

Characterization of Illegally Marketed GNSS Jammers

Marc García-Bermúdez
EMC Electromagnetic BCN, S.L.
EMC Barcelona
Barcelona, Spain
0009-0008-9618-7178

Jordi Solé-Lloveras
EMC Electromagnetic BCN, S.L.
EMC Barcelona
Barcelona, Spain
0000-0003-1631-1172

Marco A. Azpúrua
EMC Electromagnetic BCN, S.L.
EMC Barcelona
Barcelona, Spain
0000-0001-8078-5116

Abstract— This paper studies the evolution and impact of low-cost Global Navigation Satellite System (GNSS) jammers, which pose a significant threat to devices that use geolocation. Three illegally marketed jammers with distinct morphologies have been characterized in power and frequency occupancy, using time and frequency domain measurements. Also, the jammers potential effective range is approximated. The study compares both methodologies with the aim of advocating for the use of time domain measurements to provide more detailed insights into jamming influence and behavior using spectrograms and probability distribution analysis. The results show that these devices employ chirp signals or modulated wideband noise to disrupt the pseudo range acquisition by corrupting the data transmitted by satellites, masking the signals, or blocking and saturating receivers of GNSS systems utilizing signals in the L1, E1, B1, and G1 frequency bands. The study further highlights the accessibility and effectiveness of such illegal devices, underscoring the need for jamming detection techniques.

Keywords—GNSS, intentional electromagnetic interference, jammer, navigation systems, radio interference

I. INTRODUCTION

Global Navigation Satellite System (GNSS) technologies are a critical component of modern civil, space, scientific and military infrastructures. However, the proliferation of illegal jamming devices might become a threat to these infrastructures. These electronic devices emit signals to interfere with GNSS communications in order to evade geolocation intentionally. Using these devices for malicious purposes, including theft, kidnapping, smuggling, evasion of justice, evidence tampering, or terrorism, represents a significant security breach in modern critical systems that use geolocation. Consequently, jammers are illegal in numerous countries, including Spain [1]. However, these devices can still be easily and cheaply purchased from online retailers who advertise them as privacy protection devices.

The Finnish Transport and Communications Agency (Traficom) reported 106 instances of GPS disruption during 2024. These incidents involved the use of jammers in vehicles to alter their location, allowing to corrupt the tachographs data and to hide the stops or routes taken by vehicles to their respective companies [2]. Another controversy occurred in West Sussex this year when a Mercedes-Benz C63 AMG was stolen. A jammer device disabled the vehicle's GPS signals. Fortunately, the vehicle was recovered a few hours later thanks to its Stolen Vehicle Recovery (SVR) system [3]. The growing number of reported jamming cases has led the Federal Communications Commission (FCC) to investigate Amazon and other companies for selling devices designed to jam radio frequencies [4].

Numerous studies have analyzed the characteristics of jammer signals and their impact on GNSS communications to develop methods to protect GNSS receivers. Prior research has demonstrated that most jammers utilize narrowband or instantaneous chirp signals to disrupt communication [5]. These jamming signals are emitted at a center frequency proximate to that of GPS signals, which convey pseudo ranges with potential for geolocation.

Several techniques have been developed to maintain reliable signal reception to mitigate jamming in GNSS systems. Antenna-based methods like controlled reception pattern antennas and adaptive antenna arrays use beamforming to suppress interference [6],[7]. Signal processing techniques, including notch filtering and time-frequency analysis, help isolate and remove jamming signals [8][9]. Spread spectrum methods, such as Direct Sequence Spread Spectrum and frequency hopping, enhance signal robustness [10][11]. Additionally, advanced algorithms like Kalman filtering and machine learning-based detection further improve resistance by tracking signal states and classifying interference [12][13]. However, these techniques are predominantly implemented in military-grade receivers or systems with high-security requirements outside the scope of this paper.

In recent years, jamming devices have evolved, allowing the design of jammers that are easier to use, extremely cheap, and easy to buy online, thus resulting in a greater potential to damage GNSS communications. Therefore, this paper aims to update the state of illegal jammers by analyzing three low-cost GNSS jammers with different morphologies. The study focuses first on the characterization of the jamming signals that become electromagnetic interference (EMI) in terms of waveform, power, frequency range, statistics, and effective distance. Secondly, the technical characteristics of the jammers characterized are analyzed and compared with other studies to evaluate the evolution of these illegal devices. Finally, the conclusions review the most common characteristics of GNSS jammers and their emitted signals, and then the real effectiveness of these devices and the improvements of the jamming characterization using time domain measures are discussed.

