Software Defined Radio Applications Using USB Receptors

Byron R. Sanga, Andres M. Villavicencio, Vladimir Sanchez Padilla, *Member, IAENG*,
Stephanie Villacis Alvia, Ronald A. Ponguillo, *Member, IAENG*

***Abstract*— This article considers the functioning of communication devices due to specific ranges of bandwidth and the type of modulation they work, constraining in some cases communication out of this range. Software Defined Radio solves this problem using software and embedded systems allowing to control communication parameters, having many USB devices to facilitate both signal transmission and reception according to the requirements and necessities of applications.**

***Index Terms*—Embedded Systems, GNU-Radio, SDR, USB DVB-T.**

I. Introduction

In 1991 Joe Mitola first used the term 'Software-Radio' to define a programmable radio frequency system [1]. Software Defined Radio (SDR) is termed to a combination between hardware and software by which signals are processed either for transmission or reception in radio communication systems, whose parameters and functionality in the physical layer of the OSI model can be configured by an application in accordance with communication standards established by different protocols [2]. It can be seen as a set of interaction between software and hardware, understood as programmable devices such as FPGA, Beaglebone, Beagleboard, Arduino, among others, so that harnessing can be maximized depending on the software version, as well as the programmer skills [3], leading to cost savings for telecommunications companies, as SDR allows multitask without the need of new hardware. In other words, SDR is a methodology capable of converting hardware problems in software problems [2], becoming useful in the academic field due to the growing trend of free software, which is reflected in fruitful research projects through easy connection devices to the computer, making this technology accessible and interesting. A basic block diagram is shown in Fig.1 [4].

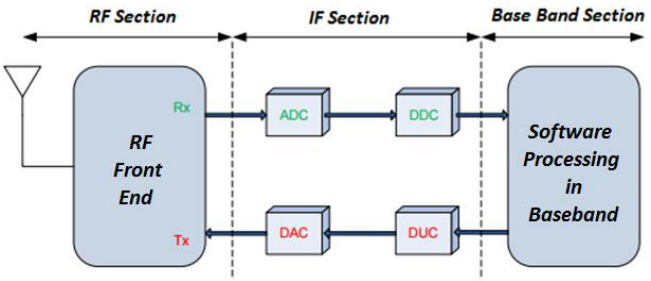

Fig. 1. SDR basic block design.

II. SDR Types

In the case of the SDR technology it can be classified into five types detailed below [5]:

A. Type I

One of the most common and easily accessible. An attractive reason is that its implementation is easily identifiable, because uses the sound card of a computer as a digitizer, implementing the same software as the processor.

Within this type of SDR there are certain classifications:

- ***Type Ia:*** Requires sound card feeding.
- ***Type Ib:*** Sound card requires a mode with an approximate frequency of 12Khz signal.
- ***Type Ic:*** One of the most powerful and required by programmers; it is required to feed the sound card with intermediate frequencies.
- ***Type Id:*** Differs from the previous ones, because it can process specialized signals between a digitizer and processor.

B. Type II

Deploys an input makes receiving and capturing the signal for further processing.

C. Type III

Requires the use of an analog IF since it receives the same signals for finally processing.

D. Type IV

Unlike the previous ones, is responsible for receiving the signal which comes directly from the frequency that is working, so it also uses special receivers that will be processing in a continuous way the signal.

E. Type V

For this type is require the use of a server that will be in

Manuscript received July 12, 2016.

The authors are with the Escuela Superior Politécnica del Litoral, ESPOL, Faculty of Electrical and Computer Engineering, Campus Gustavo Galindo, Km 30.5 Via Perimetral, P.O. Box 09-01-5863, Guayaquil, Ecuador (email: {byresang, avillavi, vladsanc, stedvill, rponguil}@espol.edu.ec), website: www.espol.edu.ec

V. Sanchez Padilla is a Lecturer of the Telematics Department and part-time collaborator of the Master's Program in Telecommunications at the Escuela Superior Politécnica del Litoral, ESPOL, Faculty of Electrical and Computer Engineering, Campus Gustavo Galindo, Km 30.5 Via Perimetral, P.O. Box 09-01-5863, Guayaquil, Ecuador.

R. A. Ponguillo is the Coordinator of the Basic Electronics Area and a Researcher of the Vision and Robotics Center at the Escuela Superior Politécnica del Litoral, ESPOL, Faculty of Electrical and Computer Engineering, Campus Gustavo Galindo, Km 30.5 Via Perimetral, P.O. Box 09-01-5863, Guayaquil, Ecuador.

