DESIGN AND ANALYSIS OF AN INTERFERENCE GENERATION CIRCUIT FOR A HANDHELD UAV SUPPRESSION DEVICE

Tran Xuan Tinh[1,*], Nguyen Trong Ha[1], Sai Van Thuan[1], Nguyen Trung Minh[1], Tran Ngoc Hieu[1]

DOI: https://doi.org/10.57001/huih5804.2026.111

ABSTRACT

The rapid proliferation of unmanned aerial vehicles (UAVs) has introduced significant security challenges in both civilian and military environments. UAVs rely heavily on radio-frequency (RF) communication links for command, telemetry, video transmission, and satellite-based navigation (GNSS). Disrupting these RF links through intentional broadband interference represents a viable approach to degrade UAV operational capability. This paper presents a theoretical and simulation-based study of broadband interference generation for personal UAV suppression systems. The work focuses on signal modeling, performance metrics such as Jamming-to-Signal Ratio (JSR), Signal-to-Interference-plus-Noise Ratio (SINR), Carrier-to-Noise density ratio (C/N_0), and Bit Error Rate (BER). A multi-band interference generation framework is analyzed using system-level modeling and MATLAB simulations. Results demonstrate the quantitative relationship between interference bandwidth, power spectral density, and degradation of GNSS signal quality. The study provides a rigorous analytical foundation for evaluating interference-based UAV countermeasure systems in constrained portable platforms.

Keywords: *UAV suppression, broadband interference, JSR, SINR, GNSS degradation, system modeling.*

[1]Air Defense - Air Force Academy, Vietnam
[*]Email: tinhpk79@gmail.com
Received: 07/3/2026
Revised: 07/5/2026
Accepted: 25/5/2026

1. INTRODUCTION

The rapid proliferation of unmanned aerial vehicles (UAVs) in both civilian and defense domains has significantly transformed low-altitude airspace operations. Compact commercial UAVs equipped with high-resolution cameras, long-range telemetry, and autonomous navigation systems are now widely deployed in surveillance, logistics, agriculture, infrastructure inspection, and disaster response. However, their accessibility and affordability have also introduced serious security concerns, particularly in restricted or sensitive areas. Unauthorized UAV intrusions may pose threats to airports, military installations, governmental facilities, and critical infrastructure.

Modern UAV platforms rely heavily on radio-frequency (RF) subsystems for three essential functions: command and control (C2) communication, telemetry/data transmission, and satellite-based navigation through Global Navigation Satellite Systems (GNSS). Due to this strong RF dependency, UAV systems are inherently vulnerable to intentional interference and signal manipulation. Recent research has highlighted the increasing prevalence of GNSS jamming and spoofing incidents worldwide, emphasizing the need for systematic analysis and mitigation strategies [1, 5].

From a signal processing perspective, interference can degrade the effective carrier-to-noise density ratio (C/N_0) at the receiver, resulting in loss of lock, tracking instability, or complete denial of service. Ioannides et al. [1] provide a comprehensive overview of recent advances in GNSS jamming and spoofing detection techniques, demonstrating that broadband interference can significantly reduce receiver robustness. Similarly, Ghizzo et al. [2] analyze the impact of jamming on GNSS automatic gain control (AGC) mechanisms, showing how interference alters receiver internal behavior and degrades signal acquisition performance. These findings indicate that GNSS-based navigation remains highly sensitive to elevated interference power spectral density.

In parallel, machine learning approaches have been proposed to identify and classify interference patterns in

GNSS systems. Ghanbarzade and Soleimani [3] demonstrate that deep learning techniques can effectively detect jamming and spoofing signals with high accuracy, further confirming the measurable and quantifiable impact of interference on satellite navigation signals. Additionally, mitigation-oriented studies such as Elmusrati [5] and recent deep-learning-based interference suppression frameworks [6] emphasize the importance of modeling interference characteristics in order to design effective countermeasures.

