Investigating the Effects of Intentional Interference on Conventional and Spread Spectrum Systems

André A. Anjos*, Murilo P. Reis*, and Rausley A. A. de Souza†‡,
*Universidade Federal de Uberlândia (UFU), Patos de Minas, MG, Brazil
†National Institute of Telecommunications, Inatel, Santa Rita do Sapucaí, MG, Brazil
‡University of Sydney, Sydney, NSW, Australia
Email: {andre.anjos,murilopereiradosreis}@ufu.br, rausley@inatel.br

***Abstract*—The dissemination of digital communications raises concerns about their possible malicious use. Countermeasures with intentional interference can be used to inhibit the misuse of these technologies. This article compares the effectiveness of some jamming techniques, namely (i) single-tone, (ii) multi-tones, (iii) narrow-band noise (NBN), (iv) tone pulse, (v) NBN pulse, and (vi) swept jamming. The jamming techniques are evaluated against conventional binary phase shift keying (BPSK) and direct sequence spread spectrum (DSSS) communication systems. Based on the bit error rate curves obtained through the simulation, the performance of the two systems under the action of each jamming technique evaluated in the work is compared. It is confirmed that the spread spectrum brings significant performance gains in interference scenarios. Furthermore, single-tone jamming is the most effective technique against conventional BPSK systems. Regarding the DSSS system, the most effective jamming technique will depend on the signal-to-interference-plus-noise ratio (SINR) under which the interfered receiver is evaluated.**

***Index Terms*—Jammer, RF interference, digital communication, spread spectrum.**

I. Introduction

As unmanned aerial vehicles (UAVs), also known as drones, have advanced in technology, their private use has become more accessible. However, concerns about individuals or groups using these devices maliciously have also grown alongside this proliferation. In 2014, the group Daesh adopted the use of both commercial and homemade UAVs for actions in Syria and Iraq [1]. In 2015, a notorious incident involving a professional-use photographic drone occurred in Tijuana, a Mexican city bordering the United States. The vehicle, laden with methamphetamine, was found by authorities after plummeting from the sky. Since then, hundreds of similar incidents have been reported [2]. Events like these raise society's and security institutions' level of caution and spark debates about the need for oversight of such devices.

While signal suppression is necessary in certain situations, as previously mentioned, resistance to possible interference is desired for legitimate applications. In recent years, the need to add robustness to wireless communications, such as that for UAV operations, has increased interest in using spread spectrum (SS) to suppress interference. Although the use of SS techniques is not new [3], interest in its application to enhance the security of various types of communication remains current. Researchers from the National University of Defense Technology in China presented a study in 2020 [4] that evaluated the effectiveness of these SS techniques against narrow-band interfering signals, where the SS system was highly successful in mitigating the effects of interference.

Recent publications focus on studying direct sequence spread spectrum (DSSS), especially in its anti-interference application. The work of Munir and Maud [5] evaluated the use of variable spreading sequences as a means of adding security to communication. The technique proved promising in this regard but was also burdened with complicated synchronization between transmitter and receiver. A 2018 study [6] evaluated three jamming techniques, namely single-tone, narrow-band, and correlated jamming based on pseudo-code phase-shift keying (PSK) modulation, acting on DSSS underwater acoustic communications. In the evaluated situation, where the interfering agent perfectly knows the characteristics of the target signal, correlated jamming was slightly more effective than single-tone, while narrow-band jamming performed worse than both.

Although interference is an undesirable element in many cases, its use as a security method has also been explored. Cooperative jamming, where artificial noise transmission obscures the message, aiming to prevent interception by an intruder [7], [8], is one such example. Techniques of this type can be applied, for example, but not exclusively, to UAVs [9], IoT [10], or other types of communication networks [11]. Applications like these support the paradigm of using intentional interference to protect against malicious agents.

