SDR Receivers as a New Challenge to Cybersecurity Wireless Technology

Roman Bybyk[1], Ivan Opirskyy[1], and Mike McIntosh[2]

[1] *Lviv Polytechnic National University, Stepana Bandery str, 12, Lviv, 79000, Ukraine*
[2] *STEELCASE, 901 44th str. SE, Grand Rapids, MI 49508, USA*

Abstract

This article research which cybersecurity threats exist and what cyber-attack is, and what categories these threats are divided into, as well as what threats SDR receivers can be used for. Considered what an SDR receiver is. The SDR receivers themselves and the scheme of a modern SDR receiver are considered. The characteristics of several modern SDR receivers and their comparison in the price category were considered, and the best one was chosen among them. Examples of the block diagrams and schemes of modern SDR receivers were given, and the principle of operation of SDR receivers is described. Also in this article, 2 experiments with examples will be carried out, namely listening to GSM by means of HackRF and by means of the 'Wireshark' program.

Keywords

Software Defined Radio, Global System for Mobile Communications, cybersecurity, cyberattack, cyber threat I/Q, analog-to-digital converter.

1. Introduction

We're used radio systems everywhere. They're exist, as the separate receiving and transmitting devices, or are part of other devices such as GPS, mobile phone, laptop, router, etc.

The modern using of the radio devices requires unification of equipment, so that it can be used for different tasks and purposes. Currently, one of the promising areas improvement of telecommunications are - use of software-controlled radio stations (SDR - Software Defined Radio), the operation of which involves changing the operating parameters, using the principle of software control. This approach is designed to resolve the problem of compatibility of radios, that have different parameters, or belong to different hardware platforms. As follows, radios that support SDR technology must operate in the presence of several standards and multiple users.

Software Defined Radio (SDR) is a radio communication system where components that have been traditionally implemented in hardware (e.g. mixers, filters, amplifiers, modulators/demodulators, detectors, etc.) are instead implemented by means of software on a personal computer or embedded system.[1] While the concept of SDR is not new, the rapidly evolving capabilities of digital electronics render practical many processes which were once only theoretically possible. A basic SDR system may consist of a personal computer equipped with a sound card, or other analog-to-digital converter, preceded by some form of RF front end. Significant amounts of signal processing are handed over to the general-purpose processor, rather than being done in special-purpose hardware (electronic circuits). Such a design produces a radio which can receive and transmit widely different radio protocols (sometimes referred to as waveforms) based solely on the software used.

SDR technology has long been attractive to manufacturers, wireless operators and military services, as a single hardware platform can be adapted to the large number of waveforms that are added to software in the process. As a result, hardware elements such as filters, mixers, amplifiers, detectors, modulators and demodulators become unnecessary. At the same time, we get a multifunctional platform

CPITS-II-2021: Cybersecurity Providing in Information and Telecommunication Systems, October 26, 2021, Kyiv, Ukraine
EMAIL: romanbub3@gmail.com (R. Bybyk); iopirsky@gmail.com (I. Opirskyy); mmcintosshh@gmail.com (M. McIntosh)
ORCID: 0000-0002-9506-014X (R. Bybyk); 0000-0002-8461-8996 (I. Opirskyy); 0000-0002-8199-8073 (M. McIntosh)

that has a potentially many modes of operation and a set of frequency bands, switching between which is done automatically and dynamically in the technical part remotely [1].

2. Analysis of current cybersecurity threats

In the 1950s, the word “cyber” referred to cybernetics, science of understanding the control and motion of machines and animals. Next was word “cyber,” which means “computerized.” The word "cyberspace" mean reliable physical space, which for some people, existed for the electronic activities of computing devices.

Today, it may be actively used to describe information security questions [2-4]. Since it's hard to imagine how digital signals which passing through wire can represent an attack, we moved on to visualizing the digital phenomenon as physical.

A cyberattack is any offensive maneuver that targets computer information systems, computer networks, infrastructures, or personal computer devices. An attacker is a person or process that attempts to access data, functions, or other restricted areas of the system without authorization, potentially with malicious intent.

Cybersecurity threats fall into three broad categories of intent. Attackers seek espionage for financial gain or disruption (including corporate espionage - patent theft or state espionage). Virtually every cyber threat falls into one of these three modes. From the point of view of attack technique, malicious actors have a huge number of options. [5-7]

The following are the 10 most common types of cyber threats [7]:

1. Malware - software that performs a malicious task on the target device or network, such as data corruption or system hijacking.

2. Phishing - use fake communication, such as an email, to trick the receiver into opening it and carrying out the instructions inside, such as providing a credit card number. “The goal is to steal sensitive data like credit card and login information or to install malware on the victim’s machine,” Cisco reports.

3. Spear Phishing - a more subtle form of phishing, when an attacker learns about the victim and pretends to be someone he knows and trusts.

4. “Man in the Middle” (MitM) attack - occurs when hackers insert themselves into a two-party transaction. After interrupting the traffic, they can filter and steal data, according to Cisco. MiTM attacks often occur when a visitor uses an unsecured public Wi-Fi network. Attackers insert themselves between the visitor and the network, and then use malware to install software and use data maliciously.

5. Trojans - it is a type of malware that enters the target system, similar to one thing, e.g standard software, but then releases malicious code once in the host system.

6. Ransomware - an attack that involves encrypting data on the target system and demanding a ransom in exchange for allowing the user to regain access to the data.

7. Denial of Service attack or Distributed Denial of Service Attack (DDoS) - when an attacker takes over many (perhaps thousands) devices and uses them to call the functions of the target system, such as a website, which causes it to fail due to demand overload.

8. Attacks on IoT Devices - IoT devices, such as industrial sensors, are vulnerable to several types of cyber threats

9. Data Breaches - it is data theft by an attacker. The motives for data breaches are crime (IE theft of personal data), the desire to embarrass an institution (for example, Edward Snowden or DNC hacking) and espionage.

10. Malware on Mobile Apps - mobile devices are vulnerable to malware attacks, as are other computing devices

Cyber threats are never static. Most threats follow the standard structures described above. However, they are becoming more powerful. For example, there is a new generation of “zero-day” threats that can surprise security because they do not have digital signatures detected.