Beyond GNSS, UAV communication links operating in ISM bands are also susceptible to interference. Arif and Kim [4] analyze UAV-assisted cellular networks under jamming scenarios and show that communication efficiency degrades rapidly when interference power exceeds certain thresholds. These studies collectively underscore the importance of quantitatively evaluating interference effects on UAV subsystems rather than treating them qualitatively.

Despite substantial research on jamming detection and mitigation, fewer works provide a unified analytical framework linking interference bandwidth, power distribution, propagation characteristics, and UAV communication degradation within the constraints of portable suppression platforms. In personal-level systems, limitations in transmitted power, antenna size, and energy capacity impose strict trade-offs between interference bandwidth and power spectral density. Therefore, a rigorous theoretical model is required to assess how interference parameters translate into measurable performance degradation metrics such as Jamming-to-Signal Ratio (JSR), Signal-to-Interference-plus-Noise Ratio (SINR), Bit Error Rate (BER), and C/N_0 reduction.

This paper addresses this gap by developing a comprehensive analytical and simulation-based framework for broadband interference generation in personal UAV suppression systems. The main contributions are as follows:

1. A unified signal model describing UAV communication under interference conditions.

2. Analytical derivation of relationships among JSR, SINR, BER, and C/N_0 degradation.

3. Evaluation of interference bandwidth trade-offs under limited transmitted power.

4. Simulation-based quantification of GNSS signal degradation.

The presented analysis provides a structured foundation for evaluating interference-based UAV countermeasure systems and contributes to a deeper understanding of RF vulnerability in modern UAV architectures.

Figure 1. Image of a personal mobile jamming device

2. SYSTEM MODEL

To evaluate the effectiveness of interference signals in UAV systems, it is necessary to establish a mathematical model describing the interaction between the useful signal, the interference signal, and the background noise of the system. Based on this model, several characteristic parameters can be defined, such as power spectral density (PSD), jamming-to-signal ratio (JSR), signal-to-interference-plus-noise ratio (SINR), and bit error rate (BER). These parameters allow a quantitative evaluation of the degradation in the wireless communication link of UAV systems in the presence of interference.

Under interference conditions, the signal received at the UAV receiver can be expressed as:

$$r(t) = s(t) + j(t) + n(t) \quad (1)$$

where:

s(t) is the useful signal, including the control signal or GNSS navigation signal;

j(t) is the intentional interference signal generated by the suppression device;

n(t) represents the thermal noise of the receiver, typically modeled as additive white Gaussian noise (AWGN).

In the frequency domain, the received signal can be written as

$$R(f) = S(f) + J(f) + N(f) \quad (2)$$

If the interference signal is assumed to be broadband Gaussian noise, its power spectral density can be considered approximately flat over the interference bandwidth. Therefore, the impact of interference mainly depends on the transmitted power and the bandwidth of the interference signal.

Assuming that the total interference power is P_j and that it is uniformly distributed over a bandwidth B_j, the average power spectral density of the interference signal is given by

$$PSD_j = \frac{P_j}{B_j} \quad (3)$$

This expression shows the relationship between transmitted power and interference bandwidth. When the interference bandwidth increases while the transmitted power remains constant, the power density per unit frequency decreases. As a result, the interference effectiveness at a particular frequency becomes weaker. Conversely, when the bandwidth decreases, the power density increases but the spectral coverage becomes narrower. Therefore, selecting an appropriate interference bandwidth becomes an important optimization problem for portable suppression devices with limited transmission power.

To evaluate the relative strength of the interference signal compared with the useful signal, the jamming-to-signal ratio (JSR) is defined as:

$$JSR = \frac{P_j}{P_s} \quad (4)$$

Where P_s is the power of the useful signal at the receiver.

In practice, JSR is often expressed in decibel form as:

$$JSR_{db} = 10\log_{10}(P_j) - 10\log_{10}(P_s) \quad (5)$$

A higher JSR indicates a stronger interference effect. In GNSS systems using spread-spectrum techniques, the JSR must exceed a certain threshold in order to significantly degrade the receiver's signal acquisition capability.

