ORIGINAL RESEARCH **Open access**

Analysis of GNSS Vulnerability in Unmanned Aerial Vehicles under Software-Defined Radio–Based Interference Scenarios

Santiago Morales[1*], Laura Rojas[2], Camila Vega[1], Diego Molina[3]

Abstract

The spoofing and jamming of Global Navigation Satellite System signals persist as a significant threat during both general aviation and Unmanned Aerial Vehicle missions. Given that aircraft depend on auxiliary navigation support systems like INS, a compromised Global Navigation Satellite System signal renders Unmanned Aerial Vehicles virtually uncontrollable, heightening risks to airspace activities and people on the ground. This article primarily examines the influence of the inexpensive Software-Defined Radio, HackRF One 1.0, on the operational safety of Unmanned Aerial Vehicles. Given the widespread availability of Software-Defined Radio units today—some of which are relatively inexpensive—understanding their potential impact on Unmanned Aerial Vehicle safety is essential. Creating artificial interference that could constitute a genuine threat within the ever-growing Unmanned Aerial Vehicles airspace is deemed impermissible.

Keywords UAV, GNSS, Jamming, Interference

*Correspondence:
Santiago Morales
santiago.morales@agro.uba.ar
[1] Department of AI for Soybean and Sunflower Phenotyping in Pampas, Faculty of Agriculture, University of Buenos Aires, Buenos Aires, Argentina
[2] Department of Machine Learning for Leaf Area Index (LAI) Estimation, Faculty of Agriculture, Pontifical Catholic University of Chile, Santiago, Chile
[3] Department of Smart Drought Monitoring, Faculty of Agriculture, National University of La Plata, La Plata, Argentina

Introduction

Owing to the relentless expansion of Global Navigation Satellite Systems (GNSS), exemplified by Galileo (Europe's system) and Beidou (China's system), along with ongoing enhancements to established navigation systems like GLONASS (Russia's system) and the American Global Position System (GPS), a more extensive array of new signals can now be harnessed, ensuring superior performance and precision [1, 2]. In addition to the well-known uses of positioning and navigation, a growing number of future applications are expected to rely on a stable timing reference supplied by GNSS [3]. This holds for Unmanned Aerial Vehicles (UAVs), a sector whose adoption and appeal are surging rapidly [4]. The onboard positioning systems of UAVs depend considerably on GPS and GLONASS satellite constellations [5].

The term Software-Defined Radio (SDR) was introduced in the 1990s by its originator, Joseph Mitola, to describe a category of radios capable of being reprogrammed and reconfigured through software changes instead of hardware modifications [6-8]. The SDR paradigm has matured over recent decades, yet, in general, such devices follow the

This is an open access article distributed under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License (CC BY-NC-SA 4.0), which permits non-commercial use, distribution, reproduction, and adaptation in any medium or format, provided that appropriate credit is given to the original author(s) and source, a link to the license is provided, and any changes made are indicated. Adapted material must be distributed under the same license.

© 2024 The Author(s). | Published by Agro Intelligence Research Press

architecture depicted in **Figure 1**. An SDR comprises three core sections: an RF/IF module, a digital front-end module, and a baseband processing unit [9, 10].

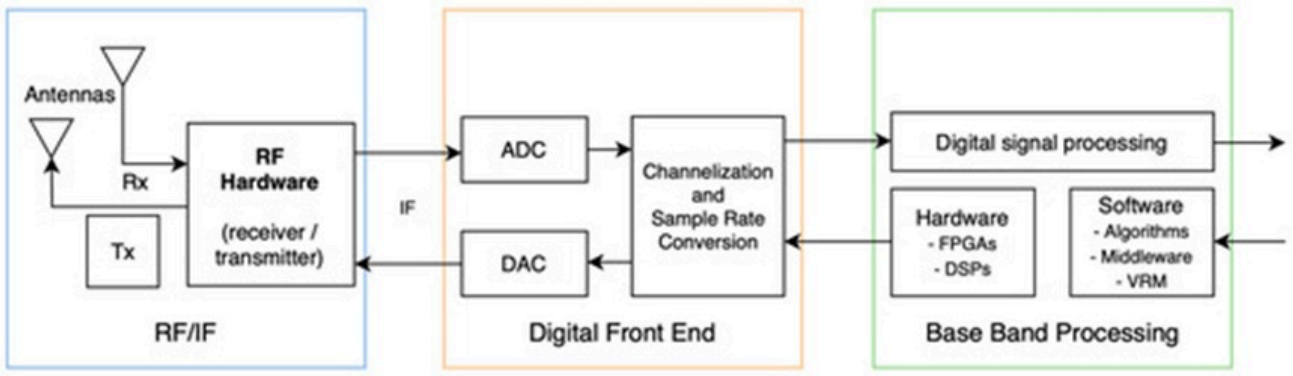


Figure 1. Scheme of SDR.

The RF/IF and digital front-end sections are implemented using hardware based on diverse module designs from different manufacturers [11-13]. These building blocks exist in multiple variants, which manufacturers tailor to their distinct objectives. The baseband processing section consists of a user-configurable hardware-software solution for the targeted SDR deployment [14, 15]. This segment handles signal filtering, demodulation, modulation, encoding, decoding, post-processing, and evaluation, delivering output to either a computer or a dedicated application [16].

Drawing on earlier research, GNSS interference comprises two distinct sub-issues [17-20]. The first concerns interference affecting not only air transportation but also intelligent transport systems [21]. The second sub-issue involves the detection and geolocation of the aforementioned GNSS signal interference [22]. Such interference usually poses little concern for military and specialist applications, as their transmissions are often encrypted and exhibit stronger resistance to disruption, using two or more carrier frequencies for broadcasting [23]. Publicly accessible offerings, such as those operating on a single frequency, exhibit weaker resilience to interference [24-27].

Based on the definition outlined in “Doc 8071-Manual on Testing of Radio Navigation Aids-Volume II”, making GNSS receivers resistant to spoofing can be accomplished by properly engineering the Receiver Autonomous Integrity Monitoring (RAIM) fault-detection algorithms, alongside the RAIM fault-detection and exclusion algorithms built into aviation receiver sets [28]. Deliberate harmful interference (jamming) aimed at GNSS is likewise a prospect, as it is for every radio navigation system [29]. It must be stressed that unauthorized interference is unlawful and warrants action by the relevant authorities [28].

Interference can be classified by its features, including type, mean frequency, signal interference bandwidth, power, and time-domain manifestations [30, 31]. Varieties of interference comprise sine wave interference, single-tone carrier wave interference, interference from AM, FM, or PM modulated signals disturbing a broader spectrum, or noise interference—a randomly produced signal such as white or pink noise [32]. Interference classified by its position relative to the signal’s mean frequency falls into “out of band,” “near the band,” or “in band” categories [33-35]. Bandwidth differentiates wideband from narrowband interference [36]. Interference power is the ratio of the carrier signal strength to the interference signal strength, commonly referred to as the Jammer-to-Signal (J/S) ratio [36, 37]. Furthermore, interference can occur in the time domain, transmitted steadily, in discrete intervals, or in bursts, described by pulse width or pulses per second [36]. Interference on the GPS L1 frequency can appear in the transmitted spectrum in various forms, as the signal is spread [38].

The challenges of spoofing and jamming have received considerable scholarly attention in the past, yet the emerging application space of UAVs brings this topic back to the forefront. As noted previously, uninterrupted growth and increasingly convenient consumer access are increasing the density of UAV operations in the airspace, thereby elevating

© 2024 The Author(s). | Published by Agro Intelligence Research Press

the risk of collisions with manned aircraft, other UAVs, or bystanders. The smooth functioning of UAVs is confronted by an escalating menace—purposeful disruption of GNSS signals [39]. This disruption appears in two dominant guises: jamming and spoofing. Jamming refers to the deliberate emission of radio-frequency energy to interrupt communications [40]. For UAVs, this amounts to a direct assault on their navigational capabilities, which could lead to dangerous outcomes [41]. In the GNSS context, jamming entails transmitting on the exact frequencies used by GNSS signals. Such interference can drown out or overwhelm legitimate satellite transmissions, resulting in a total loss of satellite lock [40, 41]. The premeditated nature of jamming distinguishes it from unintentional interference; it is a purposeful act aimed at incapacitating GNSS communication or navigation infrastructure. UAVs are critically dependent on GNSS for precise navigation, and jamming represents a major hazard to UAV missions by producing navigational mistakes, loss of command, or outright collapse of the vehicle's navigation system [42]. Apart from the immediate functional disruption, jamming provokes security alarms, particularly when UAVs are assigned to surveillance, disaster response, or other essential tasks. Malicious disruption through jamming can erode the efficiency and safety of these undertakings.

