Spectrum Sensing:
First Step Towards Cognitive Radio

Seth Myers

Mobile Computing EE 787

May 7, 2009

Introduction

The integration of wireless communications and computing power has enabled recent advances in software defined radio (SDR) such as the GNU Radio platform. The capability to use software to intelligently configure transmission parameters in response to perceived changes in the operating environment adaptive is giving further impetus to the development of ‘cognitive radio technology.’ Cognitive radio seeks to better utilize the electromagnetic ‘wifi’ spectrum, chiefly by sensing underutilized bandwidth and helping the various transmitting agents, typically mobile agents, to negotiate and most efficiently use such available bandwidth. Cognitive Radio is considered as one of the key candidates for fourth generation (4G) wireless technology [1]; the field of ‘cognitive radio’ was considered to have been launched with the 2000 thesis of J. Mittola [2]. Use of underutilized bandwidth requires a sensing of the traffic across the spectrum of available bandwidths, which will be the focus of this project.

Background

The author’s interest in this area stems in part from a consideration of the use of wireless communication technology in the ‘smart grid’ vision of the electric power system, in which two-way communication (and even distributed communication and processing) permeates the various devices on the electric power grid [3]-[5]. The use of distributed computing and communication challenges related to the electric power grid is discussed in [3], while [4] lays out the various issues related to the use of wireless communications in power systems, specifically the drawbacks of reliability and noisy electrical environments, counterbalanced by the possible benefits of cost and installation savings in laying down physically wired communication systems, distributed intelligence and system optimization, and emergency response capabilities during blackouts and load shedding events, among others.

The recent focus on cognitive radio technology, as in [1], as well as the advent of software defined radio such as gnu radio [6], has led to projects integrating gnu radio and cognitive technology such as from the Virginia Tech “Cognitive Wireless Technology” lab [7]-[8]. Over 100 articles on cognitive radios can be found with a search on IEEE Explore, with various investigations into sensing spectrum ‘holes’ (under-utilized bandwidth) [9], channel and transmission power assignment [10]-[11], and issues of PHY and MAC layer implementation[12], to mention just a very few such articles.

Project Topic: Spectrum Sensing

Project Goal

As the key first step to efficient utilization of available bandwidth is sensing the utilization of various bands in the bandwidth, the gnu radio function spectrum_sense.py (found in "gnuradio/gnuradio-examples/python/usrp/, and in the appendix) is used to sense spectrum in the IEEE 802.11 bandwidth range. This range consists specifically of the 11 sub-bands around the 2.4 GHz industrial, scientific and medical band, as laid out in IEEE 802.11a (2412 MHz to 2462 MHz in 5 MHz steps). The CSU wireless system provides wireless internet access to the campus as shown in Figure 1.