Another important parameter used to evaluate signal quality at the receiver is the signal-to-interference-plus-noise ratio (SINR), defined as

$$SINR = \frac{P_s}{P_n + P_j} \quad (6)$$

where P_n is the thermal noise power.

In many practical situations where the interference power is much greater than the noise power ($P_j \gg P_n$), the SINR can be approximated as

$$SINR \approx \frac{P_s}{P_j} \quad (7)$$

SINR directly affects the demodulation capability of the receiver. When SINR decreases below a certain threshold, the quality of the communication and control link of the UAV is significantly degraded.

For digital communication systems using BPSK modulation, the bit error rate (BER) can be expressed as

$$BER = Q\left(\sqrt{2.SINR}\right) \quad (8)$$

where the *Q(x)* function is defined as:

$$Q(x) = \frac{1}{\sqrt{2\pi}} \int_x^{\infty} e^{-t^2/2} dt \quad (9)$$

This relationship shows that as SINR decreases, the BER increases rapidly. Once BER exceeds a certain threshold, reliable communication cannot be maintained, resulting in unstable or disrupted UAV control links.

To evaluate the influence of interference as a function of distance, the free-space propagation model given by the Friis transmission equation can be used:

$$P_r = P_t G_t G_r \left(\frac{\lambda}{4\pi R}\right)^2 \quad (10)$$

where: P_t is the transmitted power; G_t, G_r are the gains of the transmitting and receiving antennas; R is the propagation distance; $\lambda = c/f$ is the wavelength.

The condition for effective interference at the UAV receiver can be expressed as: $P_{j,r}/P_{s,r} \geq \gamma \Leftrightarrow P_{j,r} \geq \gamma.P_{s,r}$. Where $P_{j,r}; P_{s,r}$ represent the interference power and useful signal power at the receiver, respectively, and γ is the required JSR threshold.

In practical environments, signal attenuation is often modeled using the log-distance propagation model:

$$L(R) = L_0 + 10n\log_{10}\left(\frac{R}{R_0}\right) \quad (11)$$

Where L_0 is the path loss at reference distance R_0, and n is the path-loss exponent. The interference power at the receiver can then be expressed as:

$$P_{j,r} = \frac{P_{j,t}G_tG_r}{L(R)} \quad (12)$$

or in decibel form:

$$P_{j,r,dB} = P_{j,t,dB} + G_{t,dB} + G_{r,dB} - L(R)_{dB} \quad (13)$$

This model allows estimation of the effective interference region based on propagation distance, thereby providing an approximate evaluation of the operational range of UAV suppression devices.

3. NOISE GENERATOR CIRCUIT DESIGN

A personal UAV jamming device consists of six main components:

- Microcontroller: Responsible for selecting the jamming frequency range, adjusting jamming power, managing information, and displaying information on the screen.

- Screen: Displays information about the jamming frequency range, jamming power, battery capacity, and device temperature.

- Signal generator circuit: Generates jamming signals in the frequency ranges used by the UAV.

- Amplifier: Amplifies the jamming signal to a sufficiently high power level to send to the transmitting antenna, ensuring the UAV can be jammed within engagement range.

- Transmitting antenna: Uses a directional antenna for the gun and an omnidirectional antenna for the wearable device.

- Power supply unit: Provides power to the device.

The noise generation module consists of several functional blocks, including a primary noise generator, filter stage, VCO modulation stage, local oscillator, band-pass filter, and power supply unit.

