Design of ReconFIGUREurable Modulation System for Selective Cellular Interference with SDR

1st Diky Arif Hidayat
School of Electrical Engineering
Telkom University
Bandung, Indonesia
dikyarifhidayat07@gmail.com

2nd Eka Nadiyah Purwanianti
School of Electrical Engineering
Telkom University
Bandung, Indonesia
purwaniantynadia@gmail.com

3rd Daniel Alden Susetyo
School of Electrical Engineering
Telkom University
Bandung, Indonesia
danielaldens10@gmail.com

4th Amalia Muhammad Jasmin
School of Electrical Engineering
Telkom University
Bandung, Indonesia
amalia.m.j.890@gmail.com

5th Budi Prasetya
School of Electrical Engineering
Telkom University
Bandung, Indonesia
budiprasetya@telkomuniversity.ac.id

***Abstract*—Conventional signal interference systems are often constrained by the rigidity of hardware architecture, which limits operational flexibility and increases cost inefficiency. This research aims to overcome these limitations through the development of an adaptive signal modulation system based on Software Defined Radio (SDR) that replaces the role of static analog components with reconFIGUREurable software conFIGUREurations. The method used involves the implementation of HackRF One SDR controlled through the GNU Radio framework to perform interference emissions on strategic cellular frequency bands. Performance evaluation was carried out by comparing the real time output power profile with the technical specifications of the device and conducting a comparative analysis with conventional Digital Cellular System (DCS) modules to assess bandwidth adequacy and radiation intensity. The experimental results show that although the SDR conFIGUREuration offers high spectral agility, there are deficiencies in transmission power and bandwidth for large scale cellular coverage, requiring the integration of external amplification. However, validation testing confirmed the system's effectiveness in significantly reducing the Reference Signal Received Power (RSRP) value on the target device compared to the received power level from the Base Transceiver Station (BTS). Overall, this approach successfully improved the architectural efficiency and functional flexibility of the jammer modulation system in mitigating signals on the cellular frequency spectrum.**

***Keywords*— software defined radio, hackrf one, gnu radio, signal interference, spectral agility.**

I. INTRODUCTION

Conventional signal blocking systems, such as fixed hardware based jammers, operate by injecting electromagnetic interference through noise modulation on specific frequency bands [1], [2]. Although effective in static scenarios, this methodology has significant operational efficiency limitations due to low hardware flexibility [3]. The use of oscillators and analog filter circuits with fixed frequencies limits the scalability of the system in dealing with dynamic and congested spectrum environments. In addition, dependence on rigid physical components makes the system incapable of adapting to frequency hopping techniques or agile modern communication protocols [4], [5].

Conventional hardware based modulation architectures suf- fer from frequency rigidity due to non reconFIGUREurable local oscillators, leading to inefficiencies in multi sectoral jamming systems [3]. To overcome this, an efficient system must achieve a precise balance to generate selective interference [6]. This ensures that spectral disruptions are targeted strictly at specific mobile communication protocols, thereby preventing unwanted spillover that compromises the surrounding spec- trum integrity [7].

While Software Defined Radio (SDR) provides modulation flexibility, jamming effectiveness is often constrained by the integration complexity between software layers and front end architectures [8]. A primary challenge involves synchronizing components to generate precise, coherent noise without hardware redundancy across multiple cellular bands [9]. Misalignment between software control and RF output typically degrades spectral precision and wastes power, necessitating integrated designs that optimize operational efficiency and blocking accuracy within dynamic environments [10], [11], [12].

To overcome the limitations of conventional hardware rigidity, this research proposes a Software Defined Radio (SDR) based system design that is capable of operating dynamically on cellular frequency bands, namely 1800 MHz (LTE Band 3), 2100 MHz (LTE Band 1/IMT), and 2300 MHz (LTE Band 40) [13]. The inherent flexibility of the SDR architecture allows a single processing unit to emulate the functions of multiple analog devices through real time reconFIGUREuration of param- eters at the software layer [1], [14]. Through an integrated multi frequency approach, this system is capable of scanning and blocking the desired spectrum without the need to add hardware modulation components for each frequency band, thereby significantly improving cost efficiency and operational flexibility [15]

II. THEORETICAL BACKGROUND

The development of an effective cellular frequency scrambling system requires a deep understanding of the basic principles of radio frequency (RF) engineering and signal processing. This section provides an in depth explanation of the theoretical framework underlying the proposed GNU Radio based architecture, with a particular emphasis on jamming system principles and the core principles of SDR.