ISBN: 978-988-14047-1-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

charge of the digital signal processing, processing them partially or completely according to the required range required.

III. Digital Signal Processing

Digital Signal Processing (DSP) is a manipulation of an analog signal to convert it into digital by mathematical processes, thereby reducing the presence of noise, controlling the signal power, among other features. It represents the signal in the discrete-time domain and require equipment capable of quickly and efficiently a lot of calculations, such as a GPU or FPGA. The emergence of this technology was between the decade of the 1960's and 1970's, with the appearance of mathematical processors capable of performing millions of calculations in small amounts of time [6]. This provided the necessary technology to expand the area of applications of DSP, such as the design and deployment of digital filters, voice compression, image processing, etc.

Developments in processors speed and the rise of Analog/Digital and Digital/Analog converters, together with the development of digital communications, have expanded the scope of this technology. Today, it can be found in verifying the quality of electricity supply, radars, sound navigation, electrocardiograms diagnostic, telephony, and audio systems, among others [6]. DSP contributes to SDR by performing baseband software processing, mainly through the use of computers or embedded systems.

IV. Hardware Platform For SDR Deployment

Main platforms used in SDR are DSP for narrowband signals and FPGA for wideband signals [1], being the deployment with the latter widely used in academics and research field, mainly with the assistance of MATLAB [7].

Currently, there are devices that capture signals through an USB connection to a computer, whether radio or television, among other possible. Such transmissions can be received and processed on a computer, either on a GNU-Linux operating system [3], which is the most used because of being open source (also known as GNU-Radio), becoming in one of the most explored fields by students and researchers worldwide. It also works under Windows operating system, because it has applications that allow to set up the device for specific applications.

V. SDR-USB Applications

DVB-T (Digital Video Broadcasting Terrestrial) is a technology that is being applied in several countries, and allows embedded devices, such as USB-DVB-T, to receive different channels of audio and digital video [8].

This technology is not yet implemented in many countries, e.g., the ones from the Latin America region (Fig. 2) [8], but SDR USB-DVB-T is used by radio amateurs, students and hobbyist as spectrum analyzer, because of its relatively low cost and friendly graphical interface. DVB-T devices based on the RTL2832U chip keep some records that, after connecting to a USB 2.0, have the ability to receive radio signals, feature detected by programmer Antti Palosaari. DVB-T devices have been applied in various fields since that discovery, including attacks on the security of GSM networks, possible by installing an USB device on any computer, making it able to get the information transmitted by end users. Another application is in the field of astrology in the study of meteorites through its monitoring, with the help of television antennas [9].

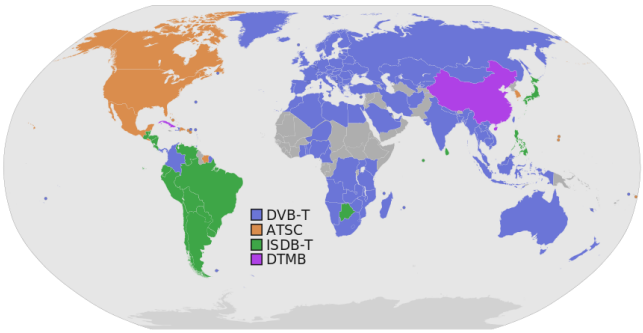

Fig. 2. Terrestrial transmission technologies worldwide.

VI. FM Radio With SDR USB-DVB-T

With SDR using USB it can be receive FM radio signals in different frequencies [8]. For the laboratory proposed is available a computer with an Intel Core I3 processor or higher, plus Windows 7 operating system or higher. The USB-RTL device to be used is the RTL2832U (Fig. 3).

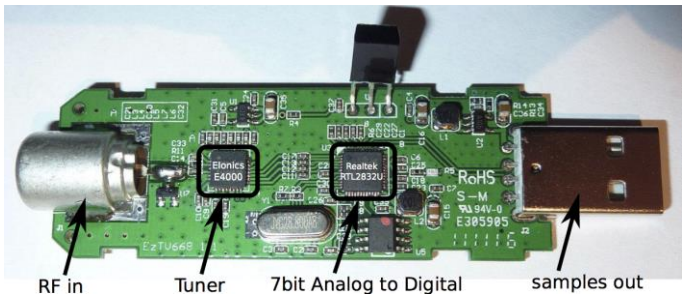

Fig. 3. RTL2832U.