Furthermore, detecting jamming can be difficult, as jammer emissions often mimic valid GNSS signals, hindering onboard receivers' ability to discriminate between genuine and counterfeit signals [43]. Alleviating the dangers of jamming requires an integrated approach encompassing technological countermeasures, regulatory frameworks, and awareness initiatives. Scientists and industry practitioners are striving to craft hardened navigation systems able to withstand jamming attacks, while oversight bodies implement measures to deter and punish jamming activities [39-43].

Spoofing, by contrast, introduces a less overt yet equally grave peril. It involves fabricating fraudulent signals that replicate legitimate GNSS signals [44]. UAVs, which depend on these signals for accurate positioning, become vulnerable to manipulation, potentially leading to security violations and safety incidents. Spoofing attacks can be remarkably intricate, supplying false positional data with high fidelity, posing dire repercussions in use cases where exact positioning is paramount [45]. This method of attack poses a substantial danger to navigation infrastructure, UAVs included, as it can deceive the vehicle's navigation system, inducing errors, loss of command, or unsanctioned re-routing. Beyond the immediate operational effects, spoofing has security consequences, weakening the reliability and effectiveness of systems deployed in contexts such as military operations or the safeguarding of critical installations. Identification remains problematic because fraudulent signals closely resemble authentic satellite transmissions, and advanced spoofing schemes preempt anti-spoofing defenses, complicating detection and neutralization [46]. Reducing spoofing threats demands resilient counter-spoofing tactics, including cryptographic protocols, signal authentication, and supplementary sensors to cross-check location data [44, 45]. A thorough grasp of spoofing's subtleties is indispensable for formulating effective defenses to secure navigation infrastructure in domains where accurate and trustworthy positioning is a fundamental requirement [46, 47]. As UAV use continues to expand into fields such as reconnaissance, package delivery, and even driverless transportation, the ramifications of GNSS disruption become ever more urgent.

Throughout this inquiry, special attention was devoted to examining pertinent literature, particularly studies that directly addressed spoofing of GPS signals targeting UAVs. Kerns *et al.* conducted an investigation titled "Unmanned Aircraft Capture and Control via GPS Spoofing," examining the feasibility of hijacking unmanned aerial vehicles mid-flight via GPS signal spoofing. The outcomes of field experimentation demonstrated that a destructive GPS-spoofing offensive against a rotorcraft UAV is feasible from both technical and operational standpoints [48].

Also in 2014, Machado-Fernandéz executed a study named "Software Defined Radio: Basic Principles and Applications," scrutinizing the hazards posed by the utilization of low-cost, commercially obtainable software-defined radio platforms. This investigation verifies that pairing an inexpensive SDR with appropriate software (often free) is serviceable for a wide range of applications, including pinpointing interference, efficiently allocating frequency assignments, detecting unauthorized spectrum users, and characterizing noise across global bands and regions [49, 50].

The concluding study, which provides a springboard for our own research, is "Risk assessment of SDR-based attacks with UAVs" by Le Roy *et al.* Its principal concern was a multifaceted analysis of off-the-shelf SDRs available on the market and their offensive impact evaluated from dual vantage points: ground-based attacks against UAVs (stationary

© 2024 The Author(s). | Published by Agro Intelligence Research Press

SDR) and UAV-based attacks against ground targets or other UAVs (mobile SDR) [24, 51]. The deductions of this study remain wholly conceptual, as the actual generation of a spoofing signal under authentic environmental circumstances is missing. None of the aforementioned investigations has focused on the ease of spoofing or jamming any desired signal in the contemporary context.

Materials and Methods

This section provides a comprehensive description of the materials and methods used throughout this study. The investigation's emphasis is on probing signal disruptions and pinpointing irregularities in the GNSS transmission. The primary research question posed is: "In what manner does the HackRF One, outfitted with an external Temperature Compensated Crystal Oscillator (TCXO), influence UAV safety and operational capability through the generation of artificial GNSS signal interference?" To answer this, a methodical appraisal of the HackRF One, augmented with an external TCXO, was undertaken to gauge its ability to generate synthetic interference within the GNSS signal and the resulting implications for UAV safety and operability.

GNSS spoofing materializes when the interference waveform I(t) mimics the structure inherent to the authentic signal s(t), leading both Gs(f) and GI(f) to exhibit identical spectral profiles and thus maximizing their overlap. Treating a spoofing signal as a stochastic process is impractical, thereby rendering the C/N0 degradation theory unsuitable. Instead, deterministic repercussions become evident within the targeted receiver. While deliberate spoofing incidents in aviation lack official documentation, multiple practical demonstrations confirm the viability of executing spoofing using modern SDR platforms and GNSS simulators [52-55]. These demonstrations reveal that spoofing poses a significant threat to GNSS infrastructure. In contrast to spoofing, GNSS jamming falls under the observation of national aviation oversight bodies, which catalogue instances of GNSS signal disruption. The spoofing waveform affecting a single satellite at the receive antenna can be represented as:

$$I(t) = \sqrt{2C}c_I(t - \tau_I(t))d_I(t - \tau_I(t))\cos\left(2\pi f_{RF}(t - \tau_I(t))\right), \quad (1)$$

Where the spoofing delay τI(t) relates to the actual delay τM(t) of the satellite m under consideration via an offset Δτ(t) [52]:

$$\tau_I(t) = \tau_m(t) + \Delta\tau(t) \quad (2)$$

Many distinct spoofing attack variants can materialize, dictated by the spoofing delay I(t) configuration and the spoofing device's power level CI(t). Appraising the impact of a spoofing event can be strengthened by evaluating the GNSS receiver's correlation outputs when it encounters both legitimate and counterfeit signals concurrently. Spoofing is engineered to corrupt the GNSS receiver's position fix and timing data estimations. GNSS receivers are built upon the modulated ranging code C(t) and the navigation data payload d(t) carried within the Open Service GNSS signal, both of which remain predictable to any capable spoofer. This reality breeds two attack classes: those targeting the navigation message and those targeting the code level. When assessing the spoofing threat at varying levels of complexity, one must treat the trajectory of SDR technology and potential adversary capabilities as uncertain variables. For illustration, according to the foundational theory of correlation values, a spoofing transmission must nearly replicate the delay and frequency of the authentic signal. At the same time, its power level CI(t) must not greatly outstrip that of the genuine signal C(t) if it is to remain undetected by a GNSS receiver locked in tracking mode. A sophisticated spoofing operation requires precise awareness of the user's trajectory relative to the GNSS satellite constellation and the spoofer's geographic location. This knowledge enables the construction of a bogus signal that matches the relative delay, power magnitude, and Doppler shift as perceived by the targeted UAV's receiver, thereby significantly complicating detection. Moreover, the spoofer must adjust for internal hardware latencies, clock discrepancies, and antenna gain pattern variations at both the transmit and receive ends.

© 2024 The Author(s). | Published by Agro Intelligence Research Press

The countermeasures installed in receivers to repel spoofing attempts closely parallel techniques used for interference identification and suppression. The critical distinction, however, is that anti-spoofing safeguards can additionally be woven into the GNSS architecture at the system level via signal design choices. Exploiting SDR for the creation and testing of counterfeit GNSS signals is advantageous because of its inherent flexibility, enabling swift parameter adjustments and diverse scenario emulation, while offering notable cost benefits relative to conventional testing apparatus.

The HackRF One, noted for its modest price tag and extensive deployment, was selected for its ability to both transmit and receive radio signals across a broad frequency range from 1 MHz to 6 GHz. The hardware attributes of the HackRF One, alongside similar alternatives that were reviewed but ultimately passed over based on defined benchmarks, are detailed in **Table 1**. **Table 1** lays out the technical parameters of three elementary SDR platforms: the HackRF One, the bladeRF, and the ADALM-PLUTO. Although these platforms share the overarching goal of fulfilling the study's aims, the HackRF One was ultimately singled out for its favorable cost-to-capability ratio and its prevalent application within the targeted frequency range. **Table 1** shows key metrics, including frequency coverage, RF bandwidth, sampling rate, transmit power, and unit cost for each platform, providing a perspective on their respective aptitudes in this research setting.

Table 1. Specifications of SDR devices [24, 28, 36].

Device	Frequency range	RF bandwidth	Sampling rate	Transmit power	Price (EUR)
HackRF One	1 MHz–6 GHz	20 MHz	20 MSPS	Max 10 dBm	280
BladeRF x-A4	47 MHz–6 GHz	56 MHz	61.44 MSPS	Max 8 dBm	540
ADALM-PLUTO	325–3800 MHz	20 MHz	61.44 MSPS	6 dBm	230

The investigative methodology guiding this paper revolves around a structured procedure designed to explore the effects and practical achievability of generating artificial interference using a Software-Defined Radio instrument, specifically the HackRF One version 1.0 running custom-compiled source code. The methodological sequence encompassed these pivotal phases:

· Device setup: the HackRF One was retrofitted with an external TCXO to sharpen its accuracy and overall performance.

