International Conference KNOWLEDGE-BASED ORGANIZATION
Vol. XXXI No 3 2025

SDR SYSTEM FOR REAL-TIME FHSS COMMUNICATIONS DETECTION AND JAMMING

Mirela ȘORECĂU*, George-Eduard POPA, Emil ȘORECĂU*, Paul BECHET***

***Technical University of Cluj-Napoca, Romania**
****"Nicolae Bălcescu" Land Forces Academy, Sibiu, Romania**
sorecau.mirela@armyacademy.ro

Abstract: *This study presents the development of a software-defined radio (SDR) system for automatically detecting frequency-hopping signals and generating targeted jamming on them. The system is set up on the GNU Radio platform, using an ADALM-Pluto transceiver and custom function blocks in Python. This includes an adaptive threshold detector designed to analyze noise level dynamics and trigger automated responses. Real-time detection of active frequencies allows for precise initiation of RF jamming sequences, making the solution effective in situations where a quick reaction is necessary. Validation was achieved through a series of laboratory tests using both simulated signals and real transmissions with frequency hopping rates of up to 1000 frequency hops per second. The experimental results show that the system reliably identifies spectral activity and can apply coherent and localized jamming in the vicinity of the directional antenna. The results show that the system can be used to monitor radio frequencies and to create electronic countermeasures (ECM) against frequency agile communications.*

Keywords: Frequency Hopping, Radio jamming, Software Defined Radio, GNU Radio, Spectrum monitoring

1. Introduction

Spread spectrum techniques are implemented to increase the robustness of communications against electromagnetic interference, intentional jamming and unauthorized interception. These methods involve spreading the useful signal over a significantly wider frequency band than is necessary to transmit information. Spreading can be accomplished by various schemes, the most common being direct sequence (DSSS), frequency hopping (FHSS), time hopping (THSS), as well as hybrid configurations combining these techniques [1]. Of these, frequency hopping offers the highest level of protection against directional jamming and eavesdropping and is thus preferred in military and security applications [2]. The method consists of rapidly varying the carrier frequency according to a pseudo-random algorithm synchronized between transmitter and receiver. In practical implementations, especially in the VHF and UHF bands, FHSS signals predominantly use frequency or phase modulation schemes, depending on the application requirements and radio channel conditions. The mathematical representation of frequency hopping signals is given by the expression [3]:

$$s(t) = \sum_{n=-\infty}^{\infty} p(t - nT)Acos[2\pi f_k + \varphi(t)] \quad (1)$$

where, p(t) = rectangular pulse with amplitude equal to 1, f_k = indicates the

DOI: 10.2478/kbo-2025-0093

carrier frequency used in the current interval, selected from a predefined set according to a hopping sequence and T = transmit duration at one frequency (dwell time).

Radio jamming is defined as the deliberate emission of electromagnetic signals intended to disturb, degrade or block the normal functioning of authorized radio communication systems by impairing reception at the target receiver.

In military applications, an advanced and effective form of jamming is repeater jamming (repeater jamming or follower jamming), which directly targets FHSS communications systems [4]. These systems pseudo-randomly modify the carrier frequency at short intervals, thereby reducing the probability of interception or interference.

A repeater jammer intercepts the radio signal, analyzes it in real time, and retransmits a jamming signal on the same frequency before the receiver completes the transition to the next frequency in the hopping sequence [5]. In more sophisticated scenarios, the jamming may include algorithms to estimate or identify the frequency sequence and hop rate, thus allowing future channel prediction and proactive jamming of the communication.

The effectiveness of the repetition jamming depends on two critical parameters of the target system: the hopping rate and the total number of frequencies available for hopping.

A higher hop rate significantly reduces the response window of the jamming, decreasing the chances of jamming success. In addition, a fundamental parameter of spread-spectrum systems is the processing gain, defined as the ratio of the bandwidth in which the spreading is realized to the bandwidth of the information signal [6]. A higher processing gain indicates higher resilience to interference. For example, the use of 50 frequencies spread over the entire range 30-88 MHz provides more effective protection against jamming than 200 frequencies spread over a narrow range, such as 30-40 MHz, due to the wider spectral coverage and the increased difficulty to jam the entire domain simultaneously.