New tests on different digital communication systems and reception scenarios are still necessary to aim for a deeper understanding of the various available jammers and select the most effective jamming technique for each case. To that

This work was partially supported by Rede Nacional de Ensino e Pesquisa (RNP), with resources from Ministério da Ciência, Tecnologia e Inovações (MCTIC), under the Brazil 6G Project of the Radiocommunication Reference Center (Centro de Referência em Radiocomunicações (CRR)) of the National Institute of Telecommunications (Instituto Nacional de Telecomunicações (Inatel)), Brazil, under Grant 01245.010604/2020-14, by Minas Gerais Research Foundation (FAPEMIG) (RED-00194-23), under Minas Gerais Research Network in 5G and 6G project, by CNPq (Grant References 311470/2021-1 and 403827/2021-3), by the projects XGM-AFCCT-2024-2-5-1 and XGM-FCRH-2024-2-1-1 supported by xGMobile – EMBRAPII-Inatel Competence Center on 5G and 6G Networks, with financial resources from the PPI IoT/Manufatura 4.0 from MCTI grant number 052/2023, signed with EMBRAPII, and by Fapemig (PPE-00124-23).

end, in this paper, a wide set of simulations are conducted covering transmission and reception of a BPSK and a DSSS (used in practical drone communication) systems alongside six jamming techniques: (i) single-tone, (ii) multi-tone, (iii) narrow-band noise (NBN), (iv) tone pulse, (v) NBN pulse, and (vi) swept; each of these jammers operating against both BPSK and DSSS. In the simulations, both systems' performances are evaluated in terms of bit error rate (BER) for various values of jammer-to-signal ratio (JSR), which also takes into account the thermal noise present in the receivers. The results draw several conclusions regarding the feasibility of using each type of jammer, considering the two communication systems under analysis.

The rest of the article is divided as follows. Section II briefly describes some principles of digital modulation and intentional interference in communications systems. Section III presents a detailed simulation setup. The results are presented in Section IV. Finally, Section V provides some concluding remarks.

II. Principles of Digital Modulation and Radiofrequency Interference

A. BPSK Communication Systems

The binary phase shift keying (BPSK) modulation has been chosen to represent the conventional non-spread spectrum system since it has the best BER performance under additive white Gaussian noise (AWGN) channel among digital modulations [12]. BPSK modulation is composed of two antipodal symbols, meaning that the symbols have equal energies but inverted phases. Their signal expressions can be written as $s_1(t) = \sqrt{2E_\mathrm{b}/T_\mathrm{b}} \cos 2\pi f_\mathrm{c} t$ and $s_2(t) = -\sqrt{2E_\mathrm{b}/T_\mathrm{b}} \cos 2\pi f_\mathrm{c} t$, where E_b is the average bit energy, T_b is the bit interval, and f_c is the carrier frequency. Being antipodal, the BPSK modulation has only one basis function $\phi_1(t)$ of unitary energy given by $\phi_1 = \sqrt{2/T_\mathrm{b}} \cos 2\pi f_\mathrm{c} t$, $0 \leq t < T_\mathrm{b}$.

1) BPSK transmission: A converter receives equiprobable information bits, either 0 or 1, and returns corresponding signal levels of $-\sqrt{E_\mathrm{b}}$ and $\sqrt{E_\mathrm{b}}$, respectively. This output is then multiplied by the base function $\phi_1(t)$, resulting in the BPSK signal.

2) BPSK reception: In order to achieve coherent detection, the receiver must generate a local basis function that is in phase with the received signal. Given that BPSK modulation is unidimensional, only a single correlator is required by the receiver. Subsequently, bit-time integration and a sample-and-hold process are performed. Finally, a decision block checks whether the result is positive or negative, thereby estimating the transmitted bit. The BER of BPSK over an AWGN channel with a noise power spectral density (PSD) of N_0 is given by

$$P_\mathrm{b} = \frac{1}{2} \mathrm{erfc}\left(\sqrt{\frac{E_\mathrm{b}}{N_0}}\right), \tag{1}$$

where $\mathrm{erfc}(\cdot)$ is the complementary error function.