· Signal synthesis: A GPS satellite arrangement was defined employing a GPS broadcast ephemeris file sourced from NASA. This dataset was manipulated to produce a binary file suitable for signal dissemination via the "gps-sdr-sim" software on Hack RF One.

· Signal broadcasting: The synthesized GPS signal was radiated by the HackRF One at a predetermined frequency. The emission process was monitored and corroborated through a spectrum analyzer.

· Signal capture and examination: The radiated signal was scrutinized using an NV08C-CSM integrated satellite navigation receiver module. Data on signal acquisition, including heading deviations, precision indicators (e.g., 2DRMS), and interference-induced effects on the receiver, were logged and analyzed.

· Evaluation of interference strength and reach: calculations and assessments were undertaken to establish the interference power magnitude, the critical interference cutoff, and the farthest effective range at which the interference could impair the GNSS receiver.

· Recording and cross-comparison: outcomes from the emitted spoof signal were compared with reference data gathered without the synthetic signal present to gauge changes in the receiver's operational performance and positional accuracy.

© 2024 The Author(s). | Published by Agro Intelligence Research Press

In summary, the methodological workflow encompassed preparing the SDR instrument **(Figure 2)**, synthesizing and transmitting artificial signals, capturing and analyzing those signals with dedicated instrumentation, and assessing their impact on the GNSS receiver. The procedural steps were systematically arranged, seeking to replicate and assess the prospective hazard posed by fabricated interference to GNSS signal reception and navigation infrastructure.

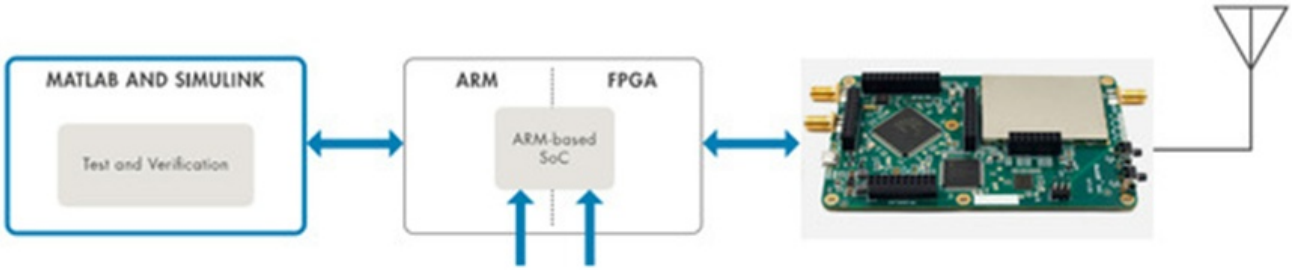


Figure 2. Scheme of SDR configuration for GNSS signal transmitting.

Seeing that the focal point was the straightforwardness of generating and radiating an artificial spoof signal, the Windows operating environment was adopted. Although the selected SDR, the HackRF One, is a highly dependable device within its price segment, it falls short of the precision required to spoof the GPS signal; consequently, installing an external TCXO, which bolsters the SDR's performance, became mandatory. Upon fitting the TCXO into the HackRF One, confirming the two elements' cooperation is vital. This validation can be executed by issuing the following command into the Command Prompt: "hackrf_debug -i5351c -n 0 -r". An unsuccessful return would signal a lack of proper coordination, as portrayed in **Figure 3**, while evidence of successful collaboration would appear as shown in **Figure 4**.

```
D:\gps-sdr-sim-win32-master\gps-sdr-sim-win32gui\hackrf>hackrf_si5351c.exe -n  0 -r
[  0] -> 0x51
```

Figure 3. Faulty response from SDR.

```
D:\gps-sdr-sim-win32-master\gps-sdr-sim-win32gui\hackrf>hackrf_si5351c.exe -n  0 -r
[  0] -> 0x01
```

Figure 4. Correct answer from SDR.

In the follow-up measurement, the procedure was carried out with the GLONASS receiver deactivated. This arrangement allowed us to validate the receiver's ability to reacquire lock and resolve a position once the signal was recovered.

Results and Discussion

Generation of GPS signal

Upon completing the setup phase, producing a GPS signal becomes feasible, with the satellite constellation specified through a GPS broadcast ephemeris file. The daily GPS broadcast ephemeris file (brdc) merges navigation files from individual stations into a single, consolidated source. All essential data were retrieved from the NASA online portal [56]. After obtaining the most current file, a binary file meant for signal distribution is generated using the command: "gps-sdr-sim -e brdc3500.23n -l 50.080759,14.437993,100". The items listed below explain each component of the command:

· "gps sdr-sim" refers to the software utility that links the resultant binary file and distributes it via the RTL-SDR HackRF One;

© 2024 The Author(s). | Published by Agro Intelligence Research Press

- "-e <gps_nav>" points to the RINEX navigation file holding GPS ephemerides;
- "brdc3500.23n" is the newest daily GPS broadcast ephemeris file, routinely released by NASA each day;
- -l <location>" supplies the latitude, longitude, and height coordinates (static mode), e.g., 50.080759,14.437993,100.

Figure 5 shows the binary file generation procedure after entering the target GPS location. To meet the paper's requirements, the authors entered the GPS coordinates for Prague.

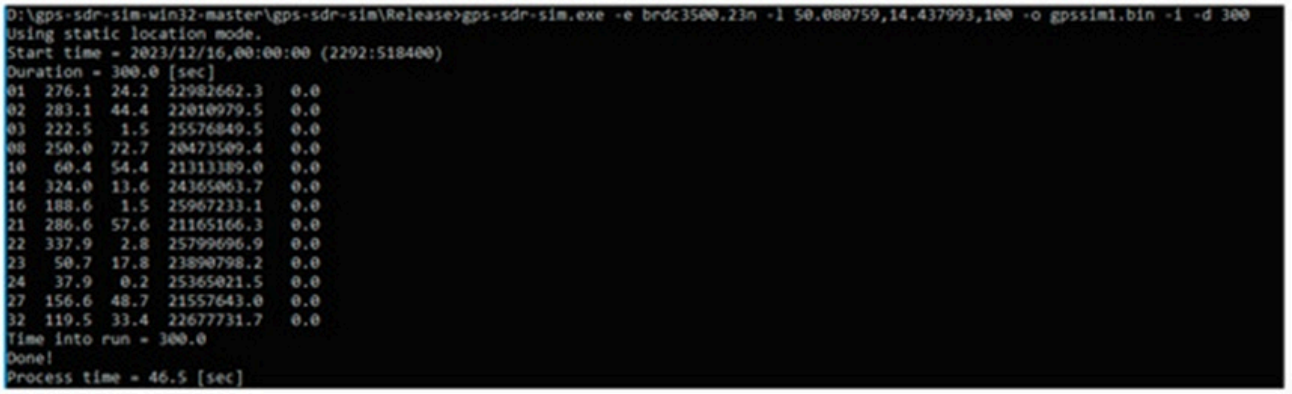


Figure 5. Process of generating a binary file.

Once the entire binary file is built, radiating the spoof signal becomes achievable **(Figure 6)**. Launching the transmission involves running the subsequent command: "hackrf_transfer -t gpssim.bin -f 1575420000 -s 2600000 -a 1 -x 0."



Figure 6. Process of transmitting the spoof signal.

One may confirm the 1575.42 MHz transmitted signal using an RF Explorer spectrum analyzer. **Figure 7** presents the spectral region around 1575 MHz when no emission is occurring.

© 2024 The Author(s). | Published by Agro Intelligence Research Press



Figure 7. Spectral analysis of the spectrum of interest.

In **Figure 8**, the designated signal is radiated from the SDR HackRF One, augmented with an external TCXO. The spectrum analyzer verifies that this signal is indeed propagating at −66.0 dB.