As for SDR (Software Defined radio), SDR can be used to threaten wireless communication in both receive and transmit mode. Depending on the capabilities offered by the hardware (such as operating frequencies) and the software that runs (including plug-ins). Attack vectors may also include the following possible SDR threats [8–12]:

- Sniffing – it is a method that the SDR performs in receive mode and affects the confidentiality of the transmission, whether it is only encrypted as long as the software is available. In addition to the message itself, we can also get: the identity of the sender and recipient, the moment of setting and disabling the transmission, the level of signal intensity, the type of modulation, the frequency band used, etc.
- Side-Channel Attack – it is a method that consists of collecting and analyzing information on physical parameters, such as noise or radiation, from integrated circuits during processing operations. The SDR in reception mode carries out this non-invasive attack, affecting the confidentiality of the transmission, which is very difficult to detect.
- Jamming – it is a forbidden service (DoS) attack in which the transmission is blocked either with acceptance or with the radiating end. In this case, the SDR reproduces radio frequency signals to introduce noise into the radio channel or channels used. This attack affects the availability of information.
- Spoofing – knowing the features of the communication protocol, it is possible to use an erroneous but valid signal using SDR for the attacked receiving equipment. It can possibly use an erroneous signal to send erroneous data or even enter malicious code to fully or partially control the receiver changing its performance, degrading transmission, or making it vulnerable to other attacks.
- Replay attack – using this attack, the SDR captures the transmission, copies it, and then forwards it. In this way, it can become a legitimate device (counterfeit) in the communication network or simply send copies, humiliating the connection or even causing a flood DoS attack.
- Flood attack – is a type of DDoS attack that aims to make a server inaccessible to legitimate traffic by consuming all available server resources.
- Re-injection attack – this is an attack similar ‘Replay Attack’, but in this case the message changes before being sent. Thus, the integrity and confidentiality of the transfer is violated.

SDR receivers and their construction

In a traditional superheterodyne receiver, signal processing is performed entirely by electronic circuits (see Figure 1). The signal frequency is reduced to an intermediate frequency (RF), after which processing is performed. The first SDR receivers used an ADC instead of a demodulator. Demodulation and partial filtering of the signal was performed in a signal processor. Modern ADCs are much faster, so DSP can perform more functions. For DSP to work, need to know the amplitude and phase of the signals. The received signal is divided into two components: in-phase (I) and quadrature (Q), shifted by 90˚ [7].

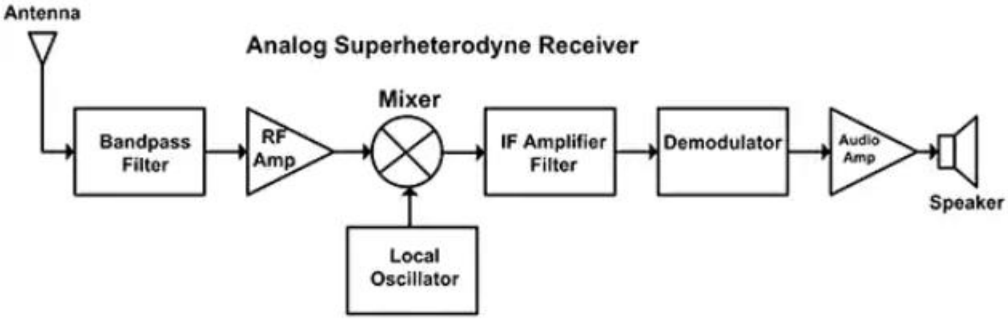


Figure 1: Block diagram of superheterodyne reception

The scheme of a modern SDR-receiver is shown in Figure 2. The input signal is amplified by a low-noise amplifier and divided into components I and Q by mixing with the local oscillator signal (to obtain a quadrature component, there is an additional phase shift of 90˚). The local oscillator frequency is adjusted to the signal frequency so that the difference between the output signals of the mixers is zero in the absence of modulation. For a modulated signal, it will be equal to the output modulated signal. This method is called direct conversion or conversion with zero intermediate frequency [7].

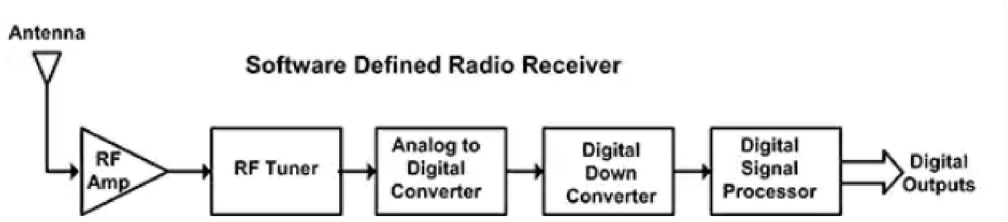


Figure 2: Scheme of a modern SDR receiver

In modern transmitters, the DSP modulator separates the components transmitted to I and Q and transmits them to the boost converter (see Figure 2) and the DAC.

The signal is filtered and fed to the mixer to increase the frequency to the transmission frequency. Then the signal passes through the amplifier and is fed to the antenna. As the speed of the converters increases, the scheme becomes simpler. The latest models are a filter and a low-noise amplifier. Commercial receivers use up to 30 MHz band. The digital method performs the following functions: filtering (LF, HF, band and notch filters), modulation (AM, FM, QAM, OFDM, etc.), demodulation, equalization, compression and recovery, spectrum analysis.[5]

New types of modulation and related procedures have the general term "waveform". After changing the software, the radio is switched to a different frequency and transmission protocol. The advantage of SDR is the simplicity of the hardware. Standard radio frequency circuits are reduced to a minimum, their cost is reduced. The signal processor takes over most of the functions that were previously performed in analog circuits. This approach is very successful, given the flexibility of software implementation and the ability to compensate for some unwanted effects that occur in the hardware. Moreover, the software implementation allows you to eliminate continuity, change and supplement the functionality of the device and improve its performance with minimal cost. In particular, SDR allows you to quickly add new types of modulation, transmission protocols and more. In the case of hardware implementation, this would require the production of a new scheme. There are also disadvantages to SDR. The first is the complexity of the software, development costs, including time, higher power consumption and, in some cases, limited frequency range [5].