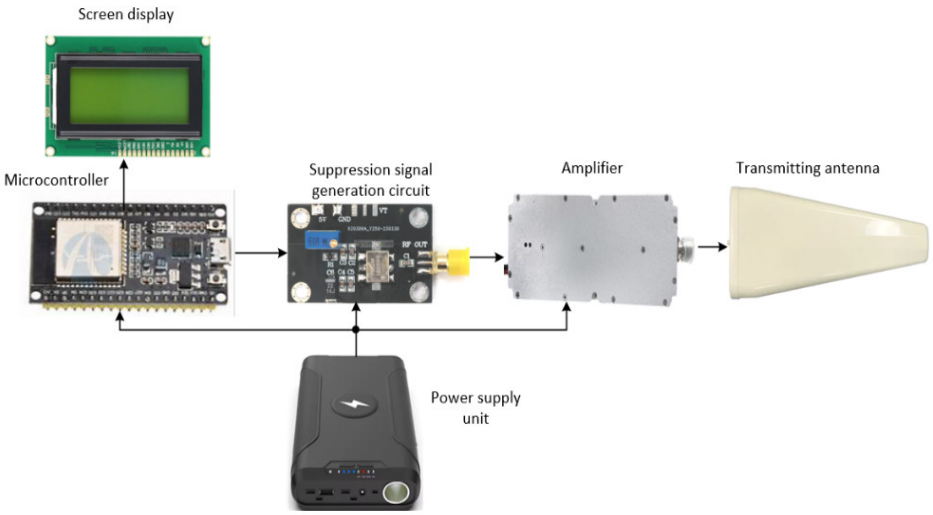

Figure 2. Diagram of the main components in a mobile jamming device

The operating principle is as follows. The primary noise generator produces a pseudo-random noise sequence. This noise signal is first passed through a filter with a specified bandwidth and then fed into the modulation stage. The local oscillator generates the desired carrier frequency and, through a phase-locked loop mechanism, controls the VCO modulator to produce an interference signal at the target frequency bands described in Section 2 with an approximate bandwidth of 80 MHz. The generated signal then passes through a band-pass filter to suppress higher-order harmonic components before being amplified and transmitted to the antenna.

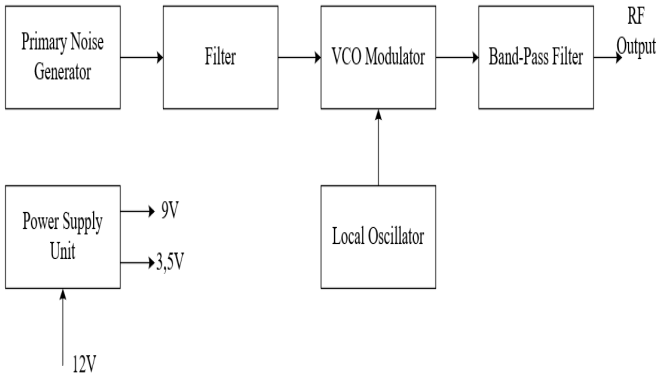

Figure 3. Block diagram of the noise generator circuit

The primary noise generator is implemented using a Zener diode 1N5235, which is biased and buffered by a single 2N3904 transistor. Zener diodes are capable of producing broadband noise signals covering frequencies from the audio range up to more than 100MHz. The generated noise signal is then amplified using an LM386 amplifier and filtered before entering the modulation stage.