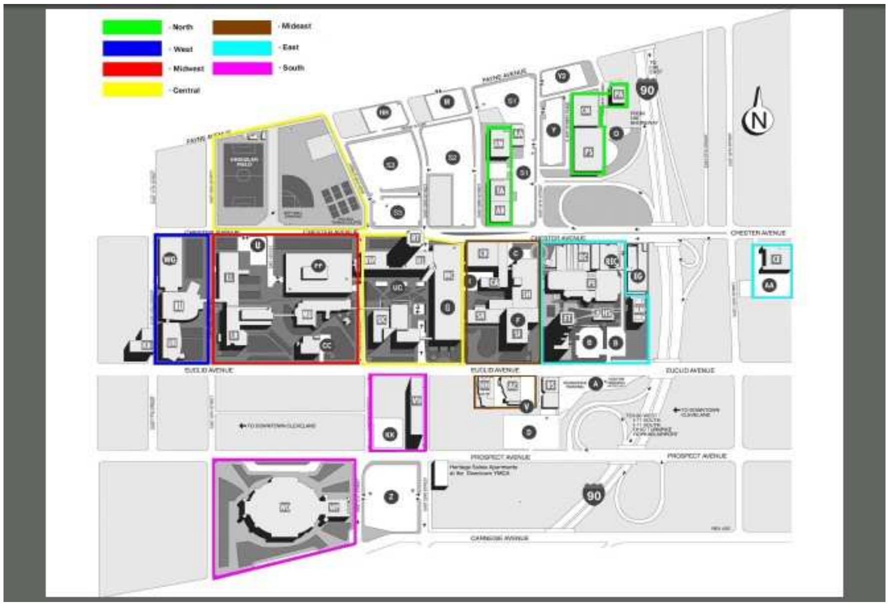

Figure 1: Cleveland State University Wireless Coverage Map

Each area or building receives coverage at the 2.4 GHz range, as defined by the 802.11 standards as the Industrial, Scientific and Medical" (ISM) band. This band, consisting of the 11 channels from 2.412 to 2.462 GHz, utilizes the three overlapping channels 1 (2.412GHz), 6 (2.437 GHz) and 11 (2.462 GHz) over which to offer internet service. Coverage may vary among the different channels at different points of the same floor, and the pattern may be alternated going from floor to floor in a building so as to minimize overlap and interference vertically as well as horizontally. IEEE standard 802.11b governs this type of coverage, as shown in Figure 2a.

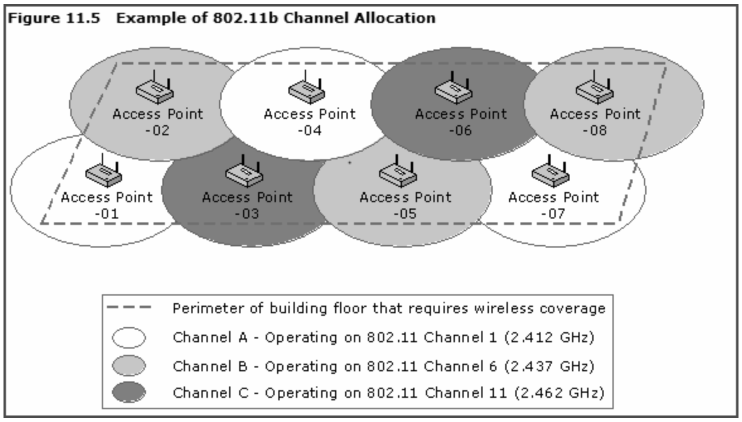

Figure 2a 802.11b In-Building Coverage (courtesy of http://technet.microsoft.com/)

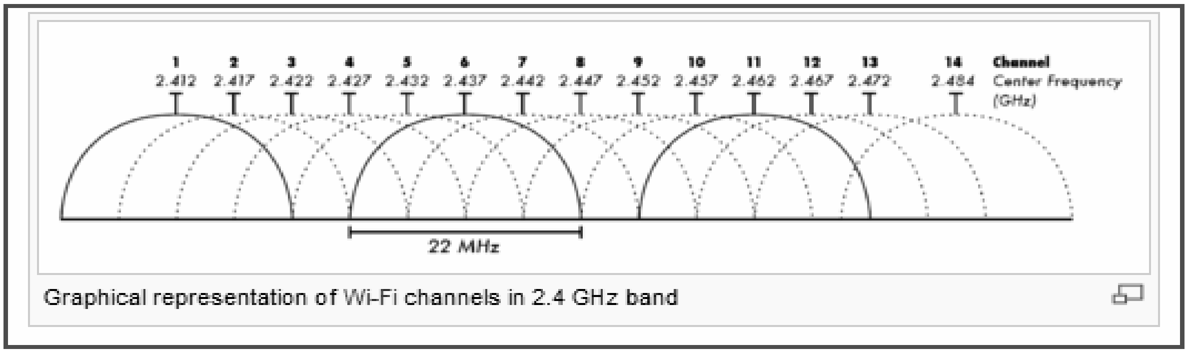

Figure 2b Channels 1,6,11 in WiFi 2.4 GHz Band (courtesy of Wikipedia)

This investigation involves measuring the strength of signal from various areas in the CSU coverage system, as well as to investigate the pattern of channel usage within a building.

The 2.4 – 2.4835 GHz frequency range represents one of the three bands of unlicensed radio spectrum, and accommodates any 802.11 system, as well as microwave ovens and Bluetooth devices. The other unlicensed spectra are the 902 – 928 MHz range, which is available for use by cordless phones, baby monitors and wireless LANs, and the 5.725 – 5.785 GHz range, which is presently unused.