An SDR receiver is a universal device that can combine the functions of various other radio devices. Following the concept of SDR, the ideal SDR receiver should contain as few elements as possible. Today, there are many SDR receivers in the world, both expensive and cheap. Examples of SDR receivers are given in Table 1 [13].

More interesting in terms of price / quality is LimeSDR. The device costs $ 300, allows you to work with frequencies from 100 kHz to 3.8 GHz, has a 12-bit ADC, a sampling frequency of 61.44 MS / s and a bandwidth of 61 MHz, can receive and transmit a signal in full-duplex mode. That is, the device allows you to work with most interesting frequencies (Bluetooth, GSM, 3G, 4G, GPS, ZigBee, LoRa), except for 5.8 GHz. But it's not such a big loss, if at first you are not going to hack Wi-Fi or any wireless video transmitters [13].

Table 1.
Examples of SDR receivers

SDR	Frequency range	Frequency band	Sampling frequency	ADC/ DAC	Radio chip	Interface	Number of channels per transmission	Number of receiving channels	Price
HackRF One	1MHz-6GHz	20MHz	20MHz	8 bit	MAX5864, MAX2837, RFFC5072	USB 2.0	1	1	299$
Ettus B200	70MHz-6GHz	61.44MHz	61.4MHz	12 bit	AD9364	USB 3.0	1	1	686$
Ettus B210	70MHz-6GHz	61.44Mhz	61.44MHz	12 bit	AD9361	USB 3.0	2	2	1119$
BladeRF	300MHz-3.8GHz	40MHz	40MHZ	12 bit	LMS6002M	USB 3.0	1	1	420$ (650$)
RTL-SDR	22MHz-2.2GHz	3.2MHz	3.2MHz	8 bit	RTL2832U	USB 2.0	0	1	~10$
Lime-SDR	100kHz-3.8GHz	61.44Mhz	61.44MHz	12 bit	LMS7002M	USB 3.0	2	2	299$
Lime-SDR-mini	10MHz-3.5GHz	30.72MHz	30.72MHz	12 bit	LMS7002M	USB 3.0	1	1	159$

3. Principles of SDR receivers, and their application

The possibilities of using SDR technology are quite diverse. This can be a radio, transceiver, panoramic spectrum analyzer or SDR path of a traditional transceiver, which will significantly expand the capabilities of the latter.

Let's analyze what actions can be performed through SDR receivers:

- Interception of radio conversations – data on servicemen, etc., which have an SDR radio station and built-in global positioning systems (GPS), can be broadcast on the network so that all network correspondents, or only the commander, can know and even see on a real map of the area (when connecting a tablet or computer), where they are located.
- Configuration of the DRM transmitter – will need a good high-frequency RF antenna to receive DRM signals. A simple long wire in the attic can work well. An antenna with a magnetic loop can also be a good choice.
- GSM interception – the process of reverse code conversion (occurs by the recipient) to the form of the original symbolic system (specified by the sender), to obtain the original message.
- Experiments with LTE – measurement in mobile networks, currently only possible with expensive special devices, can be effectively performed by combining and adapting open source SDR tools. These methods allow academies to study mobile networks with moderate resources, as well as to study and optimize the health of these networks.
- Jamming – for now GPS is the most widely used and well-known example of a Global Navigation Satellite System, and since the system relies on GPS positioning to take the next step, it is important to understand GPS vulnerabilities and recognize threats such as jamming and counterfeiting. Data jamming and forgery can be openly purchased online for a low price. Software-defined radio (SDR) technology also takes flexibility and cost-effectiveness to a whole new level.

Based on the above list, let’s consider the example of listening to GSM using HackRF and Wireshark, as well as the second experiment with software generation and signal reception [14].

Regarding the first example of GSM listening, it is first we need to determine the frequency of the local GSM station ad determine the starting points using frequencies (the example shown in the figure below is constant channels at 952 MHz and 944.2 MHz—these frequencies will be the starting points) [15].

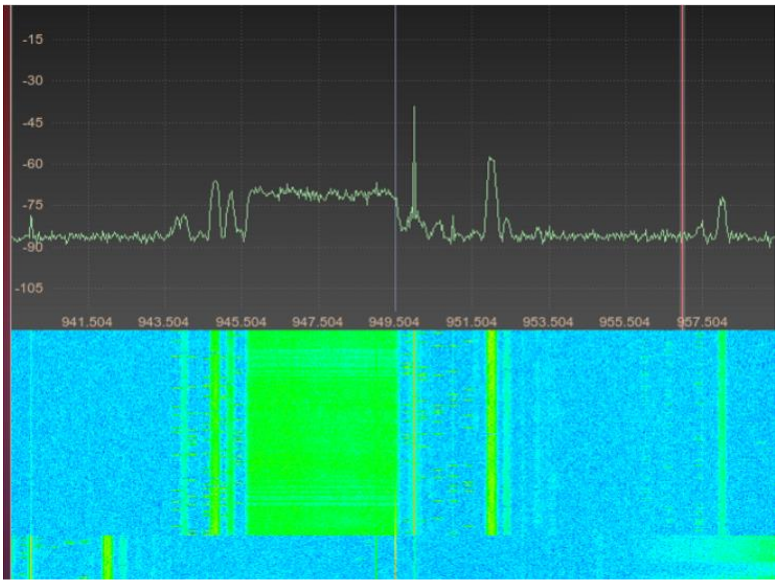
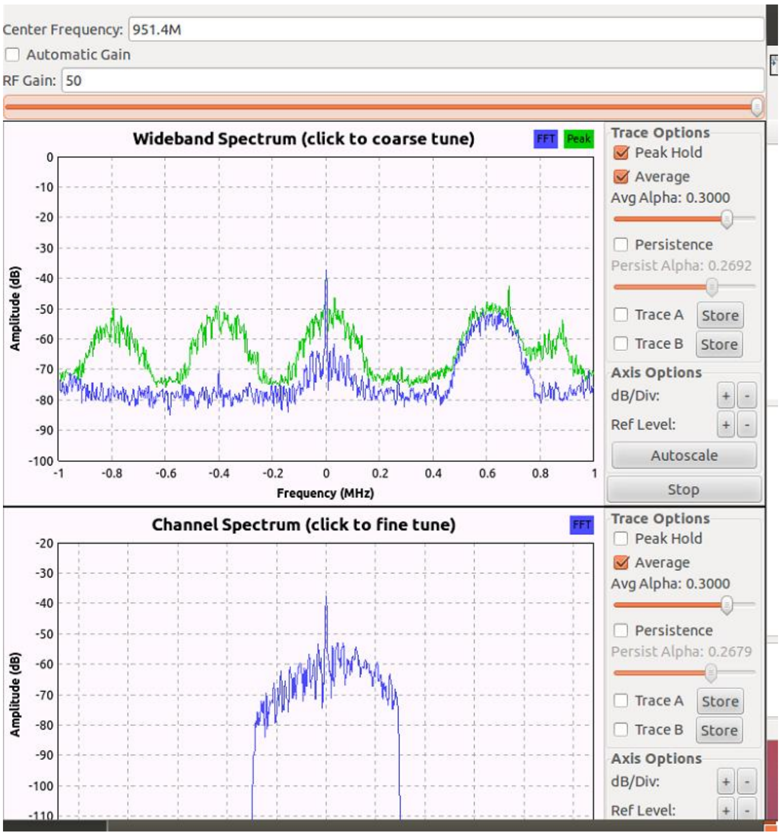