A. Jammer System Principles

Jamming operates based on the basic principle of electromagnetic interference, where interference signals are deliberately transmitted to reduce the SINR at the target receiver [2]. Theoretically, the effectiveness of this process is determined by the jammer to signal ratio (J/S), which determines the level of communication interference by drowning out legitimate carrier signals with high density noise or modulated interference. In physical implementation, as illustrated in FIGUREure 1, the jamming signal is synthesized through SDR and then amplified through a power amplifier to achieve the target distance re- quired for effective spectral suppression. This amplified signal is then transmitted through a planar collinear antenna array, which serves to focus the interference energy onto the targeted spatial domain. This forces a drastic reduction in the RSRP value and breaks the connection between the base station (BS) and the User Equipment (UE) in the specified coverage area.

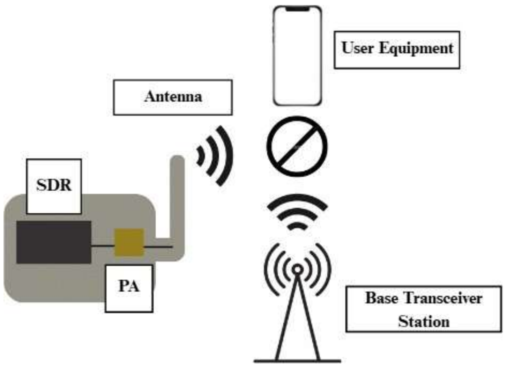

FIGURE 1
Jammer System Physical Implementation

B. Software Defined Radio with GNU Radio

Software Defined Radio (SDR) represents a transformative paradigm shift by transitioning from rigid hardware centric architectures to versatile, software implemented functionalities supported by frameworks like GNU Radio [11]. This technology leverages software based protocols to achieve high reconFIGUREurability, where incoming analog signals are digitized via high speed Analog to Digital Converters (ADC) and processed using Field Programmable Gate Arrays (FPGA). As illustrated in the RF front end architecture in FIGUREure 2, the system utilizes a MAX5864 ADC/DAC interfaced with an NXP LPC43xx microcontroller, employing synthesizers and mixers for frequency upconversion. Although the USB 2.0

High Speed interface constrains the operational bandwidth to approximately 20 MHz, this capacity is sufficient for targeted cellular bands at 1800 MHz, 2100 MHz, and 2300 MHz. By executing baseband and intermediate frequency (IF) process- ing in the digital domain, the protocol stack and physical layer can be dynamically updated on universal hardware to support diverse transmission formats [4].

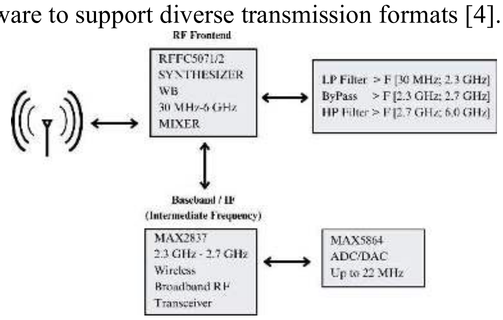

FIGURE 2
HackRF One front end/baseband

C. RF Architecture and Signal Processing Flow

The communication architecture in this system utilizes the SDR principle to efficiently connect analog and digital domains through flexible hardware integration. Analog radio frequency signals interact with the system through an antenna that is directly connected to the RF frontend module via a coaxial connector, where the processing path is divided into reception and transmission mechanisms to maintain data integrity [4]. At the digital frontend stage, high speed analog to digital and digital to analog converters convert the signal, enabling baseband processing to be performed computationally within the central processing unit (CPU) or FPGA in FIGUREure
3. At this layer, the signal undergoes sample reduction and sample rate conversion before being forwarded to the host device via a USB interface to ensure that the data stream remains synchronized. A key feature of this design is its ability to implement various communication protocols and physical layer functions without changing the physical components. Through this software abstraction, technical parameters such as channel filtering and modulation can be dynamically adjusted, providing a high degree of scalability for experimental needs across a wide range of cellular spectrums.

