Dariusz ZMYSŁOWSKI
Military University of Technology
e-mail: dariusz.zmyslowski@wat.edu.pl; ORCID: 0000-0002-1214-1308

Michał KRYK
Military University of Technology
e-mail: michal.kryk@wat.edu.pl; ORCID: 0000-0002-6824-2247

Jan KELNER
Military University of Technology
e-mail: jan.kelner@wat.edu.pl; ORCID: 0000-0002-3902-0784

DOI: 10.55676/asi.v4i2.64

TESTING GNSS RECEIVER ROBUSTNESS FOR JAMMING

BADANIE ODPORNOŚCI ODBIORNIKA GNSS NA ZAGŁUSZANIE

Abstract

Global Navigation Satellite Systems (GNSSs) providing positioning, navigation and synchronization, has become an important element of modern systems and devices that have a crucial impact on many economy branches and the life of an common person. Literature analysis and reports from recent armed conflicts show that the use of techniques for jamming and spoofing GNSS signals is becoming increasingly. This reduces the level of safety in transport and increases the risk of improper operation of GNSS-based systems, like cellular telephony or bank sector. This paper focuses on the methodology for testing the GNSS receiver robustness for jamming. For this purpose, a broadband jamming device was developed.

Keywords: GNSS, receiver, jammer, robustness, test methodology

Streszczenie

Globalne systemy nawigacji satelitarnej (GNSS) zapewniając pozycjonowanie, nawigację i synchronizację, stały się istotnym elementem współczesnych systemów i urządzeń, które mają kluczowy wpływ na wiele gałęzi gospodarki i życie zwykłego człowieka. Analiza literatury oraz doniesienia z ostatnich konfliktów zbrojnych pokazują, że wykorzystanie technik zagłuszania i fałszowania sygnałów GNSS staje się coraz bardziej powszechne. To powoduje zmniejszenie poziomu bezpieczeństwa w transporcie oraz wzrost ryzyka niewłaściwego działania systemów opartych na GNSS. Ten artykuł poświęcony jest metodyce testowania odporności odbiornika GNSS na zagłuszanie. W tym celu opracowane zostało szerokopasmowe urządzenie zagłuszające.

Słowa kluczowe: GNSS, odbiornik, urządzenie zagłuszające, odporność, metodyka badań

Artykuł wpłynął do redakcji: 2.09.2023 / Zatwierdzono do publikacji: 30.12.2023

1. INTRODUCTION

The satellite navigation development has created new opportunities in many areas of industry, economy and science. When we talk about satellite navigation, we usually mean the global navigation satellite systems (GNSSs) and the positioning, navigation, and timing (PNT) services that these systems provide. Currently, it is difficult to imagine the functioning of many GNSS-based systems and devices that play an key role in the life of an ordinary person. Air, sea, and land transport are the basic areas of GNSS application[1]. However, modern telecommunications (i.e., GNSS are responsible for the synchronization of the time scale in extensive radiocommunication networks, including mobile telephony), banking and financial sectors, geodesy and cartography, archeology and geology, logistics, security, emergency services, other satellite systems cannot function without PNT. Of course, apart from civilian systems, most modern military systems, including communication, radar, electronic warfare, missile and guided weapon systems, and all types of vehicles are based on GNSS technology. The contemporary development of unmanned platforms, including unmanned aerial vehicles (UAVs)[2] and unmanned water vehicles (USVs)[3], with civil and military applications, would not be possible without PNT.

Considering the wide area of PNT application, it is difficult to imagine the potential damage to the economy in the event of a long-term GNSS failure. Such threats introduce numerous sources of interference, which may be unintentional (e.g., increased solar activity) or intentional (e.g., jamming and spoofing)[4]. Therefore, there is a need to monitor the availability and correctness of the received GNSS signal, provide backup PNT systems or develop GNSS receivers resistant to jamming or spoofing[5].

In this paper, we present the concept of testing the GNSS receiver robustness for jamming. We present the structure of the developed jammer that can be used in a test environment. The rest of the paper is organized as follows. Section 2 presents a brief descriptions of GNSSs, in particular their classification, used radio frequency (RF) bands, and receiver structure. Sources of interference including jamming and spoofing is considered in Section 3. The structure of the developed jammer and the initial proposal of test methodology of the GNSS receive robustness for jamming are described in Section 4. The final part contains a summary.

1 C. Specht, GPS system (in Polish: System GPS), Navigation Library (Biblioteka Nawigacji) 1 (Peplin: Wydawnictwo Bernardinum, 2007).

2 M. Specht et al., Comparative Analysis of Unmanned Aerial Vehicles Used in Photogrammetric Surveys, TransNav, International Journal on Marine Navigation and Safety Od Sea Transportation 17, no. 2 (June 1, 2023): 433–43, https://doi.org/10.12716/1001.17.02.21.

3 M. Specht et al., Assessment of the Steering Precision of a Hydrographic Unmanned Surface Vessel (USV) along Sounding Profiles Using a Low-Cost Multi-Global Navigation Satellite System (GNSS) Receiver Supported Autopilot, Sensors 19, no. 18 (September 2019): 3939, https://doi.org/10.3390/s19183939.

4 P. Sokolenko, GNSS Signal Monitoring, GPSPATRON, February 11, 2020, https://gpspatron.com/gnss-signal-monitoring/.

5 A. Felski, Methods of Improving the Jamming Resistance of GNSS Receiver, Annual of Navigation 23, no. 1 (2016): 185–98, https://doi.org/10.1515/aon-2016-0013.

 DOI: 10.55676/asi.v4i2.64

2. GLOBAL SATELLITE NAVIGATION

2.1. GNSS CLASSIFICATION

Currently, there are four GNSSs with global covarage, i.e.[6]:

- Galileo,
- Global Positioning System (GPS),
- GLObal NAvigation Satellite System (GLONASS),
- BeiDou or BeiDou Navigation Satellite System (BDS),

and two with regional covarage:

- Quasi-Zenith Satellite System (QZSS),
- Indian Regional Navigation Satellite System (IRNSS) or Navigation with Indian Constellation (NavIC).

QZSS and NavIC are sometimes called regional navigation satellite system (RNSS). According to some literature sources, Doppler Orbitography and Radio-positioning Integrated by Satellite (DORIS)[7] may also be classified as GNSS. Table 1 contains basic information about the operator and the constellation of space segment satellites (based on 8).