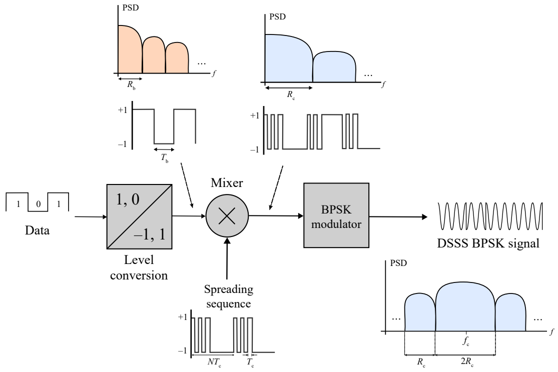

Figure 1. Block diagram of a DSSS BPSK transmitter.

B. DSSS Communication Systems

The spread spectrum (SS) technique involves widening a signal's bandwidth to a value much higher than the bandwidth normally required to transmit it. SS signals' distinct attribute is their low PSD, which makes them robust against radiofrequency (RF) interference. Suppose a hostile agent tries to jam an SS communication by applying a narrow-band interfering signal. In that case, the hindering signal will act only over a small fraction of the information, not being able to make communication unfeasible completely. The SS signals' low PSD also makes them very difficult to detect. If the PSD is sufficiently low, the signal can be kept below the noise level [12]. Some of the main SS techniques are direct-sequence SS (DSSS), frequency-hopping SS (FHSS), time-hopping SS (THSS), and chirp SS (CSS). This article uses the DSSS technique to represent an SS system since it is commonly employed in UAV communication.

1) DSSS transmission: Fig. 1 shows a block diagram representation of a DSSS transmitter. It begins with the conversion of information bits, in its unipolar form, to a bipolar form. The spectral result of this conversion is concentrated in a central lobe of width R_b Hz. Next, this resulting signal is multiplied by the pseudo-random (PN) spreading sequence of rate R_c. As a result, we have a DSSS signal in the baseband with a bandwidth equal to $1/T_\mathrm{c} = R_\mathrm{c}$, considering only the main lobe. Once the spreading process is completed, the signal is shifted to the passband and is transmitted through the communication channel. It is worth noting that the transmitted signal has a bandwidth equal to $R_\mathrm{c} \gg R_\mathrm{b}$.

2) DSSS Reception: Fig. 2 shows the block diagram of a DSSS receiver. It starts with a downconversion of the received signal from the passband to the baseband. Next, the baseband signal goes through a despreading process through correlation with a PN sequence identical to that used on the transmission side. The correlator output is sampled to generate a decision variable, which is compared with the threshold results in the estimated bits. The DSSS BER over AWGN is the same as in equation (1) [12]. In the presence of narrow-band interference, the system presents an SNRI gain, also known as processing gain (PG), which, theoretically, considering a uniformly dis-

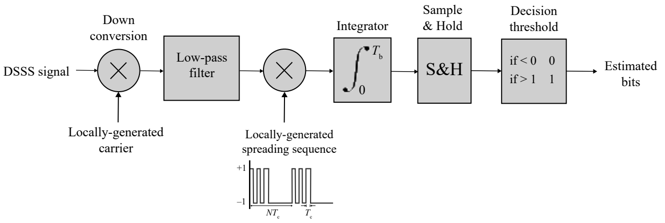

Figure 2. Block diagram of a DSSS BPSK signal reception.