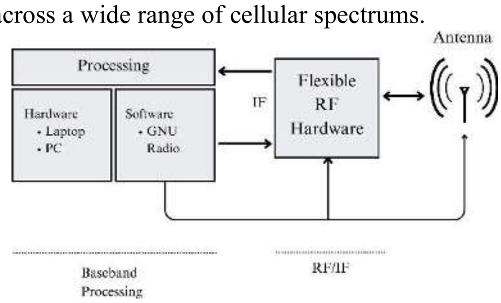

FIGURE 3
SDR Block Flow Architecture

III. METHODOLOGY

This section presents the design methodology for our GNU Radio based jammer system, detailing the system architecture, operational workflow, and simulation approach. The design integrates SDR technology with triple frequency antenna design to achieve effective jamming across 1800 MHz, 2100 MHz, and 2300 MHz cellular bands.

A. Hardware reconFIGUREurability of SDR

The proposed system architecture integrates SDR technology with external power amplifier components to generate effective signal interference in the cellular frequency band. In this system model, the software defined radio unit acts as the processing core that synthesizes the base signal through a sawtooth generator mechanism, which is then forwarded to a voltage controlled oscillator (VCO) block for frequency modulation, wich can be seen in FIGUREure 4 [3]. The modulated signal is then fed to a power amplifier unit to increase the in- tensity of electromagnetic radiation to the power level required to overcome the threshold of legitimate signals at the target receiver. The final stage of this system is the transmission of interference energy through a tri band antenna that has been specifically optimized to operate at frequencies of 1800 MHz, 2100 MHz, and 2300 MHz. This integrated conFIGUREuration allows the system to precisely focus interference energy on a specific spatial domain, thereby degrading the quality of cellular communication services in a controlled manner with- out requiring additional hardware for each different frequency band.

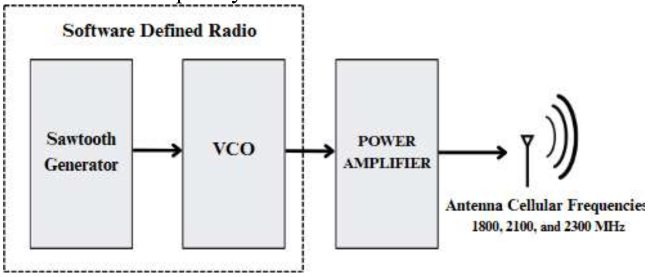

FIGURE 4
GNU Radio based Jammer System Architecture

B. Key Attributes SDR

The technical specifications of Software Defined Radio (SDR) are basic parameters that determine the integrity of the output signal and the operational limits of the device [14]. Identifying these specifications allows the determination of the maximum performance limits and inherent limitations of the device used, which can be seen in Table I. The accuracy of output power measurements is highly dependent on the technical profile of the SDR, which directly affects the validity of empirical data. Therefore, comprehensive mapping of instrument specifications, including oscillator stability and receiver sensitivity, is crucial to ensure that performance analysis results reflect actual physical phenomena, rather than artifacts of hardware limitations.

TABLE 1
SPECIFICATION HACKRF ONE

Specification Parameters	Description
Data Bandwidth	20 MHz
Sampling Accuracy	8 Bit
Operating Frequency	1 MHz to 6 GHz
Sampling Rate ADC/DAC Msps	2 Msps to 20
Power Supply/Data Port	USB 2.0

C. GNU Radio ConFIGUREuration

The SDR framework facilitates a paradigm shift by im- plementing conventional hardware functions, such as signal generators and voltage controlled oscillators (VCOs), into highly reconFIGUREurable software modules [3]. This flexibility allows for dynamic parameter adjustments across a broad frequency range. however, as illustrated in FIGUREure 5, the hard- ware faces inherent limitations in executing simultaneous multi band transmissions. To address this, the proposed architecture utilizes three discrete SDR units to operate across distinct frequency bands, integrated with external Power Amplifiers (PA) to compensate for the SDR's low output power [8]. This conFIGUREuration ensures the transmission power is sufficient to effectively degrade the signal quality between the Base Transceiver Station (BTS) and mobile devices within the targeted area.

