015.
- [8] Y. Zhao, J. Pradhan, J. Huang, and H. Sun. Experimental approach: energy-and-bandwidth spectrum sensing using gnu radio and usrp. In *Proceedings of the 2014 Conference on Research in Adaptive and Convergent Systems*, pages 174–179.
- [9] Y. Zhao, M. Song, C. Xin, and M. Wadhwa. Spectrum sensing based on three-state model to accomplish all-level fairness for co-existing multiple cognitive radio networks. In *INFOCOM, 2012 Proceedings IEEE*, pages 1782–1790.