Journal of Alasmarya University: Basic and Applied Sciences
Vol. 6, No. 5, December 2021, Special Issue for Forth Conference on Engineering Science and Technology (CEST-2021)
مجلة الجامعة الأسمرية: العلوم الأساسية والتطبيقية
المجلد 6 ،العدد 5، ديسمبر 2021، عدد خاص بالمؤتمر الرابع للعلوم الهندسية والتقنية (CEST-2021)

Implementation of FM Receiver/Transmitter and Smart Keyless Car Using GNU Radio Companion with HackRf One

A. F. Abdullah[1,*], A. I. O. Hamoudah[2], O. S. Alarnout[3], M. A. Abouqadh[4]

[1]*Azzaytuna University, Tarhunah, Libya, a.abdullah@azu.edu.ly*
[2]*College of Electronic Technology, Tripoli, Libya, os2127145@gmail.com*
[3]*College of Electronic Technology, Tripoli, Libya, malarnaot@gmail.com*
[4]*College of Electronic Technology, Tripoli, Libya, abdofoad4055255@gmail.com*

ABSTRACT

Software Defined Radio (SDR) is a technology that supports full-features of instructions to deal with and simulate the digital and analog communications. The SDR systems encompass the platform of networked series of the Universal Software Radio Peripheral (USRP) providing a complete stand-alone radio system to acquire and process large portions of the RF spectrum. Therefore, HackRF One device can be used as either receiver or transmitter. This device has sample rate reaches up to 20 MS/sec, and operating frequency works at the range from 1MHz to 6 GHz. It is a suitable candidate for providing the SDR features. The SDR has the capability for writing custom routines in a variety of programming languages, for example Python or C++. This paper aims at implementing the receiver using HackRf one with GNU radio companion to demodulate and hear to single and/or multiple FM channels systems. Subsequently, this structure is used at the transmitter side to send files or recorded voice. This paper also explores the concept of securing the Smart Keyless Cars, which use radio frequencies to lock and unlock doors, it is done by firstly receiving or picking up the tuned frequency, saving it, and then transmitting it via Hackrf one to open or close the target door.

Keywords:

Software defined Radio.

GNU radio Companion.

HackRf One.

[*]Corresponding Author Email: a.abdullah@azu.edu.ly

1 INTRODUCTION

The radio transmitter and/or receiver deploys a technology that permits software to modify or set radio frequency (RF) functions such as the types modulation scheme, output power, or bandwidth, changes for operating parameters at the duration of pre-determined and preinstalled radio process, therefore, this system can support the reconfigurability in frequency [1]. Signal Processing is the fundamental part of presenting any communication system. Communication requires much cabling and wiring, as MOD-BUS, PROFI-BUS, CAN-BUS, Ethernet etc; which is expensive in both installation and management. To overcome that, wireless communication is adapted as an alternative as wireless Ethernet, which eliminates the cabling issue and decreases the cost of maintenance. Once the decision between wired or wireless communication is made the decision-making does not stop here, the decision is to choose a suitable scheme among various wireless techniques [2]. A Software

ISSN: 2706-9524 (Print) ISSN: 2706-9532 (Online)

Defined Radio (SDR) is recognized as one of these advanced wireless technologies. Using SDR technology provides a compactness in the size of circuits leading to less complexity and enhancing SNR. However, wireless communication may face some obstacles, which are as follows:

- The standards of commercial wireless network are constantly evolved starting from 2G to current generations. Every generation of wireless networks varies meaningfully in the link layer protocol standards to cause issues to subscribers [2].
- It is more expensive to migrate from one to other generations of wireless networks.
- The European wireless networks use time division multiple access (TDMA) based, while the USA standards are code division multiple access (CDMA) based. This generates an issue to the subscriber in terms of global facilities deployment [2].
- The limitations of deployment appear not just in the period of roaming but also during rolling-out other new features. The implementation of radio functions enabled by SDR contributes to overcoming all these issues in the infrastructure of network, for instance software modules. This simply helps to migrate from one generation to other even in roaming period [2].

In 2001, the hardware of SDR technology was as computers and buses of data instead of IF/RF frequencies [2]. While in 2005, a proposed study was conducted about the transformation of digital quadrature for generalizing SDR schemes. Therefore, one of those studies was able to reduce the sampling speed twice, while the other can minimize both sampling speed and output data rate [2]. The modern applications of radio communications applying SDR such as Radar, signal intelligence, and electronic warfare were developed in 2012 [2]. This provides the availability to implement SDR transceivers; consequently, wireless communication has become the hottest field and SDR is revolutionizing it in 2013. Many open sources as USRP and GNU Radio were utilized. In 2015, the GNU Radio was used as a simulation tool for driving the SDR transceiver hardware [2].

2 PRINCIPLES OF SOFTWARE DEFINED RADIO

A software-defined radio (SDR) system uses software for the modulation and demodulation of radio signals. This radio signal can be programmed through a software platform in order to implement multiple radio functions, meaning computer with SDR software platform as GNU Radio companion or High Definition Software Defined Radio (HDSDR) plus hardware as SDR devices can be implemented as shown in Figure 1. It can be seen that antenna is a part of this system used for transmitting radio signal, drone, satellite, and any remote key that works at a single frequency [3]. The goal of using SDR system is to generate a radio, which can receive or send a new radio protocol configuration by running new software. The SDRs have a substantial use for services regarding to cell phones, which serves variety of changing radio protocols in real time. A super heterodyne RF front end is used in SDR for converting RF signals from/ to analogy RF signals, and vice versa.