It is important to mention that all jammers employed in what follows have been operated exclusively under controlled laboratory conditions, inside an anechoic chamber, and with the sole purpose of highlighting the potential dangers of such devices that remain accessible despite their illegal nature. The authors do not endorse using jammers or any other illegal devices to interfere with radiocommunications.

II. JAMMING OVERVIEW

Jammers are electronic devices that intentionally emit signals in the RF spectrum to damage communication systems with effective ranges of a few meters to several hundred or thousands of meters. These devices, although illegal, are easy to obtain through online sellers who offer them cheaply. The simplicity and affordable price of these devices, their convenient distribution through online retailers, and the potential disruption they can cause to communication systems are the perfect combination to carry out illegal acts. For these reasons, the study of these devices and the techniques for mitigating their damage represent a topic of interest to the technical community. This section provides an overview of the current state of the art regarding jammer morphology, interference, and signal characterization.

A. Jamming devices morphology

The jammers that are marketed illegally vary in morphology; however, most of them are characterized by their small size and ease of concealment. In previous studies where commercial jammers have been characterized [14], they have been classified by their morphology in the following manner: Automotive jammers designed to plug into an automotive 12 V auxiliary power supply outlet with a monopole antenna; Jammers powered by rechargeable batteries with an external antenna; Jammers disguised as cell phones with short helical antennas. Since the publication of this article, there has been an evolution in the field of wireless signal jamming technology. The emergence of new, more sophisticated types of jammers that now use microstrip antennas and direct connection to USB or USB-C ports makes it even easier to supply, install, and use such devices.

B. Jamming Interferences

Depending on their impact on GNSS frequencies, jamming interferences can be classified as in-band or out-of-band. In-band jamming is an EMI that occurs within the same frequency band as the receiver's signal, directly disrupting GNSS signal reception. In this case, the EMI stronger signal is superimposed on the GNSS signal, impeding the receiver's capacity to extract the information of the pseudo ranges; this is commonly known as receiver blocking. Jammers that can be obtained illegally use this method, emitting in broadband, narrowband, or sweep frequencies in the same receiver signal band. Out-of-band jamming is defined as EMI occurring outside the frequency range of the receiver's signal. In this instance, the GNSS signals remain unperturbed by the EMI. However, this type of jamming exploits the vulnerabilities of the receiving equipment, such as the bandwidth of the filters utilized to obtain GNSS signals or the saturation limitations of front-end low-noise amplifiers, in order to impede the acquisition of GNSS. Nevertheless, this type of interference can also occur unintentionally, resulting from electromagnetic emissions near the receivers.

C. Jamming characterization methods

As jammers are illegal devices, there are no standardized methods for their characterization. Nevertheless, studies such as [14] and [15] demonstrate that researchers adopt varied approaches, including using RF-shielded test enclosures to prevent the emission of unauthorized signals or deploying GNSS antennas exposed to EMI to capture the jamming signal. Despite these variations, the spectrum analyzer is a common instrument employed in jammer analysis.

However, spectrum analyzers have intrinsic limitations when analyzing jammer signals. This is because, jammers frequently use techniques such as chirping, pulsing, or frequency hopping, which can be hard to identify with traditional frequency-domain analysis. For example, chirping signals that continuously sweep across frequencies may appear as transient or smeared energy, as the analyzer often captures only a portion of the chirp. Regarding the pulsed signals, their detection depends on the resolution bandwidth and sweep time of the analyzer. If the pulses are short or irregular, they might not be fully captured, leading to incomplete or misleading representations. Finally, if frequency hopping signals hop between frequencies faster than the analyzer's sweep time, many hops can go undetected, resulting in scattered peaks that fail to reflect the hopping behavior.

These limitations highlight the need for complementary or alternative measurement techniques for jamming characterization, such as time-domain measurements, which provide greater detail in the signal and allow the measurement of transient and modulation characteristics.