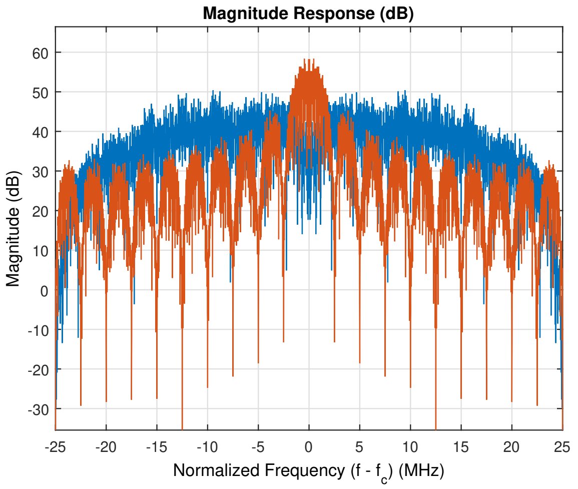

Figure 3. Estimated PSD for conventional BPSK (orange) and DSSS (blue) transmission signals. This figure is better viewed in color.

tributed interfering PSD, is given by $\text{PG} = R_\text{c}/R_\text{b}$.

C. Intentional Interference in Communication Systems

RF interference can be defined as an intrusive signal in a certain region of the spectrum where communication occurs. An important parameter for the quality of communication is the signal-to-interference-plus-noise ratio (SINR) at reception. In the presence of interference, SINR is reduced, reducing the quality of communication [13]. Signal jamming, also known as radio jamming, can be operated in several ways. It is possible to cite at least 7 types of jamming techniques, i.e., by noise, by tone, by frequency sweep, by pulse, follower jamming, smart jamming, and partial dwell jamming of FHSS systems [13]. This work covers only the first four techniques, as mentioned earlier.

1) Noise Jamming: This technique seeks to degrade the quality of communication by introducing a noisy signal into the target channel. Commonly, this jammer is a Gaussian-type signal, and its bandwidth can be narrow or as wide as the communication spectrum itself, depending on the scenario [13]. When noise jamming covers the entire spectrum where the target communication operates, it is called broad-band noise (BBN). This is useful when the information on the target signal's spectral characterization is limited. Since this type of interference is dispersed over a large band, the jamming signal tends to have low PSD and may not be able to significantly affect the target. Another way to operate noise jamming is by obstructing just one communication channel, which requires knowing exactly where in the spectrum the communication occurs. This type of jamming is called narrow-band noise (NBN) and uses less power than the previous techniques [13]. An intermediate approach between BBN and NBN jamming is called partial-band noise (PBN).

2) Tone Jamming: This type of blocking uses single or multiple continuous sinusoidal wave signals. Single-tone jamming concentrates power at a single point in the spectrum, while multi-tone jamming positions a variety of tones along the spectrum. In situations where extensive knowledge about the communication to be interfered with is not available, using multiple interfering signals increases the probability of success at the cost of dividing the jammer's power [13].

3) Swept Jamming: This method consists of a narrow-band signal, an NBN or a tonal signal, whose spectral position changes over time. The interference is positioned on a single narrow spectral position at a given moment. However, it moves through the frequency spectrum. Thus, the signal can act over an extensive frequency range [13].

4) Pulse Jamming: In this technique, an interfering signal pulses at periodic intervals. Considering a fixed interfering power, the shorter the activity time, the greater the instantaneous interfering power within this interval, increasing the chances of successfully affecting the target. Compared to other jamming techniques, this method requires a lower average power level for similar effectiveness [13].

III. Simulation Setup

In order to evaluate the effectiveness of each interference technique in compromising conventional and SS communications, a simulation was implemented in MATLAB®, which covers two transmission and reception systems: a BPSK system and a BPSK DSSS system. In addition, jammers of the following types were implemented: single-tone, multi-tone, NBN, tone pulse, NBN pulse, and frequency-swept jamming.

The communication system parameters were selected to align with those typically used in real-world drone applications, as follows: (i) bit rate: $R_\text{b} = 2.5$ Mbps; (ii) carrier frequency: $f_\text{c} = 2450$ MHz. Additionally, for the DSSS system, along with the previous parameters, the following were also considered: (iii) chip rate: $R_\text{c} = 25$ Mchips/s; (iv) PN sequence with a length of 15 chips; and $\text{PG}_\text{dB} = 10$ dB.