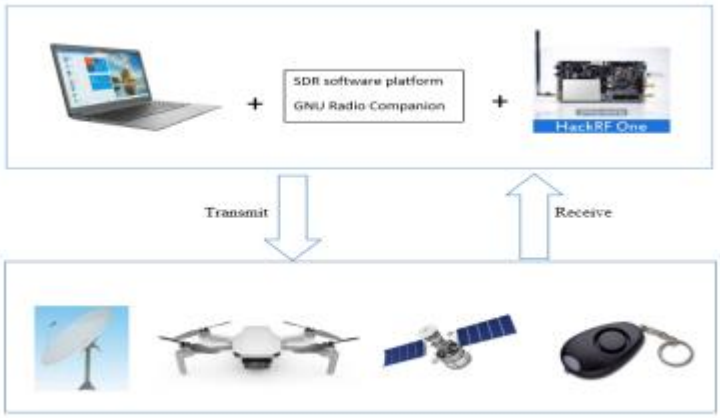


Figure 1. SDR platform with mutliple radio functions

This receiver is traditional and performs three operations: A carrier frequency that is adjusted to choose the desired signal, the filter stage is used to null out undesired signals, and lastly amplification for compensating the attenuated power is utilized. The purpose of amplification is to amplify the attenuated signal to meet the acceptable level for the demodulator circuitry [4,5]. Figure 2 demonstrates the super-heterodyne receiver, which is a type of radio receiver that uses frequency mixing to convert a received signal to a fixed intermediate frequency (IF) which can be more conveniently processed than the original carrier frequency.

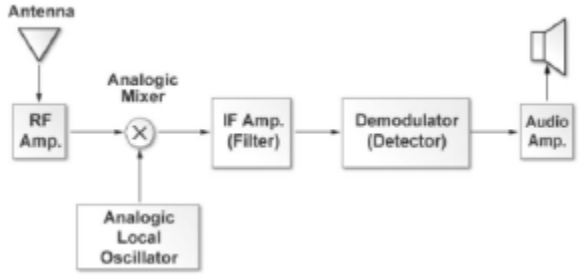


Figure 2. Internal blocks of superheterodyne reciever [6

As seen from Figure 2, the antenna picks up the weak signal (RF signal) and feeds it to RF amplifier. This amplifier provides some initial gain and selectivity. The output of the RF amplifier is applied to the mixer input, which receives also an input form the local oscillator to produce the difference of frequencies known as intermediate frequency (IF) and then signal is filtered to remove the effect of higher frequencies components. The signal is then amplified by one or more IF amplifier stages. The highly amplified IF stages is applied to detector circuits to recover the original modulating information. At the output, the detector circuit is fed to audio and power amplifier, which provide a sufficient gain to operate a speaker. Automatic Gain Control (AGC) circuit is an important key for this receiver, which is considered by RF and IF amplifiers and demodulation stage. The AGC is used to keep a constant output voltage level over a wide range of RF input signal levels. In addition, there is also automatic frequency control (AFC) circuit, which generates AFC signal that is used for

adjusting and stabilizing the frequency of the local oscillator [6]. For example, if the system is designed to receive a frequency modulation (FM) station at 100.7MHz and the IF is set to 10.7MHz, the local oscillator should be placed at 90MHz.The operation is known as down conversion. The following stage is a bandpass filter that attenuates every signal except a specific portion of the spectrum. A Common centre frequencies for the IF stage are 455 kHz and 10.7 MHz for commercial amplitude modulation (AM) and FM respectively. Likewise, for commercial FM, the bandwidth is approximately 100 kHz and for AM is above 5 kHz, consistent with the channel spacing that is 200kHz for AM and 10 kHz for FM [7]. At the end, the demodulator recovers the original modulating signal from the IF amplifier's output employing one of several alternatives. For example, for AM an envelope detector is used, and for FM a frequency discriminator is applied. Further processing of the signal is performed depending on the purpose for which the receiver is intended. In a common home radio, the demodulated output is passed to an audio amplifier that is connected to a speaker [6].

The SDR is defined as a collection of hardware and software technologies, which are implemented through modifiable software or firmware operating on programmable processing technologies. These devices include Field Programmable Gate Arrays (FPGA), Digital Signal Processors (DSP), and General Purpose Processors (GPP), programmable System on Chip (SoC) or other application specific programmable processors. The use of these technologies allows new wireless features and capabilities to be added to existing radio systems without requiring new hardware [6].

The SDR can currently be used to implement simple radio modem technologies. In the long run, SDR is expected to become the dominant technology in radio communications. The followings are some of the things that SDR can do that have not been possible before:

- It can be reconfigured; for example, the universal communication device would reconfigure itself appropriately for the environment. It could be a cordless phone one minute, a cell phone the next, a wireless Internet gadget the next, and a GPS receiver is the next.
- It can be quickly and easily upgraded with enhanced features. In fact, the upgrade could be delivered over-the-air.
- It can talk and listen to multiple channels at the same time.

New kinds of radios can be built that have never existed before. Smart radios or cognitive radios (CRs) can look at the utilization of the RF spectrum in their immediate neighbourhood and configure themselves for the best performance. For typical SDR process, let having a radio antenna station, which transmits an analog signal, this signal should be modulated through SDR hardware to be converted to digital signal internal the hardware SDR circuit, after that the signal is processed through real time digital signal processing applications. Figure3 (a) demonstrates the key knowledge of SDR structure and (b) and (c) represent the receiver and transmitter of SDR block diagram [2,7].