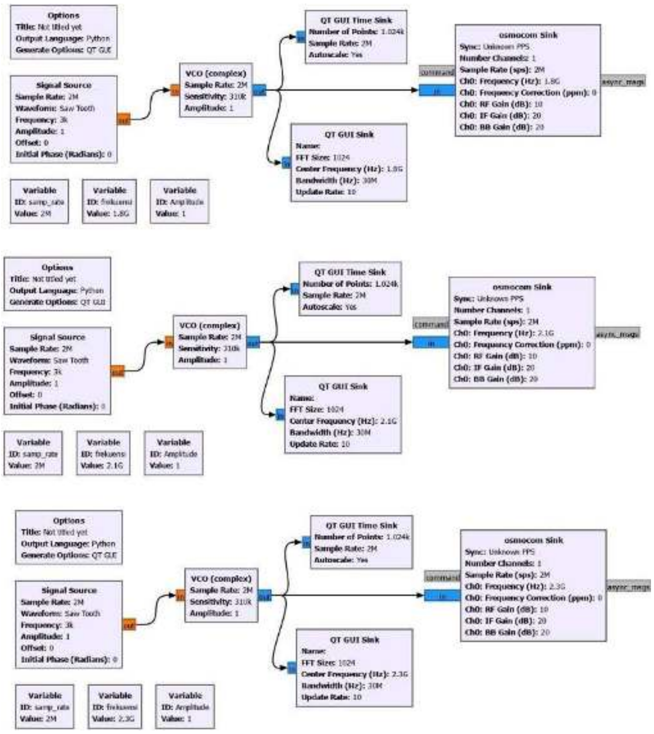

FIGURE 5
Block ConFIGUREuration GNU Radio

D. Signal Processing Workflow

The signal processing mechanism in the proposed archi- tecture adopts a digital wave synthesis approach conFIGUREured through the GNU Radio environment to generate coherent interference. The initial stage involves a Signal Source block that generates a periodic reference signal as the basis for modulation to create a noise spectrum. This signal is then integrated with a Voltage Controlled Oscillator or VCO block to transform amplitude variations into agile frequency shifts, enabling the system to effectively cover the targeted band- width. To ensure process integrity and avoid data synchro- nization failures between software and hardware, the signal flow is continuously visualized using the QT GUI Sink block, which displays the time domain and frequency domain si- multaneously [7]. As the final stage in the processing chain, the Osmocom Sink block acts as a hardware abstraction that converts the digital sample stream into physical instructions for the SDR device. Through synchronization of gain and sample rate parameters in this block, the device is able to transmit interference signals with high precision on the 1800 MHz, 2100 MHz, and 2300 MHz cellular frequency bands to achieve optimal degradation of service quality on the target device.

E. Measurement and Validation Setup

System validation procedures are performed to ensure that interference signals from GNU Radio and HackRF One meet technical parameters prior to field testing. The initial stage uses a spectrum analyzer to verify the accuracy of the center frequency and bandwidth on three target bands, in order to ensure that noise energy is concentrated without spectral leakage. Next, power measurements are performed to calibrate the gain and ensure that the amplifier output remains within the linearity limits to prevent harmonic distortion. Blocking effectiveness is then validated by monitoring RSSI and SINR degradation on mobile devices to determine the Interference to Signal Ratio

(ISR) threshold capable of breaking synchroniza- tion [6]. All measurement data is rigorously cross referenced against the manufacturer's SDR technical specifications and datasheet constraints to ensure the system operates at its opti- mal capacity while maintaining signal integrity and preventing hardware saturation during prolonged operation.