The simulated BPSK and DSSS transmitter and receiver modules were designed in accordance with the theoretical frameworks outlined in Section II A and B. Fig. 3 presents the simulated normalized estimated PSD considering unitary power for signals from both transmission techniques for the aforementioned parameters.

A. Jammers Simulation

Six jamming techniques were implemented in MATLAB®. Once enabled, the interference will be added to the transmitted

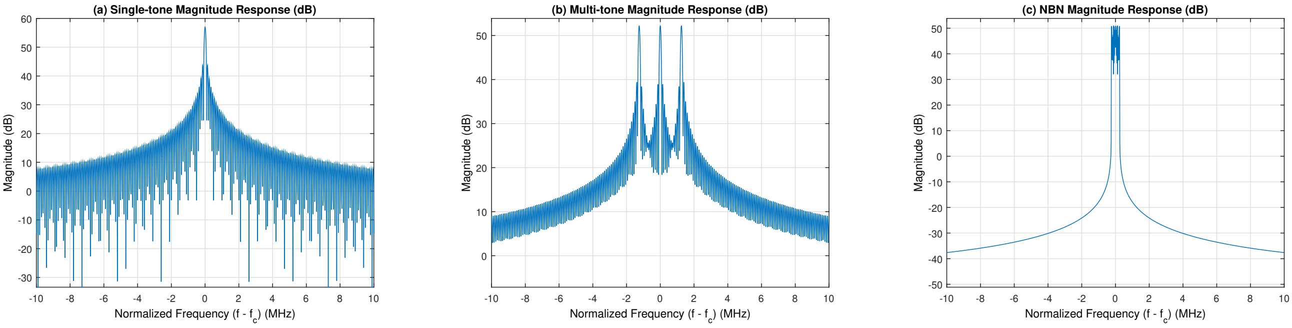

Figure 4. Normalized power spectrum density for (a) single-tone, (b) multi-tone, and (c) NBN jammers.

signal, degrading the quality of reception and, consequently, increasing the BER. The following is a description of each jamming technique's software implementation and parameters.

1) Single-tone Jammer: The single-tone jammer is generated by a single cosinusoidal signal $\cos(2\pi f_c t)$, where f_c is the spectral position of the jamming tone, defined here to be equal to the carrier frequency of the signal being jammed, which in our case is $f_c = 2450$ MHz, also utilized as center frequency operation for all subsequent jammers.

2) Multi-tone Jammer: In this case, the jamming signal is generated by the sum of multiple cosines with different frequencies. We considered three tones: one positioned at the same frequency as the signal's carrier and the other two equally spaced from the central one by 1.25 MHz. This spacing corresponds to a shift of $1/2$ of the system's bit rate. Therefore, the jamming tones were placed at 2448.75 MHz, 2450 MHz, and 2451.25 MHz.

3) NBN Jammer: The NBN signal is generated from a vector containing AWGN samples filtered through a 35th-order IIR low-pass filter with a cutoff frequency of 0.5 MHz, which corresponds to 20% of the considered bit rate. Finally, the filtered base-band samples are then translated to the operating center frequency of $f_c = 2450$ MHz.

4) Tonal Pulse Jammer: The jamming signal, in this case, is generated similarly to the tone jammer, but with a key difference: the interfering signal is active for only a fraction of the total simulation time, creating a burst effect. Given the same interference power, this approach results in a higher amplitude of the interfering signal compared to the single-tone technique, but with activity confined to a smaller portion of the simulation time. In the scenario considered, the jamming activity is designed to occur for only 10% of the total simulation time.

5) NBN Pulse Jammer: In this method, the interfering vector signal is first generated as a conventional NBN signal and then limited to a specific time range, similar to regular tone pulse jamming. The interference activity is also designed to occur for only 10% of the total simulation time.