Table 1. Basic information about GNSS space segment

GNSS	Operator (country)	Coverage	Altitude (km)	Satellites in orbit
GPS	US Space Force (USA)	Global	20 180	31
GLONASS	Roscosmos (Russia)	Global	19 130	24
Galileo	GSA and ESA (EU)	Global	23 222	26
BDS/BeiDou	CNSA (China)	Global	21 528 (MEO satellites) 35 786 (GEO and IGSO satellites)	48
QZSS	JAXA (Japan)	Regional	32 000 (perigee) 40 000 (apogee)	4
IRNSS/NavIC	ISRO (India)	Regional	36 000	8

Source: own study.

In every GNSS, we can distinguish three basic segments, i.e., space, ground (control), and user[9,10]. The GNSS structure is shown in Figure 1.

6 E. Kaplan and Ch.J. Hegarty, Understanding GPS/GNSS: Principles and Applications, 3rd ed., GNSS Technology and Applications Series (Boston, MA, USA; London, UK: Artech House, 2017).

7 Ang Liu et al., Using DORIS Data for Validating Real-Time GNSS Ionosphere Maps, Advances in Space Research, New Results from DORIS for Science and Society, 72, no. 1 (July 1, 2023): 115–28, https://doi.org/10.1016/j.asr2023.01.05. New Results from DORIS for Science and Society, 72, no. 1 (July 1, 2023.

8 NovAtel Inc., What Are Global Navigation Satellite Systems?, NovAtel, accessed November 28, 2023, https://novatel.com/tech-talk/an-introduction-to-gnss/what-are-global-navigation-satellite--systems-gnss.

9 C. Specht, GPS system (in Polish: System GPS).

10 E. Kaplan and Ch.J. Hegarty, Understanding GPS/GNSS.

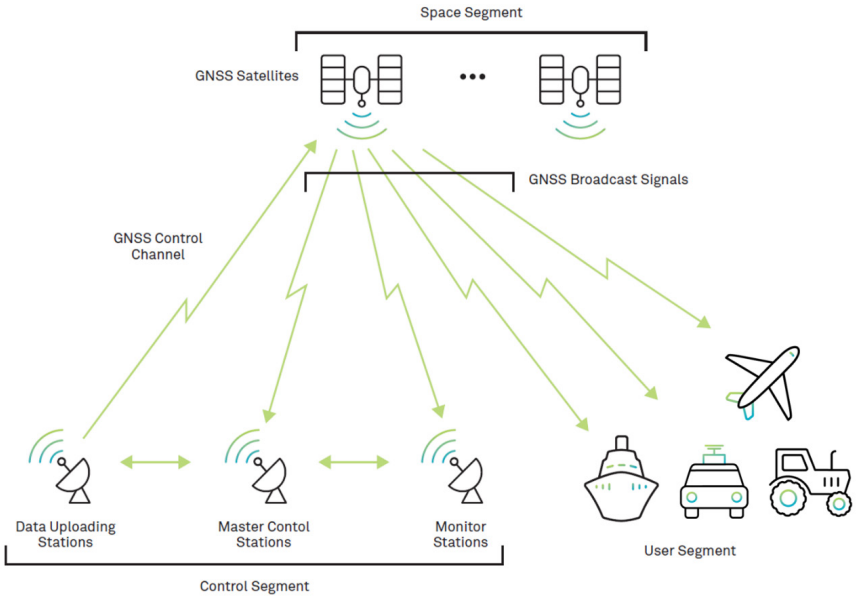

Fig. 1. Structure of GNSS
Source: NovAtel Inc., What Are Global Navigation Satellite Systems?

The GNSS operator is responsible for ensuring the reliable working of the space and ground segments. The user segment includes all devices that use GNSS signals to provide PNT services.

It is worth emphasizing that satellite based augmentation systems (SBASs), which are locally used mainly in air transport, are also based on GNSSs. This group of systems includes[11]:

- Wide Area Augmentation System (WAAS) in USA,
- European Geostationary Navigation Overlay Service (EGNOS) in Europe,
- GPS Aided Geo Augmented Navigation (GAGAN) in India,
- Multi-functional Satellite Augmentation System (MSAS) in Japan,
- System of Differential Correction and Monitorin (SDCM) in Russia.

In addition, QZSS and the OmniSTAR system from the Dutch company Fugro N.V. are sometimes included among SBASs.

2.2. GNSS BANDS

GNSSs are radio navigation systems. This means that the radio signals emitted by the space segment satellites are used to determine the position or time scale of the GNSS receiver. Signals from different GNSS satellites use the same RF bands. The utilization of code-division multiple access (CDMA) allows the receiver to detect several signals

[11] F. van Diggelen, A-GPS: Assisted GPS, GNSS, and SBAS, GNSS Technology and Applications Series (Boston, MA, USA: Artech House, 2009).

 DOI: 10.55676/asi.v4i2.64

received from different satellites in the same RF band[12]. In the case of GLONASS, additionally frequency-division multiple access (FDMA) is used. Generally, two primary RF bands are specified in the GNSSs spectrum, i.e., lower-band (~1100–1300 MHz) and upper-band (~1550–1610 MHz) sometimes denoted as L2 and L1, respectively. Figure 2 depicts detailed designations of the RF bands used by each GNSSs.

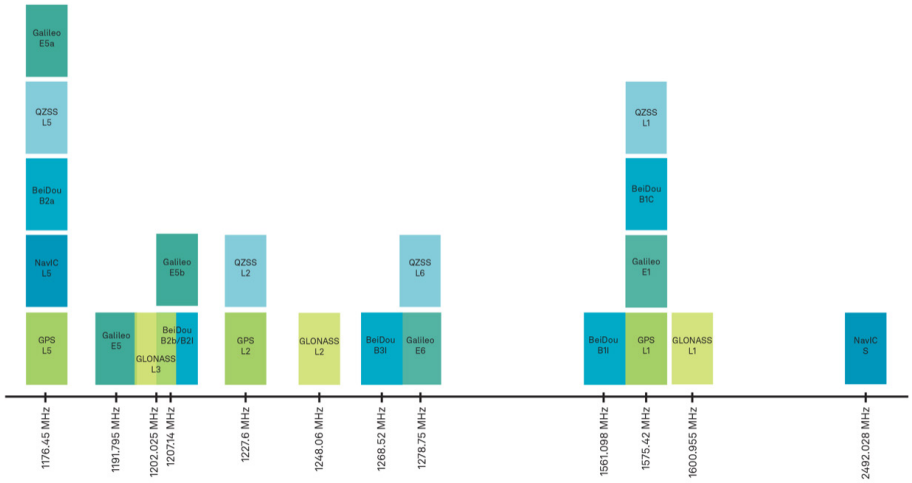

Fig. 2. RF bands of GNSSs

Source: NovAtel Inc., What Are Global Navigation Satellite Systems?