Figure 3: Determining the frequencies of starting points

After that, we need to enter the GSM frequency in the Wireshark as the midrange.



Center Frequency: 951.4M

□ Automatic Gain

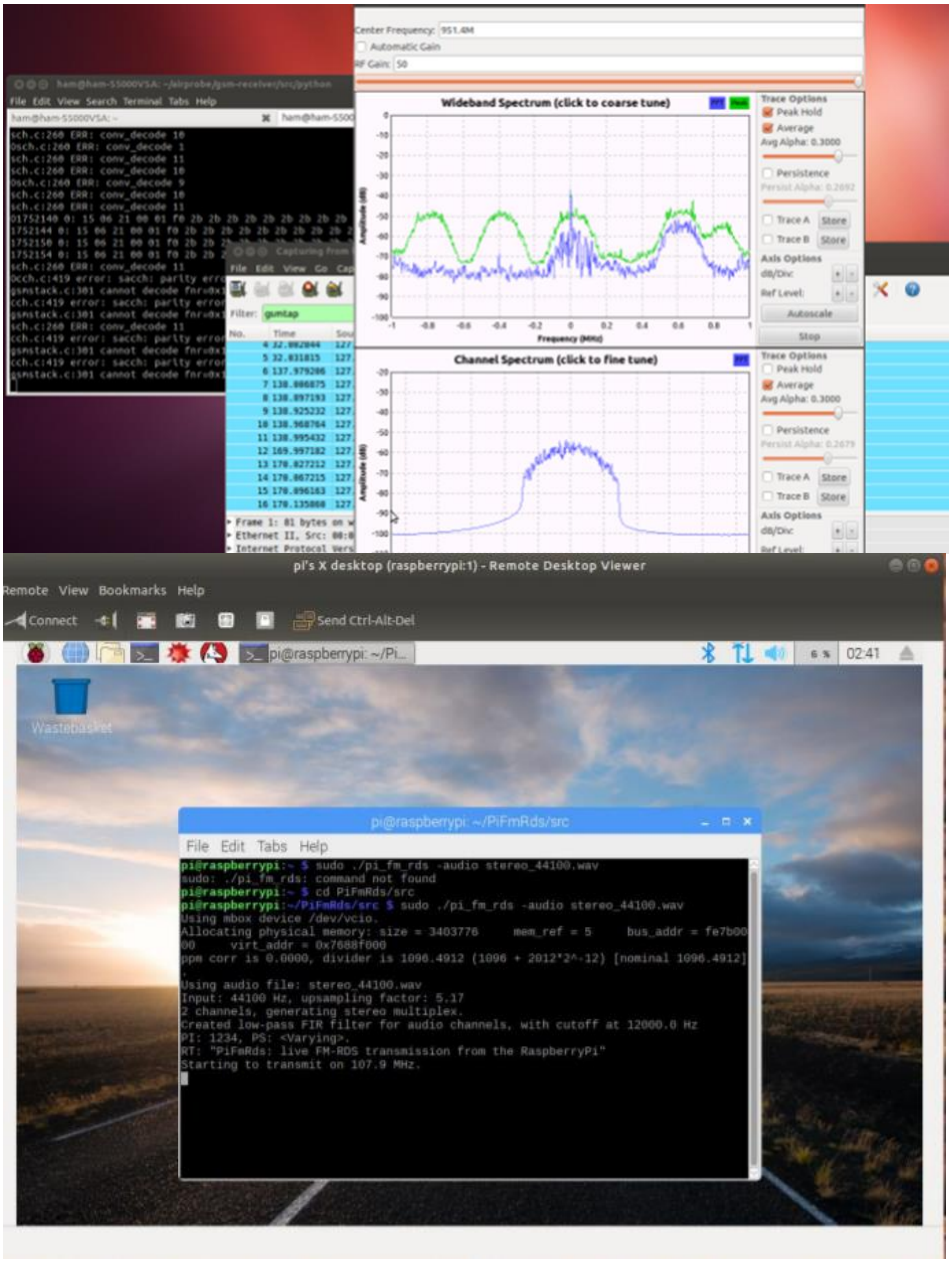
RF Gain: 50

Figure 4: Input of GSM frequency to the ‘Wireshark’ program

We will see that only the signal of the correct sequence (blue graph) sometimes exceeds the peak value (green graph), thus showing that it is a constant channel. Now you need to start decoding. In the window, we need to click on the middle of this frequency jump.