6) Swept Jammer: In this technique, the jammer uses a single tone at any given time: at the beginning of the transmission, the interference is at 2448 MHz and increases up to it shifts to 2452 MHz. The considered swept time was 40 ms.

For illustrative purposes, Fig. 4 shows some normalized PSDs considering a unitary power for three types of jammers: (a) single-tone, (b) multi-tone, and (c) NBN. Notice that the level of the three tones in the multi-tone technique (Fig. 4(b)) is lower than that of the single-tone technique (Fig. 4(a)) because it needs to split its power across three frequency positions. Additionally, the average level of the NBN technique (Fig. 4(c)) is lower than that of the other two since it spreads the power over a wider frequency range. The PSD for the tonal pulse and NBN pulse techniques during activation would be similar to those shown in Fig. 4(a) and Fig. 4(b), respectively, but with higher levels, as these techniques concentrate all power within a 10% simulation time interval. The swept jammer technique would have an instantaneous spectrum similar to that shown in Fig. 4(a), but with a dynamic tone that changes its position over time.

IV. Numerical Results

To generate the performance curves presented in this section, the jammer-to-signal ratio (JSR), denoted by J/P, was varied incrementally from 0 dB to 30 dB. For each performance point, 10^6 bits were transmitted, and the BER at the receiver was estimated by dividing the number of error bits by the total number of transmitted bits. In addition to external interference, a simulated AWGN channel with an E_b/N_0 ratio of 20 dB was considered for all evaluated cases[1]. It is worth noting that the most effective jamming technique results in the highest BER values.

A. Comparison of the Jammers over BPSK

The BER curves of the conventional BPSK system under attack by each evaluated jammer are shown in Fig. 5(a). Analyzing the results, it can be observed that all evaluated jamming techniques, except for the multi-tone method, achieve a BER $> 10^{-3}$ for all values of JSR. Single-tone is the most effective technique for disrupting communication, as it

[1] The $E_b/N_0 = 20$ dB value has been chosen because it is commonly encountered in practical communication systems, providing a very low BER for BPSK and DSSS systems. In the presence of jammers, considering a JSR from 0 to 30 dB, the interfering power is much higher than the AWGN noise power; thus, the JSR in dB $\approx -$SINR in dB.

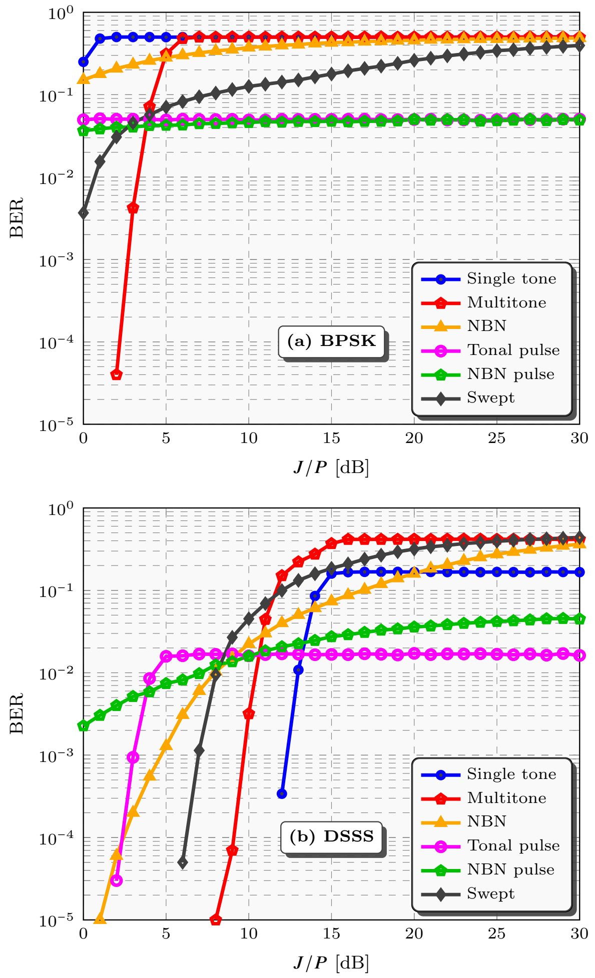

Figure 5. BER curves of (a) BPSK and (b) DSSS systems under jamming attack.