2.3. GNSS RECEIVER

The GNSS receiver is the basic device in the user segment. This segment is represented by various devices, from ordinary ones used for location and navigation mainly in wheeled vehicles, through receivers used in UAVs to those dedicated to special applications, e.g., time scale distribution for synchronization purposes (e.g., in telecommunications, banking sector), high-precision measurement devices (e.g., in geodesy), or precise military receivers. Moreover, this type of devices also includes integrated circuits (chipsets) installed in other devices (e.g., smartphones or the above-mentioned car navigation receivers), which provide access to the PNT from a dedicated application. In 2023, the value of global GNSS chip market is estimated

[12] J. Sanz Subirana, J.M. Juan Zornoza, and M. Hernández-Pajares, GNSS Data Processing. Volume I: Fundamentals and Algorithms (Noordwijk, the Netherlands: European Space Agency (ESA) Communications, May 2013), https://gssc.esa.int/navipedia/GNSS_Book/ESA_GNSS-Book_TM-23_Vol_I.pdf.

at USD 6.16 billion. The value of this market in 2028 is estimated at USD 8.13 billion, which gives a compound annual growth rate (CAGR) of 5.71%[13].

The classification of GNSS receivers may concern the supported systemy (e.g., single – or multi-GNSS receivers – see Table 1), the used RF bands (see Figure 2), or the area of application. J. Dudczyk & D. Zmysłowski[14] proposed the use of the Wroclaw taxonomy to evaluate GNSS receivers, which can also be used in their classification.

Figure 3 shows the architecture of a typical GNSS receiver. In the receiver, we can highlight the receiving antenna, RF front-end, local oscillator, and signal processing block, which might be implemented in software.

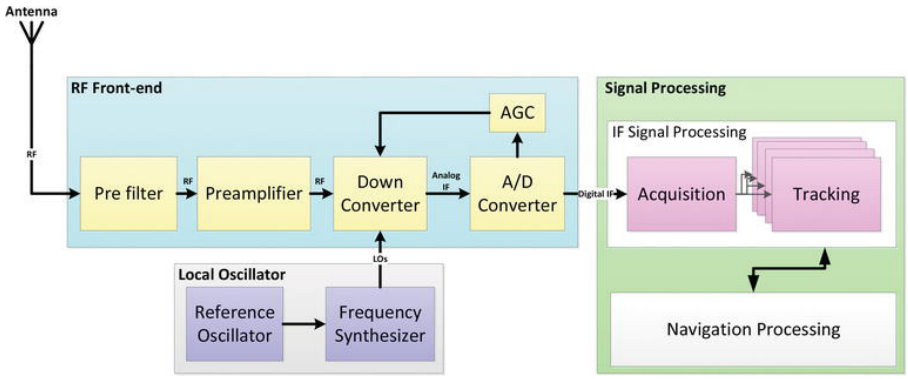

Fig. 3. Architecture of GNSS receiver

Source: M. Tamazin et al., GNSSs, Signals, and Receivers, in Multifunctional Operation and Application of GPS (IntechOpen, 2018), https://doi.org/10.5772/intechopen.74677.

3. GNSS INTERFERENCE

Interference is any type of external factor that causes to incorrectly function of the system. The classification of GNSS interference is presented in many papers, e.g.,[15,16]. In GNSS, we can distinguish unintentional and intentional interference, as illustrated

[13] Research and Markets Ltd., Global GNSS Chip Market (2023-2028) by Type, Applications, and Geography, Competitive Analysis, Impact of Covid-19, Impact of Economic Slowdown & Impending Recession with Ansoff Analysis, Research and Markets, accessed November 28, 2023, https://www.researchandmarkets.com/reports/5585671/global-gnss-chip-market-2023-2028-by-type.

[14] J. Dudczyk and D. Zmysłowski, Wroclaw Taxonomy Method in the Assessment of GNSS Receivers (Metoda Taksonomii Wrocławskiej w Ocenie Odbiorników GNSS), Electronics – Constructions, Technologies, Applications (Elektronika – Konstrukcje, Technologie, Zastosowania) 60, no. 1 (January 2019): 25–29, https://doi.org/10.15199/13.2019.1.3.

[15] S.M. Sánchez-Naranjo et al., GNSS Vulnerabilities, in Multi-Technology Positioning, ed. Jari Nurmi et al. (Cham, Switzerland: Springer International Publishing, 2017), 55–77, https://doi.org/10.1007/978-3-319-50427-8_4.

[16] D. Zmysłowski, Application of Wroclaw Taxonomy in Classification of GNSS Interferences in Business Use, in 2021 38th International Business Information Management Conference (IBIMA) (Seville, Spain, 2021), 7468–73.

 DOI: 10.55676/asi.v4i2.64

in Figure 4. Multipath propagation[17] occurring, e.g., in street canyons or generally in urban areas, atmospheric phenomena such as scintillations[18] or effects caused by increased solar activity[19], and interference from other radio systems (e.g., TV broadcating, cellular networks[20], or radar systems[21]) operating in adjacent RF bands are examples of unintentional interference. Intentional interference includes jamming and spoofing[22]. In GNSS, jamming techniques similar to those used in other radio communication systems, e.g., in 5G mobile networks[23], are sometimes used.