III. METHODOLOGY

For three different jammers, we measured the jamming signals in the controlled environment of a 3 m distance full anechoic chamber. The experimental setup includes a Schaffner CBL6143 log periodic antenna (0.7 GHz to 3 GHz) as a receiver and an R&S RTO64 (10 GSa/s and a bandwidth of 3 GHz) as the measurement instrument using the emiGO software developed by EMC Barcelona, which enables the fast acquisition of the spectrum using measures in the time domain. An R&S Test Receiver model ESPI3 was used for the frequency-swept measurements.

Through over-the-air measurements, the jammer emissions are characterized in terms of frequency, repetitiveness, and amplitude statistics. We also intend to obtain the power of the EMI in the different GNSS frequencies and estimate the effective radius of masking GNSS signals.

The diagram in Fig. 1 shows the implemented experiment setup.

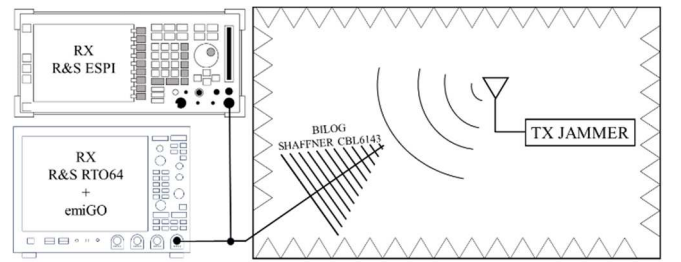


Fig. 1. Experiment setup.

The low-cost GNSS jamming devices considered are shown in Table I.

TABLE I. List of jammers used during the experiments.

ID	JAMMER TYPE
J1	USB GNSS jammer with a microstrip antenna
J2	USB-C GNSS jammer with one antenna
J3	Tunable jammer for GSM/DCS/3G/CDMA with four antennas

The J1 and J2 jammers are compact, user-friendly devices that require only one connection to a USB port to operate. These devices are readily available through the AliExpress platform at a cost ranging between 25 € and 35 €. In contrast, the J3 jammer is a larger and more sophisticated device, not designed to interfere with GNSS bands, but it can interfere with multiple frequency bands simultaneously and features tunable capabilities that, when properly configured, allow to interfere with GNSS bands. Fig. 2 shows the physical design of these jammers.

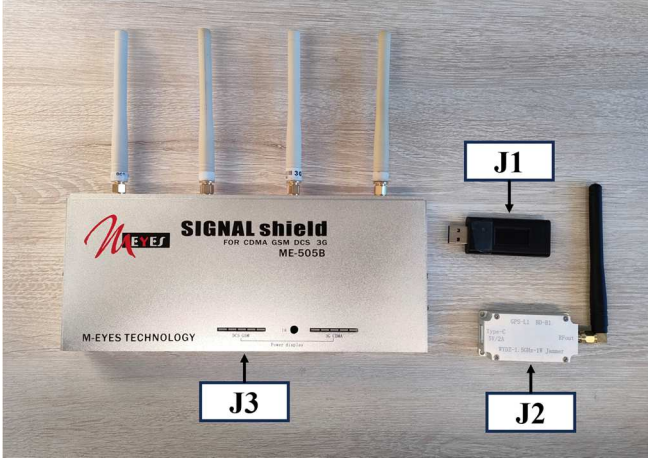


Fig. 2. Jammers used for the experiments.

IV. RESULTS

This section presents the results from the characterization of the jammers.

First, the spectrum derived from the time-domain (R&S RTO + emiGO) and frequency-domain (R&S ESPI3) measurements is presented and compared. Subsequently, the spectrograms generated from time-domain data are introduced. Then, the statistical analysis of the interference patterns is examined. Finally, the maximum effective range for these devices to mask GNSS communications is discussed.

A. Spectrum

Fig.3 shows the spectrum of J1. This broadband signal ranges from 1560 MHz to 1590 MHz, with its center at 1575 MHz, which precisely aligns with the emission frequency of the L1 band. The received signal power is -30 dBm, which can interfere with the L1 band for GPS, SBAS, and QZSS systems and the E1 band for Galileo and B1. Furthermore, this jamming signal may also affect the B1 band of the BeiDou system to a lesser extent (1561.098 MHz).