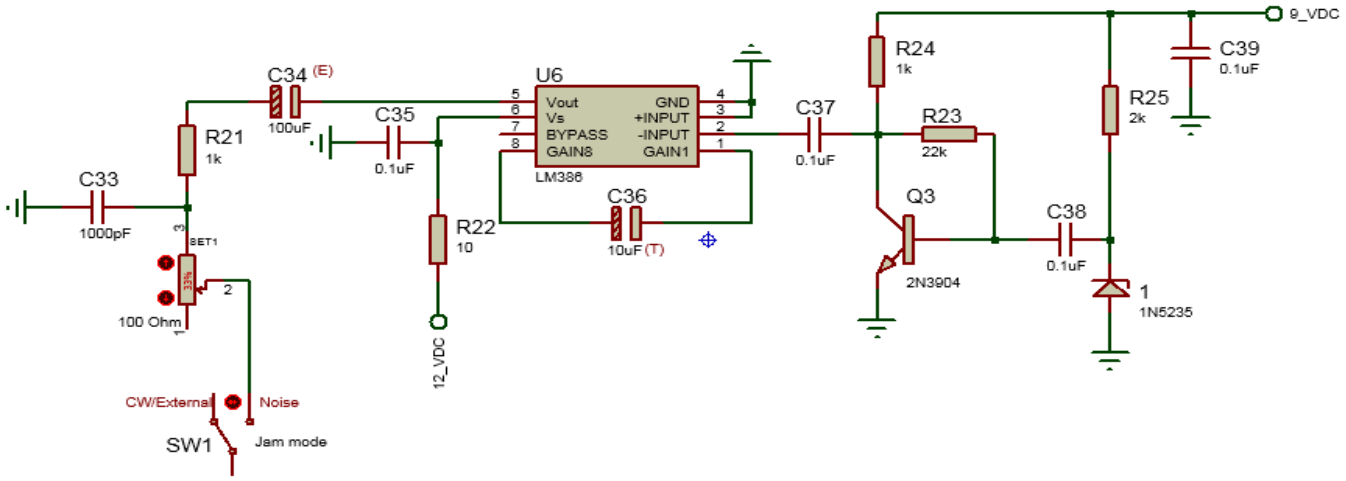

Figure 4. Schematic diagram of the primary noise generation circuit

For the internal oscillator circuit, the Motorola MC145151 integrated circuit is used to configure the output frequency. This chip has 28 pins, of which pins RA2-RA0 and N13-N0 are used to configure the output frequency via programmable division ratios as shown in the following Table 1.

Table 1. Configure the output frequency via division ratios

RA2	RA1	RA0	Decimal value
0	0	0	8
0	0	1	128
0	1	0	256
0	1	1	512
1	0	0	1024
1	0	1	2048
1	1	0	2410
1	1	1	8192

The output frequency of the local oscillator is determined according to the following equation:

$$f_{out} = f_{in} \cdot \frac{N}{R} \quad (14)$$

where: f_{out} is the output frequency of the oscillator; f_{in} is the reference frequency generated by the crystal oscillator; N is the decimal value of the binary word formed by bits N13-N0; R is the decimal value corresponding to bits RA2-RA0.

For example, when the reference frequency is 2.048MHz, the RA bits are set to 101 (corresponding to 2048), and the N bits correspond to the decimal value 5492, the output frequency becomes approximately 5.492MHz.