Project Setup

The experimental setup involved use of GNU radio implemented on Ubuntu Linux residing theSunxVM Virtual Box running on a Windows based laptop computer. The universal software radio peripheral (USRP) device was used to physically implement signal reception, utilizing the the RFX2400 daughterboard for 2.4 GHz range reception, as described in Figure 3. 'Wireless Device A' represents the CSU transmission system at the various locations on campus, while 'Wireless Device B' represents the Software Defined Radio (SDR) + USRP reception system.

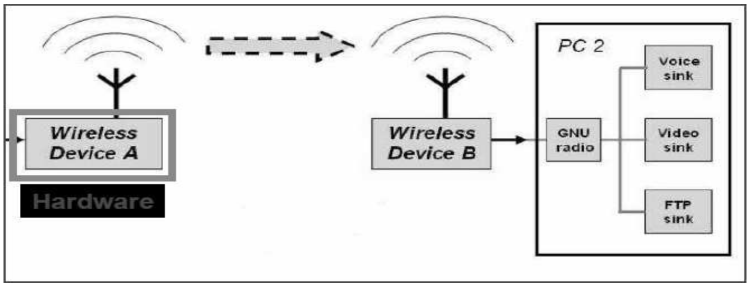

Figure 3 2.4 GHz Reception Setup

Results

Figure 4 shows the results of testing the setup with a microwave oven at home.

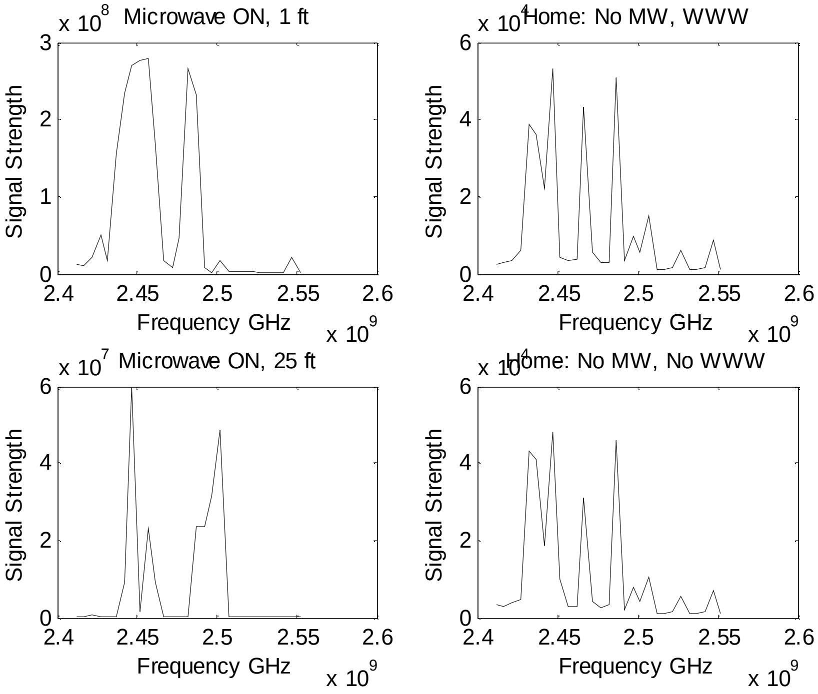

Figure 4: Microwave Oven Spectrum Usage; Ambient Environment

The top left results show microwave oven emissions measured 1 foot from the oven, while beneath it is the measurement 25 feet away, with about a 50% decrease in the strength of signal. The results on the right side of Figure 4 show the ambient environment with no microwave oven, in particular showing any interference due to the wireless network at my home; the bottom figure shows the ambient environment with my wireless router (Belkin 2.4 GHz, 802.11g) turned off (the scale for these results is x 10^4, considerably less than the magnitude of the microwave oven signal shown; the double peak on the “Microwave on” graphs are thus due solely to the microwave transmission, and not the ambient environment, as originally suspected).