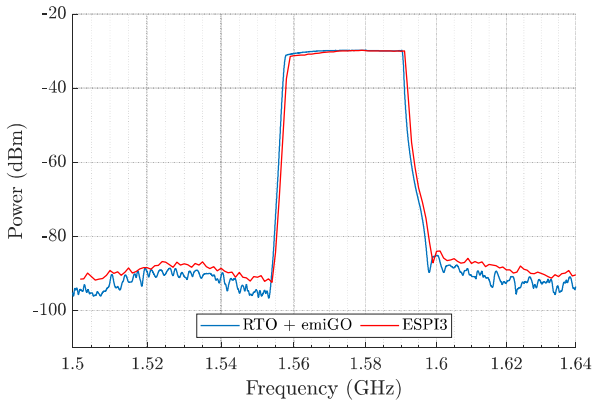


Fig. 3. J1 emission spectrum.

The spectrum of J2 also shows a broadband signal composed of modulated noise in the frequency range of 1530 MHz to 1620 MHz, with a bandwidth of 90 MHz and a central frequency at 1575 MHz, which again corresponds to the central frequency of L1. However, the frequency range with the greatest impact on EMI spans from 1553 MHz to 1595 MHz, with a bandwidth of 42 MHz and an average power of -30 dBm, similar to J1. The maximum lobes at the edges are located at 1555 MHz and 1593 MHz, with a power of -25 dBm. These lobes are not centered on any specific central frequency within the GNSS bands but would affect systems that use L1, E1, B1, and G1 bands.

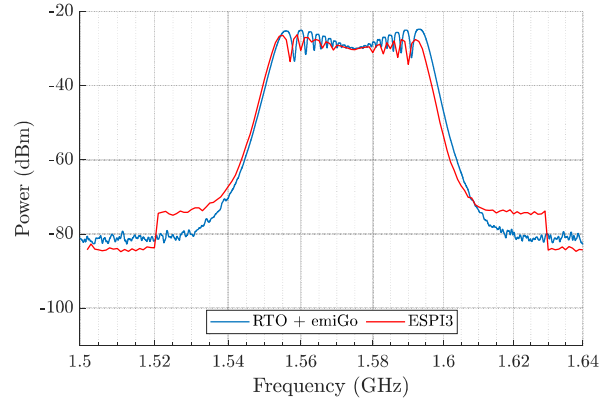


Fig. 4. J2 emission spectrum.

The spectrum of J3 reveals two bands in the range of interest: the first spans from 1521 MHz to 1581 MHz with a bandwidth of 60 MHz, and the second extends from 1596 MHz to 1622 MHz with a bandwidth of 26 MHz. The average power of these signals is -74 dBm and -69 dBm, respectively. This relatively low power, in comparison to the EMIs observed for J1 and J2, is attributed to the fact that this device is mainly intended to interfere mobile communications, and because the power is distributed to transmit simultaneously across multiple bands. The jamming of GNSS systems is achieved by tuning the device to use the spurious components produced. Also, none of the four antennas is specified for GNSS, making the radiation less efficient. Nevertheless, both chirps remain potentially disruptive to the transmissions of GPS, SBAS, and QZSS systems in L1, Galileo in E1, BeiDou in B1I and B1C, and Glonass in G1.

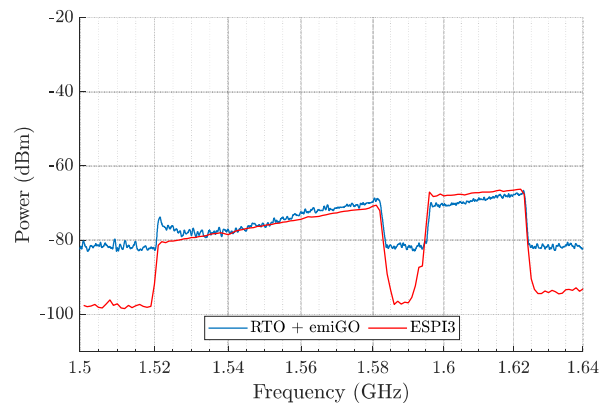


Fig. 5. J3 emission spectrum.

As can be seen in all the previous figures, the spectrums derived from the time domain scan and the frequency swept are coincident. However, time-domain measurements offer additional features presented in what follows.

B. Spectrogram

One of the primary advantages of conducting emissions measurements in the time domain is the ability to generate a spectrogram. This representation, which displays time on the vertical axis, frequency on the horizontal axis, and signal power as a color gradient, offers a comprehensive view of the jamming signal's behavior across both domains. Furthermore, it facilitates identifying and classifying the signal under analysis.