IV. EXPERIMENTAL RESULT

This chapter evaluates the SDR signal output measurements resulting from the conFIGUREuration to validate the specified fre- quency performance and power output for jamming. The re- sults demonstrate the jammer effectiveness in blocking cellular signals, while confirming the functional integration between the conFIGUREuration system and the transmitter device.

A. Software Defined Radio

Based on the test results after conFIGUREuration at the cellular frequency, SDR proved capable of transmitting random signals without information in FIGUREure 6. However, due to bandwidth and gain limitations, the random signal power generated was unable to cover the overall cellular signal power at the target frequency [13]. As a result, this system is only capable of functioning in the simulation stage and is not yet effective for jamming real cellular devices. In addition, the limitation of Osmocom Sink, which only supports one transmission frequency at a time, requires the execution process to be carried out three times for each conFIGUREuration.

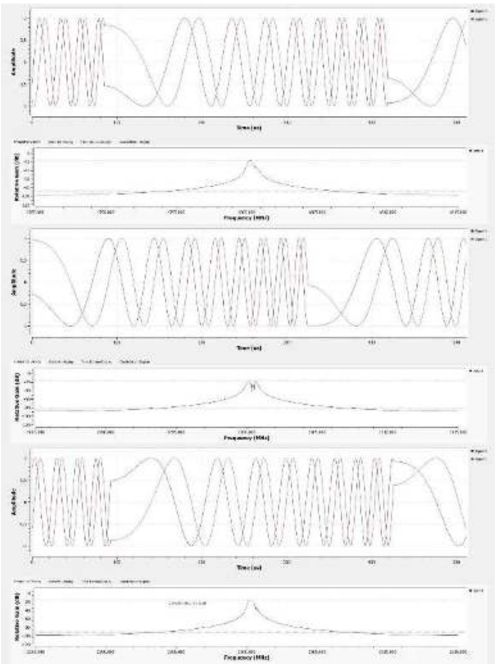

FIGURE 6
SDR ConFIGUREuration Output using GNU Radio

B. Transmission Power Analysis of SDR on a Spectrum Ana- lyzer

Transmission power analysis of the system was performed using a spectrum analyzer to verify the accuracy of frequency modulation and output signal intensity generated by the soft- ware defined radio device. Based on the measurement results displayed on the instrument, the system was successfully conFIGUREured to transmit signals in the target frequency range, namely 1800 , 2100, and 2300 MHz, proving the flexibility of the device in mapping the cellular spectrum according to software instructions [8]. Although frequency synchronization has been achieved with high precision, the device's technical profile reveals inherent limitations related to power density and available operational bandwidth in FIGUREure 7. Observations on the visual spectrum confirm that the pure output power of the SDR hardware is still below the threshold required to effectively suppress signals on a large cellular network [12].

These bandwidth and power level limitations indicate that the use of the device in real world signal interference scenarios requires additional integration with an external power ampli- fier unit to achieve an optimal interference to signal ratio without compromising spectral integrity around the operating frequency.