Figure 5 shows the results of measurements taken in some different zones of the CSU coverage area, specifically the Business building in the red ‘Midwest’ zone and the Main Classroom and Rhodes Tower buildings in the yellow ‘Central’ zone.

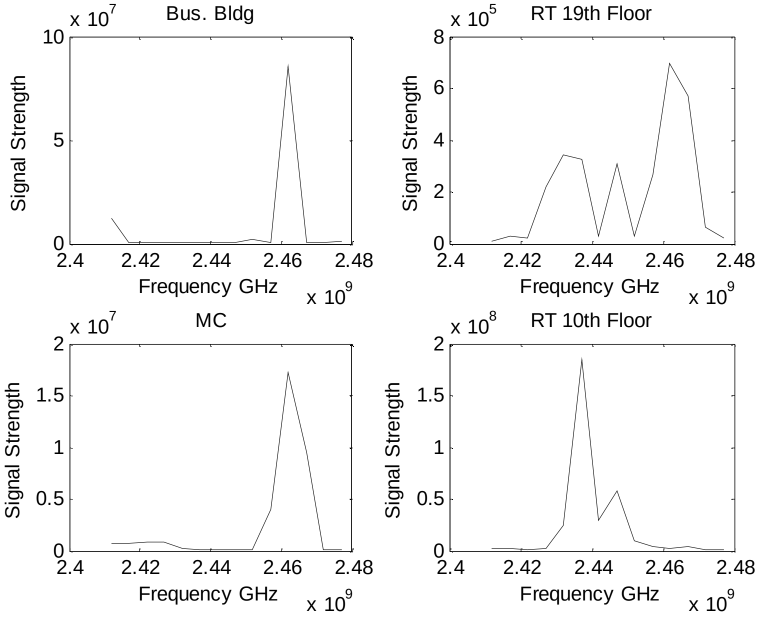

Figure 5 Signal Detection in Assorted CSU Zones

Utilization of Channel 11 (2.462GHz) is clearly observed in the measurements taken in the business building, Main Classroom (MC) and the 19th floor of Rhodes Tower, though no effort was made to detect channel usage in different parts of these buildings. The Rhodes Tower 10th floor signal appears to be Channel 6 (2.437 GHz). Some variation in strength of signal is observed between these various locations, but this is likely due to the particular locations the measurements were taken than due to signal strength due to any particular coverage zone.

The main focus of sensing spectrum usage involved measurements in the engineering building, Stillwell Hall. Figure 6a-c show the results on floors 1,2 and 3 in this building; floor 1 also has a western extension which houses a computer lab, so an extra measurement was made there.