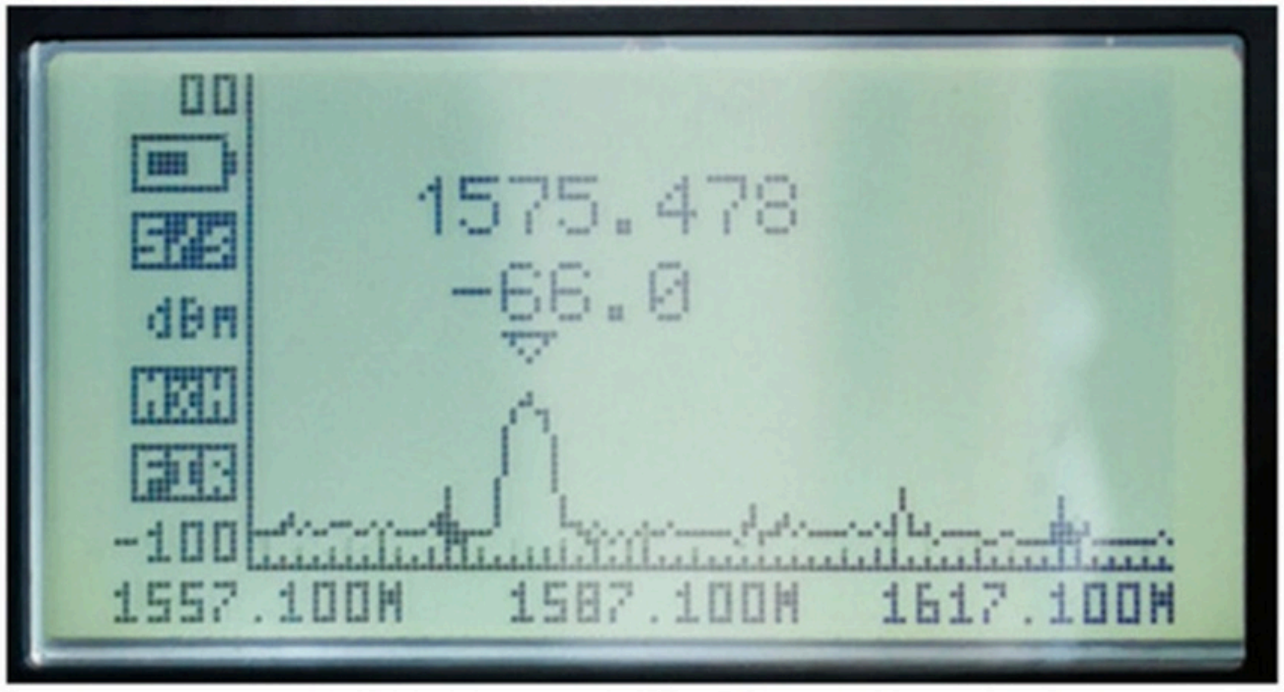


Figure 8. Spectrum of interest while transmitting the spoof signal.

While the spectrum analyzer detects the spoof signal, how receiving devices will react to this emission remains uncertain. To investigate the spoof signal, the NV08C-CSM integrated satellite navigation receiver, capable of tracking GPS, GLONASS, Galileo, and SBAS, was utilized. **Figure 9** displays the satellites currently in view from all the mentioned

© 2024 The Author(s). | Published by Agro Intelligence Research Press

constellations whose signals are receivable under ordinary circumstances. A reference measurement was taken in standard conditions **(Figure 9)**, free from any synthetically generated signal.

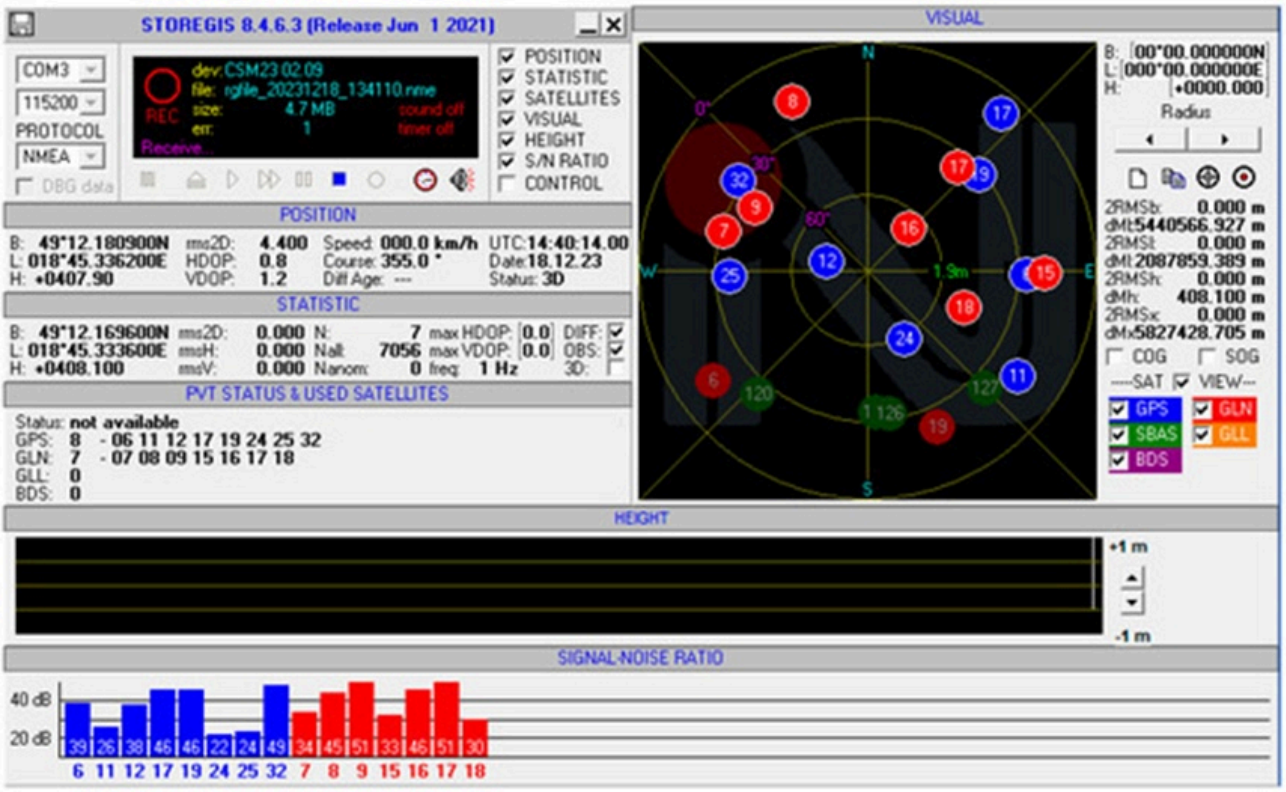


Figure 9. Course of reference measurements.

After the reference reading and satellite visibility check, the generated binary file with the targeted frequency and location can be executed. Within several seconds of activation, the NV08C-CSM receiver becomes unable to lock onto any GPS satellites, as illustrated in **Figure 10**. Even though the position did not deviate from the intended, pre-set coordinates—put differently, it was not spoofed—the transmitter's output level was substantial enough to jam the GPS receiver. Because the transmission occupied the GPS L1 band at 1575.42 MHz, the receiver could still acquire signals from the GLONASS constellation, which relies on a separate frequency. Another shift that occurred during the spoof signal emission was a change in course heading. During the reference measurement, the course held a constant value of 355.0°, but while the spoof signal was being transmitted, the course swung to 191.3°. Upon halting the spoof signal emission, the value returned to its original state.