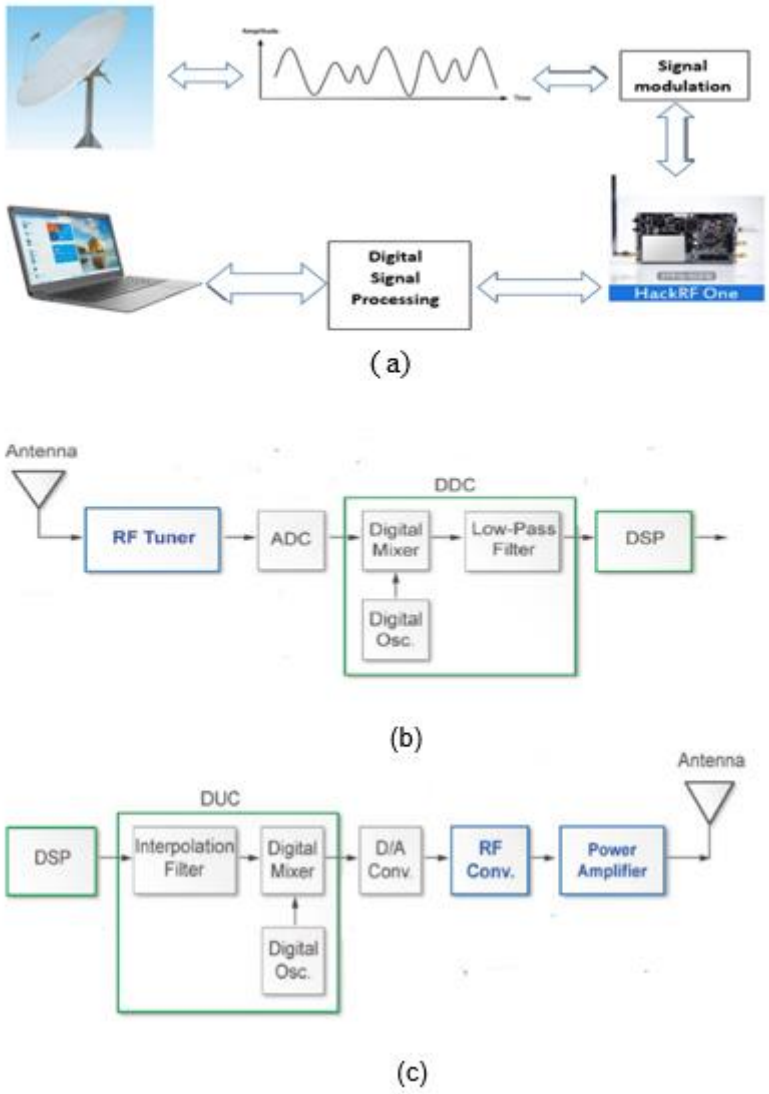


Figure 3: a) Key knowledge for SDR process, b) SDR receiver, and c) SDR transmitter [8].

For Figure 3 (b), at first, the RF tuner converts the analog signal to IF, performing the same operation that the first three blocks of the superheterodyne receiver can do. The IF signal is passed to the ADC converter in charge of changing the signal's domain, offering digital samples at its output. The samples are fed to the following stage's input which is Digital Down Converter (DDC). The DDC is commonly a monolithic chip and it stands as the key part of the SDR system. It consists of three main components: a digital mixer, digital local oscillator, and a Finite Impulse Response (FIR) low-pass filter. The components performance is similar to their analog counterparts. The digital mixer and the local oscillator shift the IF digital samples to baseband, while the FIR low-pass filter limits the bandwidth of the final signal. The DDC includes a high number of multipliers, adders and shift registers. Observing that the signals are transferred to their baseband equivalent at the digital mixer's output by the

disintegration into the I and Q counter phase components. If the tuning of the digital local oscillator is modified, the desired signal can be shifted away or towards the point where it reaches 0Hz. This variation, together with the bandwidth adjustment of the low-pass filter, defines which part of the reception is treated as a useful signal [8]. Another procedure, known as decimation, is commonly performed for reducing the sampling frequency or sample rate. Thus, the new sampling frequency in baseband is resulted from the division of the original sampling frequency by an N factor, called decimation factor. The final sample rate can be as little as twice the highest frequency component of the useful signal, as proposed by the well-known Nyquist theorem. Furthermore, practical approaches have shown that reduction can be applied up to an extra of 20% without significantly affecting the quality of the result [8]. This can be expressed numerically as is done in equation 1.

$$f_{b2} = 0.8 f_b = \frac{f_s}{N} \quad (1)$$

Where f_b is the baseband frequency, f_s is the sampling frequency, N is the decimator factor and f_{b2} is the new calculated baseband frequency after the decimation is applied. Finally, the baseband samples are passed to the Digital Signal Processing (DSP) block, where task such as demodulating and decoding are performed. For each SDR, it is important to compare the cost, frequency range, ADC resolution, and maximum instantaneous bandwidth as shown in Table 1, whether or not it can transmit, and if it has any pre-selectors built in. There are several SDR peripherals available in the market, the main features that one should take into account to make the right decision which are: capability to transmit, some devices are able to do it as apart from receiving side, frequency range that can be tuned, high bandwidths imply analyzing a huge part of the spectrum at once and more software decimation (better SNR), but it requires more Central Processing Unit (CPU) power.

There is also the sensitivity, means that the greater the sensitivity is the greater the ability to hear weak stations and produces higher SNR values. The ADC resolution is also an important feature as the higher the bit size of the ADC, the more accurate it can be when sampling. It has a direct proportion to the dynamic range and sensitivity. In addition, a high resolution implies a better ability to discern weak signals, less signal imaging and a lower noise floor. Dynamic range refers to the ability to receive weak signals when strong signals are nearby. It is strongly related with the ADC resolution and the DSP software processing [8,9]. When the dynamic range is not high enough, a strong signal can saturate the ADC, generating signal images and significantly reducing the receiver's sensitivity. This situation is known as "overloading" and it leaves no space for weak signals to be measured. System design, the number of lossy components that are part of the RF path affect the receiver performance. Noise and Interferences: The circuit board of the device should not generate interfering signals because those would be impossible to remove. Pre-selectors, as analog filters on the frontend that reduce out of band interferences and imaging. The device can switch between different pre-selectors depending on the tuned frequency [2,3].

Table 1 Comparsion of SDRs [4]

Name	Cost ($)	Frequency range (MHz)	ADC Resolution bits	Max Bandwidth (MHz)	Communication Mode	Pre-selectors
R820T RTL2832U	10-22	24-1766	8	3.2/2.4	Rx only	R820T
Airspy R2	169	24-1750	12	10	Rx only	R820T
HackRF One	299	1-6000	8	20	Half-duplex	NON
LimeSDR	299	0.1-3800	12	61.44	Full-duplex	NON
BladeRF	420-650	300-3800	12	28	Full-duplex	NON

3 PRINCIPLES OF HACKRF ONE

The HackRF One is an SDR device that has the capability to digitize the RF signal. It oprates at frequencies between 1MHz and 6GHz, this range of frequencies provides the applications of Bluetooth, FM radio, near-field communication (NFC), and cellular technology. HackRf One links with the computer to perform SDR process, such as GNU Radio Companion (GRC). The HackRf one device supports half-duplex mode service [7].

