GNU Radio and USRP for Problem-Based Learning in Communications: Case Studies in Cellular Phone Jamming and Modulation Classification

Leonardo Ramalho, Joary Fortuna, Lailson Santos, Joeldo Oliveira, and Aldebaro Klautau
LAPS/LASSE, Federal University of Pará - UFPA
CP 8619 - Rua Augusto Correa 01 - CEP 66075-110 - Bélem - Pará - Brazil
Web: www.laps.ufpa.br; www.lasse.ufpa.br.
E-mails: {leonardolr, joeldo, aldebaro}@ufpa.br, {lailson.santos, joary.fortuna}@itec.ufpa.br

ABSTRACT

The GNU Radio and USRP are important tools that can be used by students to learn the theory of various areas, such as digital signal processing and telecommunications. This work presents how the GNU Radio and USRP has been used to transmit/receive signals in wired and wireless channels for a wide range of frequencies. Two case studies are discussed: cellular phone jamming and modulation classification. When dealing with these two (and other) topics, the students get involved with several important theoretical as well as practical issues. The work summarizes strategies to benefit from the combination of GNU Radio and USRP and increase their impact on engineering education.

Keywords: GNU Radio, jammer, modulation classification, PBL, USRP.

1. INTRODUCTION

The PBL (Problem-Based Learning) is a student-centered learning method in which students are encouraged to solve real-world problems, most of the time, in groups [1], [2]. The idea is that the students can apply and learn the necessary theory in a practical way, helping them to learn the content as well as improving their thinking strategies and interpersonal relationships. In this context, the USRP (Universal Software Radio Peripheral) and GNU Radio are important tools for teaching telecommunications and associated areas, given that they are, respectively, a relatively low cost hardware and open-source software.

Figure 1 illustrates how the USRP and the GNU Radio operate together. Each one is briefly described in the sequel. The USRP is a generic hardware to transmit and/or receive signals [3]. It is composed by a motherboard that can be connected to several daughter-boards that provide a variety of interfaces from simple analog filters to complex down and up conversion circuits for many frequencies bands. Thereby, the USRP is able, with the daughter-boards, to operate in frequencies from DC to 6 GHz.

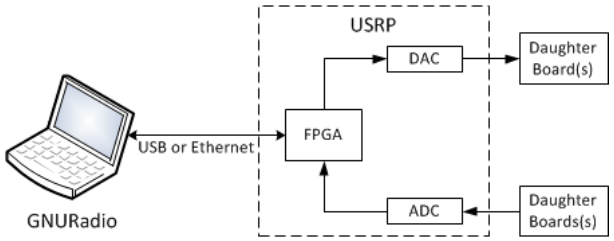

Fig. 1. Simplified block diagram of how GNU Radio and USRP can be configured.

GNU Radio is a development toolkit that provides signal processing blocks to implement software radios. Using the GNU Radio, it is possible to create (or to receive) digital data streams that can be transmitted (or sampled) by hardware (for example, the USRP) or , simply written (or read) to (from) a file [4].

Several institutions in the world have foreseen the advantages of using the USRP and GNU Radio. The 2012 IEEE Globecom conference, in Anaheim, held a session specifically about the adoption of such software radio tools for teaching purposes. Institutions such as UT Texas at Austin, USA, and RWTH Aachen University, Germany, have developed and distributed teaching material regarding several basic and advanced concepts. This work follows this trend with the specific characteristic of using PBL in projects that are of interest for research. This way one can benefit from the synergy of research and education-oriented projects, in an environment where both undergraduate and graduate students cooperate. Therefore, the approach adopted here is to describe two specific case studies and indicate the concepts that are emphasized.

The work is organized as follows. Section 2 presents the general task of how to use the GNU Radio and USRP to send/receive signals through a real channel. Sections 3 and 4 describe two case studies: cellular-phone jamming and modulation classification, both implemented with GNU

Radio and an USRP. They are followed by the conclusions.