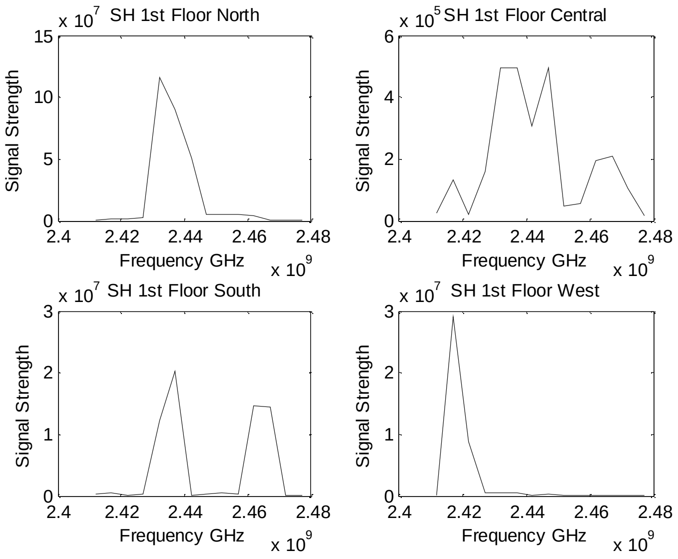

Figure 6a SH 1st Floor Coverage

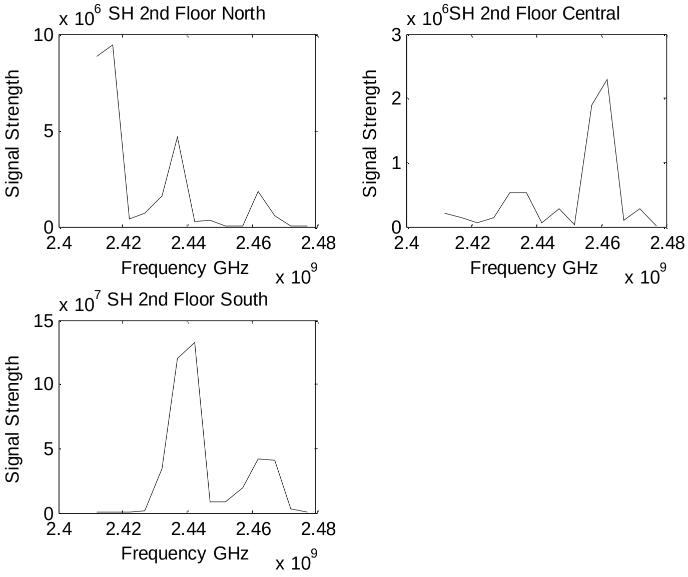

Figure 6b SH 2nd Floor Coverage

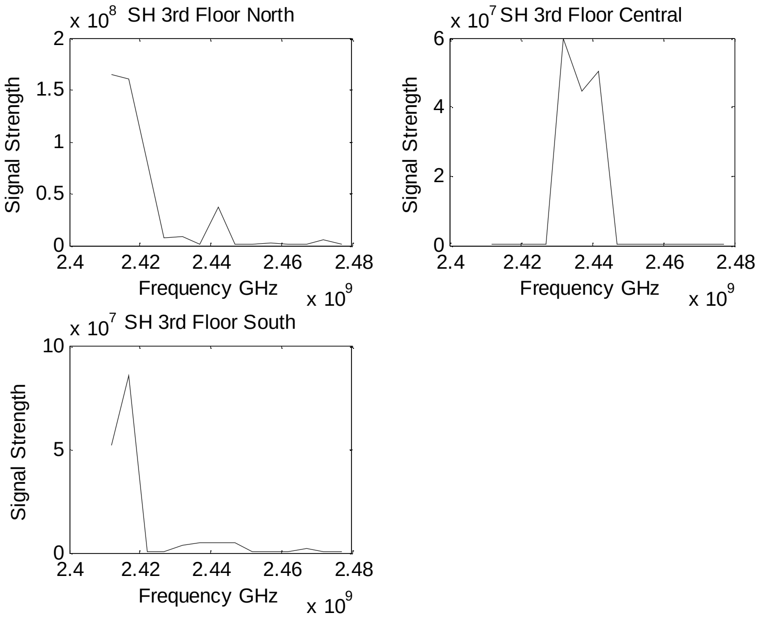

Figure 6c SH 3rd Floor Coverage

Floor 2 shows the best results as far as having a predominance of a different channel at each measurement point on the floor (North, South or Central), though detection of signals from other channels is clearly apparent. Some wireless channel snooping also revealed a mix of usage of channels 1,6 and 11 in SH 306.

Coverage at Rascal Pizza, out of the CSU coverage zone but equipped with its own wifi coverage, shows a usage of channel 11 in the following figure, though the sensing system would appear to be slightly miscalibrated as the peak appears to be more like at channel 10, 2.457 GHz. These results were made with sensing every 5 MHz, exactly at the expected channel frequencies, though it must be recalled that the 5 MHz increments are merely the center frequency for the particular channels, whereas the entire channel range involves a window of +/- 11 MHz from the center frequency.