© 2024 The Author(s). | Published by Agro Intelligence Research Press

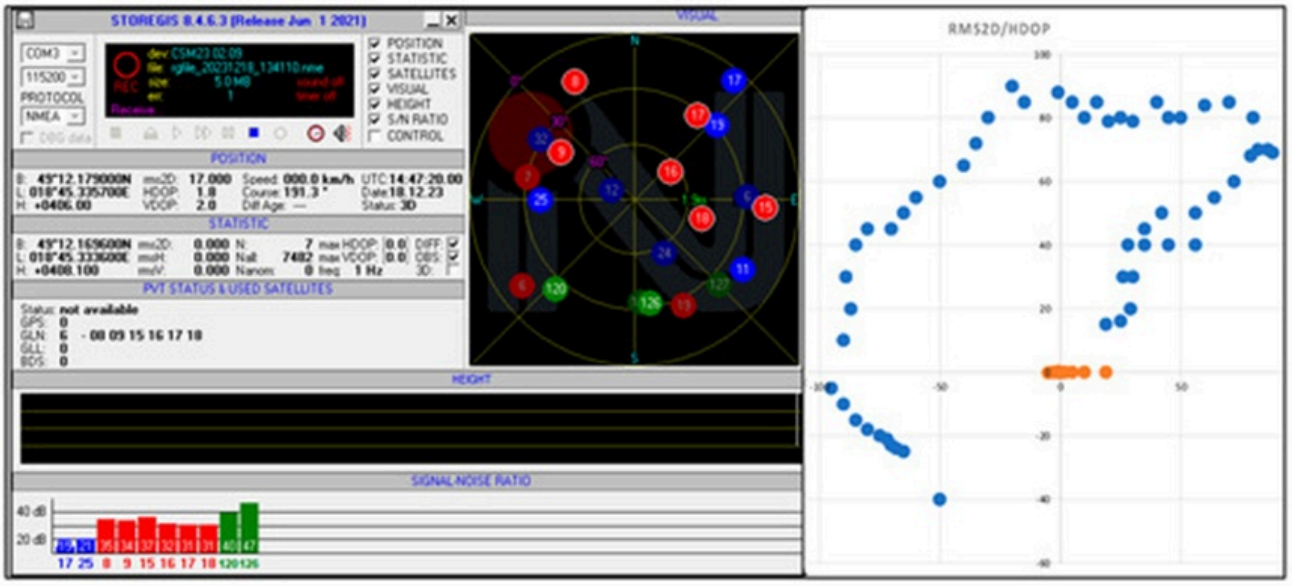
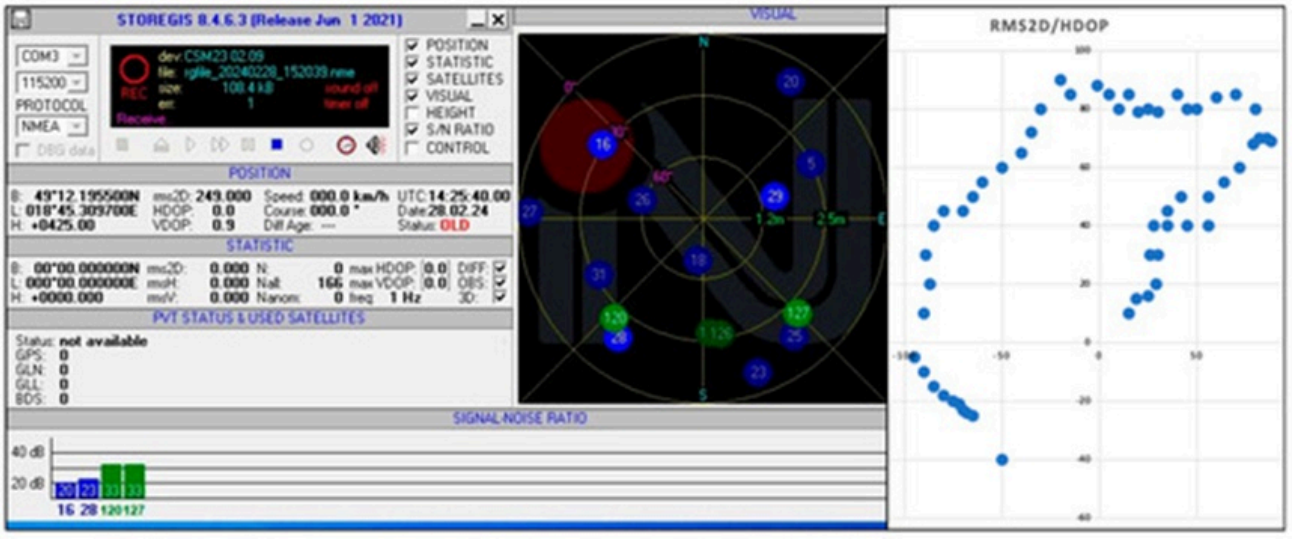


Figure 10. Course of measurements during the transmission of a spoof signal and scatter plot visualization.

In **Figure 10**, the scatter plot shows the progression of measurements during spoof signal transmission. It incorporates a scatter plot graphic that demonstrates the consequences of radiating a spoof signal on GPS receiver accuracy. The graph shows the deviation in course and the RMS2D readings, which represent the positional fix error induced by the transmitted spoof signal. The peak RMS2D in **Figure 9** is roughly four times that of the reference measurement, emphasizing the disruption to GPS signal reception caused by the interference.

In the next measurement, reception of GLONASS signals and SBAS satellite augmentation were disabled. With this arrangement, we examined the receiver's ability to regain lock and produce a position after signal restoration. **Figure 11** presents a scatter plot of the measurement sequence during transmission of a spoof signal without an operational GLONASS receiver. The graph illustrates deviations in the course and RMS2D figures, reflecting the positional fix error caused by the transmitted spoof signal under these conditions. The highest RMS2D value in **Figure 11** is markedly elevated relative to the reference measurement, indicating a substantial increase in error due to the absence of a functioning GLONASS receiver during spoof signal emission.



© 2024 The Author(s). | Published by Agro Intelligence Research Press

Figure 11. Course of measurements during the transmission of a spoof signal without an active GLONASS receiver and scatter plot visualization.

The RMS2D figure is particularly striking. As shown in **Figure 10**, the peak RMS2D value reaches 17.0, corresponding to approximately a fourfold increase over the reference measurement. In the second test case **(Figure 11)**, the peak RMS2D value reaches 249.0, indicating a roughly 57-fold increase relative to the reference measurement. This error, however, predominantly results from the outright loss of the GPS L1C signal, without any corroborating reference from other satellite navigation constellations. This measurement unit can likewise be called 2DRMS, which stands for "Twice Distance Root Mean Square Error." Even though 2DRMS concerns measurement in two-dimensional space—specifically, horizontal space—the "2D" in this abbreviation means "Twice Distance." The crucial factor lies in signal reception accuracy. There are many accuracy metrics, each designed for specific systems, since the errors inherent in position coordinates determined by a GPS or GLONASS receiver are not static but fluctuate statistically. Observing the reported position of a stationary receiving apparatus over a period reveals that it drifts or wanders. Rendering these shifting coordinates as a visual representation yields a scatter plot. The position is inherently three-dimensional, yet it can be assessed independently for horizontal or vertical accuracy. **Table 2** compiles the most frequently used measurement method categories, along with their dimensionality, precision probability, and typical usage context.

Table 2. Accuracy measures and typical usage.

Accuracy measure	Number of dimensions	Probability (%)	Common application
Root mean square (rms)	1	68	Vertical positioning
Root mean square (rms)	2	63–68	Horizontal positioning
Root mean square (rms)	3	61–68	Three-dimensional positioning
Twice distance root mean square (2 drms)	2	95–98	Horizontal positioning
Circular error probable (CEP)	2	50	Horizontal positioning
Horizontal 95% accuracy (R95)	2	95	Horizontal positioning
Spherical error probable (SEP)	3	50	Three-dimensional positioning

The most commonly applied measurement methods include root mean square, twice distance rms, circular error probable, horizontal 95% accuracy, and spherical error probable. Root mean square is characterized as the square root of the mean of the squared errors. The twice-distance rms is defined as twice the root-mean-square of the horizontal errors. Circular error probable signifies a circle's radius, centered on the true antenna position, containing 50% of the points within the horizontal scatter plot. Horizontal 95% accuracy is characterized by a circle's radius, centered on the true antenna position, that contains 95% of the points in the horizontal scatter plot. Spherical error probable denotes a sphere's radius, centered on the true antenna position, containing 50% of the points within the three-dimensional scatter plot. Each of these measurement approaches has its own merits, drawbacks, and precision probability [49].

Table 3 presents a side-by-side comparison of the practical test findings for UAV GNSS receivers with various configurations, along with whether they feature jamming/spoofing detection capabilities. Each column corresponds to a different UAV model, and the rows specify the GNSS receiver arrangement and whether jamming/spoofing detection features are present, indicated as "Yes" or "No."

Table 3. The practical test on a UAV GNSS receiver with various GNSS receiver configurations.

Platform	GNSS module and compass	GNSS reception and navigation	Interference mitigation description	Test equipment	Jamming/Spoofing detection

© 2024 The Author(s). | Published by Agro Intelligence Research Press

		rate			
3DR IRIS+ 	Ublox NEO-6M-0 module, HMC5883L compass	Supports concurrent reception of up to 1 GNSS, with a navigation update rate of up to 5 Hz	The NEO-M6 series includes a continuous-wave (narrowband) interference monitor for detecting jammers. It reports suspected or confirmed jamming by analyzing background noise and identifying significant deviations.	HackRF One	Yes / No
Tarot 650 v2.2 	Ublox NEO-M8N module, IST8310 compass	Supports concurrent reception of up to 3 GNSS, with up to 10 Hz navigation rate (single GNSS)	The NEO-M8N incorporates spoofing detection features that notify the system when incoming signals appear abnormal. It performs multiple consistency checks across signal parameters to detect irregularities.	HackRF One	Yes / Yes
DJI Inspire 2 	Ublox M8 module, M8030 TK	Supports concurrent reception of up to 2 GNSS, with up to 10 Hz navigation rate	The NEO-M8 series includes spoofing-detection mechanisms that alert the host system when signals appear suspicious, using multiple cross-checks to detect inconsistencies in received data.	HackRF One	Yes / Yes
Sky Hunter 	MATEKSYS M8Q-5883	Supports concurrent reception of up to 2 GNSS, and a single GNSS navigation rate of up to 18 Hz	The NEO-M8Q module provides spoofing detection by flagging suspicious signals. It evaluates multiple signal parameters and checks for inconsistencies across them.	HackRF One	Yes / Yes

This set of measurements meets the objective laid out in the preceding investigation by providing concrete data and understanding of how different categories of GNSS receivers behave when confronted with signal interference and manipulation. These findings could be used to evaluate the security and dependability of UAVs subjected to artificial interference, and to craft measures that strengthen resilience against such threats. Ultimately, this measurement effort contributes to a richer understanding of the potential risks and challenges of operating drones in environments where GNSS signals may be subject to interference.