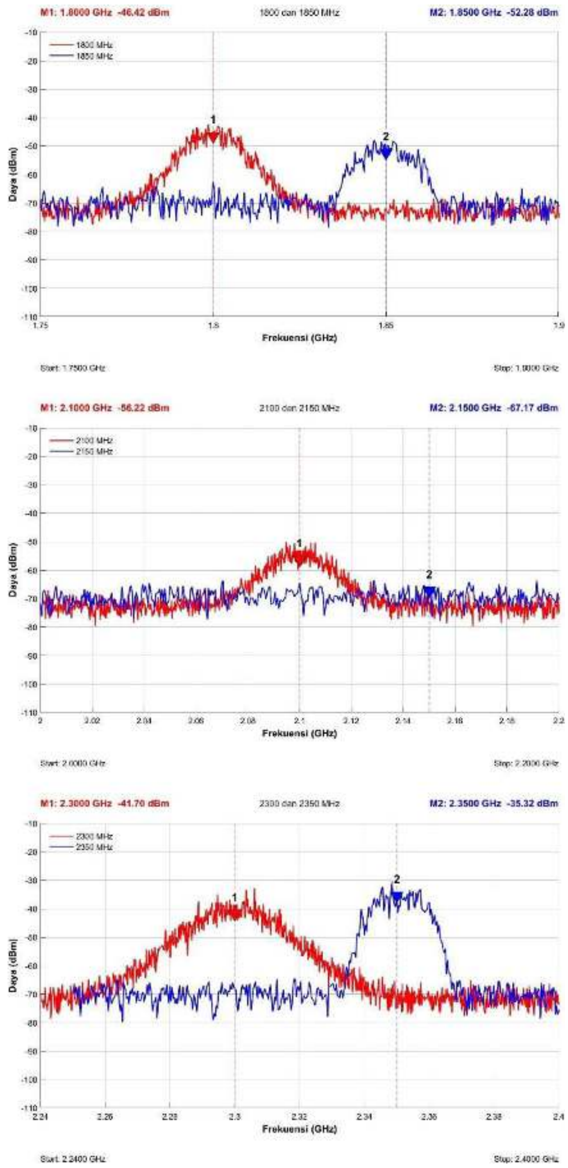

FIGURE 7
Power and Bandwidth Comparison Graph on the Spectrum Analyzer Output

C. Evaluation of DCS Modul Frequency Band Transmission Power

This experiment was systematically designed by adjusting the distance between the transmitter antenna (Tx) and receiver antenna (Rx) within a range of 1 to 5 meters, with two tests conducted at different center frequencies on each band [6]. Given the inherent limitations of the Software Defined Radio (SDR) platform, such as narrow bandwidth and low output power, this study integrated a special external jammer module as the main signal source to ensure frequency stability and high spectral power density [10]. On the receiver side, the LibreVNA device is operated in Spectrum Analyzer mode to monitor the spectral characteristics of interference with high resolution, while the data acquisition process focuses on critical metrics such as power spectrum magnitude and Received Signal Reference Power (RSRP) in FIGUREure 8 [9]. Through this comprehensive hardware integration, each measurement stage is able to quantitatively capture signal degradation phenomena, providing an accurate picture of the impact of interference on communication quality in various distance scenarios.