2. GR COMPANION FOR TASKS USING THE EXISTING FUNCTIONALITIES IN GNU RADIO

The GNU Radio project provides a set of signal processing blocks that can be aggregated to build flow-graphs. These blocks are written in C++ and run in Python, which brings several advantages, such as easy instantiation and connection of existing blocks and easy GUI (Graphical User Interface) creation, as shown in Figure 2. The user only needs knowledge of how each block works, which is an invitation to the proper study of algorithms that process the samples in frames (or blocks).

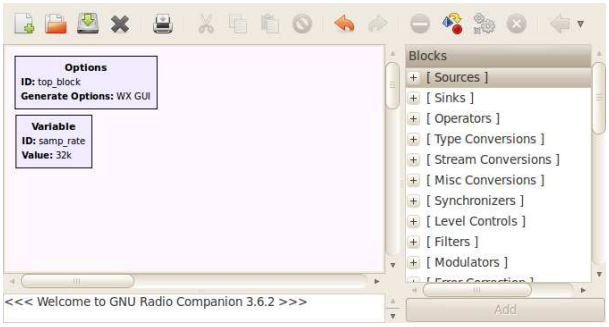

Fig. 2. GNU Radio graphical user interface.

The existing blocks in GNU Radio cover various applications from simple mathematical operations to complex digital filtering, modulators/demodulators, channel coding blocks, voice codecs and others.

A special class of blocks are the input/output blocks. They create an interface with the real world, the most known of them are UHD (USRP hardware driver) blocks and Audio blocks.

The UHD blocks are created to use the USRP and normally put/get signals from wireless medium. Alternatively, the audio blocks put/get the signal from sound card.

2.1. Wireless transmission example using USRP

At the Federal University of Para, students with access to a USRP use the GNU Radio to transmit signals through wireless channels. As an example of the procedures, this subsection presents a wireless digital communication using BPSK (binary phase-shift keying) modulation.

As it is well-known, in BPSK modulation there are only two symbols, representing the bits 0 or 1. They are separated by a π phase shifting. The bits 0 and 1 could be represented by [5]:

$$s_0(t) = \sqrt{\frac{2E}{T}}\cos(2\pi f_c t) \quad (1)$$

$$s_1(t) = \sqrt{\frac{2E}{T}}\cos(2\pi f_c t + \pi) \quad (2)$$

where

E is the symbol energy ;
T is the symbol Period;
t is a any time, $0 \leq t \leq T$;
f_c is the carrier frequency.

Figure 3 shows the blocks used in a bit transmission over wireless channel. The block *Vector Source* sends a vector specified by the user. When executing this project, the vector is composed by 0s and 1s; the block repeats the vector whenever it reaches the end. The *Vector Source* output is connected to a *Packet Encoder* which is responsible for encoding the data, such that the receiver can find the beginning of the transmitted data.

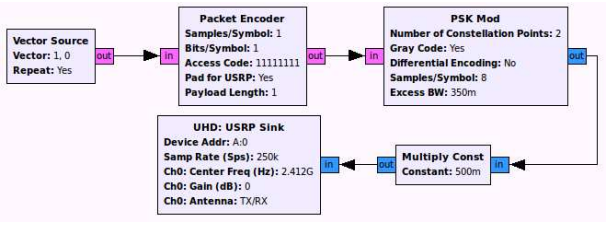

Fig. 3. GNU Radio BPSK transmitter flow graph.

After the encoder, the encoding data are sent to *PSK Mod* which is responsible to modulate the information using PSK. In this block, it is possible use different configurations like if it is desired use gray code and differential encoding as well as the number of points in constellations, among others. In this example, the *PSK Mod* was configured as a BPSK modulator.