The latest crop of GNSS receivers already demonstrates robustness and the ability to detect interference under certain limiting conditions, while the latest firmware upgrades have also begun to counteract spoofing. Still, the question remains whether we can secure GNSS signal resilience against interference across all future scenarios. This goal proves demanding as the field of signal interference continues to advance. Persistent innovation and investigation are vital for conceiving and implementing effective methods to safeguard GNSS signals. This requires not only upgrading the receivers themselves but also crafting better algorithms and protocols for detecting and neutralizing interference, as well as cooperating with other technology sectors to assemble increasingly complex and robust systems.

Guarding GNSS signals against interference will require not only technical breakthroughs but also global cooperation and appropriate legal and regulatory structures. It constitutes a challenge we must address collectively to ensure reliable, secure GNSS-based navigation across all scenarios.

© 2024 The Author(s). | Published by Agro Intelligence Research Press

Power and distance of interfering signal assessment

The ratio of Jamming to Signal strength can be computed through the following expression:

$$\frac{J}{S} = J_R - S_R(\mathrm{dB}), \quad (3)$$

Where JR stands for the received power value of the interfering signal (dBm or dBW) and SR stands for the received power value of the satellite signal (dBm or dBW) [49].

The critical threshold (J/S)C, which represents a particular interference level beyond which the GNSS receiver ceases to function, spans approximately 37-60 dB, as established through numerous experimental trials reported across multiple published studies [49]. The exact (J/S)C value shifts depending on both the class of GNSS receiver and the nature of the interfering waveform employed. Interference stemming from white noise or narrowband signals must be transmitted at significantly greater power to achieve total denial of service, so steeper (J/S)C values accompany these. A wideband interfering signal (e.g., a chirp waveform) demands lower power, meaning a reduced (J/S)C value applies. Working out the critical distance, presuming free-space spreading, relies on the equation:

$$P_r(d) = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2 L} \ (\mathrm{W}), \quad (4)$$

Where Pr denotes the signal power captured at a separation d from the transmitter, Pt denotes the radiated signal power, Gt and Gr represent the transmit and receive antenna gains, respectively, and λ denotes the wavelength of the radiated signal. L covers receiver losses unrelated to propagation [49].

GNSS signals generally reach Earth's surface with a power level around −125 dBm. The specification governing GPS signals on the L1 and L2 frequencies states that the minimum received level for terrestrial users is −158.5 dBW (−128.5 dBm) for the C/A Code on L1 and −160 dBW (−130 dBm) for the P code on L2 [36, 51, 57, 58]. Signal amplitude is further shaped by satellite elevation angle and tropospheric and ionospheric influences. It follows from the points above that the interfering signal magnitude likely to disrupt an already-locked GNSS signal is −80 dBm or greater [59]. The exact value will fluctuate by roughly 25 dB, depending on antenna polarization, the receiver's operating bandwidth, and the receiver's sensitivity adjustment [60, 61]. The attenuation encountered during electromagnetic wave travel through space, LFSPL, is captured by the following equation:

$$L_{FSPL} = \left(\frac{4\pi d}{\lambda}\right)^2 = \left(\frac{4\pi df}{c}\right)^2, \quad (5)$$

Where LFSPL signifies the attenuation from electromagnetic wave travel across free space, d is the distance separating the interfering signal transmit antenna from the GNSS receive antenna, f is the interference frequency, c is the speed of light, and λ is the wavelength of the radiated signal [61]. If we adopt the elementary model of electromagnetic wave travel through free space (3), the environmental attenuation appears as follows **(Table 4)**.

Table 4. Attenuation of the environment in free space propagation [28].

© 2024 The Author(s). | Published by Agro Intelligence Research Press

Distance d [m]	Attenuation [dB]
10	56
100	76
1000	96
10,000	116

Reformulating **Eq. 2** into a structure amenable to substituting variables expressed in dB, we arrive at [62]:

$$P_r = P_t + G_t + G_r - L - L_{FSPL} = P_t + G_t + G_r - L - 20log_{10}\left(\frac{4\pi df}{c}\right)\ (\text{dBW}), \quad (6)$$

Should we regard receiver losses as negligible, model the receiving antenna as isotropic, and adopt the effective radiated power EIRP figure, **Eq. 4** can be rewritten as:

$$P_r = EIRP_t - 20\ log_{10}(\frac{4\pi df}{c})\ (\text{dBW}), \quad (7)$$

With the GNSS signal power level at the Earth's surface established (consult **Table 5**) and the critical ratio (J/S)C treated as a known quantity, **Eq. 2** permits the computation of the limiting interfering signal power JC reaching the GNSS receiver, which will incapacitate its proper functioning [62]. Substituting this outcome into **Eq. 5** and isolating the distance variable d yields the jammer's maximum effective range dmax, inside which the jammer can successfully impair the GNSS receiver:

$$d_{max} = \frac{c}{4\pi f} 10^{\frac{EIRP_t - J_c}{20}}\ (\text{m}) \quad (8)$$

Table 5. Frequencies and wavelengths of chosen GNSS signals.

Signal	Wavelength [m]	Frequency [MHz]
GPS L1 C/A	0.19	1575.42
GPS L2 C	0.244	1227.6
GPS L5	0.254	1176.45
Galileo E5a E5b	0.251	1191.795
Galileo E1 O/S	0.19	1575.42
Galileo E6 PRS + CS	0.234	1278.75
GLONASS G1 SP	0.189–0.186	1589.0625–1605.375

© 2024 The Author(s). | Published by Agro Intelligence Research Press

GLONASS G3 CDMA	0.249	1202
Beidou B1	0.192	1561
Beidou B2	0.248	1207

Detection and mitigation of spoofing

A wide array of receiver-level countermeasures designed to thwart spoofing attacks draws upon the same underlying concepts as interference detection and mitigation methods. The fundamental difference, however, is that anti-spoofing protections can also be incorporated at the GNSS system architecture level via deliberate signal design.

User-level approaches can be grouped according to the functions they perform. The following subsections outline the progressive phases of anti-spoofing methods, covering everything from initial identification to active neutralization.

Pre-correlation strategies exhibit markedly reduced efficacy under spoofing conditions, since spoofing emissions inherently mimic the power profile of legitimate satellite broadcasts, and actual user operating conditions (for example, the channel model) may conceal a spoofer's detectability. That said, certain proposed schemes—such as the pre-correlation detection framework rooted in the generalized likelihood ratio test (GLRT) documented in Ref. [63]—can be beneficial when dealing with basic spoofing attacks that mask the role of user channel conditions and receiver processing in shaping the null hypothesis formulation.

Another thought-provoking spoofing-detection concept appears in Ref. [64], which proposes a clock-monitoring-based detection scheme that capitalizes on the collective projection of relative delays from every spoofed satellite onto the user receiver's clock solution. Methods of this kind require precisely characterized, calibrated receiver clocks and are better suited to less sophisticated spoofers.

Multipath detection techniques constitute a defensive tool that can be potentially adapted for spoofing identification. Signal quality monitoring (SQM) algorithms rely on a test statistic constructed from correlation values at different chip spacings together with the autocorrelation function. Although these algorithms assume the channel contains only signal and noise, their utility is limited when multipath propagation is present.

Additional DSP-based spoofing detection studies have probed the spectral architecture of GNSS signals, focusing on consolidating spectral lines via Doppler removal and leveraging the estimated variance of spectral regions containing only noise as a detection metric, gauged against spoof-free baseline conditions [65]. Time-frequency analysis via multiresolution algorithms has likewise been harnessed to tease apart the relative Doppler of extraneous (spoofing) signals from line-of-sight signals through eigen-decomposition of the autocorrelation matrix. This same technique extends to mitigation, where a notch filter can be deployed to strip spoofed signals after classification based on Doppler estimates.

A procedure for verifying and separating authentic signals from spoofed ones is presented in Ref. [66], which leverages a kinematic user's ability to discern and categorize spoofed signals by examining correlations in channel gain and Doppler across the spoofed satellite population. Building on this, Ref. [67] advances a mitigation technique that systematically purges spoofing signals from the received waveform. This method assumes that authentic and spoofed signals are tracked independently and that the spoofer fails to account for the user's movement relative to the spoofer's position.