HackRF one could be used to virtually implement different technologies such as: AM/FM radio, Bluetooth, ZigBee, or WiFi. HackRF One can also be full duplex if two HackRF devices are used together. At the receiver side the RF signal is received by HackRF One and then internally converted to digital signal (form of samples), the digital signal is then proceeded to further DSP processing. However, in case of using HackRF One as a transmitter, the digital signal is internally converted to analogy signal, and connected to power amplifier in order to increase the strength of the created signal to be able to propagate for long distance [9]. The circuit components can be explained as follows:

- Xilinx DS311 XC2C64A: it is FPGA, which is designed for high-end communication applications with low power consumption and high reliability. It has over 30 input/output ports, and fast communication between pins (4.6ns delay between each other).
- NXP LPC432OFBD144: It is a combination of ARM M4 processor and MO co-processor that is designed for DSP embedded system applications.
- MAXIM MAX5864: It is a combination of Ultra-low power analog to digital (ADC) converter and (DAC), this module handles the sampling of received analog signal and converting internally produced signal.

- MAXIM MAX 2837: It is wireless broadband transceiver (2.3-2.7 GHz), it is ideal for 4G/LTE system application. It includes programmable low pass channel filter at the receiver form 1.75 MHz to 28MHz and anti-aliasing filter at the transmitter.
- Si 5351: it is clock signal generator that can generate up to 8 non-integer related frequencies form 2.5kHz to 200MHz. It can replace crystal oscillator, voltage controlled oscillator (VOC) and phase locked loop (PLL). It has low power consumption.
- RFFC 5072: It is a combination of PLL and wideband synthesizer (VOC) with the range from 85MHz to 4200MHz.
- ANT 500: It is the antenna that is connected to HackRf One with operation range from 75 to 1000 MHz, in this case the system avoids using an amplification to prevent over power situation and possible damage to the amplifier as there is no filter between the antenna and amplifier [10].

Figure 4. HackRf One Circuit

4 IMPLEMENTATION AND RESULTS

In this paper, the simulation using GNU radio companion with Hackrf One is performed to receive RF signal, which allows implementing an SDR and providing graphical support. For this paper, the GNU Radio companion runs under Windows 10. In this way, a wide range of frequencies can be easily captured, filtered, or otherwise modified in real time. The GNU Radio supports different platforms of hardware such as HackRf One, which requires an installation of the gr-osmosdr. It supports a huge frequency range including high frequency (HF), very high frequency (VHF), and ultra-high frequency (UHF) bands. Hence, various techniques can be simulated using this device such as: AM/FM radio, Bluetooth, ZigBee, or WiFi. In [11], it is explained that the process for implementing SDR system can be performed by using Hackrf one as a hardware which is linked to the computer with GNU

radio companion software to process the received RF signal, demodulate it and then display the results as well as hear the received channel as shown in Figure (5).

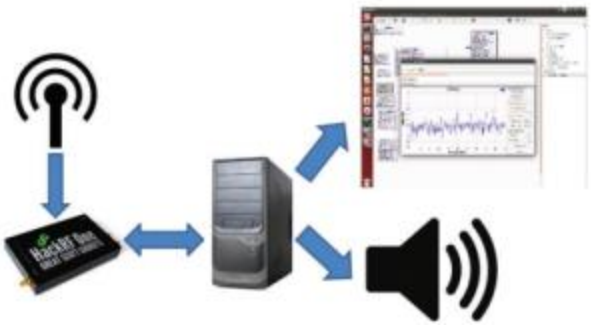


Figure 5. Simple structure of proposed system [11].

A frequency modulation (FM)-based signal is received and demodulated. In this type of modulation, the modulating signal is proportional to the variation between the carrier and its center frequencies. The FM possesses better fidelity and noise immunity, thus it is heavily used in FM radio broadcasting. The FM radio broadcasting approximately ranges between 88 and 106 MHz. The target of this section is to listen to some of these commercial FM channels. In this design, the Hackrf One is installed to work on windows system and programmed using GNU radio companion (GRC) via graphical block diagrams interface. HackRf One also has the capability for supporting dual and multiple FM received signals. The design is developed to receive a local FM signal at frequency of 88.8 MHz. Figure 6 shows the GRC flow graph of FM radio receiver. It presents the blocks of HackRf One, rational resampler, wideband FM receive/demodulator, low pass Filter, and audio sink.

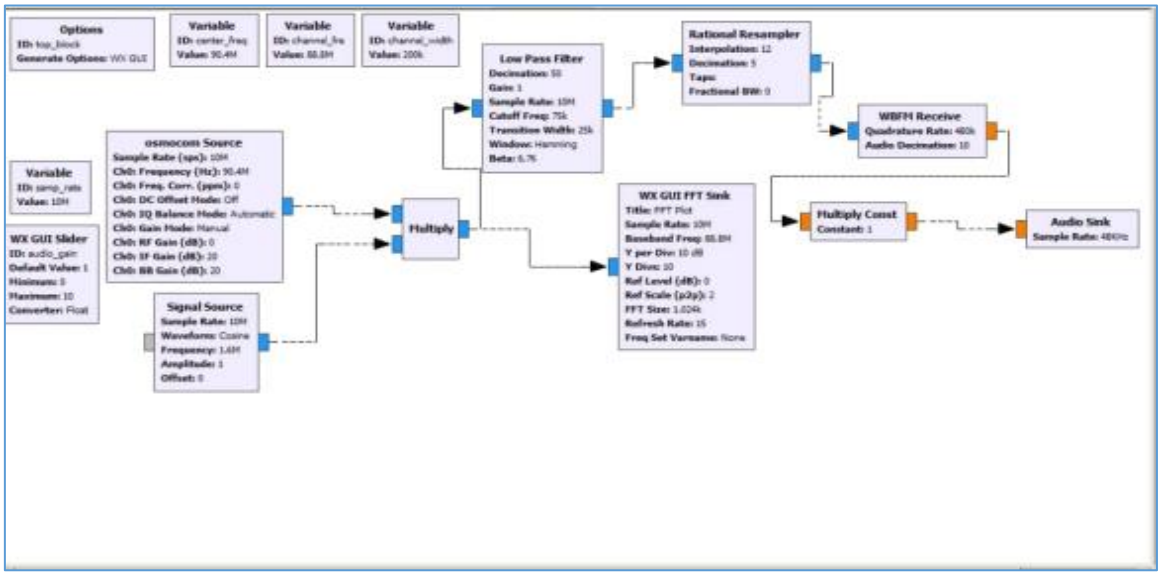


Figure 6. FM Radio Receiver GRC Flowgraph.