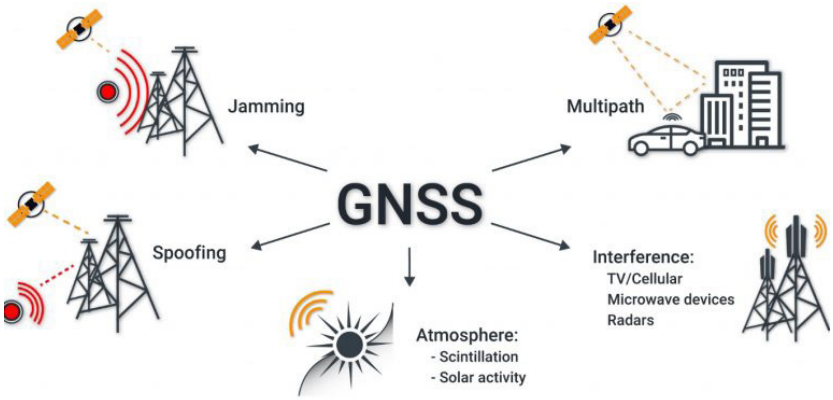

Fig. 4. GNSS interference

Source: P. Sokolenko, GNSS Signal Monitoring.

17 J.M. Kelner, C. Ziółkowski, Evaluation of Angle Spread and Power Balance for Design of Radio Links with Directional Antennas in Multipath Environment, Physical Communication 32 (February 1, 2019): 242–51, https://doi.org/10.1016/j.phycom.2018.12.005.

18 W. Qin and F. Dovis, Effects of Interference Mitigation Methods on Scintillation Detection, in 2018 9th ESA Workshop on Satellite NavigationTechnologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC) (Noordwijk, the Netherlands, 2018), 1–8, https://doi.org/10.1109/NAVITEC.2018.8642644.

19 X. Yue et al., The Effect of Solar Radio Bursts on the GNSS Radio Occultation Signals, Journal of Geophysical Research: Space Physics 118, no. 9 (2013): 5906–18, https://doi.org/10.1002/jgra.50525.

20 J. Wojtuń, C. Ziółkowski, and J.M. Kelner, Modification of Simple Antenna Pattern Models for Inter-Beam Interference Assessment in Massive Multiple-Input–Multiple-Output Systems, Sensors 23, no. 22 (January 2023): 9022, https://doi.org/10.3390/s23229022.

21 M. Wróbel and J.M. Kelner, On Research Directions in Coexistence Areas of Radar and Communication Systems, in 2021 38th International Business Information Management Association (IBIMA) (2021 38th International Business Information Management Association (IBIMA), Seville, Spain, 2021), 405–11, https://ibima.org/accepted-paper/on-research-directions-in-coexistence-areas-of-radar-and-communication-systems/.

22 A. Felski, Let Us Prepare the Officer of the Watch on Jamming and Spoofing, TransNav, International Journal on Marine Navigation and Safety Od Sea Transportation 13, no. 4 (December 2019): 847–51, https://doi.org/10.12716/1001.13.04.18.

23 P. Skokowski et al., Jamming and Jamming Mitigation for Selected 5G Military Scenarios, Procedia Computer Science, 2022 International Conference on Military Communication and Information Systems (ICMCIS), 205 (2022): 258–67, https://doi.org/10.1016/j.procs.2022.09.027.

W. Paluszyński[24] points out the threats resulting from the disruption of the time scale distributed by GNSS. On the one hand, this illustrates how important GNSSs are for the modern economy of every country, and on the other hand - how great a threat is the use of jamming, spoofing, or cyberattacks on GNSSs. For this reason, it is recommended to monitor the GNSS signal and use local highly stable clocks (i.e., rubidium/cesium frequency standards or time servers) in case of GNSS failure or interference.

Jamming involves the transmission of an interfering signal in the RF band(s) of GNSS, which prevents the receiver from decoding GNSS signals. Whereas, spoofing involves the transmission of false signals similar to the structure of GNSS signals, which after decoded in the receiver, causes incorrect determination of its position and time scale[25]. Figure 5 illustrates the ideas of these two types of intentional interference.

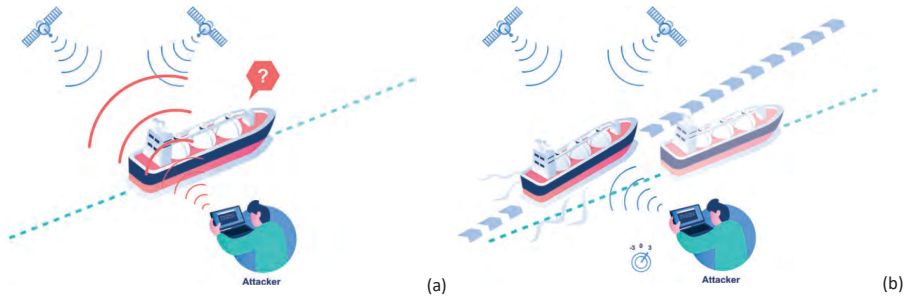

Fig. 5. Idea of (a) jamming and (b) spoofing
Source: Intertanko.

R. Bauernfeind et al.[26] oraz D. Borio et al.[27] present an overview of small commercial jammers, the used jamming signals, their impact on the operation of GNSS receivers and anti-jamming solutions. The authors assigned the tested devices to one of four classes depending on the used signal[28, 29]:

- Class I: continuous wave jammer,

24 W. Paluszyński, Underestimated Threat – Source and Distribution of Time (Niedoceniane Zagrożenie – Źródło i Dystrybucja Czasu), in Cybersecurity. Redefining Threats (Cyberbezpieczeństwo. Redefinicja Zagrożeń), ed. Bolesław Szafrański (Warsaw, Poland: Military University of Technology, 2023).

25 Intertanko, Jamming and Spoofing of Global Navigation Satellite Systems (GNSS) (London, UK: Intertanko, 2019).

26 T. Kraus, R. Bauernfeind, and B. Eissfeller, Survey of In-Car Jammers - Analysis and Modeling of the RF Signals and IF Samples (Suitable for Active Signal Cancelation), in Proceedings of the 2011 24th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS) (Portland, OR, USA: Institute of Navigation (ION), 2011), 430–35, http://www.ion.org/publications/abstract.cfm?jp=p&articleID=9605.

27 D. Borio et al., Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers, Proceedings of the IEEE 104, no. 6 (June 2016): 1233–45, https://doi.org/10.1109/JPROC.2016.2543266.

28 T. Kraus, R. Bauernfeind, and B. Eissfeller, Survey of In-Car Jammers - Analysis and Modeling of the RF Signals and IF Samples (Suitable for Active Signal Cancelation).