The following section presents the spectrograms corresponding to the emissions of each jammer under study, accompanied by an analysis of their behavior and potential impact on GNSS receivers.

Fig. 6 displays the spectrogram of J1, which reveals the distinctive spectral profile of a chirp signal with a period of 0.25 ms and a bandwidth of 30 MHz. A jamming signal with these characteristics is designed to interfere by effectively masking the useful signal and corrupting the pseudorange data transmitted by the satellites, thereby hindering the localization process. Given its sufficiently high power, this chirp could also potentially saturate the receivers.

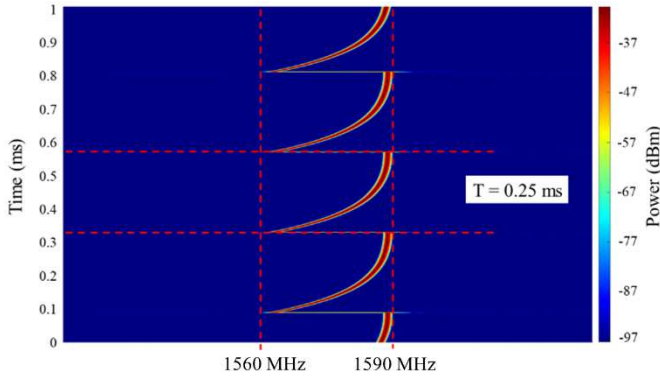


Fig. 6. Spectrogram of J1 emissions.

Fig. 7 presents the spectrogram of J2. The spectral profile shows a wideband stationary signal composed of modulated noise. The spectrogram reveals that the jamming signal of J2 is persistent over time, suggesting that the primary objective of the device is to saturate the receivers, preventing the acquisition of the signal or fully disrupting communication rather than occasionally damaging the pseudo-ranges data.

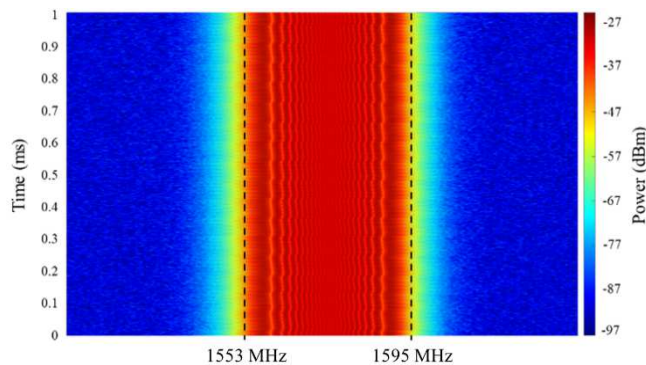


Fig. 7. Spectrogram of J2 emissions.

Fig. 8 illustrates the spectrogram of J3, which exhibits two chirps with bandwidths of 60 MHz and 26 MHz, respectively. Although these chirps are less intense than J1, because they are generated by spurious components produced by a fine tuning of the interference bands, they have a shorter duration with a

period of 20 μ s, which results in a more consistent impact on GNSS communications across the affected frequency bands than J1 but without being as constant as J2. In contrast to the previous spectrograms, Fig. 5 shows a background with a higher noise density, this effect is attributed to the jammer multi-frequency simultaneous emissions.

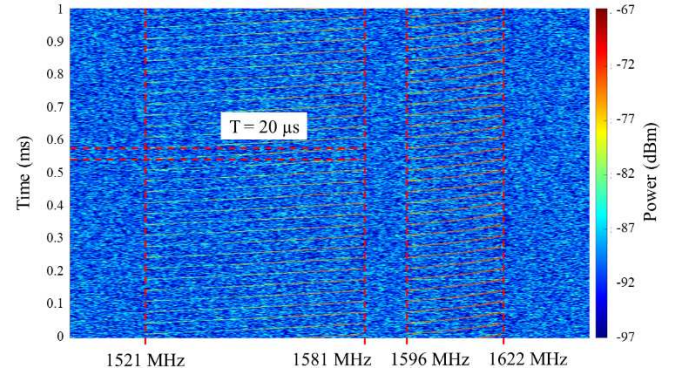


Fig. 8. J3 EMI spectrogram

C. Statistics

The probability density function of the jammer emissions power is calculated for the three samples. For these calculations, a bandwidth of 1 MHz and a central frequency of 1575 MHz, corresponding to L1, were used. Fig. 9 presents the obtained results.