Now we can view that the gsm data comesto the 'Wireshark'. As mentioned earlier, the synchronized signal floats, so to maintain the specified frequency, you must continue to click on the circuit. As ridiculous as it may sound, but by wrapping the HackRF in a towel (or something similar), you will increase the thermal stability of the clock signal and reduce the scatter. This method probably will not seem very useful to you, but at least it shows the huge potential of HackRF

Regarding the second experiment with software generation and signal reception. The point of the experiment is to generate, transmit and receive a radio signal with the help of improvised means, software method, as well as to evaluate its characteristics. The purpose of the experiment is to estimate the time required to organize this type of communication and to assess the very possibility of such a connection.



```
sch.c:260 ERR: conv_decode 10
0sch.c:260 ERR: conv_decode 1
sch.c:260 ERR: conv_decode 11
sch.c:260 ERR: conv_decode 10
0sch.c:260 ERR: conv_decode 9
sch.c:260 ERR: conv_decode 10
sch.c:260 ERR: conv_decode 11
01752140 0: 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b
1752144 0: 15 06 21 00 01 f0 2b 2b 2b 2b 2b 2b 2b 2b 2b 2
1752150 0: 15 06 21 00 01 f0 2b 2b 2
1752154 0: 15 06 21 00 01 f0 2b 2b 2
sch.c:260 ERR: conv_decode 11
0cch.c:419 error: sacch: parity erro
gsmstack.c:301 cannot decode fnr=0x1
cch.c:419 error: sacch: parity error
gsmstack.c:301 cannot decode fnr=0x1
sch.c:260 ERR: conv_decode 11
cch.c:419 error: sacch: parity error
gsmstack.c:301 cannot decode fnr=0x1
cch.c:419 error: sacch: parity error
gsmstack.c:301 cannot decode fnr=0x1
```

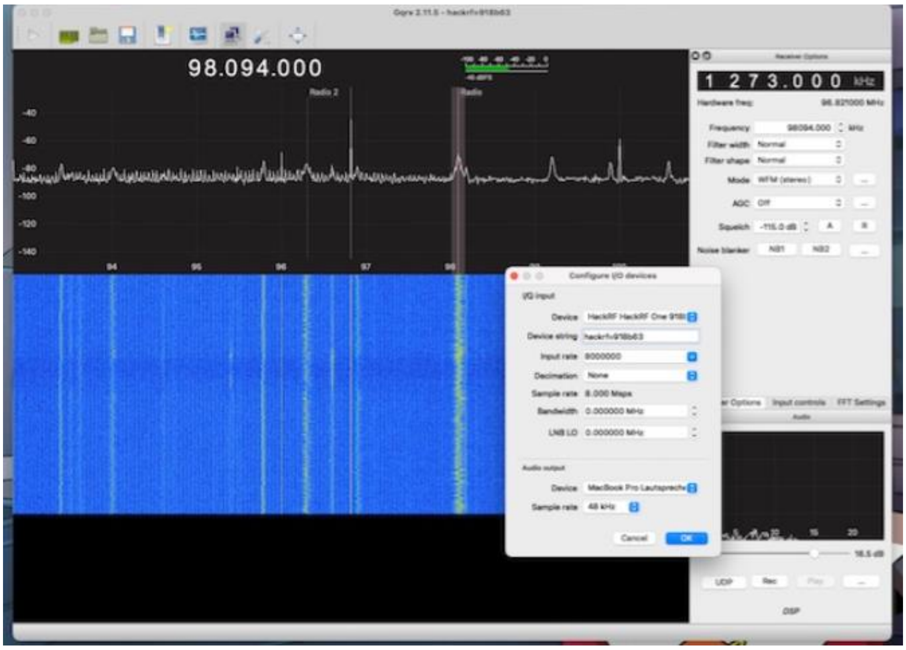
```
 4 32.802844  127
 5 32.831815  127
 6 137.979286 127
 7 138.886875 127
 8 138.897193 127
 9 138.925232 127
10 138.968764 127
11 138.995432 127
12 169.997182 127
13 170.827212 127
14 170.867215 127
15 170.896183 127
16 170.135868 127
▸ Frame 1: 81 bytes on w
▸ Ethernet II, Src: 00:0
▸ Internet Protocol Vers
```

```
pi@raspberrypi:~ $ sudo ./pi_fm_rds -audio stereo_44100.wav
sudo: ./pi_fm_rds: command not found
pi@raspberrypi:~ $ cd PiFmRds/src
pi@raspberrypi:~/PiFmRds/src $ sudo ./pi_fm_rds -audio stereo_44100.wav
Using mbox device /dev/vcio.
Allocating physical memory: size = 3403776     mem_ref = 5     bus_addr = fe7b00
00     virt_addr = 0x7688f000
ppm corr is 0.0000, divider is 1096.4912 (1096 + 2012*2^-12) [nominal 1096.4912]
.
Using audio file: stereo_44100.wav
Input: 44100 Hz, upsampling factor: 5.17
2 channels, generating stereo multiplex.
Created low-pass FIR filter for audio channels, with cutoff at 12000.0 Hz
PI: 1234, PS: <Varying>.
RT: "PiFmRds: live FM-RDS transmission from the RaspberryPi"
Starting to transmit on 107.9 MHz.
```

Figure 5: Getting GSM data in the ‘Wireshark’ program

As software that will act as a source of radio signal, was chosen open-source project PiFmRds, which allows you to frequently modulate audio files in .wav format, and accordingly change the voltage level on one of the 26 GPIO pins of the Raspberry 3. To the required port antenna was connected, in the form of a copper wire approximately 60 cm long. Now the emitted signal must be received and processed.

At the initial state of the experiment, since the radiation was conducted in the FM band, the desired signal was received by the FM receiver in the smartphone. The power of the Raspberry was enough to ensure that the sound quality did not fall at up to 100 m, provided there were no obstacles between the Raspberry and the phone. Since there was only a HackRF One receiver at hand, it was decided to use it. GQRX software has been installed on your computer - a graphical shell for GNU Radio.