To effectively use electromagnetic jamming, it is first necessary to monitor the spectrum in the desired band. This involves using a system that can detect and record active frequencies, including frequency-hopping signals. Intercepting these signals becomes much harder when the hopping rate is more than 1000 hops per second [7]. Commercial high-performance monitoring systems are often expensive and difficult to use in tactical environments because of their size and weight. Scalability and portability of these solutions pose significant challenges in the context of field operations. In this respect, a portable, low-cost solution capable of both complex signal reception and interference generation on the identified frequencies is required.

The SDR technology supports the development of such flexible, reconfigurable and easy-to-integrate systems in various scenarios through the GNU Radio framework [8-9]. This work is based on the ADALM-Pluto SDR platform, a low-cost device equipped with one receive and one transmit channel, operable in full-duplex mode [10]. The ADALM-Pluto platform is distinguished by its exceptional performance-to-cost ratio in the low-cost SDR category, in comparison to other devices such as RTL-SDR and HackRF One. Due to the required portability, data processing was implemented using a Raspberry Pi platform, and the display interface was implemented using a compact display that can be embedded in mobile applications. The developed receiver system is characterized by its complete mobility, allowing it to monitor and record the electromagnetic spectrum. Additionally, it can generate real-time jamming on previously identified frequencies.

2. Materials and Methods

Analog Devices' ADALM-PLUTO SDR (PlutoSDR), a compact and portable SDR transceiver based on the AD9363 chip, which provides bidirectional (TX/RX) functionality in a nominal frequency range of 325 MHz to 3.8 GHz, was used for radio signal acquisition and generation. The device has been software extended to operate within the 70 MHz to 6 GHz range for experimental purposes.

PlutoSDR facilitates an instantaneous bandwidth of up to 20 MHz, with the potential to extend up to 56 MHz in specific configurations. The primary means of communication with the host system is USB 2.0. The programming and control of the device was achieved through the utilization of either MATLAB/Simulink or the GNU Radio development environment, depending on the specific stage of the experimental process.

Table 1 Technical characteristics of SDR

Specification	Details
Frequency Range	325 MHz – 3.8 GHz (extended to 70 – 6 GHz)
BW	Up to 20 MHz
A/D and D/A	12-bit, 61.44 MSPS
Integrated SoC	ARM Cortex-A9 + FPGA
Maximum TX	~ +7 dBm
Interface	USB 2.0
Power Supply	5V via USB
Dimensions	96 × 61 × 19 mm

The previous table illustrates the technical characteristics of the SDR in question, while Figure 1 explains the primary hardware components.

Figure 1: ADALM-PLUTO detailed component view

An omnidirectional antenna, Schwarzbeck UBAA 9115, designed for free-field and laboratory measurement applications, was utilized for the reception of radio signals in the target band. It provides uniform horizontal coverage and is optimized for frequencies between 300 MHz and 1 GHz, with a characteristic impedance of 50 Ω and a typical gain of 0 dBi to +2 dBi in the specified range. The antenna is well-suited for the detection of low-intensity signals and is compatible with SDR equipment. In this study, the antenna is used in combination with PlutoSDR for radio spectrum monitoring.

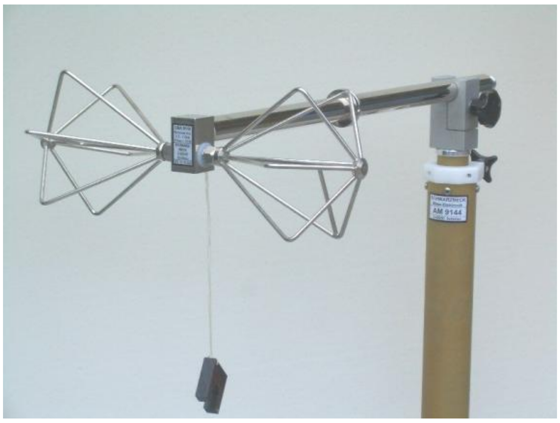

Figure 2: Schwarzbeck UBAA 9115 antenna

A HyperLOG7060 directional log-periodic directional antenna, manufactured by Aaronia AG, was utilized for the emission of jamming signals. The device under consideration covers a wide frequency range, extending from 700 MHz to 6 GHz. It is characterized by a high gain, with typical values ranging from 5 dBi to 8 dBi, depending on the specific frequency.

Figure 3: HyperLOG 7060 directional log-periodic directional antenna

The directional design of the antenna focused electromagnetic energy in a specific area, thereby enhancing the jamming efficiency and mitigating off-directional emissions. The antenna was mounted on an adjustable tripod and aligned in the direction of the target to maximize the controlled interference effect.