The value of the samples in *PSK Mod* output is modified (multiplied by a constant) by *Multiply Const* block, such that the power of modulated signal can be changed. Lastly, in transmitter, the signal is sent to *UHD: USRP Sink* block which is responsible for interact with the USRP. This block has several parameters that are used by the hardware like sampling frequency, carrier frequency and what antenna is being used on the daughter-board.

Figure 4 shows the blocks used in reception of wireless BPSK signals. The *UHD: USRP Source* block abstracts all the hardware in reception (USRP and daughters-boards) and its outputs are the samples of the received signal in baseband. In this block, like the *UHD: USRP Sink*, it is possible to define several parameters of the hardware. The *UHD: USRP Source* output is connected to *PSK Demod* block that demodulates the PSK signal (BPSK in this example), recovering the encoding data. After the demodulation, the encoding data is sent to *Packet Decoder* block which decodes the data and outputs the bits (the information sent by *Vector Source*). Once the information was recovered, the *Char to Float* block converts the byte in float, so that the information can be used by others blocks.

For this wireless example, the students used an USRP with two daughter-boards (RX2400) and two antennas,

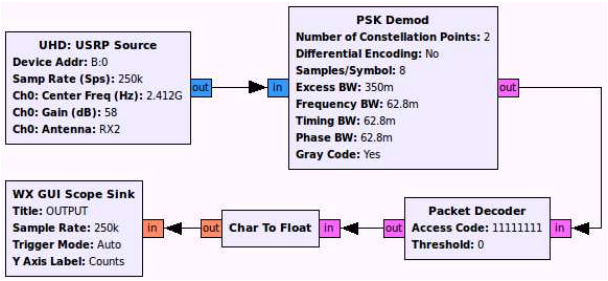

Fig. 4. GNU Radio BPSK receiver flow graph.

each one used on transmitter and receiver, as shown in Figure 5. It was sent a sequence of 0s and 1s. Figures 6 and 7 show the FFTs of the transmitted and received signal, respectively.

This wireless experiment allows students to implement and study several telecommunication concepts, such as channel estimation, noise analysis and modulation development.

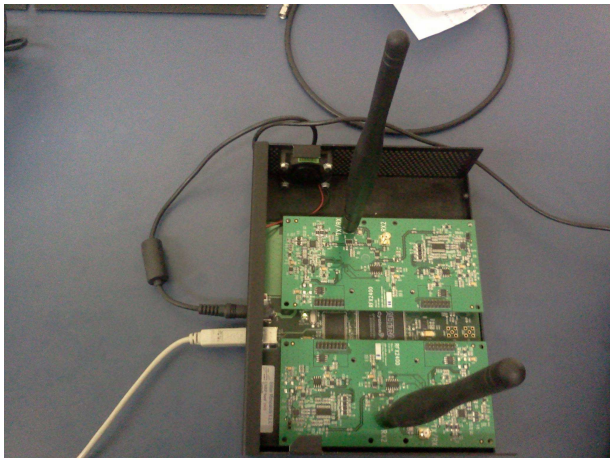

Fig. 5. USRP transmitter and receiver BPSK.

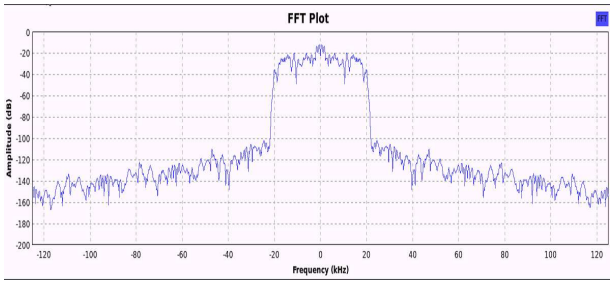

Fig. 6. BPSK transmit signal spectrum.

2.2. Wired transmission example using the sound card

Projects involving wired communications are good tasks to start with, given that the channel is better controlled than the wireless channel. This subsection presents an example using the sound card.