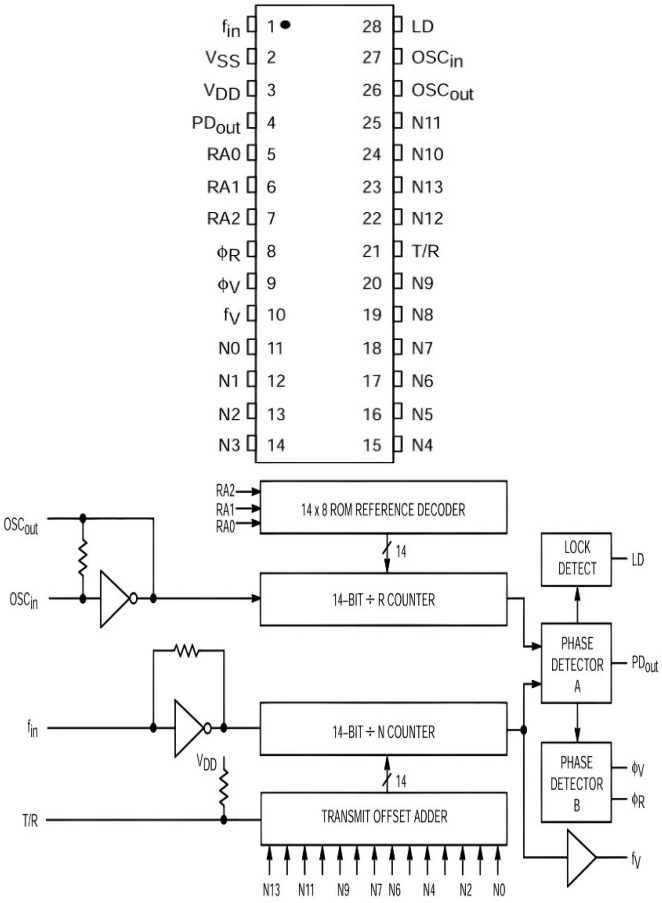

Figure 5. Pinout diagram of IC MC145151

A bandpass filter allows signals within the desired frequency range to pass through while eliminating out-of-band interference. To design an 80MHz bandpass filter, specific parameters must be determined and a suitable filter structure selected. For example: Center frequency f_0 = 1.5GHz; bandwidth BW = 80MHz (from 1.46GHz to 1.54GHz); in-band attenuation: A_p = 3dB; out-of-band attenuation: A_s = 60dB; system impedance: Z_o = 50Ω.