To create the RF signal processing and analysis application, the GNU Radio platform was used. This platform integrated several functional blocks, which are described below.

The PlutoSDR Source block allows the acquisition of radio signals from the ADALM-PLUTO transceiver. This block provides complete control over essential reception parameters including center frequency, sampling rate and bandwidth.

The Log Power FFT block is used to transform the signal from the time domain to the frequency domain, applying the Fast Fourier Transform (FFT) algorithm. The result is converted to a logarithmic scale (dB), which facilitates identification of predominant signals and noise level analysis.

Vector Source is a data generation block that outputs a defined sequence of values (vector), useful in testing or defining fixed conditions, such as frequency limits or masking certain bands.

The QT GUI Vector Sink block is used to visualize vector data in a static, graphical form. This feature enables the display of results in the frequency or time domain, thereby facilitating effective comparisons between signals and analysis of the spectrum at specific points in time.

The QT GUI Waterfall Sink is a graphical display of the spectrum over time in the form of a spectrogram (representation of the signal in three dimensions: time, frequency and power as a function of color).

The QT GUI Msg Push Button QT GUI block introduces an interactive control element into the application. It generates a message when pressed, which can be used to trigger actions in other blocks - such as resetting an output file or initiating a new analysis cycle.

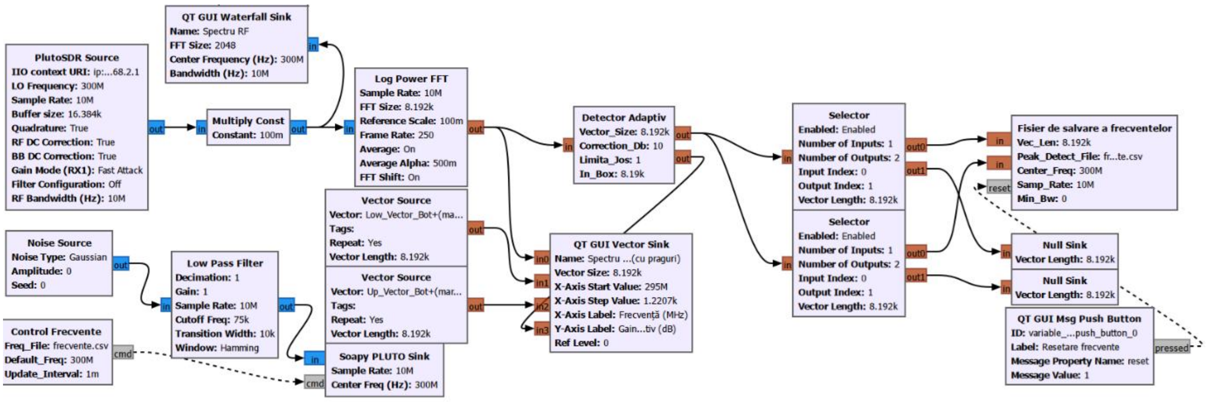

Figure 4: GNU Radio software implementation flowgraph

A substantial original contribution of this work is the development of two customized Python language blocks, integrated into the GNU Radio platform, that extend the standard functionality of the spectral analysis environment. The initial block, dedicated to adaptive thresholding, is founded on the 20th percentile principle and aims to identify the real-time average noise level in the analyzed RF spectrum. According to the established reference level, users are permitted to input an offset value measured in decibels (dB). This offset value serves to establish the effective detection threshold, thereby ensuring the identification of signals that significantly deviate from the background noise. The threshold undergoes continuous adaptation to ensure robust detection in dynamic environments, with the capacity to adjust to spectral variations.

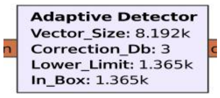

Figure 5: Adaptive thresholding block

The second block has been engineered to process signals that exceed the threshold, thereby providing advanced automatic analysis capabilities. This module is designed to calculate various metrics for each detected signal, including the center frequency, time of occurrence, bandwidth, and other relevant metadata. The extracted information is subsequently stored in a CSV file, enabling the user to undertake further analysis of the collected data or incorporate it into automated processing workflows. This approach enables the application to transcend the limitations of basic FFT visualization.

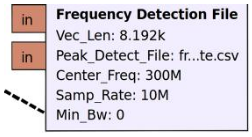

Figure 6: Frequency detection and saveing block

The frequencies detected and previously saved in a *.CSV file by the spectral analysis module were used to create a flowgraph dedicated to the controlled emission. This flowgraph automatically imports the list of frequencies from the CSV file and sequentially processes them, emitting a signal on each frequency at a predefined time interval.