29 D. Borio et al., Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers.

 DOI: 10.55676/asi.v4i2.64

- Class II: chirp jammer with one saw-tooth function,
- Class III: chirp jammer with multi saw-tooth functions,
- Class IV: chirp jammer with frequency bursts.

A higher class represents better efficiency in jamming the GNSS receivers.

J. Zidan et al.[30] proposed a survey of methods for jamming, detection, and mitigation. The last one may be classified into three subgroups, i.e., antenna-based, receiver-based, and navigation processor-based techniques. Whereas, M.L. Psiaki and T.E. Humphreys[31] describe a classification of spoofing attacks and methods of their detection. Generally, we may highlight replay spoofing or meaconing, signal-level spoofing, or data-level spoofing[32]. G.X. Gao et al.[33] present a review of techniques for counteracting intentional and unintentional interference in GNSS receivers. H.P. Kim et al.[34] show an interesting solution based on GNSS cloud-data processing.

4. TESTING GNSS RECEIVER ROBUSTNESS FOR JAMMING

With the development of intentional interference techniques, methods of avoiding, mitigating, or canceling them appear and are implemented in modern GNSS receivers[35, 36, 37, 38]. In this paper, we propose a method for testing receiver robustness for jamming. To this aim, a jammer was made, which will be the basis for the developed measurement test-bed.

4.1. GNSS JAMMER

For the purposes of testing the GNSS receiver robustness for jamming, we have developed the jammer as a part of the measurement test-bed, which consists of:

- two Keysight (Agilent) E4438C ESG Vector Signal Generators, 250 kHz to 6 GHz[39],

30 J. Zidan et al., GNSS Vulnerabilities and Existing Solutions: A Review of the Literature, IEEE Access 9 (2021): 153960–76, https://doi.org/10.1109/ACCESS.2020.2973759.

31 M.L. Psiaki and T.E. Humphreys, GNSS Spoofing and Detection, Proceedings of the IEEE 104, no. 6 (June 2016): 1258–70, https://doi.org/10.1109/JPROC.2016.2526658.

32 D. Zmysłowski, Application of Wroclaw Taxonomy in Classification of GNSS Interferences in Business Use.

33 G.X. Gao et al., Protecting GNSS Receivers from Jamming and Interference, Proceedings of the IEEE 104, no. 6 (June 2016): 1327–38, https://doi.org/10.1109/JPROC.2016.2525938.

34 H.-P. Kim, G.-G. Jin, and J.-H. Won, GNSS Cloud-Data Processing Technique for Jamming Detection, Identification, and Localisation, IET Radar, Sonar & Navigation 14, no. 8 (2020): 1143–49, https://doi.org/10.1049/iet-rsn.2019.0518.

35 J. Zidan et al., GNSS Vulnerabilities and Existing Solutions.

36 G.X. Gao et al., Protecting GNSS Receivers from Jamming and Interference. transportation, communication, and finance

37 D. Borio et al., Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers.

38 J. Magiera, and R.J. Katulski, Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing, Journal of Applied Research and Technology 13, no. 1 (February 2015): 45–57, https://doi.org/10.1016/S1665-6423(15)30004-3.

39 Keysight, Keysight (Agilent) E4438C ESG Vector Signal Generator. Data Sheet, Data sheet (USA: Keysight Technologies (Agilent Technologies), February 28, 2019), https://www.keysight.com/ie/en/assets/7018-01039/data-sheets-archived/5988-4039.pdf.

- Mini-Circuits ZHL-30W-252-S+ High Power Amplifier , 0.7 to 2.5 GHz[40],
- Mini-Circuits ZFRSC-123-S+ 2 Ways Resistive Power Splitter, DC to 12 GHz, 50 Ω[41],
- Two Mini-Circuits VAT-5A+ 5 dB Fixed Attenuators, DC to 6 GHz, 50Ω,
- transmitting antenna, Technical Antennas Ultra Wide Band 600 MHz to 6.5 GHz Parabolic Grid Cellular Data SigInt[42],
- fiders connecting all test-bed elements,
- 26.5 V power supply for the amplifier ZHL-30W-252-S+.

The connected jammer components, except the transmitting antenna, are shown in Figure 6. Each Keysight E4438C can generate a broadband signal with a bandwidth of 80 MHz. Thanks to this, one of the generators was responsible for jamming the lower-band, while the other generator was responsible for jamming the upper-band.

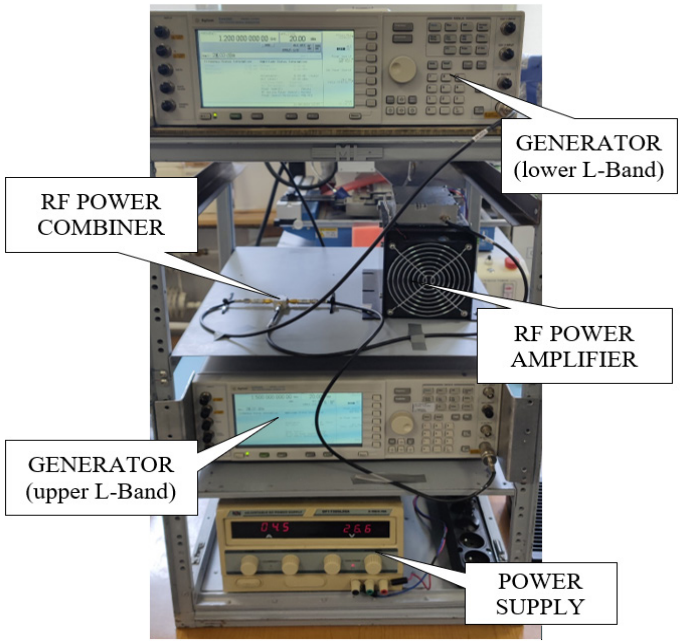

Fig. 6. Developed GNSS jammer

Source: own study.

[40] Mini-Circuits, High Power Amplifier, 0.7 to 2.5 GHz | ZHL-30W-252-S+ | Mini-Circuits, Mini-Circuits, accessed November 29, 2023, https://www.minicircuits.com/WebStore/dashboard.html?model=ZHL-30W-252-S%2B.