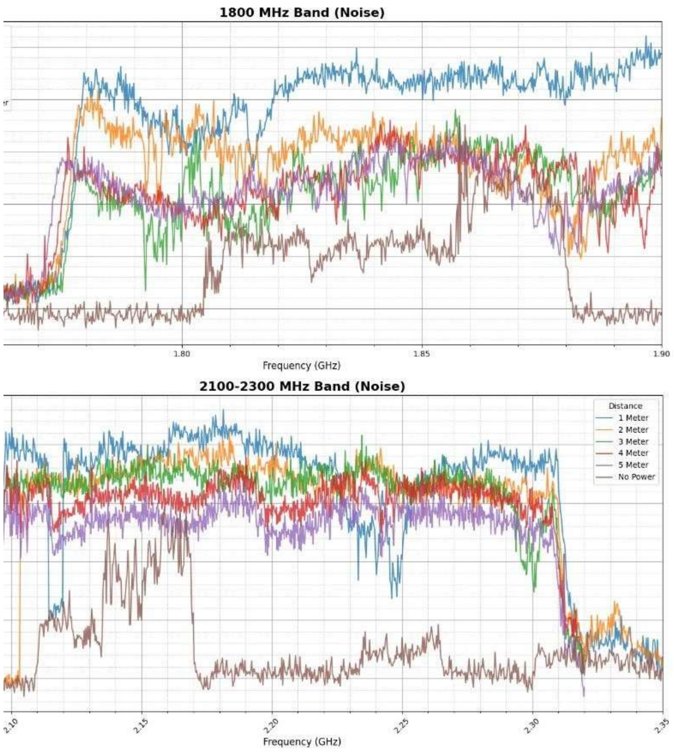

FIGURE 8
Power Test Results Graph Transmit Frequency 1800–2300 MHz

D. The Effectiveness of Jammer Transmission in Interfering with Cellular Devices

Testing of the jammer module in the 1800–1995 MHz and 2100–2300 MHz frequency ranges showed high spec- tral effectiveness, successfully overlapping with the downlink transmission frequency of the Base Transceiver Station (BTS) [1]. This spectral coverage was verified through real time spectrum graph observation using LibreVNA, which confirmed high power spectral density (PSD) across the entire target frequency range . The experimental results, as summarized in Table II, show that the device achieves optimal performance in suppressing cellular signals by significantly reducing the Signal to Interference and Noise Ratio (SINR) [15]. This phenomenon indicates the deliberate domination of noise and interference in the target spectrum, which effectively hides the Reference Signal (RS) and hinders the decoding process by the User Equipment (UE). Specifically, at a distance of 1 meter, the jammer forces the RSRP to reach a minimum threshold of -116 dB, causing an almost instantaneous network disconnection with a latency of only 4.3 seconds [5]. As the physical distance increases to 5 meters, a measurable recovery in RSRP values and an increase in connection disconnection latency are observed.

TABLE 2
RSRP Test Results and Connection Time Based on Distance

Dist.	Test 1		Test 2		Test 3		Average	
(m)	RSRP (dB)	Time (s)	RSRP (dB)	Time (s)	RSRP (dB)	Time (s)	RSRP (dB)	Time (s)
1	-118	6	-114	4	-116	3	-116.0	4.3
2	-113	8	-111	7	-115	7	-113.0	7.3
3	-109	10	-110	14	-111	12	-110.0	12.0
4	-110	21	-108	22	-109	21	-109.0	21.3
5	-108	26	-108	27	-110	28	-108.7	27.0

V. Conclusion

This study demonstrates an increase in the efficiency of signal modulation system architecture through the implemen- tation of Software Defined Radio (SDR) capable of operating dynamically on the cellular frequency spectrum. The use of HackRF One integrated with the GNU Radio framework allows the consolidation of various conventional hardware functions, such as signal generators and voltage controlled oscillators (VCOs), into a single, highly reconFIGUREurable soft- ware module. The experimental results confirm the capability of SDR in abstracting the functionality of multiple hardware devices simultaneously, which provides operational flexibility to adjust technical parameters in real time without relying on the addition of physical instruments. Although the system offers superior spectral agility, overall performance is still limited by inherent device parameters, specifically a data bandwidth of 20 MHz and 8 bit sampling accuracy, as well as low output power levels. These findings indicate that to achieve optimal signal suppression effectiveness in cellular networks, the system requires the integration of an external power amplification stage to compensate for the limitations of the SDR's internal amplification, or a transition to a platform with higher amplification density and bandwidth specifications.

VI. Aknowledgements

The authors express their gratitude to the GNU Radio team for providing the essential software framework for system design. Special appreciation is extended to the PUI-PT IS-IoT laboratory for granting access to the signal jamming system software. Furthermore, the authors thank their academic advi- sors and colleagues for their invaluable guidance and technical support during the experimental and evaluation phases.

References

[1] S. Xia and Q. Wu, "Mitigating the Electromagnetic Coupling Between the Tx and Rx Channels in Software-Defined Radio Through a Digital-Domain Cancellation Algorithm," *IEEE Transactions on Electromagnetic Compatibility*, vol. 66, no. 5, pp. 1389–1398, Oct. 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10608440/

[2] Z. U. A. Tariq, E. Baccour, A. Erbad, and M. Hamdi, "Reinforcement Learning for Resilient Aerial-IRS Assisted Wireless Communications Networks in the Presence of Multiple Jammers," *IEEE Open Journal of*

the Communications Society, vol. 5, pp. 15–37, 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10325598/

[3] A. Thavai, M. Subhedar, Y. Thakur, and M. Patil, "Design an RF Up-Down Convertor using Software Defined Radio and GNU Radio," *Journal of Mobile Multimedia*, pp. 901–916, Oct. 2024. [Online]. Available: https://journals.riverpublishers.com/index.php/JMM/article/view/24999