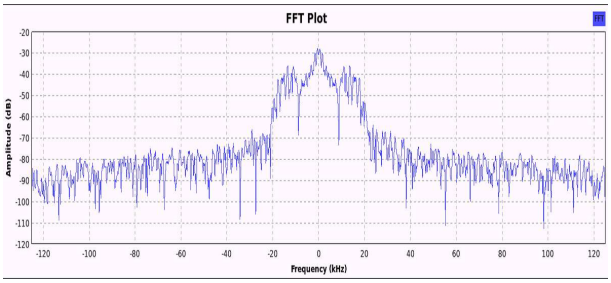

Fig. 7. BPSK received signal spectrum.

To exemplify the data transmission using a sound card, the authors created a flow-graph transmitting/receiving a QAM signal. GNU Radio already has QAM modulator and demodulator, so we only need to instantiate and connect the blocks using GNU Radio GUI (GNU Radio-companion), QAM transmitter flow-graph can be seen in Figure 8, and QAM receiver can be seen in Figure 9.

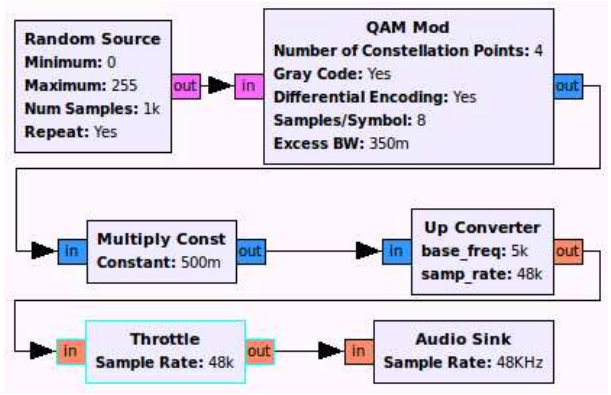

Fig. 8. GNU Radio QAM transmitter flow graph.

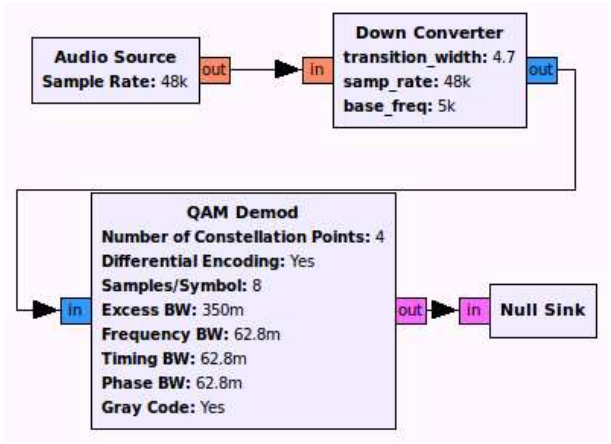

Fig. 9. GNU Radio QAM receiver flow graph.

To exemplify the signal processing blocks, we add *Up Converter* and *Down Converter* Blocks, they do not exist as original blocks on GNU Radio, but we create then using a special feature called Hier Block which allows

the encapsulation of multiple blocks into a single. The *Up Converter* Hier Block can be seen in Figure 10 and the *Down Converter* Hier Block was created similarly.

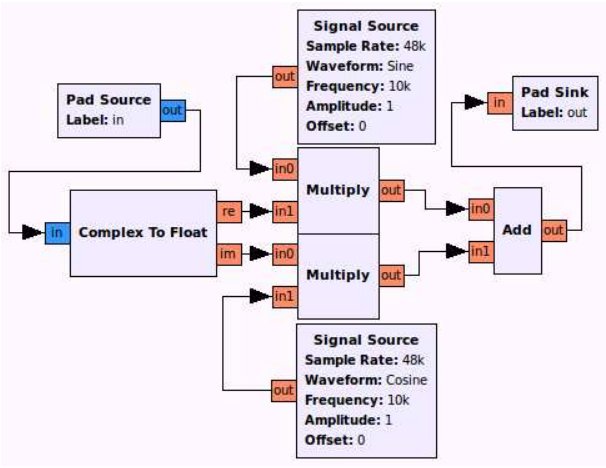

Fig. 10. Up Converter Hier Block.