yields a BER $= 0.5$ across all JSR levels, indicating complete degradation of the communication link. For values of $J/P \geq 6$ dB, multi-tone jamming starts to present the same result as its single-tone counterpart and NBN jamming, despite converging to BER $= 0.5$, presents slightly lower performance than the latter two. Swept jamming achieved lower performance than the above-mentioned, except for $J/P < 4$, which performs better than the multi-tone technique. Tonal pulse and NBN pulse jamming have approximately a constant BER $= 0.05$ for any JSR values. It occurs because they can corrupt the transmitted bits totally, but only for 10% of simulation time during the active period.

The aforementioned observations highlight the significant vulnerability of the BPSK modulation scheme to intentional jamming attacks. In narrow-band communication, most information is concentrated on the central frequency (see the BPSK PSD in Fig. 3). By concentrating its power in this spectral position, single-tone interference has been more successful in disrupting communication than other techniques. Similarly, the NBN method also concentrates interfering power on f_c, although less effectively. In multi-tone jamming, the signal being distributed across three tones becomes less concentrated on f_c, making its performance worse at lower JSRs than the single-tone. The single-tone technique is the easiest to construct in terms of implementation complexity, requiring only an oscillator at the central frequency and a power amplification system.

B. Comparison of the Jammers over DSSS

The BER curves of the DSSS system under attack by each evaluated jammer are shown in Fig. 5(b). It can be seen that for $J/P < 4$ dB, the NBN pulse jammer is the only method capable of introducing some BER on the DSSS communication. This demonstrates the robustness of this technology against deliberate interferences. For $4 \leq J/P \leq 8$ dB, the tone pulse jamming starts to perform slightly better than the NBN pulse technique but keeps its BER ≈ 0.016 for all subsequent JSRs. In the same range, NBN interference begins to have BER $> 10^{-3}$, but inferior to the ones obtained for the latter two mentioned techniques. For $8 < J/P \leq 11$ dB, swept jamming outperforms all methods, and most BER curves intersect each other. For $J/P \geq 12$ dB, the multi-tone jamming is the most effective in causing bit errors, and above $J/P \geq 20$ dB, each curve tends towards its stabilization level (maximum BER for each technique).

In summary, pulsed techniques (NBN and tonal) have proven effective against the SS system for lower JSR values compared to the other jammers, suggesting that they could be a good option when the jammer device has power limitations. On the other hand, for high JSR values, they have achieved the poorest performance, i.e., lowest BER, since they concentrated their higher interfering power in only a fraction of the jammer's total operating time. Three techniques (multi-tone, swept, and NBN) tend to have BERs close to 50% at high JSR values. The single-tone jamming has presented the lowest performance among all evaluated techniques over DSSS for $J/P \leq 13$ dB. This is because it concentrates its total power in only one point of the frequency spectrum, being low effective against the wide frequency SS signal. In addition, the DSSS processing gain has more effect under narrow-band jamming [12].

The results demonstrate the advantages of using the SS technique in mitigating all examined jammers compared to conventional systems. By comparing Figs. 5(a) and 5(b), it can be realized that DSSS has exhibited greater resistance against all tested interferences, as indicated by the rightward shift in each jammer's curve, suggesting the need for higher interfering power to disrupt communication. Additionally, a downward shift in single-tone and tonal pulse cases reflects a reduction in the maximum possible BER for these techniques.