[4] M. Gummineni and T. R. Polipalli, "Implementation of ReconFIGUREurable Transceiver using GNU Radio and HackRF One," *Wireless Personal Communications*, vol. 112, no. 2, pp. 889–905, May 2020. [Online]. Available: http://link.springer.com/10.1007/s11277-020-07080-0

[5] Rustamaji, S. Kliwati, and W. Widada, "The angle of arrival estimation of frequency-hopping cooperative object based on software-defined radio," *Scientific Reports*, vol. 14, no. 1, p. 7732, Apr. 2024. [Online]. Available: https://www.nature.com/articles/s41598-024-58488-8

[6] M. Z. Khan, A. Taha, W. Taylor, M. A. Imran, and Q. H. Abbasi, "Non-Invasive Localization Using Software-Defined Radios," *IEEE Sensors Journal*, vol. 22, no. 9, pp. 9018–9026, May 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9738615/

[7] D. Kafetzis, S. Vassilaras, G. Vardoulias, and I. Koutsopoulos, "Software-Defined Networking Meets Software-Defined Radio in Mobile ad hoc Networks: State of the Art and Future Directions," *IEEE Access*, vol. 10, pp. 9989–10 014, 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9684421/

[8] Z. Htay, Z. Ghassemlooy, M. M. Abadi, A. Burton, N. Mohan, and S. Zvanovec, "Performance Analysis and Software-Defined Implementation of Real-Time MIMO FSO With Adaptive Switching in GNU Radio Platform," *IEEE Access*, vol. 9, pp. 92 168–92 177, 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9466115/

[9] J. Manco, I. Dayoub, A. Nafkha, M. Alibakhshikenari, and H. B. Thameur, "Spectrum Sensing Using Software Defined Radio for Cognitive Radio Networks: A Survey," *IEEE Access*, vol. 10, pp. 131 887–131 908, 2022. [Online]. Available: https://ieeexplore.ieee.org/ document/9989359/

[10] R. Ferreira, J. Gaspar, P. Sebastia˜o, and N. Souto, "A Software Defined Radio Based Anti-UAV Mobile System with Jamming and Spoofing Capabilities," *Sensors*, vol. 22, no. 4, p. 1487, Feb. 2022. [Online]. Available: https://www.mdpi.com/1424-8220/22/4/1487

[11] E. Faulkner, Z. Yun, S. Zhou, Z. J. Shi, S. Han, and G. B. Giannakis, "An Advanced GNU Radio Receiver of IEEE 802.15.4 OQPSK Physical Layer," *IEEE Internet of Things Journal*, vol. 8, no. 11, pp. 9206–9218, Jun. 2021. [Online]. Available: https: //ieeexplore.ieee.org/document/9348953/

[12] A. Daud, M. B. Khan, A. B. Khattak, S. A. K. Tanoli, A. Mustafa, M. Rehman, and O. L. A. Lo´pez, "Next-Generation Security: Detecting Suspicious Liquids Through Software Defined Radio Frequency Sensing and Machine Learning," *IEEE Sensors Journal*, vol. 24, no. 5, pp. 7140–7152, Mar. 2024. [Online]. Available: https://ieeexplore.ieee.org/document/10400410/

[13] M. Marey and H. Mostafa, "Turbo Modulation Identification Algorithm for OFDM Software-Defined Radios," *IEEE Communications Letters*, vol. 25, no. 5, pp. 1707–1711, May 2021. [Online]. Available: https://ieeexplore.ieee.org/document/9335963/

[14] D. M. Molla, H. Badis, L. George, and M. Berbineau, "Software Defined Radio Platforms for Wireless Technologies," *IEEE Access*, vol. 10, pp. 26 203–26 229, 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9721283/

[15] Z. Dai, Y. He, V. Tran, N. Trigoni, and A. Markham, "DeepAoANet: Learning Angle of Arrival From Software Defined Radios With Deep Neural Networks," *IEEE Access*, vol. 10, pp. 3164–3176, 2022. [Online]. Available: https://ieeexplore.ieee.org/document/9667511/