Gqrx 2.11.5 - hackrf=918b63

98.094.000

Receiver Options

1 273.000 kHz

Hardware freq: 96.821000 MHz

Frequency 98094.000 kHz
Filter width Normal
Filter shape Normal
Mode WFM (stereo)
AGC Off
Squelch -115.0 dB

Configure I/O devices

I/Q input

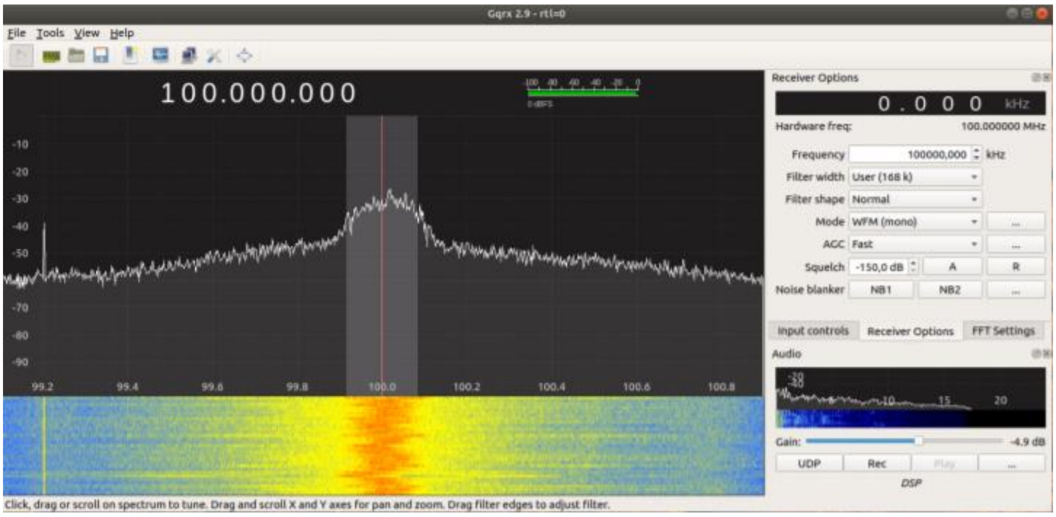
Device HackRF HackRF One 918
Device string hackrf=918b63
Input rate 8000000
Decimation None
Sample rate 8.000 Msps
Bandwidth 0.000000 MHz
LNB LO 0.000000 MHz

Audio output

Device MacBook Pro Lautsprecher
Sample rate 48 kHz

Figure 6: Selected device in the 'GQRX' program

Select the connected device and click "Start


Gqrx 2.9 - rtl=0

100.000.000

Receiver Options

0.000 kHz

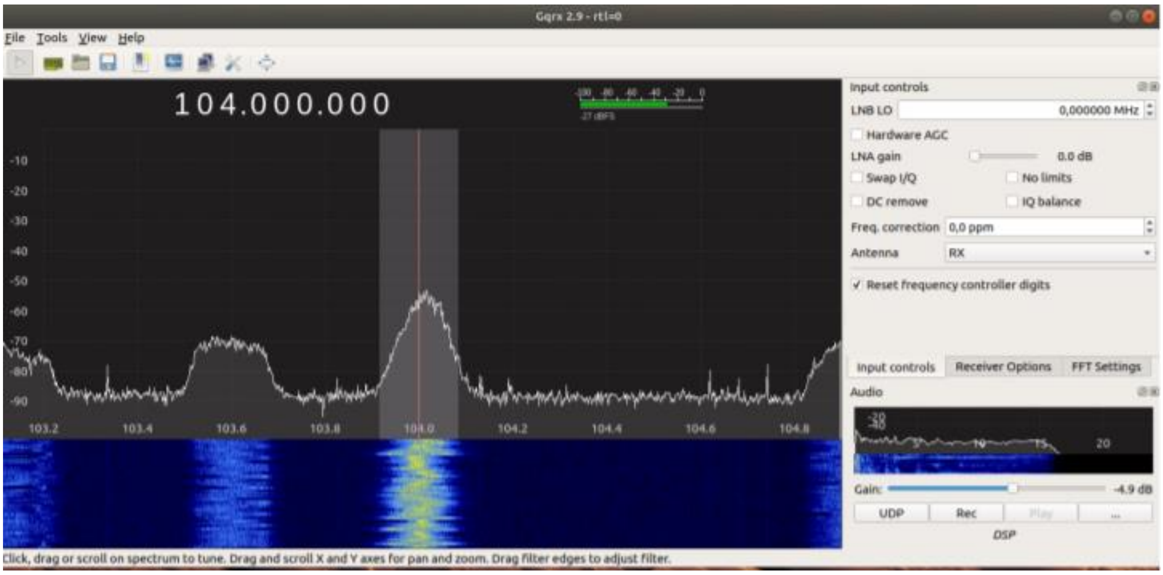
Hardware freq: 100.000000 MHz

Frequency 100000,000 kHz
Filter width User (168 k)
Filter shape Normal
Mode WFM (mono)
AGC Fast
Squelch -150,0 dB
Gain: -4.9 dB

Click, drag or scroll on spectrum to tune. Drag and scroll X and Y axes for pan and zoom. Drag filter edges to adjust filter.

Figure 7: Our FM station

We can see our FM station. The signal is quite strong due to the fact that the transmitter and receiver are at a distance of less than 1 m from each other. In addition, our station occupies a very wide frequency band, and the lack of filters is very well observed. Tuned to a standard FM station to check the correct operation of the receiver.