All data flowing through flow-graph can be stored in files to subsequent analysis, but in this particular case, we will use graphical sinks to see data flowing in real time GUI.

The frequency spectrum of generated QAM signal can be seen in Figure 11. The generated QAM signal is up converted to a given frequency (5 kHz in this case), as can be seen in Figure 12.

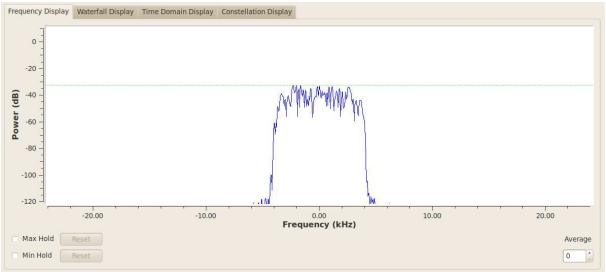

Fig. 11. Baseband QAM signal in the transmitter.

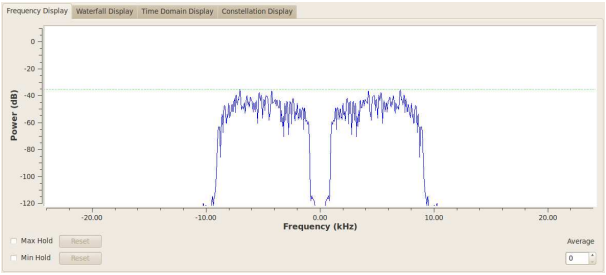

Fig. 12. Upconverted QAM signal in the transmitter.

After going through a real channel, consisting of a loopback cable connecting sound card output to sound card input, the received signal is show in Figure 13. The received signal is down converted to baseband and can be seen in Figure 14.

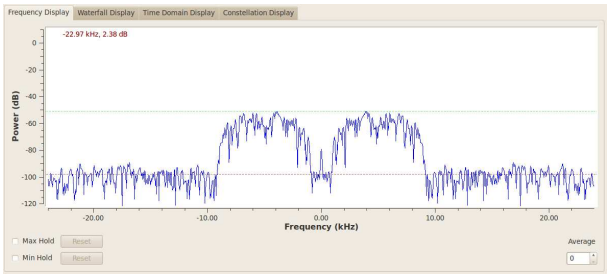

Fig. 13. QAM signal in the input of the receiver.

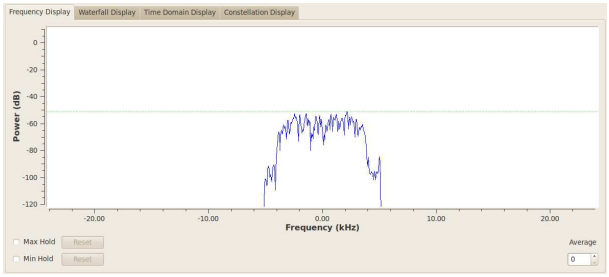

Fig. 14. QAM signal in receiver, after downconversion.

3. Case Study: Cellular Phone Jamming

The number of cell phone subscriptions reached almost 6 billion and there were 105 countries where the mobile-cellular subscription exceeded the number of inhabitants by end of 2011 [6]. Cell phones are used everywhere, but in some places its use is inconvenient or even illegal. Thus, a jammer is an important device that can block (part of) communication in a determined area (e. g. theater, church, prisons).

The attack to a communications system can be implemented in various ways. A jammer can work in the physical layer, link layer or even in higher layers [7]. There are a lot of jammer implementations in literature [8] [9] [10]. The jammer presented here exploits the vulnerability of the physical layer by sending a signal (noise, here called 'signal jammer') that substantially reduces the SNR (Signal-to-Noise Ratio) of the communication.