An alternative tactic leverages the correlation observed in carrier-phase measurements between genuine and spoofed satellites, using either a moving [68] or a dual-antenna [69, 70] setup. As shown in **Figure 9**, the carrier phases across spoofed satellites are strongly correlated because they all share the same direction of arrival (DOA). Although this technique is resilient, it incurs increased costs and system complexity and remains limited to detection.

In broad terms, the performance of any algorithm aimed at spoofing detection, characterization, and discrimination can be degraded in complex multipath environments and when pitted against highly adept spoofers who either compensate for

© 2024 The Author(s). | Published by Agro Intelligence Research Press

the relative dynamics between the user and the spoofer or inject a measure of independence among the spoofing signals.

Ultimately, a careful appraisal of the capabilities inherent in the discussed techniques across varied environments and operational contexts is necessary, as most validation efforts have occurred in open terrain or at airfields. Additionally, receiver-based countermeasures ought to be evaluated under a range of spoofing scenarios, weighing their performance relative to spoofing sophistication and across dissimilar receiver architectures. Open-loop architectures, for example, may be unable to exploit carrier-phase measurements.

Beyond that, analyzing how these techniques perform—whether deployed singly or jointly—should be mapped against critical metrics and user-level demands unique to each scenario and application. To illustrate, a technique with a high detection likelihood may also suffer from prolonged detection latency, potentially giving a spoofer enough time to corrupt the receiver's tracking loops. In light of the numerous factors bearing on user-level techniques, the GNSS community has increasingly shifted its focus to system-level interventions as a more comprehensive approach to the spoofing threat.

As a closing overview, **Table 6** delineates the divergent capabilities of spoofing detection and mitigation methods and their respective degrees of suitability when implemented at the receiver level.

Table 6. Spoofing detection/mitigation using receiver-based techniques.

Stage	Detection methods	Mitigation methods
Pre-correlation	AGC and ADC monitoring	Blanking or channel exclusion
Pre-correlation	Signal spectrum analysis	Channel exclusion
Pre-correlation	—	Use of multi-antenna elements
Post-correlation	Correlator spectral analysis	Notch filtering, SEDLL
Post-correlation	SQM and channel cross-correlation analysis	Channel exclusion
Post-correlation	INS integration	GNSS exclusion; tight channel exclusion; spoofing signal removal (ultra-tight)
Post-correlation	Monitoring of C/N0, PR noise, PVT, RAIM clock	Channel exclusion
Post-correlation	—	Multi-antenna elements

As the evidence shows, the chosen equipment, the HackRF One, together with the requisite peripherals, can be used to produce arbitrary signals; hence, with this apparatus, any frequency can be jammed or spoofed, with the GLONASS frequency serving as just one example. Drawing on the experimental data, the authors' synthetic spoof signal was strong enough to jam the GPS receiver, causing it to fail to lock onto any GPS satellites. Likewise, the 2DRMS accuracy eroded sharply during the spoof signal trial. In the reference trial, conducted without any synthetic transmission, the 2 drms figure was 2.4, which, according to the table, corresponds to an accuracy exceeding 97%. Once the constructed spoof signal was radiated, however, two notable phenomena occurred. The 2drms reading dropped drastically (by over 76.6%), as the measured 2 drms value climbed to 20.8. The other effect concerned the course heading. During the reference trial, the

© 2024 The Author(s). | Published by Agro Intelligence Research Press

course held firm at 355.0°; during the spoof signal trial, however, this value swung sharply to 191.3°, signifying that the course flipped nearly completely in the reverse direction.

Table 7 lists the probability figures for drms (root mean square) and 2 drms (twice the distance root mean square error) over a range of standard deviation ratios (σy/σx). **Table 5** demonstrates the relationship between these standard deviation ratios and the probabilities associated with both drms and 2 drms, shedding light on the statistical likelihoods of these quantities as a function of the positioning system's standard deviations. It shows how different standard deviation ratios shape the probability distributions for drms and 2 drms alike, both of which represent fundamental accuracy metrics for judging the precision of positioning systems.

Table 7. Probabilities of drms and 2 drms [51].

σ_y/σ_x	p (2 drms)	2 drms	p (1 drms)	1 drms
0.0	0.9545	2.0	0.6827	1.0
0.25	0.9591	2.0616	0.6815	1.0308
0.5	0.9697	2.2361	0.6629	1.1180
0.75	0.9787	2.5	0.6392	1.25
1.0	0.9816	2.8284	0.6320	1.4142

The inquiry into how the HackRF One, paired with an external TCXO, shapes UAV safety and operability through the deliberate injection of artificial GNSS signal disturbance has uncovered meaningful insights. The outcomes reveal the extent to which UAVs remain defenseless against the synthetic interference generated by the HackRF One, posing potential safety risks and operational hazards. The observed collapse of GPS receivers and the steep erosion of positional accuracy metrics while a spoofed signal was being broadcast reinforce the pressing need for robust countermeasures capable of nullifying the identified threats.

Beyond this, the investigation spotlights the concrete, real-world fallout of such interference in settings where UAVs lean heavily upon GNSS signals for navigation and position fixing. The discussion explores the broader implications of these findings for the UAV sector as a whole, emphasizing the need to develop sophisticated detection architectures and hardened technologies to counter illicit interference.

Already more than a dozen years ago, a team at the University of Texas at Austin laid bare how readily civilian UAVs fall prey to GPS spoofing attacks; they later recreated the feat before officials from the FAA and DHS [71]. Not long after, in mid-2013, the same University of Texas at Austin group pulled off a successful spoofing of a privately owned yacht's position employing their apparatus [72]. At the 2015 DefCon conference, specialists from Qihoo 360 unveiled an inexpensive GPS spoofer capable of fabricating the locations displayed by smartphones and vehicle navigation systems [73]. Collectively, the academic researchers and the FAA and DHS experts shone a spotlight on the sweeping dangers that unsecured civil GPS technology poses to critical infrastructure and called for steps to harden spoof resistance, including a requirement that UAVs and other essential GNSS-anchored systems carry spoof-resilient navigation equipment.

While the HackRF One demonstrated its flexibility and usefulness across multiple application domains, including the creation of artificial interference, our investigation provides an initial foothold for deeper research. Follow-up studies should branch into additional experiments spanning diverse signal families while remaining mindful of the ever-evolving landscape of jamming and spoofing technologies. Furthermore, integrating machine learning and artificial intelligence with SDR platforms could enhance the ability to distinguish authentic from hostile transmissions, aiding the development of a safer UAV operational ecosystem.

© 2024 The Author(s). | Published by Agro Intelligence Research Press

Conclusion

Summing up, the mushrooming density of UAVs in shared airspace poses a grave safety dilemma, rooted in the ease with which signals can be jammed or spoofed. This fragility, felt most keenly within the GNSS sphere, poses a material hazard to general aviation undertakings. In light of the deepening reliance on UAVs across a sweeping range of missions —from reconnaissance to logistics and beyond—the need for robust countermeasures to insulate against potential disruptions from spoofing or jamming signals has become critical.

This research focused primarily on gauging the influence of the SDR HackRF One on UAV safety. By corroborating the device's ability to generate synthetic interference potent enough to knock a GPS receiver offline, our study brings into sharp relief the potential hazards such interference poses in genuine operational scenarios. The data showed that transmitting a bogus GPS spoof signal left the receiver unable to acquire any visible satellites. This breakdown was both severe and dangerous, hinting at an acute risk should it manifest in live operational conditions. The methodological blueprint followed a sequential arc: configuring the SDR unit, synthesizing and radiating signals, dissecting their impact on the GNSS receiver, and systematically appraising the interference. Most tellingly, course deviations and accuracy degradation became apparent once interference set in, with dramatic swings in heading readings and metrics such as RMS2D. In a further measurement round with the GLONASS receiver switched off, heading swung wildly, and the RMS2D metric soared far above the baseline. The RMS2D number ballooned to roughly 57 times the reference level, a direct result of the total forfeiture of the GPS L1C signal, with no recourse to any alternate satellite navigation constellation. These results pound home the absolute necessity of incorporating diverse scenarios and configurations when judging how interference gnaws at GNSS receiver performance.

The wider consequences of this work are indispensable for truly grasping the intrinsic frailties woven into GNSS signals and the tangible perils introduced by unauthorized interference. Equally, the research spotlights the urgent need for resilient countermeasures to shield UAV operations in airspace from the potential havoc caused by spoofing or jamming signals. Even as the HackRF One platform demonstrated its adaptability and practical value for numerous UAV-related applications, leveraging it to detect spoofed GNSS signals adds a layer of benefit to hardening the UAV safety posture in the airspace. Future scholarly work should delve deeper into developing sophisticated detection mechanisms and battle-hardened technologies to insulate UAVs from the shifting threats in the jamming and spoofing environment.