The Osmocom Source is the block that communicates with the HackRF hardware and provides signal from the hardware for further processing. The sample rate and frequency band

IF gain can be set in the Osmocom Source block. The WX FFT (Fast Fourier Transform) Sink displays the received signals in the frequency domain. The frequency of the received FM radio signal can be set according to the multiplication term of the frequency in Osmocom Source (f_1) and the frequency of the signal source block (f_2). The received FM signal will be at $f_1 - f_2$.

Rational Resampler usually performs interpolation and decimation function to vary/adjust the sampling rate. The received signal from the Hackrf One source block is decimated by five times. The decimation is a way to get more bits out of ADC, for example, the sampling rate decreases from 10Msps to 0.48Msps, by doing so, an extra bit out of ADC is gained. Decimation has to be done carefully as using wrong decimation leads to overlapping of signals of interest with its neighbouring signals. It performs filtering operation, thus only the signal of interest is allowed through LPF. Before decimation in Rational Resampler, a low pass filter is used to select the WBFM signal of interest. The typical bandwidth of WBFM radio station is about 200 KHz, by decimating it by five the bandwidth is multiplied by five times. Since LPF cut-off frequency is measured for only one side of the bandwidth, the cut-off frequency is set to 75 KHz.

The transition width of LPF defines the sharpness of our filter, therefore, the smaller the transition width, the greater the CPU time consumed for doing calculations. Here, the transition width is set to 25 kHz, which almost utilizes 100% of the CPU and the filter functions faster. The sampling rate is set to 10MHz. In this design, demodulation operation is performed on the received signal. Quadrature rate is varied to indicate the rate at which the demodulated signals are passed out. The quadrature rate is set to 480 KHz because 0.5 Msps is the sampling rate after decimation. The audio decimation is also set to 10 as it decreases the 0.5 Msps decimated signal to 50 KHz audio output signal, which can be easily converted to 48 KHz, which is used in soundcards. Figure 7, demonstrates the results obtained by the previous implementation, and the FM channel received is the common local channel in Libya (88.8 MHz).

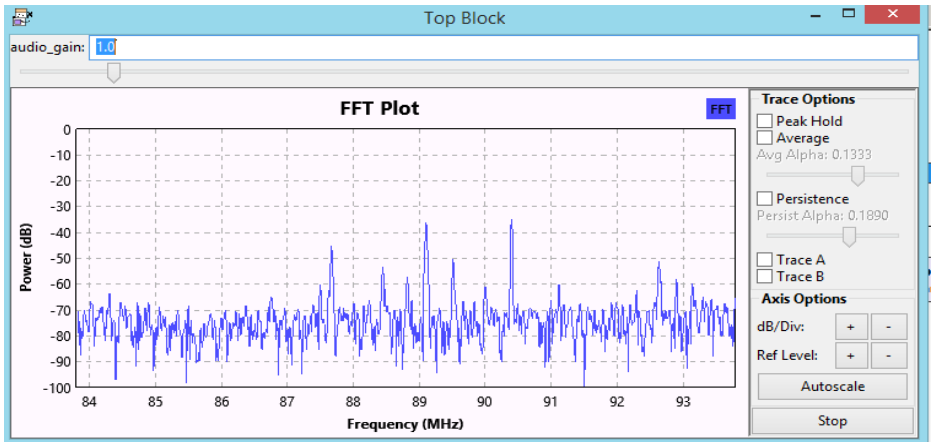


Figure 7. Receive Local FM radio Channel at 88.8 MHz

It is also possible to receive several FM stations concurrently by duplicating the FM signal receiving blocks and adding the received signals before sending them to the Audio Sink. Such capability can be useful for a multi-station monitoring system. Figure 8 shows how to receive two channels concurrently. This can be applied for several channels due to the HackRf One has an advantages of the reconfigurability. Figure 9 represents the FFT sink extracted FM local signals with frequencies 88.8 MHz and 97.7MHz respectively.