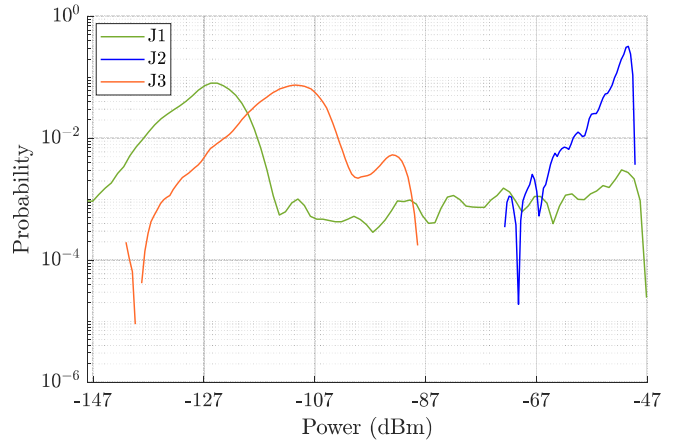


Fig. 9. Probability density distribution of jammer signal power.

J1 and J3 exhibit a bimodal probability distribution. Although subtle, J1 presents a secondary mode in the range of -30 dBm, corresponding to the peak values observed in the chirp spectrum. However, since the chirp predominantly sweeps through other frequencies, its primary mode, which is associated with the highest probability, appears at values close to the instrument's noise floor. This behavior can be seen in the spectrogram shown in Fig.3, where the blue region corresponds to the instrument's background noise. J3 features a secondary mode at approximately -70 dBm associated with the chirp maximum power transmission, while the device's background noise is observed at -90 dBm. These representations highlight the sweeping behavior of these kinds of jammers that employ variable frequencies to corrupt the pseudoranges of data transmitted by GNSS satellites.

In contrast, J2 exhibits a probability distribution where the signal is predominantly transmitted at -30 dBm, with the power distribution less sparse than the other two jammers. This jamming signal, emitted constantly at full power, aims to

mask GNSS signals or block GNSS receivers to avoid pseudorange acquisition.

In conclusion, Fig. 9 depicts two distinct types of probability distributions, each employing fundamentally different mechanisms to disrupt GNSS communications: one primarily targets the corruption of acquired data, while the other seeks to obstruct the reception of signals entirely.

D. Distance

The free-space path loss (PL_{FS}) was employed to approximate the potential effective jamming range, d , of the tested devices (1). This approach assumes a simplified scenario where power losses are solely attributed to the signal's propagation distance and the gains of the transmitting and receiving antennas. For this analysis, L1 band ($f=1575$ MHz) has been used, the antenna gains have been set to a typical value of low directivity antennas ($G_{Tx}=G_{Rx}=3$ dB). The same gain has been assumed for all three devices since, due to their illegality, no datasheets are available, and these values cannot be consulted. The substitution method could be applied to J2 and J3 to estimate their gain; however, typical values allow us to generalize this simplification to other jammers with similar characteristics. It has been considered that the jamming signal will be effective as long as it can fully mask GNSS signals.

$$PL_{FS} = 20\log_{10}(d) + 20\log_{10}(f) - G_{Tx} - G_{Rx} - 147,6 \text{ dB} \quad (1)$$

For jammers J1 and J2, assuming an average signal transmission power of -30 dBm and a GNSS signal with a typical reception power of -120 dBm, the maximum range that jammers can effectively mask the GPS signal is approximately 1 km. Nevertheless, GNSS signals with a lower power level of about -130 dBm could be masked by these jammers in a range of 3 to 4 km. However, in a realistic scenario, the jamming signal would be subject to additional losses, including diffraction and reflection losses when encountering obstacles during propagation, as well as scattering losses due to interactions with small particles of dust or water. These effects would reduce the maximum effective distance for GNSS signal masking. However, a more in-depth analysis would be required to fully assess the impact of these losses, considering the real complexity of the environment, which is beyond the scope of this paper.