Figure 15 shows a simplified block diagram that can be used for jamming. The GNU Radio generates the signal jammer and the center frequency (F_C), then send them to USRP that uses its DAC (digital-to-analog converter) to send the signal (in baseband) to the daughter-board (in this project, the RFX900). All analog circuits necessary to move the signal in the frequency range of 700-1050 MHz is within the RFX900. However, other daughter-boards could be used to operate in others frequencies range.

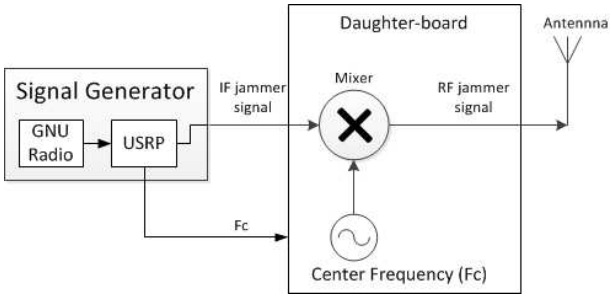

Fig. 15. Simplified block diagram of a jammer using the USRP and GNU Radio.

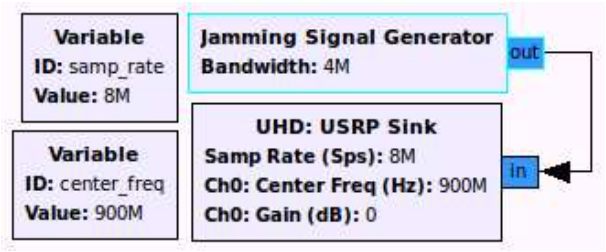

Fig. 16. Blocks used in GNU Radio to generate the signal jammer.

Figure 16 shows the blocks in GNU Radio to create the signal jammer. A Hier Block was created, the *Jamming Signal Generator*, which encapsulated all the processing used to generate the signal jammer in baseband. The GNU Radio, with the USRP, allows change the center frequency and the bandwidth of the signal jammer. Figure 17 shows the signal jammer on the output of the RFX900.

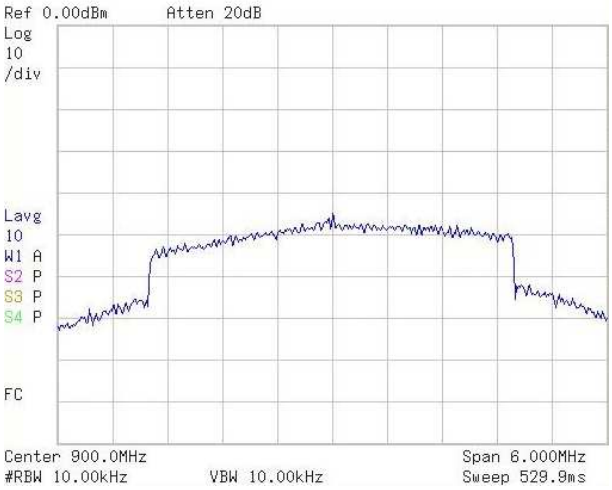

Fig. 17. Signal of the jammer after mixer.

The N9320B spectrum analyzer from Agilent Instruments has been used to generate the Figure 17. The Resolution (RBW) is 10KHz and the range of frequencies from 897-903 MHz are shown. As can be seen, the signal jammer is centered in 900 MHz and its bandwidth is 4 MHz. Besides using virtual instrumentation such as the FFT scope in GNU Radio, it is interesting for the students to deal with actual equipments, as the ones they will face when working in industry. Hence, at UFPA, some of the experiments are verified using spectrum analyzers and digital oscilloscopes.