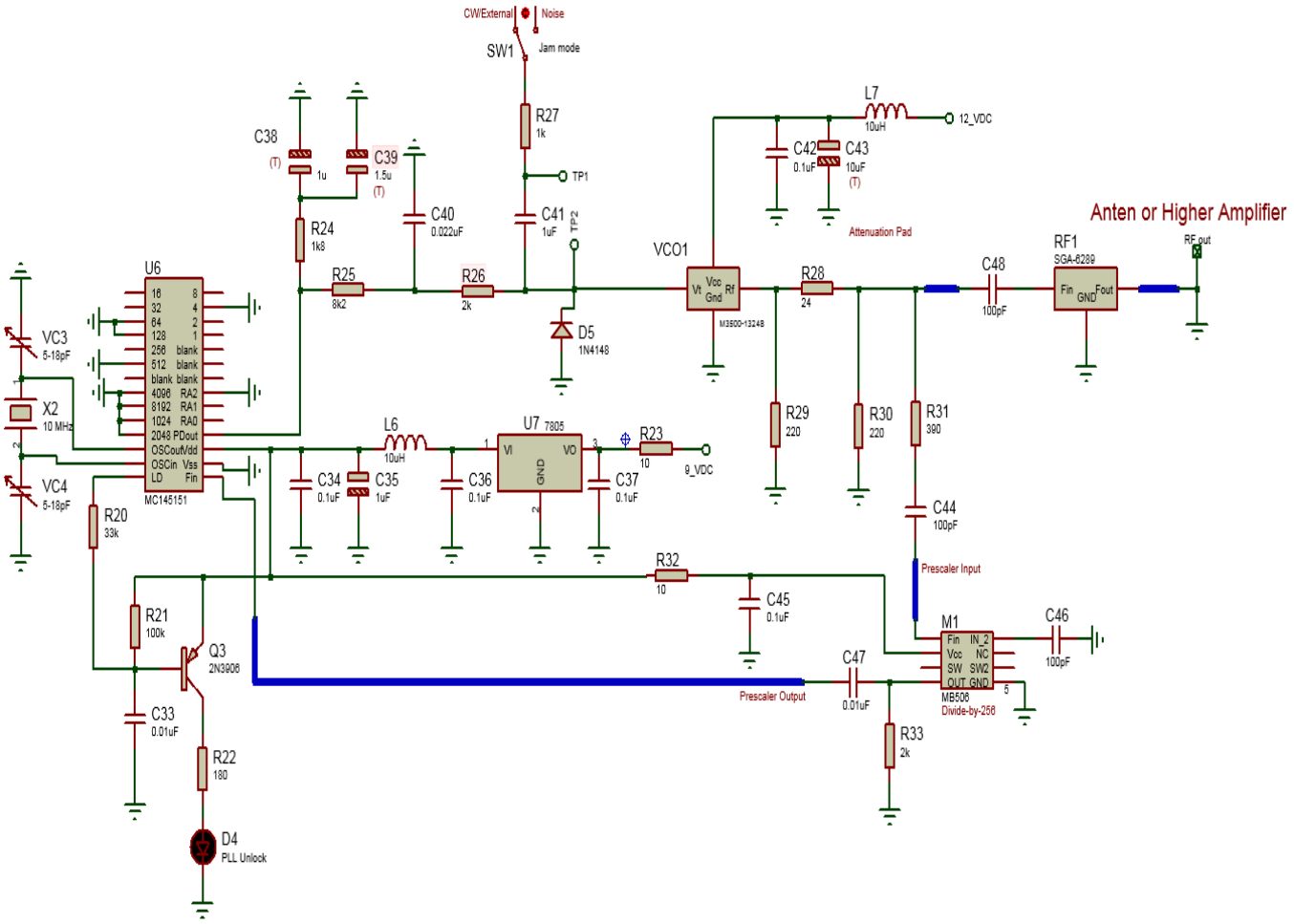

Figure 6. Schematic diagram of the external oscillator and mixer circuit

The Nth-order filter is calculated using the formula:

$$N = \frac{\log\left(\frac{10^{(A_s/10)}-1}{10^{(A_p/10)}-1}\right)}{2\log\left(f_s/f_p\right)} \quad (15)$$

Where: $f_p = f_o; f_s = f_p + BW/2$ hoặc $f_s = f_p - BW/2$

Replace the calculated data:

$$N = \frac{\log\left(\frac{10^{(60/10)}-1}{10^{(3/10)}-1}\right)}{2\log\left(1.58/1.5\right)} \quad (16)$$

The results show that the 5th or 6th order filter meets the desired attenuation requirements.

4. SIMULATION RESULTS

To evaluate the proposed interference generation architecture, simulations were performed using MATLAB. The objective of the simulation is to analyze the characteristics of the generated interference signal and its effect on signals operating in GNSS frequency bands.