The implementation ensures that the frequencies are processed cyclically, and parameters such as transmit duration per frequency, signal amplitude, and waveform can be configured by the user. This approach enables the system to achieve targeted spectral interference, thereby minimizing the impact on other bands while maximizing the effectiveness of the interference on the identified transmissions.

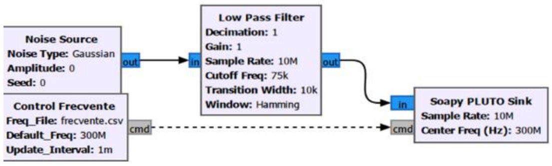

Figure 7: Controlled emission implementation

A graphical user interface (GUI) has been developed and integrated within the GNU Radio Companion application to facilitate interaction with the RF detection and jamming system. This graphical user interface (GUI) offers two distinct functionalities: real-time spectrum monitoring and jamming transmission control.

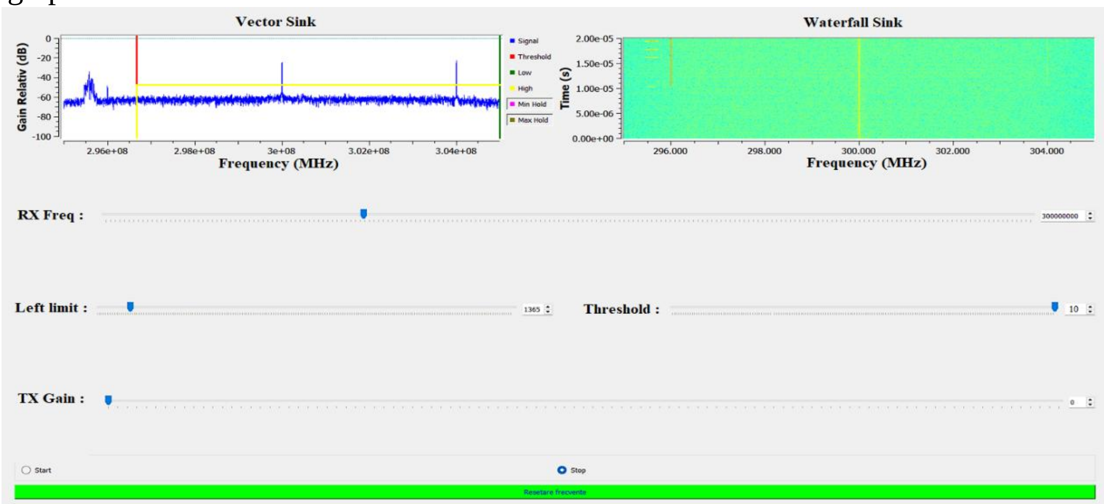

Figure 8: User interface for RF detection and jamming system

This interface renders the system accessible and straightforward to operate, while concurrently providing an intuitive visualization of the radio spectrum and a flexible mechanism for real-time RF interference control.

3. Results and Discussions

A series of laboratory tests were performed to evaluate the ability of the spectral sensing system to identify dynamic signals. The tests focused on frequency hopping signal recognition. The objective of the tests was to ascertain the robustness and sensitivity of the adaptive algorithm under controlled conditions. The test setup included a laptop, an Adalm-Pluto SDR, and an R&S SMW200A signal generator configured as a variable signal source.

To validate the system, three successive tests were performed, in which the generator was programmed to output a -85 dBm signal in a 10 MHz band between 295 MHz and 305 MHz. The frequency steps were executed in 1 MHz steps, thus comprising a total of 10 distinct channels. In each instance, the system was evaluated according to its capacity to accurately detect the occurrence of each signal in the monitored band, irrespective of its position on the frequency axis.

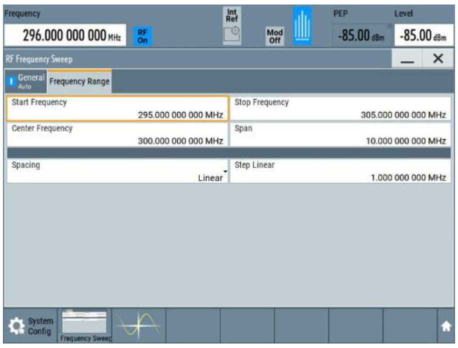

Figure 9: R&S SMW200A signal generator configuration

Test 1 - Frequency hopping detection (Sweep time: 10 ms / 100 hops/s).