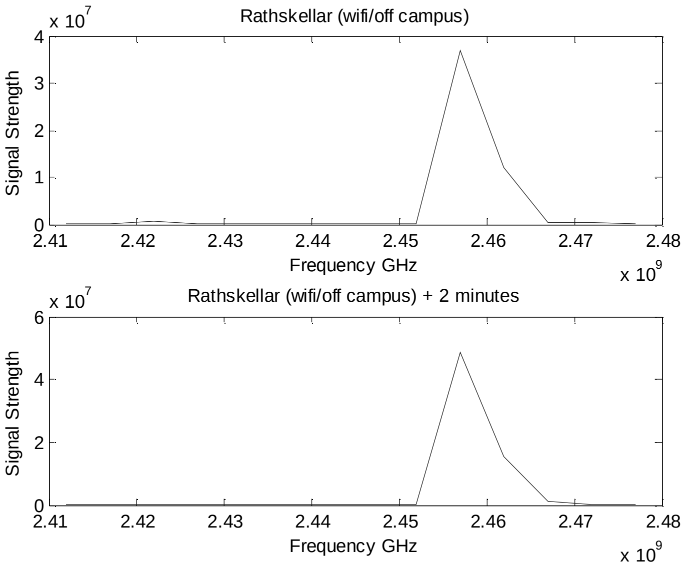

Figure 7 Spectrum Usage at Rathskellar/Rascalhouse WiFi Spot

Discussion

The results just shown demonstrate, as discussed above, the predominance of channels 1 (2.412 GHz), 6 (2.437 GHz) and 11 (2.462 GHz) in the CSU wifi coverage network. Strength of signal does not vary appreciably from zone to zone, but is more likely dependent on measurement position in the particular zone (open hallway vs. enclosed classroom, etc.). Results from the three floors of Stillwell Hall did not exactly exhibit an ideally expected floor-to-floor switching of main coverage channels (say channel 1 on 1 S, channel 6 on 2 South, 11 on floor 3 South), but did show the various channel usages thoughout the building. A more detailed knowledge of exact broadcast points would help towards this end.

Appendix

The sole gnuradio function used for this exercise is usrp_spectrum_sense.py, found in gnuradio/gnuradio-examples/python/usrp. It is invoked in the following manner, with the following option set for appropriate output:

```
Sudo python usrp_spectrum_sense.py 2.4095G 2.502G –F 3 > file.tr
```

```
        parser.add_option("-F", "--fft-size", type="int", default=256,
                          help="specify number of FFT bins
[default=%default]")
```

The typical output of running usrp_spectrum_sense.py would give the signal strength for each frequency tested in terms of the sums of the squares of the FFT magnitudes. By default, these values are sorted into 256 different bins and the results are outputted to either the screen or a file. These bins run from the 0 Hz 1st bin to an upper value 256th bin (the value of this FFT frequency was not clear). Using the "–F" option allows this strength of signal measurement to be reduced to a more manageable number of bins, covering still the entire FFT decomposition spectrum. I ended up using 3 bins then summing these results together to get an indication of the overall strength ofsignal (at least 2 bins are required, otherwise a "division by zero" error occurs in the code execution).

Setting the frequency analysis, and output, points, are accomplished by judicious use of frequency limits in the command line, as well as the step size, "self.freq_step." This step size is calculated as a function of the usrp_rate, which turns out to be 4 MHz. The original code multiplies this rate by .75, but I changed that to 1.25 to get exact 5 MHz steps. More accurate results would result from a smaller step size, but these results proved qualitatively successful enough. The relevant portion of code from usrp_spectrum_sense.py is as follows:

```
# Set the freq_step to 75% of the actual data throughput.
        # This allows us to discard the bins on both ends of the spectrum.

        ## NEXT LINE IS THE ONLY CHANGE NECESSARY
        self.freq_step = 0.75 * usrp_rate  # use 1.25 for 5 MHz step
        self.min_center_freq = self.min_freq + self.freq_step/2

        nsteps = math.ceil((self.max_freq - self.min_freq) /
self.freq_step)

        self.max_center_freq = self.min_center_freq + (nsteps *
self.freq_step)

        self.next_freq = self.min_center_freq
        etc.
```

Finally, the signal strength and frequency value need to be outputted, so the main loop of usrp_spectrum)_sense.py has the following:

```
def main_loop(tb):
    while 1:

        # Get the next message sent from the C++ code (blocking call).
        # It contains the center frequency and the mag squared of the
# fft

        m = parse_msg(tb.msgq.delete_head())


      # Print center freq so we know that something is happening...
        print m.center_freq

        # FIXME do something useful with the data...

        # m.data are the mag_squared of the fft output (they are in the
        # standard order.  I.e., bin 0 == DC.)
        # You'll probably want to do the equivalent of "fftshift" on them
```