[41] Mini-Circuits, 2 Ways Resistive Power Splitter, DC - 12000 MHz, 50Ω | ZFRSC-123-S+ | Mini-Circuits, Mini-Circuits, accessed November 29, 2023, https://www.minicircuits.com/WebStore/dashboard.html?model=ZFRSC-123-S%2B.

[42] Technical Antennas, Ultra Wide Band 600MHz-6.5GHz Parabolic Grid Cellular Data SigInt, TechnicalAntennas.com, accessed November 29, 2023, https://technicalantennas.com/products/ultra-wide-band-parabolic-grid.

 DOI: 10.55676/asi.v4i2.64

The use of an RF power combiner, which consisted of a ZFRSC-123-S+ splitter and two VAT-5A+ attenuators, allowed for summing two signals generated in two GNSS bands and feeding them to a single ZHL-30W-252-S+ power amplifier. Then, the signal from the amplifier was fed to the transmitting antenna.

Figure 7 illustrates the spectrum of the signal generated by the GNSS jammer. In this case, we see a signal emitted in two bands in which GNSSs operate. In the developed jammer, we used a broadband chirp/burst signal, which allows the device to be assigned to class IV (see Section 3).

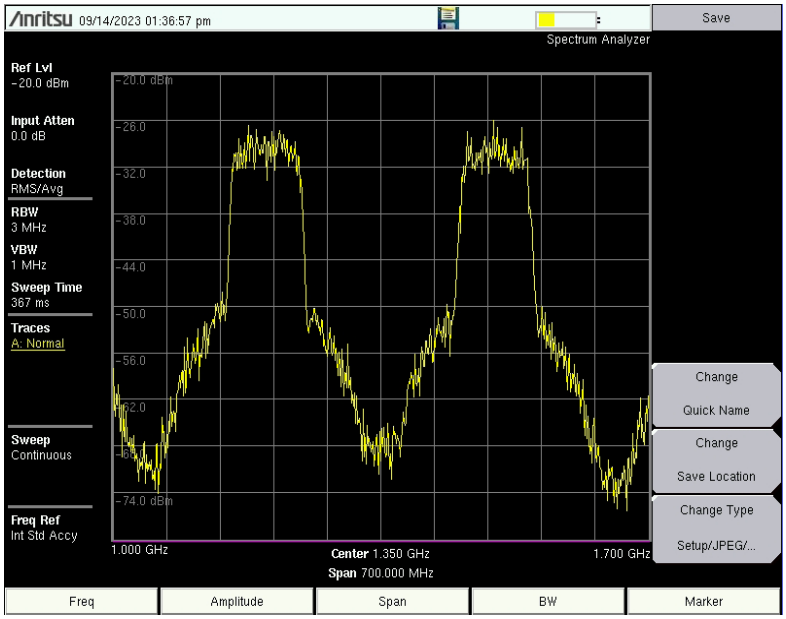

Fig. 7. Spectrum of GNSS jammer signal

Source: own study.

4.2. TEST ENVIRONMENTS

The utlization of GNSS jammers, like other jamming devices (e.g., in anti-drone systems[43]), is regulated by national law[44]. Basically, this type of devices can only be used by appropriate services and the military in strictly defined situations. For this reason, tests of GNSS receiver robustness for jamming should be carried out in appropriate places/measurement environments.

[43] D. Zmysłowski, P. Skokowski, and J.M. Kelner, Anti-Drone Sensors, Effectors, and Systems – A Concise Overview, TransNav – International Journal on Marine Navigation and Safety of Sea Transportation 17, no. 2 (June 2023): 455–61, https://doi.org/10.12716/1001.17.02.23.

[44] UKE, Komunikat w sprawie urządzeń zagłuszających, Urząd Komunikacji Elektronicznej (UKE), November 24, 2017, https://bip.uke.gov.pl/ostrzezeniawyroby-niezgodne/komunikat-w-sprawie-urzadzen-zagluszajacych,2.html.

To this aim, we plan to prepare an appropriate measurement environment in the semi-anechoic chamber (SAC)[45] of the Military University of Technology (i.e., our Electromagnetic Compatibility Laboratory). However, it should be noted that SAC provides isolation of the external electromagnetic environment from the internal environment. This makes testing the GNSS receiver impossible. In this case, we plan to use a GNSS simulator[46] that will generate signals from a artificial (virtual) constellation of selected GNSSs.

The use of a jammer on the experimental proving ground is an approach that does not require the use of a GNSS simulator. In this case, the military unit supervising the proving ground must have appropriate consent to use this type of signal sources. Figure 8 shows the developed jammer with the transmitting antenna located on the measurement proving ground. Such a test environment is ideal for testing the robustness of GNSS receivers that UAVs are equipped.

Fig. 8. GNSS jammer in field study environment
Source: own study.

4.3. TEST METHODOLOGY

Performing reliable measurements of a GNSS receiver robustness for jamming requires the use of appropriate measurement procedures. Such a procedure should be

[45] L. Nowosielski et al., Implementation of Remote Control for the AM 524 Antenna Amplifier Unit System in SAC Chambers, Electronics 12, no. 21 (November 2023): 4416, https://doi.org/10.3390/electronics12214416.

[46] D. Zmysłowski and J.M. Kelner, Concept of Using Simulators in Susceptibility Assessment of GNSS Services to Intentional Interferences, Annual of Navigation, n.d., (in preparation).

 DOI: 10.55676/asi.v4i2.64

developed and tested for reference GNSS receivers that are characterized by defined immunity, e.g., a receiver resistant and not resistant to jamming. Only then is it possible to test other GNSS receivers as a device under test (DUT).

Currently, the authors prepare a test environment in SAC, want to purchase reference GNSS receivers, and develop appropriate test procedures.

5. SUMMARY

This paper focuses on investigating the robustness of GNSS receiver for jamming. In the initial part, short characteristics of GNSSs, the used RF bands and GNSS receivers are presented. Then, the issue of GNSS interference, with particular emphasis on jamming and spoofing, was outlined. Considering the GNSS jammers classification, a dual-band class IV device was developed using two broadband vector generators. This device will be the basis for the development of measurement procedures for assessing the GNSS receiver robustness for jamming in the conditions of an artificial GNSS environment generated in the SAC using a GNSS simulator, which is a plan for the authors' future work.