The initial evaluation includes the identification of fast frequency hopping signals, as depicted in Quicklook 1 simulation, which is commonly used in tactical and operational communications.

The behavior of the detection system under a dynamic FHSS communication scenario was observed. The R&S SMW200A signal generator was configured with a sweep time of 10 milliseconds, corresponding to a speed of 100 frequency hops per second.

The objective of this evaluation was to assess the system's capacity to respond to rapid frequency shifts, like those observed in practical scenarios. The implemented system demonstrated effective functionality, successfully identifying each active frequency within a single sweep cycle. The detection was made possible by the implementation of an adaptive threshold algorithm, which autonomously identified energy spikes that surpassed the standard deviation of the noise level. The collected information was displayed in real time in the graphical user interface, and the spectrogram and frequency list accurately confirmed the position of each hop in the spectrum.

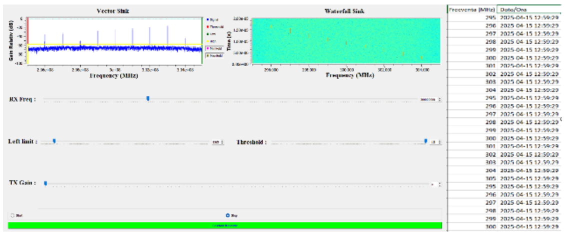

Figure 10: Test 1 - Frequency hopping detection (Sweep time: 10 ms / 100 hops/s)

Test 2 - High frequency sweep detection (Sweep time: 1 ms / 1000 hops/s).

The second test aimed to explore the upper limit of system detection under extreme conditions. The signal generator was set for a sweep time of 1 ms, which means 1000 frequency hops per second, an extremely high speed used in practice only by specialized equipment for maximum jamming and interception protection. The duration of each channel's activation was found to be remarkably brief, with an average duration of approximately 100 microseconds. This limitation posed a significant challenge to the receiver's capacity to observe and respond promptly.

In this test, it was found that the system failed to detect all frequencies in a single iteration, due to the very short time the signal was present on each frequency. However, by continuously running the application and accumulating the results in the output file, the system was gradually able to record all 10 channels, confirming the detection. This test highlighted the practical performance threshold of the system, providing useful information for the calibration of future versions to extend the detection capabilities in ultra-fast hopping regimes.

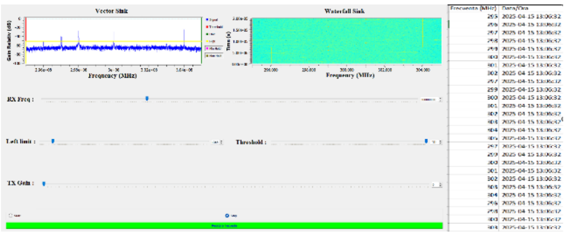

Figure 11: Test 2 - High frequency sweep detection (Sweep time: 1 ms / 1000 sweeps/s)

At the same time, it was observed that the frequency plot (FFT) and spectrogram (waterfall) in the GUI failed to visibly track fast frequency hops. These tools, being dependent on a wider time window and the graphical update rate, cannot capture short events at this speed. Consequently, despite the efficacy of the algorithmic detection, which accumulated data in the background, the real-time visualization did not accurately reflect the signal dynamics.

Test 3 - Detection and jamming of a real radio station with frequency hopping (300 hops/s).

In the next test, a real FHSS transmitting radio station configured to operate at 300 frequency hops per second, corresponding to the Quicklook 2 mode, was used for the first time. This mode is characteristic of advanced communications with high spectral mobility, where the active signal remains on each frequency for only about 3 ms, after which it quickly hops to a new frequency in the allocated band.

The detection system was activated a few seconds before the jamming began, allowing the active frequencies to be recorded. The adaptive threshold-based detection algorithm performed stably and without false detections, correctly identifying all frequencies used by the radio station in a short time. The analysis of the generated CSV file as well as the graphical representation of the spectrograms indicated that the same frequencies were repeatedly detected, indicating that the synchronization between the detection algorithm and the spectral hops of the signal was efficient.

After the detection phase, the jamming system was activated, using the directional antenna oriented towards the transmitting station. The jamming emission was controlled by the GNU Radio application, which transmitted the noise signal on the detected frequencies in a cyclic sequence synchronized with the previously saved list.

The results demonstrated that the jamming was effective: in the vicinity of the directive antenna, the level of the jamming signal was constantly higher than the useful signal, which resulted in blocking the radio communication and making it impossible for the receiver to receive the data correctly.