To jam the cellular phone, is necessary send the signal jammer in the band of frequencies which the cell-phones operate. These frequencies can vary, depending on the country and the mobile network operator. However the USRP and the daughter-boards can serve applications in various frequencies, including the frequencies of cellular-phones.

4. Case Study: Modulation Classification

The Automatic Classification Modulation (ACM) consists in identifying the modulation schema of a transmitted signal with a high probability of success in a low range of observations. Detailed discussions about the subject are found in [11] and [12]. ACM has been used for decades in military systems and others applications. Recently the interest in ACM was renewed by research in cognitive radio [13]. Most of the ACM proposed methods [14] were inspired on pattern recognition techniques [15] and/or detection/estimation theory [16]. There are several studies in the literature that use simulated data and models that vary in complexity channels including AWGN and fading channels. However, as pointed out in [11] (Section 5), there is a great difficulty in comparing the various methods proposed. Among the reasons is the lack of a public database of modulated signals. To minimize this problem the authors have been organizing and freely providing signals [17] for example of BPSK, 4-PAM, 16-QAM and 8-PSK modulations.

The developed dataset allows greater ease in building benchmarks to compare results among different groups of researchers. As an example, Figure 18 from [18] shows the result of applying the bases in ACM using three classifiers, the CSS-SVM (with and without SNR knowledge), cummulant and the ALRT upper bound (see [18] for details). The graph shows the curve of probability of correct classification (PCC) as a function of SNR.

The bases were generated with GNU Radio by transmitting random numbers through the wireless channel and capturing the symbols modified by the channel. It was used AWGN channel and SNR ranging from 0 to 15dB. The file name contains the information of the modulation signal, the SNR and if is *full, train, test and validation*. The *full* file indicates that the file contains all samples taken in the generation of bases. Files with *train, test and validation* contains samples extracted from the *full* file for use in ACM. The file extension is *raw* to indicate that the content file contains only the samples of complex symbols, without any other additional information. The contents of the files are arranged in binary format where each sample

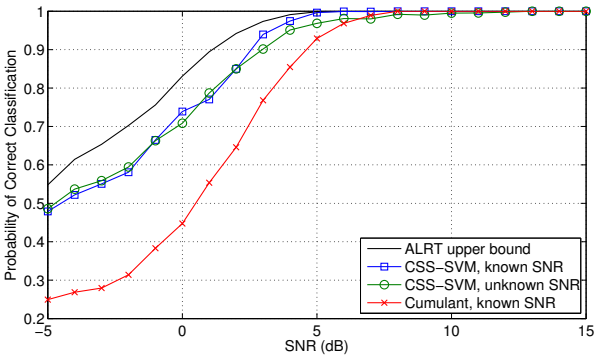

Fig. 18. Results of three ACM classifiers using the same modulation bases. [18]

occupies 8 byte being the first 4 bytes corresponding to the component I and the remaining 4 bytes containing the component Q. The order of the data is *little endian*, or least significant byte first. The dataset assists researchers when comparing different results and assist students that can use them without having to generate the signals.

5. Conclusions

This work described two case studies on using the GNU Radio and USRP for education. One important aspect is that the topics allow both graduate and undergraduate students to benefit from the experiments.

Various aspects of practical importance can be explored with the help of these tools. For example, the compromise between time resolution and frequency can be exploited by analyzing signals and graphs of bit error rate versus signal to noise ration can be compared with theoretical expressions. The tools also allow the investigation of modern modulation techniques, such as discrete multitone and OFDM.

An interesting aspect of using open source tools and datasets is that it has been found that reproducible research results cause greater impact [19]. However, this requires the availability of low cost hardware and software and public databases.

The GNU Radio and the USRP surely allow students to develop projects and effectively apply the theory of important and difficult areas such as digital signal processing and telecommunications. Educational institutions can use the PBL method and improve the learning experience of their students by using the GNU Radio and USRP. Among the advantages, one can relatively quickly setup and see the results of a experiment; algorithms can be easily implemented and performed. The experience shows that every time a experiment is successful, the student typically feels more motivated to study and continue learning about the theme.