ABBREVIATIONS

BDS – BeiDou Navigation Satellite System
CAGR – compound annual growth rate
CDMA – code-division multiple access
DORIS – Doppler Orbitography and Radio-positioning Integrated by Satellite
DUT – device under test
EGNOS – European Geostationary Navigation Overlay Service
ESA – European Space Agency
EU – European Union
FDMA – frequency-division multiple access
GAGAN – GPS Aided Geo Augmented Navigation
GEO – geostationary orbit
GLONASS – GLObal NAvigation Satellite System
GNSS – global navigation satellite system
GPS – Global Positioning System
GSA – European Global Navigation Satellite Systems Supervisory Authority
IGSO – inclined geosynchronous orbit
IRNSS – Indian Regional Navigation Satellite System
MSAS – Multi-functional Satellite Augmentation System
MEO – medium Earth orbit
NavIC – Navigation with Indian Constellation
PNT – positioning, navigation, and timing
QZSS – Quasi-Zenith Satellite System
RF – radio frequency

RNSS – regional navigation satellite system
SAC – semi anechoic chamber
SBAS – satellite based augmentation system
SDCM – System of Differential Correction and Monitoring
UAV – unmanned aerial vehicle
USA – United States
USD – United States dollar
USV – unmanned surface vehicle
WAAS – Wide Area Augmentation System

REFERENCES

Borio D., Dovis F., Kuusniemi H., Lo Presti L., Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers. Proceedings of the IEEE 104, no. 6 (June 2016): 1233–45. https://doi.org/10.1109/JPROC.2016.2543266.

Diggelen F. van, A-GPS: Assisted GPS, GNSS, and SBAS. GNSS Technology and Applications Series. Boston, MA, USA: Artech House, 2009.

Dudczyk J., Zmysłowski D., Wroclaw Taxonomy Method in the Assessment of GNSS Receivers (Metoda Taksonomii Wrocławskiej w Ocenie Odbiorników GNSS). Electronics – Constructions, Technologies, Applications (Elektronika – Konstrukcje, Technologie, Zastosowania) 60, no. 1 (January 2019): 25–29. https://doi.org/10.15199/13.2019.1.3.

Felski A., Let Us Prepare the Officer of the Watch on Jamming and Spoofing. TransNav, International Journal on Marine Navigation and Safety Od Sea Transportation 13, no. 4 (December 2019): 847–51. https://doi.org/10.12716/1001.13.04.18.

Methods of Improving the Jamming Resistance of GNSS Receiver. Annual of Navigation 23, no. 1 (2016): 185–98. https://doi.org/10.1515/aon-2016-0013.

Gao G.X., Sgammini M., Lu M., Kubo N., Protecting GNSS Receivers from Jamming and Interference. Proceedings of the IEEE 104, no. 6 (June 2016): 1327–38. https://doi.org/10.1109/JPROC.2016.2525938.

Intertanko. Jamming and Spoofing of Global Navigation Satellite Systems (GNSS). London, UK: Intertanko, 2019.

Kaplan E., Hegarty J.Ch., Understanding GPS/GNSS: Principles and Applications. 3rd ed. GNSS Technology and Applications Series. Boston, MA, USA; London, UK: Artech House, 2017.

Kelner J.M., Ziółkowski C., Evaluation of Angle Spread and Power Balance for Design of Radio Links with Directional Antennas in Multipath Environment. Physical Communication 32 (February 1, 2019): 242–51. https://doi.org/10.1016/j.phycom.2018.12.005.

Keysight. Keysight (Agilent) E4438C ESG Vector Signal Generator. Data Sheet. Data sheet. USA: Keysight Technologies (Agilent Technologies), February 28, 2019. https://www.keysight.com/ie/en/assets/7018-01039/data-sheets-archived/5988-4039.pdf.

 DOI: 10.55676/asi.v4i2.64

Kim H.-P., Jin G.-G., Won J.-H., GNSS Cloud-Data Processing Technique for Jamming Detection, Identification, and Localisation. IET Radar, Sonar & Navigation 14, no. 8 (2020): 1143–49. https://doi.org/10.1049/iet-rsn.2019.0518.

Kraus T., Bauernfeind R., Eissfeller B., Survey of In-Car Jammers - Analysis and Modeling of the RF Signals and IF Samples (Suitable for Active Signal Cancelation). In Proceedings of the 2011 24th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS), 430–35. Portland, OR, USA: Institute of Navigation (ION), 2011. http://www.ion.org/publications/abstract.cfm?jp=p&articleID=9605.

Liu A., Wang N., Dettmering D., Li Z., Schmidt M., Wang L., Yuan H., Using DORIS Data for Validating Real-Time GNSS Ionosphere Maps. Advances in Space Research, New Results from DORIS for Science and Society, 72, no. 1 (July 1, 2023): 115–28. https://doi.org/10.1016/j.asr.2023.01.050.

Magiera J., Katulski R.J., Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing. Journal of Applied Research and Technology 13, no. 1 (February 2015): 45–57. https://doi.org/10.1016/S1665-6423(15)30004-3.

Mini-Circuits. 2 Ways Resistive Power Splitter, DC - 12000 MHz, 50Ω | ZFRSC-123-S+ | Mini-Circuits. Mini-Circuits. Accessed November 29, 2023. https://www.minicircuits.com/WebStore/dashboard.html?model=ZFRSC-123-S%2B.

High Power Amplifier, 0.7 to 2.5 GHz | ZHL-30W-252-S+ | Mini-Circuits. Mini-Circuits. Accessed November 29, 2023. https://www.minicircuits.com/WebStore/dashboard.html?model=ZHL-30W-252-S%2B.

NovAtel Inc. What Are Global Navigation Satellite Systems? NovAtel. Accessed November 28, 2023. https://novatel.com/tech-talk/an-introduction-to-gnss/what-are-global-navigation-satellite-systems-gnss.

Nowosielski L., Kelner J.M., Dudziński B., Rychlicki M., Implementation of Remote Control for the AM 524 Antenna Amplifier Unit System in SAC Chambers. Electronics 12, no. 21 (November 2023): 4416. https://doi.org/10.3390/electronics12214416.