It must be installed a suitable generic driver to the device by Zadig application, thereby the device is ready for use. You need to install and run the application SDR#V1.0.0 (Fig. 4). The application is set by selecting the source device that receives the signal, in this case the RTL-USB Dongle. Then, it must be selected the type of radio signal, which will be Wide-Band FM (WFM). A 15 dB gain is provided to obtain adequate signal. The receiver is tuned to select the desired broadcasting radio station. As a result, the chosen radio station can be listened and it is visualized the behavior of the signal spectrum received (Fig. 5).

VII. Security With SDR

Development of technology concerning to communication refers the fact that networks are less dependent on physical structures (e.g., cabling), resulting in wireless communications, such as Wi-MAX, TETRA, Wi-Fi, DMR, LTE with virtual connection benefits. Within the scope of security it has been emphasized to operate in ISM unlicensed bands, like Wi-Fi or Bluetooth, making attacks to be focus on this kind of transmission [10], being necessary to consider a more comprehensive analysis of

ISBN: 978-988-14047-1-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

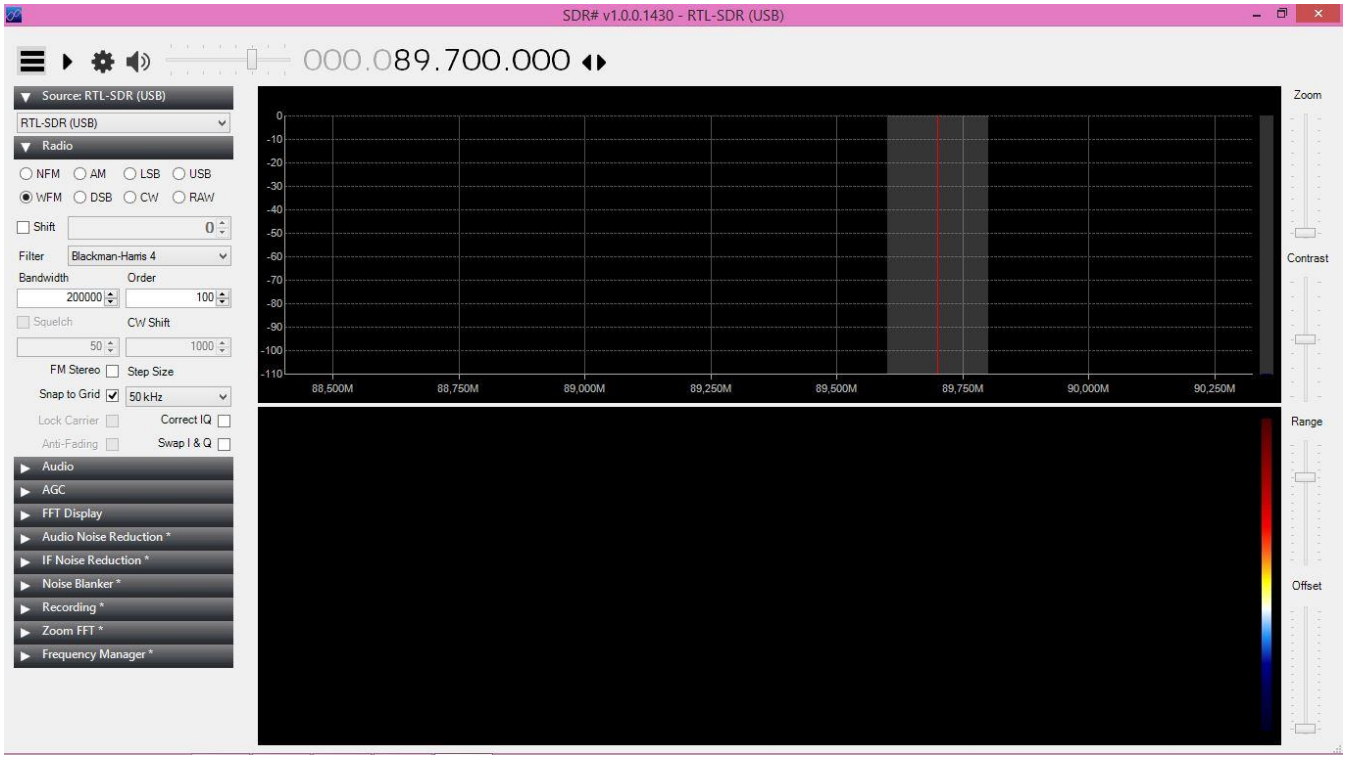

Fig. 4. Screenshot during execution of the application SDR # V1.0.0.