References

[1] W. Akili, "On implementation of problem-based learning in engineering education: Thoughts, strategies and working models," in *Frontiers in Education Conference (FIE), 2011*, oct. 2011, pp. S3B–1 –S3B–6.

[2] L. R. J. Costa, M. Honkala, and A. Lehtovuori, "Applying the problem-based learning approach to teach elementary circuit analysis," *Education, IEEE Transactions on*, vol. 50, no. 1, pp. 41 –48, feb. 2007.

[3] "Ettus research LLC," 2012, http://www.ettus.com/.

[4] "The GNU Radio Project," 2012, http://gnuradio.org.

[5] S. Haykin, *Communication Systems*, Jhon Wiley and Son, 2001.

[6] International Telecommunication Union, "Key statistical highlights: ITU data release June 2012," 2013, http://www.itu.int/ITU-D/ict/statistics/material/pdf/2011%20Statistical%20highlights_June_2012.pdf.

[7] K. Pelechrinis, M. Iliofotou, and S.V. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *Communications Surveys Tutorials, IEEE*, vol. 13, no. 2, pp. 245 –257, quarter 2011.

[8] S.W. Shah, M.I. Babar, M.N. Arbab, K.M. Yahya, G. Ahmad, T. Adnan, and A. Masood, "Cell phone jammer," in *Multitopic Conference, 2008. INMIC 2008. IEEE International*, dec. 2008, pp. 579 –580.

[9] N.K. Mishra, "Development of GSM - 900 mobile jammer: An approach to overcome existing limitation of jammer," in *Wireless Communication and Sensor Networks (WCSN), 2009 Fifth IEEE Conference on*, Dec. 2009, pp. 1 –4.

[10] D.S.V. Araujo, J.C.A. Santos, and M.H.C. Dias, "A dual band steerable cell phones jammer," in *Microwave and Optoelectronics Conference, 2007. IMOC 2007. SBMO/IEEE MTT-S International*, 29 2007-nov. 1 2007, pp. 611 –615.

[11] O. A. Dobre, A. Abdi, Y. Bar-Ness Y., and W. Su, "Blind modulation classification: A concept whose time has come," in *IEEE Sarnoff Symposium*, 2005, pp. 223–228.

[12] T. Yucek and H. Arslan, "A survey of spectrum sensing algorithms for cognitive radio applications," *Communications Surveys Tutorials, IEEE*, vol. 11, no. 1, pp. 116 –130, quarter 2009.

[13] S. Haykin, "Cognitive radio: Brain-empowered wireless communications," *IEEE Journal on Selected Areas in Communications*, vol. 23, n. 2, pp. 144–150, Feb. 2005.

[14] A. Fehske, J. Gaeddert, and J.H. Reed, "A new approach to signal classification using spectral correlation and neural networks," in *First IEEE International Symposium on New Frontiers in Dynamic Spectrum Access Networks, 2005. DySPAN 2005.*, Baltimore, MD, USA, pp. 144–150.

[15] R. Duda, P. Hart, and D. Stork, *Pattern classification*, Wiley, 2001.

[16] H. Van Trees, *Detection, estimation, and modulation theory*, Wiley, 2003.

[17] "Ufpatelecom," *http://www.laps.ufpa.br/ufpatelecom/*, 2009.

[18] F. Muller, C. Cardoso, and A. Klautau, "A front end for discriminative learning in automatic modulation classification," *IEEE Commun. Lett.*, vol. 15, no. 4, pp. 443–445, Apr. 2011.

[19] Patrick Vandewalle, Jelena Kovacevic, and Martin Vetterli, "Reproducible research in signal processing - what, why, and how," *IEEE Signal Processing Magazine*, vol. 26, no. 3, pp. 37–47, 2009.