LNB LO 0,000000 MHz

LNA gain 0.0 dB

Freq. correction 0,0 ppm

Antenna RX

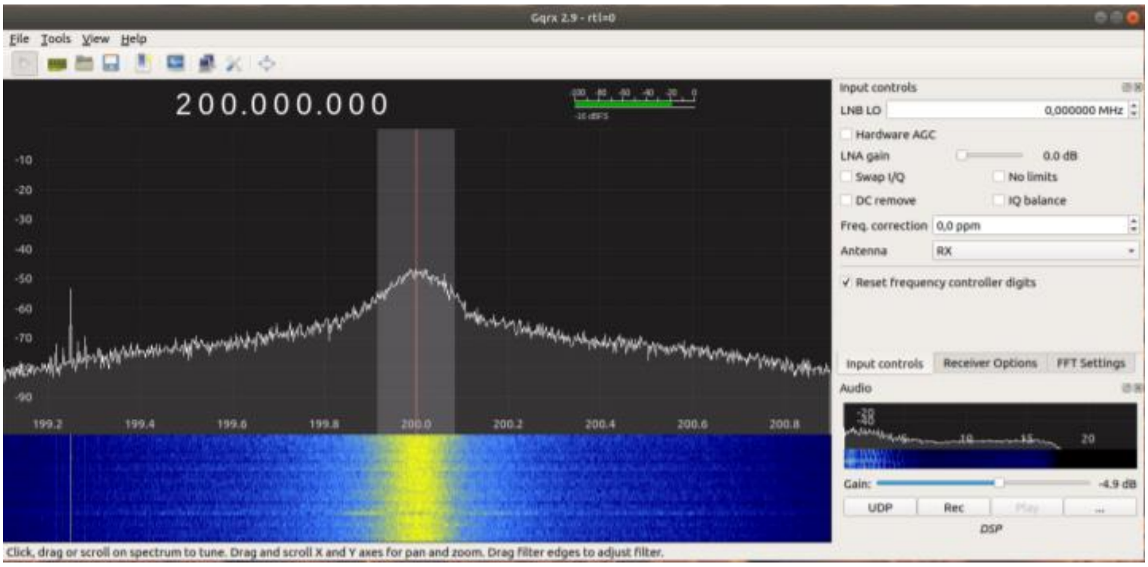
✓ Reset frequency controller digits

Gain: -4.9 dB

Click, drag or scroll on spectrum to tune. Drag and scroll X and Y axes for pan and zoom. Drag filter edges to adjust filter.

Figure 8: Our FM station

If we increase the gain of the receiver a little bit, we can see other radio stations even better.



LNB LO 0,000000 MHz

LNA gain 0.0 dB

Freq. correction 0,0 ppm

Antenna RX

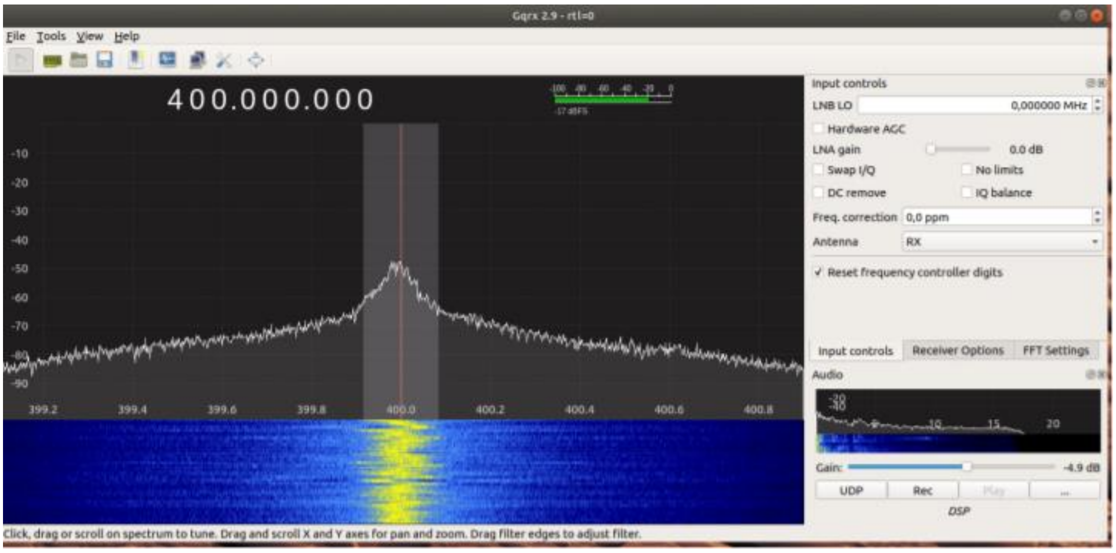
✓ Reset frequency controller digits

Gain: -4.9 dB

Click, drag or scroll on spectrum to tune. Drag and scroll X and Y axes for pan and zoom. Drag filter edges to adjust filter.

Figure 9: View of the other FM stations

Since the radio signal on the Raspberry doesn't pass through any filters, it was predicted very strong radiation on the harmonics of the main signal. As we can see, the predictions came true, and not only on the first harmonic, but up to 4.



Input controls

LNB LO 0,000000 MHz

□ Hardware AGC

LNA gain 0.0 dB

□ Swap I/Q □ No limits

□ DC remove □ IQ balance

Freq. correction 0,0 ppm

Antenna RX

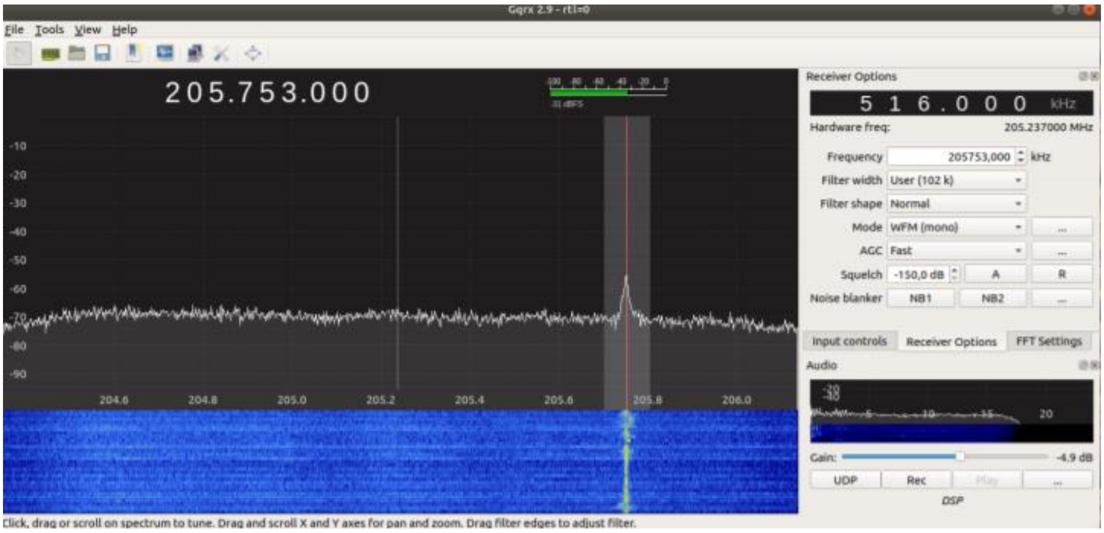
✓ Reset frequency controller digits

Gain: -4.9 dB

Click, drag or scroll on spectrum to tune. Drag and scroll X and Y axes for pan and zoom. Drag filter edges to adjust filter.