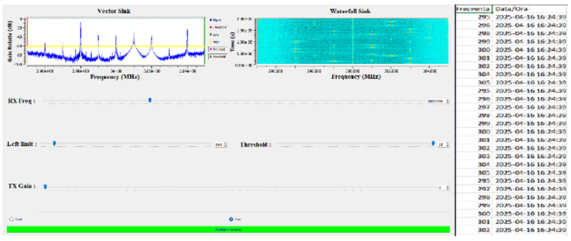

Figure 12: Test 3 - Detection and jamming of a radio station with 300 hops/s

This test validated the complete operation of the system, from the fast detection in real FHSS mode to the reactive electronic countermeasure action. The performances obtained confirm the applicability of the system in communication monitoring and neutralization scenarios in controlled or operational environments.

4. Conclusion

This paper presented the development and validation of an SDR system capable of detecting radio signals in real time and generating targeted jamming on them, with applicability in FHSS communication scenarios. The platform has been implemented in GNU Radio, using the Adalm-Pluto device and custom blocks developed in Python, including an adaptive detection module based on noise level analysis and a processing block for the detected frequencies.

Laboratory tests have confirmed the functionality and robustness of the system against dynamic signals, including those with fast frequency hops (up to 1000). However, in extreme conditions characterized by hop durations of less than 1 millisecond, complete detection was only achieved by recording values for a longer acquisition time; in less than 1 second, all hop frequencies were recorded. The algorithm demonstrated an effective real-time response capability for this type of signal, with a maximum of 300 hops, corresponding to the Quicklook 2 operating mode. In addition, it was demonstrated that the operator can effectively adjust the adaptive threshold without significantly introducing false detections.

The reactive jamming module, which is activated based on the frequencies that were previously detected, allowed the jamming of signals near the directional antenna. The results from the real radio station test show that the system has potential for applications like spectrum monitoring, EM risk assessment, and electronic countermeasures in controlled environments.

In conclusion, the proposed system provides a complete, modular and scalable solution for detection and response to dynamic radio signals. Future work will include integration into distributed SDR architectures, optimization of algorithms for congested environments, and support for complex modulations. Due to its potential operational use, the deployment of reactive jamming capabilities must adhere to applicable military regulations and rules of engagement. This ensures compliance with legal constraints and ethical standards in electronic warfare operations.

References

[1] Munteanu R., Mitran R., Bechet P. Metode numerice pentru detectia semnalelor radio. Editura MediaMira, Cluj-Napoca, ISBN 978-973-713-309-0, 2013.

[2] Ristić, V., Todorović, B.M., Stojanović, N. Frequency hopping spread spectrum: History, principles and applications. Vojnotehnicki glasnik. 2022; Vol. (70): 856-876.

[3] Burel, G. Detection of spread spectrum transmissions using fluctuations of correlation estimators.IEEE - ISPACS, Honolulu. 2000.

[4] Mpitziopoulos, A., Gavalas, D. An effective defensive node against jamming attacks in sensor networks. Secur. Commun. Networks. 2009; Vol. (2): 145-163.

[5] Stojanović, N., Todorović, B.M., Ristić, V. Analysis of repeater jamming of a slow frequency hopping radio. Vojnotehnicki glasnik. 2022; Vol. (70): 664-679.

[6] Torrieri, D. Principles of spread-spectrum communication systems. Springer Publishing Company: Berlin/Heidelberg, Germany. 2015.

[7] Sorecau, M., Şorecău, E., Cîrstea, R., Bechet, P. Enhanced Spectrum Monitoring Capabilities Based on Software-Defined Radio Systems: Validation of a Real Time Frequency Hopping Signal Detection. International conference KBO. 2024; Vol. (30): 162 - 171.

[8] Wright, D.P., Ball, E.A. Highly Portable, Low-Cost SDR Instrument for RF Propagation Studies. IEEE Transactions on Instrumentation and Measurement. 2020; Vol. (69): 5446-5457.

[9] Wyglinski, A.M., Orofino, D.P., Ettus, M.N., Rondeau, T.W. Revolutionizing software defined radio: case studies in hardware, software, and education. IEEE Communications Magazine. 2016; Vol. (56): 68-75.

[10] Sowjanya, P.L., Satyanarayana, P.V. Implementation of Transceiver module for SDR system using ADALM PLUTO platform. International journal of engineering and technology. 2018; Vol. (7): 279-284