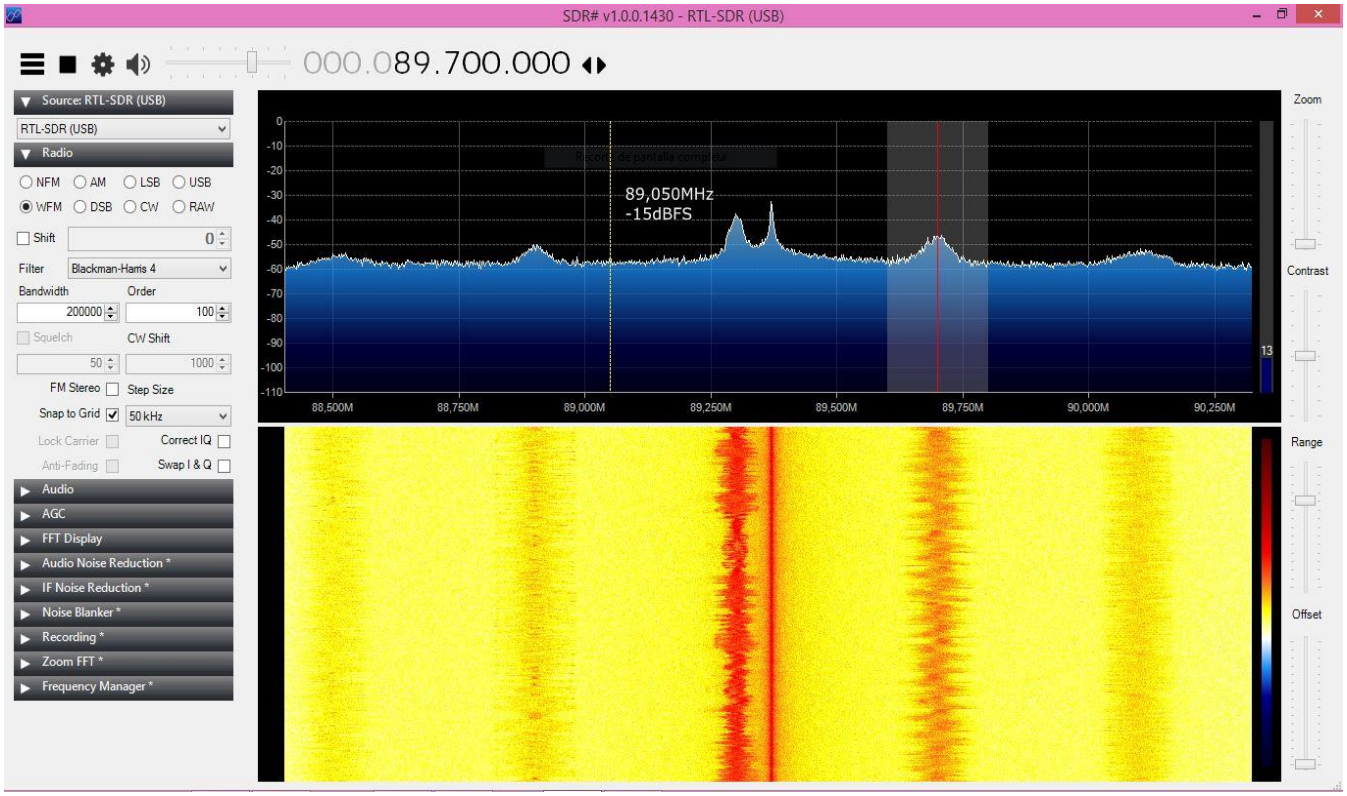

Fig. 5. Screenshot of the signal spectrum FM 89.7 MHz.

operating protocols in wireless transmission. Many radio systems implement “security by obscurity”, keeping in secret the design, deployment and algorithms (or protocols) used, allowing some reliability in communications systems, although in recent years this has not been enough, due to attackers have highlighted different types of vulnerabilities on these systems [11].

Advances in SDR have enabled a more robust security development, achieved by its accessibility and the benefits it present, such as analysis of different communication protocols (e.g., GSM, ADS-B, APRS, ACARS) which can be carried out by an RTL-SDR receiver that captures RF signals (Fig. 6) [11].

In critical infrastructure, like military or government, is necessary to realize about potential vulnerabilities in order to deploy SDR for detection of protocol violations within a topology design, even if these interferences are not caused intentionally or the attacks comes from radio jamming [10].

ISBN: 978-988-14047-1-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Fig. 6. RTL-SDR Receiver.