And I add the following line:

Print m.data

Which gives output looking like the following:

```
Using RX d'board A: Flex 2400 Rx MIMO B
gain = 45.0   # a gain value of 45 db is used for every result I obtained,
             # and is set by default by usrp_spectrum_sense from the
             #midpoint dB value
2412000000.0
(427813.21875, 39569.17578125, 26839.921875)
```

(the very first frequency result, above, is typically very high and inaccurate, so I take measurements from the 2nd set of outputted data)

```
2412000000.0
(95253.671875, 67829.6484375, 58630.76171875)
2417000000.0
(55381.6640625, 51730.50390625, 36229.67578125)
2422000000.0
(25140.361328125, 5934.392578125, 22727.86328125)
2427000000.0
(21100.572265625, 53413.015625, 70834.0703125)
2432000000.0
(294060.09375, 196044.09375, 34845.08984375)
```

```
2437000000.0
(275551.375, 107001.3125, 149790.65625)
2442000000.0
(23314.603515625, 13694.6884765625, 27311.01171875)
2447000000.0
(24594.21875, 60618.87890625, 196840.765625)
2452000000.0
(11314.142578125, 12611.4404296875, 6525.078125)
2457000000.0
(670287.6875, 813796.1875, 414993.625)
2462000000.0
(999667.1875, 499449.03125, 799586.0625)
2467000000.0
(13651.7041015625, 46699.3125, 41917.9140625)
2472000000.0
(83720.796875, 60033.015625, 141168.625)
2477000000.0
(11285.0087890625, 4587.6455078125, 6482.40966796875)
```

Plots are performed by summing these components and plotting (I use Matlab, with the command plot(x',sum(y,2)) , given the processing format.

```
x(i) = 2412000000.0;
y(i,:) = [35534196.0, 23083036.0, 27595190.0]; i=i+1;
```

etc.

References

1. M. Benedetto, Y. Hua, T. Kaiser, and X.Wang, “Cognitive Radio Technology,” IEEE Signal Processing Magazine, vol. 25, no.6, p.10 Nov. 2008.

2. J. Mitola, “Cognitive Radio: An integrated agent architecture for software defined radio,” Doctor of Technology, Royal Inst. Technology (KTH), Stockholm, Sweden, 2000.

3. M. Shahidehpour and Y. Wang, “Communication and Control in Electric Power Systems: Applications of Parallel and Distributed Computing” John Wiley & Sons, Hoboken NJ, 2003.

4. F.Cleveland, “Use of Wireless Data Communication in Power System Operation,” Power Engineering Society General Meeting 2007, Tampa, Florida, June 24-28, 2007

5. http://www.ece.cmu.edu/~electricityconference/, esp. “Review of Communication Protocols for Smart Grid AMI Systems, Coalton Bennett (Presentations/Day 1 / Session 2), Carnegie Melon University, Pittsburgh, PA, March 2009.

6. http://www.gnu.org/software/gnuradio/

7. http://www.cognitiveradio.wireless.vt.edu/dokuwiki/doku.php?id=home

8. T. Rondeau, B. Lin, D. Scaperoth, C. Bostian, “Cognitive Radio Formulation and Implementation,” First International Conference on Cognitive Radio Oriented Wireless Networks and Communications, 2006, June 8-10, 2006.

9. S.Haykin, “Cognitive Radio: Brain-Empowered Wireless Communication,” *IEEEJopurnal on Selected Areas in Communications*, vol.23, no. 2, pp. 201-220,Feb. 2005.

10. K.Hiraga, K.Akabane, H.Shiba and K. Uehara, “Channel Assignment and Reallocation Algorithms for Cognitive Radio Systems,” Proceedings of the APCC 2008.

11. A.Gupta “Power Allocation Schemes for Cognitive Radios,” in International Conference on Communications Systems: Software and Middleware Workshops, 2008, COMSWARE 2008.

12. S. Shankar, “Squeezing the Most Out of Cognitive Radio: A Joint MAC/PHY Perspective,” IEEE Conference on ICASSP 2007, vol. 4, April 15-20 2007, pp.IV-1361-1364.