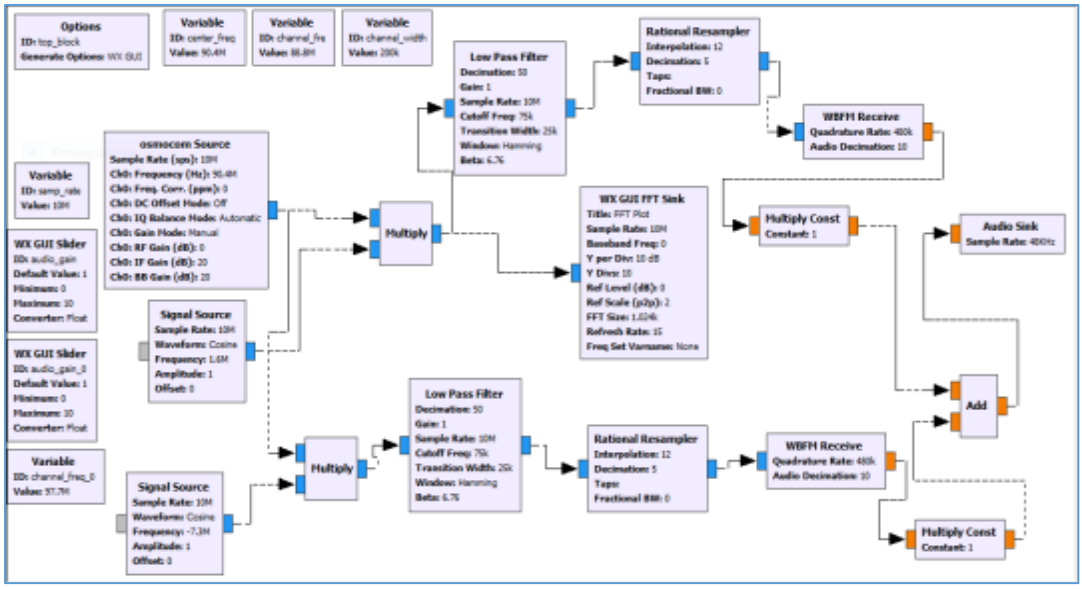


Figure 8. Implementation of dual FM channels concurrently

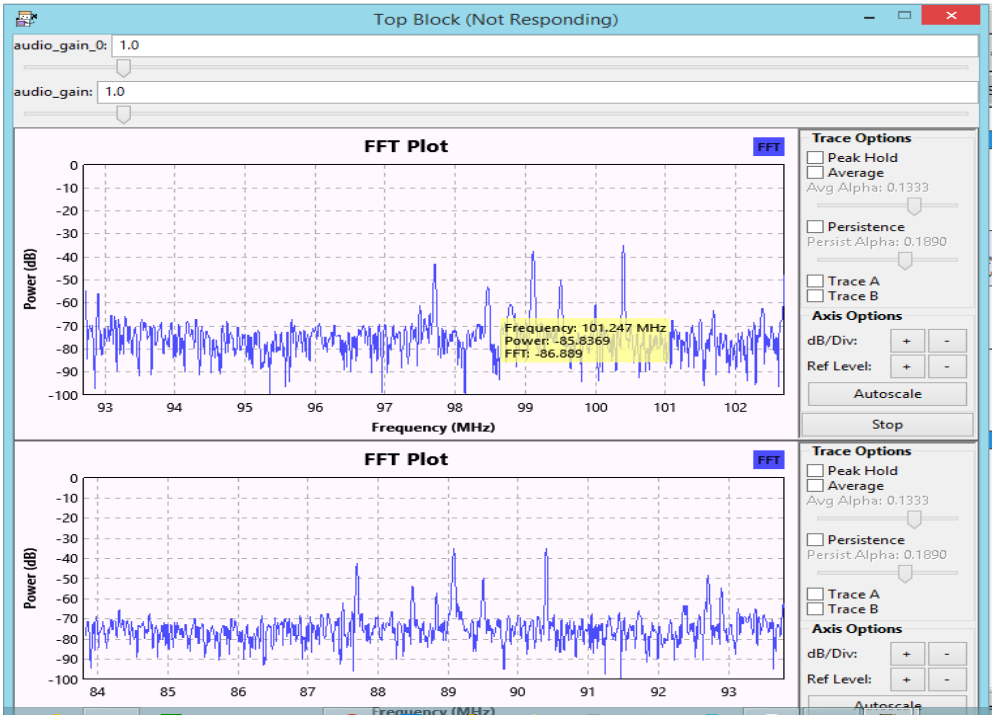
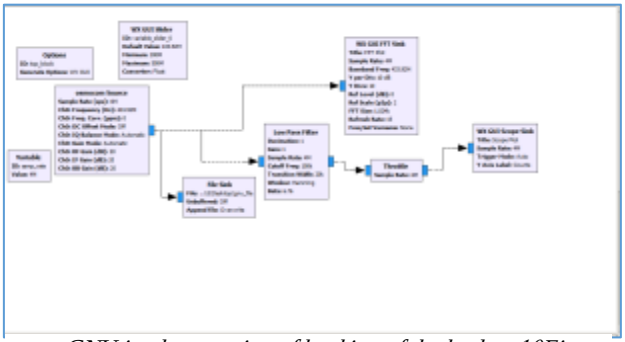


Figure 9. Receive dual local FM channels at 88.8 and 97.7 MHz respectively.

The traditional key method of locking and unlocking the door of the car required manually inserting the key in the lock. This method was impractical and being disappeared. To ease it, a concept of keyless cars is introduced [12]. An external RF hardware can be attached to the computer and the GNU Radio provides the interface to perform the logical implementation using these radio frequencies and signals. The first step is to capture the radio frequencies of the key [12]. Figure 10, explains the flow graph, which is used to capture the frequencies. The ID is set to the top block and the generate options is set to WX GUI, which is a type of frequency graph for the graphical user interface. These are the basic and default parameters, which are set in the GNU Radio Companion. The Osmocom source is an abstraction layer, which supports communicating with different hardware devices for software radio. Furthermore, it is a source, which produces digital signals that will be consumed by the next block in the flow graph. This tells the HackRf One to switch to the receiving mode via the USB. It has different parameters as the sample rate, which has been specified in the earlier stage. The channel frequency of the approximated signal and the car is also specified, which is set to 433.92 MHz. The RF gains are set to 0 to avoid any errors. In case of WX GUI Waterfall Sink: it is the graphical user interface for the user, which will show a graphical structure and show the details of the frequencies that are being emitted at every second by the rates of 2 MHz. Different parameters are defined such as the center frequency which is set to 0Hz by default and the bandwidth for the flow graph is set to 2MHz which is kept as the same for the sample rate. The captured frequencies are further stored in a file format in the computer using HackRF One and GNU Radio Companion which are based on the technology of Software Defined Radio. The peak denotes the captured frequency of the car key

as shown in Figure 10.

Replaying the captured frequencies directly on the car. Throttle Block: This is the block to define the frequencies and emit them equally and repeatedly on the car to match the required frequency to crack the lock as show in the implantation of Figure 12. Figure 13 demonstrates that the identical picked frequency (433.92 MHz) is obtained as that one received by the



. GNU implementation of hacking of the keyless 10Figure smart car

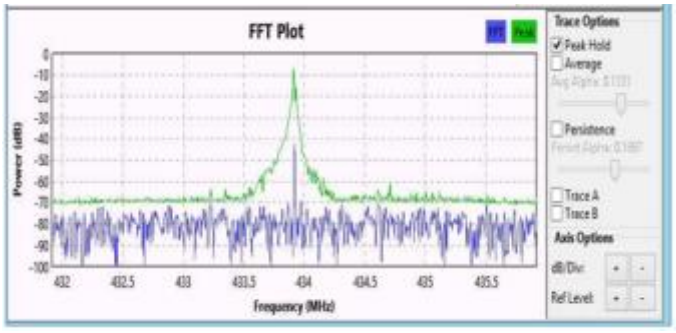


Figure 11. captured frequency of the car key.