Figure 10: Radiation on the harmonics of the main signal

It turned out to be interesting that with the help of this receiver you can listen to the audio tracks of television:



Receiver Options

5 1 6 . 0 0 0 kHz

Hardware freq: 205.237000 MHz

Frequency 205753,000 kHz

Filter width User (102 k)

Filter shape Normal

Mode WFM (mono)

AGC Fast

Squelch -150,0 dB

Noise blanker

Gain: -4.9 dB

Click, drag or scroll on spectrum to tune. Drag and scroll X and Y axes for pan and zoom. Drag filter edges to adjust filter.

Figure 11: Soundtrack of the First National TV Channel

In this picture we can see the soundtrack of the First National TV Channel.
As a result, we can say that the experiment is successful and it turned out that for amateur purposes to organize SDR - communication is not something complicated and can be performed without going beyond ready-made solutions, and it does not take much time.

4. Acknowledgements

This article analyzes current cybersecurity threats and describes cyber threats. Possible SDR threats were also considered. The principle of operation of SDR devices, and also their schemes, namely "Block diagram of the superheterodyne receiver" and "Scheme of the modern SDR receiver" is considered.
Various examples of SDR receivers were considered and analyzed, and the best one (LimeSDR) was selected. SDR radio stands out as a flexible system in terms of hardware The purpose of SDR is that the user should communicate when he needs to, with whom he should do so, and in accordance with the protocol provided for this communication. The directions in which SDR receivers can be used and what can be done with SDR are considered. In addition, examples of how to work with SDR receivers

were shown, such as listening to GSM using HackRF and Wireshark, as well as a reception experiment with software generation and signal reception. Based on the experiments, we can say that these experiments are successful, and it turned out that for amateur purposes to organize SDR - communication is not something complicated and can be done without going beyond ready solutions, and it will not take much time. Many decisions have not yet been fully worked out.

5. References

[1] D. Gutierrez, et al., Present and demonstrate choices for measurement of 4G LTE access networks through open-source Software Defined Radio (SDR) tools, "Measurement of 4G LTE Cells with SDR Technology," 25–401.

[2] V. Lakhno, et al. "Management of information protection based on the integrated implementation of decision support systems" // Eastern-european journal of enterprise technologies. Information and controlling system, vol 5, no 9(89), 36–41, 2017. https://doi.org/10.15587/1729-4061.2017.111081.

[3] V. Dudykevych, et al., A multicriterial analysis of the efficiency of conservative information security systems // Eastern-european journal of enterprise technologies. Information and controlling system, vol 3, no 9(99), 6–13, 2019. https://doi.org/10.15587/1729-4061.2019.166349

[4] R. Banakh, A. Piskozub, I. Opirskyy, Detection of MAC Spoofing Attacks in IEEE 802.11 Networks Using Signal Strength from Attackers' Devices // 1st International conference on computer science, engineering and education applications, ICCSEEA 2018. – Kiev, Ukraine, 18–20 January 2018. vol. 754, 468–477, 2019. https://doi.org/10.1007/978-3-319-91008-6_47.

[5] R. J. Lackey, D. W. Upmal, A review of the SDR (Software Defined Radio) technology, including hardware schemes and application fields. A low performance device is presented and several tests are executed with it using free software "Speakeasy: the Military Software Radio," *IEEE* Software Defined Radio: Basic Principles and Applications Communications Magazine, vol. 33, p. 56-61, 1995

[6] B. Minick, Facing Cyber Threats Head On explains that technology is not the answer to cyber security issues. People, not technology, are behind emerging cyber risks "Facing Cyber Threats Head On: Protecting Yourself and Your Business," 60 –87.

[7] V. Giannini, J. Craninckx, and A. Baschirotto. Review of the SDR (Software Defined Radio) technology, including hardware schemes and application fields. A low performance device is presented and several tests are executed with it using free software "Baseband Analog Circuits for Software Defined Radio," 30–50, 2008.

[8] R. K. Sharma, D. B. Rawat, Advances on security threats and countermeasures for cognitive radio networks: A survey. IEEE Communications Surveys and Tutorials, 17(2), 1023–1043, 2015.

[9] A. Barron, includes sections on how different types of software defined radios work, the advantages of using them, and how they are tested. It also covers future trends including the development of Direct Fourier Conversion. "Software Defined Radio: for Amateur Radio Operators and Shortwave Listeners 1st Edition," 64–90.

[10] A. T. Tunggal, "What is a Cyber Threat?" https://www.upguard.com/blog/cyber-threat

[11] V. Buriachok, V. Sokolov, P. Skladannyi, Security rating metrics for distributed wireless systems, in: Workshop of the 8th International Conference on "Mathematics. Information Technologies. Education," Modern Machine Learning Technologies and Data Science (MoMLeT and DS), vol. 2386, 222–233, 2019.

[12] TajDini, M., Sokolov, V., Skladannyi, P., Performing Sniffing and Spoofing Attack Against ADS-B and Mode S using Software Define Radio, in: IEEE International Conference on Information and Telecommunication Technologies and Radio Electronics (UkrMiCo), 2021. https://doi.org/10.1109/ukrmico52950.2021.9716665

[13] TajDini, M., Sokolov V., Buriachok V., Men-in-the-middle attack simulation on low energy wireless devices using software define radio. Workshop of the 8th International Conference on "Mathematics. Information Technologies. Education," Modern Machine Learning Technologies and Data Science (MoMLeT and DS), vol. 2386, 287–296, 2019.

[14] J N. Haziza, M. Kassab, R. Knopp, Multitechnology vehicular cooperative system based on Software Defined Radio (SDR), Communication Technologies for Vehicles, 84–95, 2012.

[15] L. Xiao, et al., Reinforcement Learning-Based NOMA Power Allocation in the Presence of Smart Jamming. IEEE Transactions on Vehicular Technology, 67(4), pp. 3377-3389, 2018.