For jammer J3, the maximum masking distance for the chirp, with a power level of -74 dBm, is approximately 6 meters, while for the chirp signal at -69 dBm, it extends to around 10 meters. Given that these distances are substantially shorter than those of the other jammers, this device can be deemed significantly less effective for masking GNSS signals. This outcome is expected, as its design is not primarily intended for the disruption of GNSS frequency bands.

V. CONCLUSIONS

Following the analysis of the state of the art in illegal jamming devices and the characterization of the three samples tested, several key conclusions can be formulated.

First, it is observed that jamming devices have evolved over time, becoming more compact, easier to use, cheap, and increasingly accessible through online vendors. These factors, added to false advertisements offering them as privacy-ensuring devices, suggest contemporary jammers remain a significant threat to applications based on GNSS and to all systems that depend on geolocation services.

Advancements in jamming technologies also present significant challenges for detecting and mitigating interference. Consequently, it is crucial to emphasize the importance of continuously evaluating and updating the techniques used for characterizing and analyzing these signals. In this context, we advocate for the use of time-domain measurements. Time-domain measurements offer the advantage of complementing signal characterization by computation of spectrograms and probability distributions. These approaches facilitate a more thorough analysis that allows a more complete jamming signal characterization and a deeper understanding of their impact mechanisms on GNSS communications.

The morphology and characteristics of the jammers evaluated in this study align with the trends identified in prior research. These devices emit chirp or wideband signals with the objectives of either corrupting the pseudo-range data transmitted by satellites or masking the signal, respectively, thereby preventing data acquisition and potentially blocking or saturating receivers. Characterizing these signals through time-domain measurements to obtain their spectrogram and probability distribution not only corroborates previous studies but also highlights the significance of this approach for analyzing jamming techniques and developing effective mitigation strategies.

Conversely, it was observed that the two jammers specifically designed to disrupt GNSS communications were more effective than the mobile communications tunable jammer. These devices emit highly disruptive signals focused on public GNSS communication bands, with an effective range of approximately 1 km to 4 km under ideal conditions. In contrast, the tunable jammer emissions in the GNSS band seem spurious and not efficiently radiated, achieving a significantly shorter effective range, typically less than 10 m.

Based on the results obtained from the characterization, it can be concluded that the jammers interfere with GPS with signals L1 C/A and L1 C, GLONASS with signal L1 C/A, Galileo with signal E1, BeiDou with Signals B1I and B1C, SBAS with L1 and finally QZSS with signals L1 C/A, L1 C and L1 S. None of the signals from the NAVIC GNSS system are interfered with by the characterized jammers.

It is important to note that a larger sample of jammers would be required to corroborate the statements above. Although this study initially aimed to analyze a larger number of devices, some purchased through online platforms were "lost" during the shipping process, probably due to restrictions or controls on their distribution. Notably, companies such as Amazon have begun implementing measures to restrict the sale of these devices, which may reflect an initial response to regulatory investigations initiated by the Federal Communications Commission (FCC) in March 2024 concerning potential violations of FCC regulations related to the marketing and sale of equipment lacking proper FCC authorization [4].

ACKNOWLEDGEMENTS

This work was supported in part by the project 21NRM06 EMC-STD, which has received funding from the European Partnership on Metrology, co-financed from the European Union's Horizon Europe Research and Innovation Programme and by the Participating States. EMC Barcelona is an ESA BIC Incubatee in Barcelona.