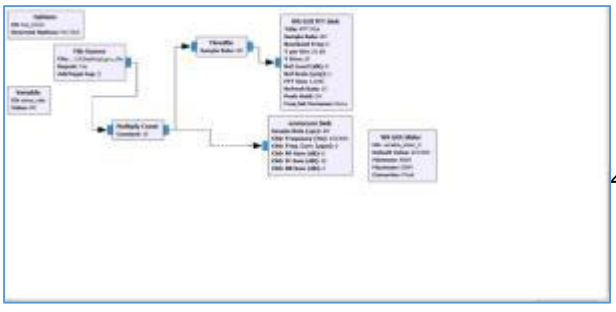


Figure 12. Use captured frequency (433.92 MHz) to open the car.

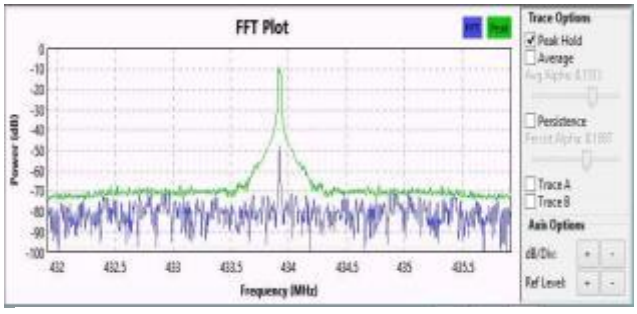


Figure 13. Identical result of captured frequncy to open the car

HackRF one. The HackRF is capable of half-duplex operation, thus it can be set as a transmitter as well. The low pass filtered output of the audio source signal will go through a resample process and WBFM Transmit for the FM modulation before being sent to the SDR hardware (Osmocom Sink) for RF transmission. For Figure 14 a, three simulations can be done, it can be used for sending a file such as music, voice, etc. It can also be used to transfer any random signal via HackRF One at a particular FM channel frequency as in this example 90.1 MHz is set, when you tune it in the radio at the car or mobile you can directly hear what you have sent as in Figures 14 b and c. Practically, this was tested and give a suitable SNR with 500 m^2. This implementation is also used for noising any channel by broadcasting your file or speech using the identical frequency as shown in the following figures.

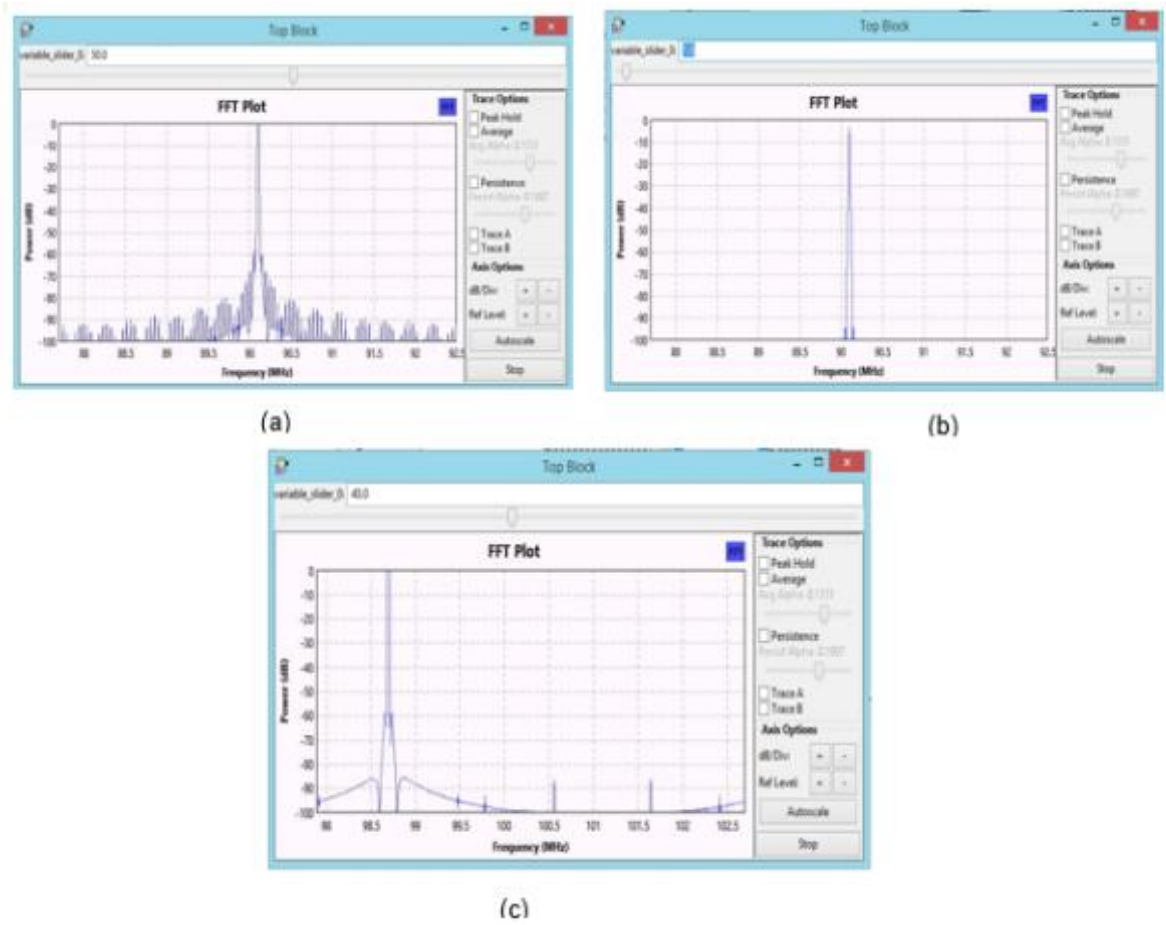


Figure 14. a) Transmission of voice over local FM channel at 90.1MHz, b) Power of voice received at 90.1 MHz, c) speech overlapping to disturb licenced FM channel at 98.7 MHz.