Paluszyński W., Underestimated Threat – Source and Distribution of Time (Niedoceniane Zagrożenie – Źródło i Dystrybucja Czasu). In Cybersecurity. Redefining Threats (Cyberbezpieczeństwo. Redefinicja Zagrożeń), edited by Bolesław Szafrański. Warsaw, Poland: Military University of Technology, 2023.

Psiaki M.L., Humphreys T.E., GNSS Spoofing and Detection. Proceedings of the IEEE 104, no. 6 (June 2016): 1258–70. https://doi.org/10.1109/JPROC.2016.2526658.

Qin W., Dovis F., Effects of Interference Mitigation Methods on Scintillation Detection. In 2018 9th ESA Workshop on Satellite NavigationTechnologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), 1–8. Noordwijk, the Netherlands, 2018. https://doi.org/10.1109/NAVITEC.2018.8642644.

Research and Markets Ltd. Global GNSS Chip Market (2023-2028) by Type, Applications, and Geography, Competitive Analysis, Impact of Covid-19, Impact of Economic Slowdown & Impending Recession with Ansoff Analysis. Research and

Markets. Accessed November 28, 2023. https://www.researchandmarkets.com/reports/5585671/global-gnss-chip-market-2023-2028-by-type.

Sánchez-Naranjo S.M., Ferrara N.G., Paśnikowski M.J., Raasakka J., Shytermeja E., Ramos-Pollán R., González Osorio F.A., et al., GNSS Vulnerabilities. In Multi-Technology Positioning, edited by Jari Nurmi, Elena-Simona Lohan, Henk Wymeersch, Gonzalo Seco-Granados, and Ossi Nykänen, 55–77. Cham, Switzerland: Springer International Publishing, 2017. https://doi.org/10.1007/978-3-319-50427-8_4.

Skokowski P., Kelner J.M., Malon K., Maślanka K., Birutis A., Vazquez M.A., Saha S., et al. Jamming and Jamming Mitigation for Selected 5G Military Scenarios. Procedia Computer Science, 2022 International Conference on Military Communication and Information Systems (ICMCIS), 205 (2022): 258–67. https://doi.org/10.1016/j.procs.2022.09.027.

Sokolenko P., GNSS Signal Monitoring. GPSPATRON, February 11, 2020. https://gpspatron.com/gnss-signal-monitoring/.

Specht C., GPS system (in Polish: System GPS). Navigation Library (Biblioteka Nawigacji) 1. Peplin: Wydawnictwo Bernardinum, 2007.

Specht M., Widźgowski S., Stateczny A., Specht C., Lewicka O., Comparative Analysis of Unmanned Aerial Vehicles Used in Photogrammetric Surveys. TransNav, International Journal on Marine Navigation and Safety Od Sea Transportation 17, no. 2 (June 1, 2023): 433–43. https://doi.org/10.12716/1001.17.02.21.

Specht M., Specht C., Lasota H., Cywiński P., Assessment of the Steering Precision of a Hydrographic Unmanned Surface Vessel (USV) along Sounding Profiles Using a Low-Cost Multi-Global Navigation Satellite System (GNSS) Receiver Supported Autopilot. Sensors 19, no. 18 (September 2019): 3939. https://doi.org/10.3390/s19183939.

Subirana J.S., Juan Zornoza J.M., Hernández-Pajares M., GNSS Data Processing. Volume I: Fundamentals and Algorithms. Noordwijk, the Netherlands: European Space Agency (ESA) Communications, May 2013. https://gssc.esa.int/navipedia/GNSS_Book/ESA_GNSS-Book_TM-23_Vol_I.pdf.

Tamazin M., Karaim M., Noureldin A., GNSSs, Signals, and Receivers. In Multifunctional Operation and Application of GPS. IntechOpen, 2018. https://doi.org/10.5772/intechopen.74677.

Technical Antennas. Ultra Wide Band 600MHz-6.5GHz Parabolic Grid Cellular Data SigInt. TechnicalAntennas.com. Accessed November 29, 2023. https://technicalantennas.com/products/ultra-wide-band-parabolic-grid.

UKE. Komunikat w sprawie urządzeń zagłuszających. Urząd Komunikacji Elektronicznej (UKE), November 24, 2017. https://bip.uke.gov.pl/ostrzezeniawyroby-niezgodne/komunikat-w-sprawie-urzadzen-zagluszajacych,2.html.

Wojtuń J., Ziółkowski C., Kelner J.M., Modification of Simple Antenna Pattern Models for Inter-Beam Interference Assessment in Massive Multiple-Input–Multiple-Output Systems. Sensors 23, no. 22 (January 2023): 9022. https://doi.org/10.3390/s23229022.

 DOI: 10.55676/asi.v4i2.64

Wróbel M., Kelner J.M., On Research Directions in Coexistence Areas of Radar and Communication Systems. In 2021 38th International Business Information Management Association (IBIMA), 405–11. Seville, Spain, 2021. https://ibima.org/accepted-paper/on-research-directions-in-coexistence-areas-of-radar-and-communication-systems/.

Yue X., Schreiner W.S, Kuo Y.-H., Zhao B., Wan W., Ren Z., Liu L., et al., The Effect of Solar Radio Bursts on the GNSS Radio Occultation Signals. Journal of Geophysical Research: Space Physics 118, no. 9 (2013): 5906–18. https://doi.org/10.1002/jgra.50525.

Zidan J., Adegoke E.I., Kampert E., Birrell S.A., Ford C.R., Higgins M.D., GNSS Vulnerabilities and Existing Solutions: A Review of the Literature. IEEE Access 9 (2021): 153960–76. https://doi.org/10.1109/ACCESS.2020.2973759.

Zmysłowski D., Application of Wroclaw Taxonomy in Classification of GNSS Interferences in Business Use. In 2021 38th International Business Information Management Conference (IBIMA), 7468–73. Seville, Spain, 2021.

Zmysłowski D., Kelner J.M., Concept of Using Simulators in Susceptibility Assessment of GNSS Services to Intentional Interferences. Annual of Navigation, n.d., (in preparation).

Zmysłowski D., Skokowski P., Kelner J.M., Anti-Drone Sensors, Effectors, and Systems – A Concise Overview. TransNav – International Journal on Marine Navigation and Safety of Sea Transportation 17, no. 2 (June 2023): 455–61. https://doi.org/10.12716/1001.17.02.23.