V. Conclusions

This work has contributed to advancing knowledge about various intentional interferences jamming conventional and SS communication systems. It has been concluded that against conventional BPSK communication, single-tone jamming is the most effective to disturb communication. However, the most effective interference technique depends on the JSR for interrupting the evaluated DSSS system. For $J/P < 4$ dB, an NBN pulse is most effective; for $4 \leq J/P \leq 8$ dB, a tonal pulse is better; for $8 < J/P \leq 11$ dB, the most adequate is swept jamming; and for a $J/P \geq 12$ dB, the best choice is multi-tone jamming. The presented conclusions not only enhance the theoretical understanding of the jamming techniques and evaluated systems but also assist in determining the most effective technique in specific practical application scenarios under different operating conditions, which could be crucial for interrupting the communication of the target system successfully.

References

[1] T. Braun, "Miniature menace: The threat of weaponized drone use by violent non-state actors," 960th Cyberspace Wing, Tech. Rep., Sep 2020, [Online]. Available: https://www.960cyber.afrc.af.mil/News/Article-Display/Article/2353270/miniature-menace-the-threat-of-weaponized-drone-use-by-violent-non-state-actors/ [Accessed: 8th Jan. 2024].

[2] T. Wright, "How many drones are smuggling drugs across the U.S. southern border?" Smithsonian Magazine, Tech. Rep., Jun 2020, [Online]. Available: https://www.smithsonianmag.com/air-space-magazine/narcodrones-180974934/ [Accessed: 10th Feb. 2024].

[3] R. A. Scholtz, "Notes on spread-spectrum history," *IEEE Trans. Commun.*, vol. 31, no. 1, pp. 82–84, Jan. 1983.

[4] X. Tan, S. Su, and X. Sun, "Research on narrowband interference suppression technology of UAV network based on spread spectrum communication," in *2020 IEEE Int. Conf. on Artificial Intelligence and Information Systems (ICAIIS)*, Mar. 2020, pp. 335–338.

[5] M. A. Munir and A. R. M. Maud, "Direct-sequence spread spectrum with variable spreading sequence for jamming immunity," in *2019 16th Int. Bhurban Conf. on Applied Sciences and Technology (IBCAST)*, Jan. 2019, pp. 933–937.

[6] L. Ma, C. Fan, W. Sun, and G. Qiao, "Comparison of jamming methods for underwater acoustic DSSS communication systems," in *2018 2nd IEEE Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC)*, May 2018, pp. 1340–1344.

[7] Y. Wu and Y. Huo, "A survey of cooperative jamming-based secure transmission for energy-limited systems," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1–11, Jan. 2021.

[8] Y. Wen, L. Liu, J. Li, Y. Li, K. Wang, S. Yu, and M. Guizani, "Covert communications aided by cooperative jamming in overlay cognitive radio networks," *IEEE Trans. Mobile Comput.*, vol. 1, no. 1, pp. 1–14, 2024, Early Access.

[9] C. Zhong, J. Yao, and J. Xu, "Secure UAV communication with cooperative jamming and trajectory control," *IEEE Commun. Lett.*, vol. 23, no. 2, pp. 286–289, Feb. 2019.

[10] Y. Huo, J. Fan, Y. Wen, and R. Li, "A cross-layer cooperative jamming scheme for social internet of things," *Tsinghua Science and Technology*, vol. 26, no. 4, pp. 523–535, Jan. 2021.

[11] Y. Zhong, F. Zhou, Y. Wang, X. Deng, and N. Al-Dhahir, "Cooperative jamming-aided secure wireless powered communication networks: A game theoretical formulation," *IEEE Commun. Lett.*, vol. 24, no. 5, pp. 1081–1085, Feb. 2020.

[12] D. A. Guimaraes, *Digital Transmission: A Simulation-Aided Introduction with VisSim/Comm.* Berlim: Springer, 2009.

[13] R. Poisel, *Modern Communications Jamming Principles and Techniques*, 2nd ed. Norwood: Artech House, 2011.