VIII. Hacking With SDR

Nowadays, radio communications are employed by both security and care services in each country, leading to be a great scope for hackers, or even a cracker, with the aim of finding bugs and alter operating systems for whether intermediate or end-user equipment [12]. An attacker can interfere with the communications systems of agencies responsible for national or civil security causing unquantifiable damage. An example of this could be a military drone manipulated by frequency blocking or by changing GPS coordinates with the goal to intercept it, using HackRF and BladeRF [13]. It is important to consider certain relevant features, such as frequency range for transmission or channel bandwidth when executing the implementation of these devices [12] (see Table I).

TABLE I
Feature Comparison of SDR Devices

	Freq. Range (MHz)	Bandwith (MHz)	ADC (Bits)	Comments
Funcube	0.150-260 410-2050	0.192	16	RX Filters
HackRF	1 to 6000	20	8	RX/TX
BladeRF	300-3800	40	12	RX/TX
USRP B200-B210	70-6000	56	16	RX/TX
SockRock Ensemble II	0.180-3	0.192	Sound card	RX/TX Filters
Airspy	24-1750	10	12	RX Filters
SDR Play	100-380 430-2000	8	12	RX Filters

When signal is received, GNU Radio is used to decode data packet. After analysis, bytes were from reverse engineering and then were able to convey their own data packets to control unmanned aircraft. For example, a jamming attack can interfere communications between an aircraft and an airport control tower, so information could be gather from its path to change the course before landing. It is also define a RTL-SDR attack for stealing accounts or identity of a user via radio communications or mobile devices. A RTL-SDR attack will be based on tuning a communication antenna for the GSM band to capture traffic that is convey and then decrypting it with rainbow tables, achieving to steal the identity of an end-user located within the same radio zone [11].

IX. Conclusion

SDR system applications using USB receivers to capture digital signals whether TV or radio, helps to establish a better communication among several radio amateurs or hobbyist. By using USB DBV-T technology, it can be set receiver mechanisms for video signal or even make some learnings about GSM network hacking. To make a good use of these devices, it should be considered to review feature specifications, either frequency or bandwidth, in order to do a better analysis of an FM signal spectrum, packet data or throughput.

Working with low-cost devices plus a few lines of programming (in any language, e.g., MATLAB or Simulink, widely used in academia), students or hobbyist can build small telecommunication laboratories, being this a didactic element to help the understanding of theoretical concepts of abstract nature.

References

[1] D. García G., José M. Riera S., P. García. “Implementación y configuración de un receptor de radio definido por software (SDR) para estudios de propagación”. Universidad Politécnica de Madrid. XXVI Simposium Nacional de URSI, ISSN 978-84-6954-327-6, 2012.

[2] J. Amador F., N. Alonso T., “RDS (Radio Definido por Software). Consideraciones para su implementación de hardware”, Revista Telem@tica Vol. 12. No. 2, mayo-agosto, 2013, p. 56-68.

[3] S. Bimbi, Vitor C. Oliveira and G. Bedicks . “Rádios Definidos por Software com aplicações GNU Radio”. Set expo Procedings- Setep v. 1, 2015. ISBN 2447-049x.

[4] Pinar D. Ivan, Murillo F. Juan. “Laboratorio de Comunicaciones Digitales Radio Definida por Software”. Departamento de Teoría de la Señal y Comunicación. Universidad de Sevilla.

[5] P. E. Colla “Apuntes sobre Radio Definida por Software.” Radio Club Córdoba, Córdoba-Argentina.

[6] J. Vignolo, “Introducción al procesamiento digital de señales”. Ediciones Universitarias de Valparaíso. Pontificia Universidad Católica de Valparaíso, ISBN 978-956-17-0426-8. 2008.

[7] J. M. Hernando Rábanos, “Transmisión por radio” 6ta Edición, Editorial Ramón Areces. ISBN 84-8004-856-5.

[8] U. Ladebusch, C. A. Liss, “Terrestrial DVB (DVB-T): A broadcast technology for stationary portable and mobile use”. Proceedings of the IEEE, Vol. 94, No. 1, January 2006.

[9] C. Sufitchi, “Detecting meteor radio echoes using the RTL/SDR USB dongle”.

[10] C. A. Balanis, “Antenna Theory: Analysis and Design”, 2nd Edition. New York, John Wiley & Sons, 1997.

[11] W. Stewart, W. Barlee, S. W. Atkinson, H. Crockett, “Software Defined Radio using MATLAB & Simulink and the RTL-SDR”. 1st Edition. UK: University of Strathclyde, 2015.

[12] E. Grayver, “Implementing Software Defined Radio”. Springer. ISBN-13:978-1441993311. 2012.

[13] A. K. Ghosh, “Introduction to Control Systems”. 2nd Edition, India, 2014.

ISBN: 978-988-14047-1-8
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)