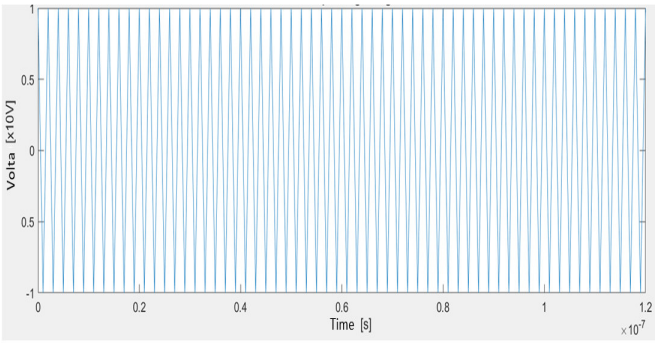

Figure 7. Carrier signal

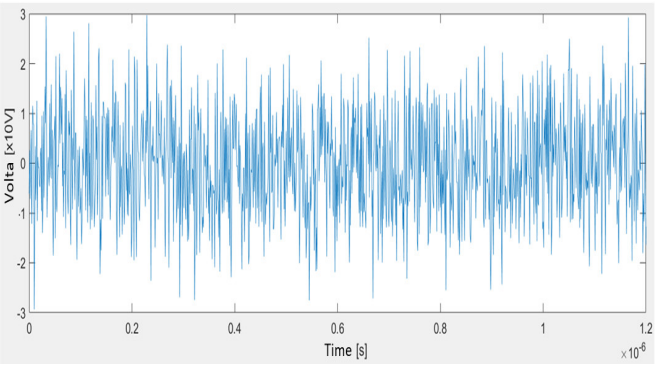

Figure 8. Noise signal

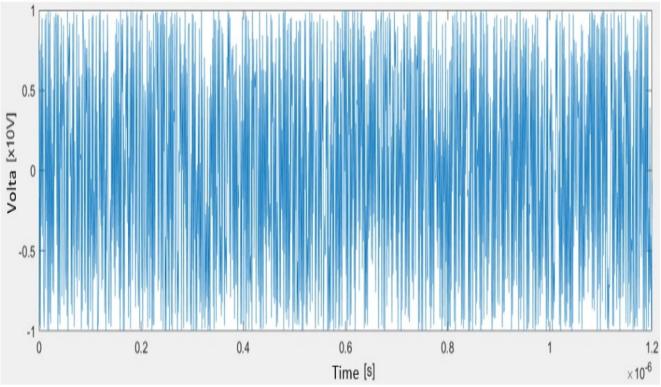

Figure 9. Modulated signal

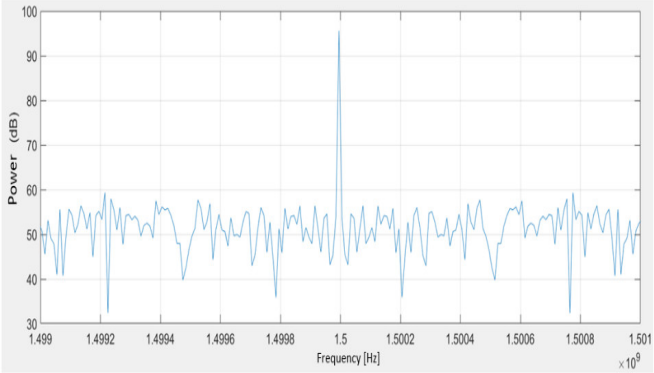

Figure 10. Signal spectrum after amplification

Figure 11. Noise band at 1.2GHz frequency

Figure 12. Noise band at 1.5GHz frequency

First, a carrier signal representing the GNSS signal was generated as a reference signal. The waveform of the carrier signal is shown in Figure 7. Next, a broadband noise signal was generated using a Gaussian random process to simulate the interference produced by the primary noise generator. The generated noise signal is illustrated in Figure 8.

The noise signal was then applied to the modulation stage where it was combined with the carrier generated by the voltage-controlled oscillator (VCO). The resulting modulated signal is shown in Figure 9. After modulation, the signal was amplified and filtered using a band-pass filter in order to limit the spectrum to the desired frequency band and suppress higher-order harmonics. The spectrum of the amplified signal is presented in Figure 10.

Finally, the frequency spectrum of the generated interference signal was analyzed around the target GNSS bands. Figures 11 and 12 illustrate the interference spectra around 1.2GHz and 1.5GHz, respectively. The results indicate that the generated noise successfully covers the intended frequency ranges.

From the simulation results, it can be observed that the proposed interference generation circuit can produce broadband interference signals with controllable center frequency. The filtering stage effectively shapes the spectrum, while the modulation stage enables flexible adjustment of the interference frequency.

5. CONCLUSION

This paper presented the analysis and modeling of a broadband interference generation architecture for personal UAV suppression systems. A theoretical framework describing the interaction between useful signals, interference signals, and noise was first established. Key performance metrics such as PSD, JSR, SINR, and BER were analyzed to evaluate the effectiveness of the interference signal.

Based on this analysis, an interference generation structure including a primary noise generator, modulation stage, local oscillator, and band-pass filtering stage was proposed. Simulation results demonstrated that the system can generate broadband interference signals covering the GNSS frequency bands around 1.2GHz and 1.5GHz.

The results confirm that the proposed architecture is capable of producing controllable interference signals suitable for disrupting RF-based UAV navigation systems.

Future work will focus on optimizing the interference bandwidth and evaluating system performance under realistic propagation conditions.

REFERENCES

[1]. G. Ioannides, et al., "Recent Advances on Jamming and Spoofing Detection in GNSS," *Sensors,* 24, 13, 4210, 2024.

[2]. E. Ghizzo, E. Djelloul, J. Lesouple, et al., "Assessing jamming and spoofing impacts on GNSS receivers: Automatic gain control (AGC)," *Signal Processing*, 2024.

[3]. A. Ghanbarzade, H. Soleimani, "GNSS/GPS Spoofing and Jamming Identification Using Machine Learning and Deep Learning," *arXiv:2501.02352*, 2025.

[4]. M. Arif, W. Kim, "Efficiency of UAV-assisted cellular networks under jamming scenarios," *Vehicular Communications*, 49, 100833, 2024.

[5]. M. Elmusrati, "GNSS Spoofing and Jamming Mitigation: A Comprehensive Review," *J. Atmos. Terrestrial Phys.,* 2025.

[6]. Chen F, et al., "GNSS interference mitigation method based on deep learning," *Frontiers in Physics*, 13, 2025.