REFERENCES

- [1] España, Jefatura del Estado, “Ley 11/2022, de 28 de junio, General de Telecomunicaciones”, «BOE» núm. 155, de 29 de junio de 2022, páginas 91253 a 91411, BOE-A-2022-10757. Available: <https://www.boe.es/eli/es/l/2022/06/28/11>.
- [2] YLE NEWS, “Finland detects more GPS jammers as drivers increasingly try to hide their tracks”, Available: <https://yle.fi/a/74-20078739>.
- [3] GBN, Felix Reeves, “Drivers warned of new signal ‘jammers’ used by criminals to steal vehicles and stay undetected”, Available: <https://www.gbnews.com/lifestyle/cars/drivers-warned-signal-jammers-car-theft>.
- [4] NBC NEWS, David Ingram, “The FCC is investigating Amazon over the alleged marketing and sale of outlawed products”, Available: https://www.nbcnews.com/tech/security/amazon-investigation-fcc-government-products-outlawed-rcna144325?cid=sm_npd_nn_tw_ma&taid=65fb4191cdbb810001abe368&utm_campaign=trueanthem&utm_medium=social.
- [5] A. Di Fonzo, M. Leonardi, G. Galati, P. Madonna and L. Sfarzo, “Software-Defined-Radio techniques against jammers for in car GNSS navigation,” *2014 IEEE Metrology for Aerospace (MetroAeroSpace)*, Benevento, Italy, 2014, pp. 320-325, doi: 10.1109/MetroAeroSpace.2014.6865942.
- [6] H. Powell, R. W. Jackson and D. -H. Kwon, “Effects of Jammer Bandwidth and Sampling Duration on CRPA Null Placement,” *2024 IEEE INC-USNC-URSI Radio Science Meeting (Joint with AP-S Symposium)*, Florence, Italy, 2024, pp. 143-144, doi: 10.23919/INC-USNC-URSI61303.2024.10632472.
- [7] Changeui Shin et al., “Implementation of an Antenna Array for Satellite Communications with the Capability of Canceling Jammers,” in *IEEE Antennas and Propagation Magazine*, vol. 55, no. 1, pp. 32-48, Feb. 2013, doi: 10.1109/MAP.2013.6474483.
- [8] S. W. Arif, A. Coskun and I. Kale, “A Novel Optimization Algorithm for Notch Bandwidth in Lattice Based Adaptive Filter for the Tracking of Interference in GPS,” *2020 IEEE International Symposium on Circuits and Systems (ISCAS)*, Seville, Spain, 2020, pp. 1-5, doi: 10.1109/ISCAS45731.2020.9181117.
- [9] P. Wang, E. Cetin, A. G. Dempster, Y. Wang and S. Wu, “Improved Characterization of GNSS Jammers Using Short-Term Time-Frequency Rényi Entropy,” in *IEEE Transactions on Aerospace and Electronic Systems*, vol. 54, no. 4, pp. 1918-1930, Aug. 2018, doi: 10.1109/TAES.2018.2805195.
- [10] T. Arbi, B. Geller and O. P. Pasquero, “Direct-Sequence Spread Spectrum with Signal Space Diversity for High Resistance to Jamming,” *MILCOM 2021 - 2021 IEEE Military Communications Conference (MILCOM)*, San Diego, CA, USA, 2021, pp. 670-676, doi: 10.1109/MILCOM52596.2021.9652967.
- [11] D. R. Kartchner and S. K. Jayaweera, “A Frequency-Hopping Game Between a Smart Jammer and a Cognitive Radio,” *2019 IEEE International Conference on Internet of Things and Intelligence System (IoTIS)*, Bali, Indonesia, 2019, pp. 12-17, doi: 10.1109/IoTIS47347.2019.8980452.
- [12] P. Wang, Y. Wang, E. Cetin, A. G. Dempster and S. Wu, “Time-Frequency Jammer Mitigation Based on Kalman Filter for GNSS Receivers,” in *IEEE Transactions on Aerospace and Electronic Systems*, vol. 55, no. 3, pp. 1561-1567, June 2019, doi: 10.1109/TAES.2018.2869507.
- [13] I. E. Mehr and F. DAVIS, “Detection and Classification of GNSS Jammers Using Convolutional Neural Networks,” *2022 International Conference on Localization and GNSS (ICL-GNSS)*, Tampere, Finland, 2022, pp. 01-06, doi: 10.1109/ICL-GNSS54081.2022.9797030.
- [14] R. H. Mitch, R. C. Dougherty, M. L. Psiaki, S. P. Powell, B. W. O’Hanlon, J. A. Bhatti, and T. E. Humphreys, “Signal characteristics of civil GPS jammers,” in *Proc. of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION/GNSS)*, Portland, OR, Sep. 2011, pp. 1907–1919.
- [15] P. Uhrich, M. Abgrall, F. Riedel, B. Chupin, J. Achkar and G. D. Rovera, “An Out-of-Band Signal Jamming GNSS L1-Band in Observatoire de Paris,” *2021 Joint Conference of the European Frequency and Time Forum and IEEE International Frequency Control Symposium (EFTF/IFCS)*, Gainesville, FL, USA, 2021, pp. 1-5, doi: 10.1109/EFTF/IFCS52194.2021.9604265.