5 CONCLUSIONS

The main contribution of this paper is to investigate the performance of SDR system with HackRf one as a hardware and GNU radio companion. The low cost of SDR HackRF One can be a good platform for implementing Wireless communication system. Receiving the frequency with different operational parameters, and different modulation techniques is possible with SDR. In this paper, various FM local channels are received and properly extracted as a single captured frequency or multiple one. This leads to that the Hackrf One is

flexible enough to be programmed as spectrum analyzer, FM receiver and transmitter and hacking. Therefore, form the results, HackRF One with GRC can be used as receiver, transmitter to send a file or overlapping with any frequency to disturb any local FM channel within a particular area of coverage, based on the test made, the possible range is $500m^2$. However, in terms of security, hackRF one shows how the man in the middle attacks or replaying attacks on the cars and vehicles using tools and techniques and frequency capturing by.

For further study, it is recommended that, the electronic devices that are used for security, they should have more techniques of encryptions in the higher layers in order to be not simply attacked by this device. On the other hand, this device provides better performance for setting up and broadcasting on any FM frequency which is kind of frequency reconfigurability. Therefore, there is still a need for searching for the other advantages that this device supports.

6 REFERENCES

[1] A. Jayanthiladevi and G. M. Kadharnawaz, Introduction and Applications of Software-Defined Radio. In *Introduction to Cognitive Radio Networks and Applications*, 2016, pp. 47-58.

[2] S. Jahnavi., C. B. Pooja, L. F. Santro and R. Vijayageetha, Implementation of Wide Band FM Receiver on RTL-SDR. *International Journal of Engineering Research & Technology (IJERT)*, 2016, 5(05).

[3] F. K. Jondral, Software-defined radio—basics and evolution to cognitive radio. *EURASIP journal on wireless communications and networking*, 2005(3), 1-9.

[4] J. D. J Rugeles , E. P. Guillen, and L. S. Cardoso, A Technical Review of Wireless security for the Internet of things: Software Defined Radio perspective, 2020, *arXiv preprint arXiv:2009.10171*.

[5] K. VonEhr, W. Neuson and B. E Dunne., Software defined radio: choosing the right system for your communications course. In *2016 ASEE annual conference & exposition*.

[6] J. R. Machado-Fernández, Software defined radio: Basic principles and applications. *Revista Facultad de Ingeniería*, 2015, *24*(38), 79-96

[7] M. Gummineni and T. R Polipalli, Implementation of reconfigurable transceiver using GNU Radio and HackRF One. Wireless Personal Communications, 2020, pp. 1-17

[8] M. J. Raúl. "Software defined radio: Basic principles and applications." Revista Facultad de Ingeniería 24.38 , pp79-96, 2015.

[9] M. L. Anand, *Principles of Communication Engineering*, 2021.

[10] M. Abirami, et al ,Exploiting GNU radio and USRP: an economical test bed for real time communication systems. *fourth international conference on computing, communications and networking technologies (ICCCNT), 2013,* (pp. 1-6).*IEEE*.

[11] D. Barrio, A. Alberto, et al. "HackRF+ GNU Radio: A software-defined radio to teach communication theory." *The International Journal of Electrical Engineering & Education* :0020720919868144, 2019

[12] Y. M. Kenia, Cyber Attacks on Smart Cars using SDR,2019.

تنفيذ مستقبل / مرسل القناة الترددية (FM) وسيارة ذكية بدون مفتاح باستخدام رفيق راديو جنو مع HACKRF

عبدالعاطى عبدالله[1،*]، عمر حموده[2]، محمد الارنووطي[3] ، عبدالرحمن ابوقدح[4]

[1] جامعة الزيتونة، ترهونة، *ليبيا*، *a.abdullah@azu.edu.ly*
[2] كلية التقنية الالكترونية، طرابلس، ليبيا، *os2127145@gmail.com*
[3] كلية التقنية الالكترونية، طرابلس، ليبيا، *malarnaot@gmail.com*
4 كلية التقنية الالكترونية، طرابلس، ليبيا، abdofoad4055255@gmail.com

الملخص

يعد الراديو المحدد بالبرمجيات (SDR) تقنية لدعم الميزات الكاملة للتعليمات للتعامل مع الاتصالات الرقمية والقياسية ومحاكاتها. تشتمل أنظمة SDR على منصة من سلسلة شبكية من Universal Software Radio Peripheral (USRP) التي توفر نظامًا لاسلكيًا كاملًا قائمًا بذاته، والحصول على أجزاء كبيرة من طيف الترددات الراديوية ومعالجتها. لذلك، يمكن استخدام جهاز HackRF One كجهاز استقبال أو جهاز إرسال، وله معدلات عينة تصل إلى 20 مللي ثانية / ثانية، ويعمل تردد التشغيل من 1 ميجا هرتز إلى 6 جيجا هرتز. إنه مرشح مناسب لتوفير ميزات حقوق السحب الخاصة. يمتلك SDR القدرة على كتابة إجراءات مخصصة في مجموعة متنوعة من لغات البرمجة، على سبيل المثال لغة بايثون أو سي ++.

تهدف هذه الورقة إلى تنفيذ جهاز الاستقبال باستخدام HackRf one مع رفيق راديو GNU لإزالة التشكيل والاستماع إلى أنظمة قنوات FM فردية و/أو متعددة. بعد ذلك، يتم استخدام هذه البنية في جانب المرسل لإرسال الملفات أو الصوت المسجل. تستكشف هذه الورقة أيضًا مفهوم تأمين السيارات الذكية بدون مفتاح، والتي تستخدم ترددات الراديو لقفل وفتح الأبواب ، ويتم ذلك أولاً عن طريق استقبال التردد المضبوط أو التقاطه وحفظه ، ثم نقله عبر Hackrf one لفتح أو إغلاق الباب المستهدف.

الكلمات الدالة:
الراديو المحدد بالبرمجيات (SDR).
رفيق راديو GNU.
HackRf One.

**البريد الإلكتروني للباحث المراسل:* *a.abdullah@azu.edu.ly*