Equally, marrying machine learning and artificial intelligence with SDR technologies could sharpen the ability to separate benign signals from hostile ones, nudging the ecosystem toward a more secure UAV operational milieu. Research efforts should likewise converge on cooperative initiatives that knit together industry players, regulatory watchdogs, and academic bodies to hammer out sweeping guidelines and benchmarks for UAV communication security. Meeting the challenges posed by potential interference demands a cross-cutting strategy that fuses know-how from telecommunications, cybersecurity, and aeronautics. Such a joint enterprise is non-negotiable for staying one step ahead of hostile actors seeking to pry open vulnerabilities in UAV communication links. As technological progress marches on relentlessly, the research community is obliged to remain forward-footed, dreaming up novel countermeasures to tame the risks entwined with GNSS interference.

Acknowledgements

The paper is an output of the project KEGA 040ŽU–4/2022 Transfer of progressive methods of education to the study program “Aircraft Maintenance Technology” and “Air Transport”.

Conflict of interest

None

© 2024 The Author(s). | Published by Agro Intelligence Research Press

Financial support

None

Ethics statement

None

Received: 15 Jan 2023 Revised: 22 Mar 2023 Accepted: 07 Apr 2023
Published online: 25 May 2024

Rights and permissions

Open Access The author(s) retain copyright. This article is licensed under the Creative Commons Attribution-NonCommercial-ShareAlike 4.0 International License. It may be shared and adapted for non-commercial purposes with appropriate attribution, an indication of changes, and distribution of adaptations under the same license. Third-party material may be subject to separate terms identified in its credit line. View the license at https://creativecommons.org/licenses/by-nc-sa/4.0/.

References

1. Hofmann-Wellenhof B, Lichtenegger H, Wasle E. GNSS-global navigation satellite systems: GPS, GLONASS, Galileo, and more. Springer and Science and Business Media: Berlin/Heidelberg, Germany, 2007; ISBN 978-3-211-73012-6.

2. Radočaj D, Plaščak I, Jurišić M. Global navigation satellite systems as state-of-the-art solutions in precision agriculture: A review of studies indexed in the Web of Science. Agriculture. 2023;13:1417.

3. Marz S, Schlicht A, Hugentobler U. Toward a geodesy and time reference in space (GETRIS): A study of apparent satellite clocks of a future GNSS satellite constellation. Geosciences. 2023;13:173.

4. Telli K, Kraa O, Himeur Y, Ouamane A, Boumehraz M, Atalla S, et al. A comprehensive review of recent research trends on unmanned aerial vehicles (uavs). Systems. 2023;11:400.

5. Budiyono A, Higashino SI. A review of the latest innovations in UAV technology. J Instrum Autom Syst. 2023;10:7–16.

6. Milota J. Software radios: Survey, critical evaluation and future directions. IEEE Aerosp Electron Syst Mag. 1993;8:25–36.

7. Del Barrio AA, Manzano JP, Maroto VM, Villarín Á, Pagán J, Zapater M, et al. HackRF+ GNU Radio: A software-defined radio to teach communication theory. Int J Electr Eng Educ. 2023;60:23–40.

8. Mori S, Mizutani K, Harada H. Software-defined radio-based 5G physical layer experimental platform for highly mobile environments. IEEE Open J Veh Technol. 2023;4:230–40.

9. Hrúz M, Bugaj M, Novák A, Kandera B, Badánik B. The use of UAV with infrared camera and RFID for airframe condition monitoring. Appl Sci. 2021;11:3737.

10. Kakkavas G, Tsitseklis K, Karyotis V, Papavassiliou S. A software defined radio cross-layer resource allocation approach for cognitive radio networks: From theory to practice. IEEE Trans Cogn Commun Netw. 2020;6:740–55.

11. Bargarai F, Abdulazeez A, Tiryaki V, Zeebaree D. Management of wireless communication systems using artificial intelligence-based software defined radio. IJIM. 2020;14:107–33.

12. Kumar BP, Paidimarry CS. Improved real time GPS RF data capturing for GNSS SDR applications. Gyroscopy Navig. 2020;11:59–67.

13. Flak P. Drone detection sensor with continuous 2.4 GHz ISM band coverage based on cost-effective SDR platform. IEEE Access. 2021;9:114574–86.

14. Aboelazm MA. Design and implementation of analog modulated signals radio monitoring receiver based on SDR technology. J Inf Hiding Multimed Signal Process. 2022;13:64–77.

15. Woh M, Lin Y, Seo S, Mahlke S, Mudge T, Chakrabarti C, et al. From soda to scotch: The evolution of a wireless baseband processor. In: Proceedings of the 2008 41st IEEE/ACM International Symposium on Microarchitecture, Lake Como, Italy; 2008. p. 152–63.

16. Zhang Z, Zhan X, Xu H. Development and validation of a low-cost GPS spoofing simulator. J Aeronaut Astronaut Aviat. 2014;46:78–86.

17. Dovis F. GNSS interference threats and countermeasures. Artech House: Norwood, MA, USA, 2015; ISBN 978-1-60807-810-3.

18. Broumandan A, Jafarnia-Jahromi A, Daneshmand S, Lachapelle G. Overview of spatial processing approaches for GNSS structural interference detection and mitigation. Proc IEEE. 2016;104:1246–57.

19. De Wilde W, Cuypers G, Sleewaegen JM, Deurloo R, Bougard B. GNSS interference in unmanned aerial systems. In: Proceedings of the 29th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2016), Oregon, Portland; 2016. p. 1465–76.

20. Motella B, Savasta S, Margaria D, Dovis F. Method for assessing the interference impact on GNSS receivers. IEEE Trans Aerosp Electron Syst. 2011;47:1416–32.

21. Qiao J, Lu Z, Lin B, Song J, Xiao Z, Wang Z, et al. A survey of GNSS interference monitoring technologies. Front Phys. 2023;11:1133316.

22. Silva Lorraine KJ, Ramarakula M. A comprehensive survey on GNSS interferences and the application of neural networks for anti-jamming. IETE J Res. 2023;69:4286–305.

23. Sun K, Zhang T. A new GNSS interference detection method based on rearranged wavelet–Hough transform. Sensors. 2021;21:1714.

24. Gadgets GS. HackRF One-Great Scott Gadgets. 2023. https://greatscottgadgets.com/hackrf/one (accessed on 30 November 2023).

25. Elghamrawy H, Karaim M, Tamazin M, Noureldin A. Experimental evaluation of the impact of different types of jamming signals on commercial GNSS receivers. Appl Sci. 2020;10:4240.

26. McGraw GA, Groves PD, Ashman BW. Robust positioning in the presence of multipath and NLOS GNSS signals. In: Position, navigation, and timing technologies in the 21st century: Integrated satellite navigation, sensor systems, and civil applications. John Wiley & Sons: Hoboken, NJ, USA, 2020; 1: 551–89.

27. Ding M, Chen W, Ding W. Performance analysis of a normal GNSS receiver model under different types of jamming signals. Measurement. 2023;214:112786.

© 2024 The Author(s). | Published by Agro Intelligence Research Press

28. ICAO. Doc 8071-manual on testing of radio navigation aids. Volume II, testing of satellite based radio navigation aids, 5th ed.; International Civil Aviation Organization: Montreal, QC, Canada, 2006.

29. Gao GX, Sgammini M, Lu M, Kubo N. Protecting GNSS receivers from jamming and interference. Proc IEEE. 2016;104:1327–38.

30. Li Y, Feng B, Zhang W. Mutual interference mitigation of millimeter-wave radar based on variational mode decomposition and signal reconstruction. Remote Sens. 2023;15:557.

31. Li A, Spano D, Krivochiza J, Domouchtsidis S, Tsinos CG, Masouros C, et al. A tutorial on interference exploitation via symbol-level precoding: Overview, state-of-the-art and future directions. IEEE Commun Surv Tutor. 2020;22:796–839.

32. Boyer M, Bouyer L, Roy JS, Campeau-Lecours A. Reducing noise, artifacts and interference in single-channel EMG signals: A review. Sensors. 2023;23:2927.

33. Ru Z, Moseley NA, Klumperink EA, Nauta B. Digitally enhanced software-defined radio receiver robust to out-of-band interference. IEEE J Solid-State Circuits. 2009;44:3359–75.

34. Rahman M, Haider A, Naghshvarianjahromi M. A systematic methodology for the time-domain ringing reduction in UWB band-notched antennas. IEEE Antennas Wirel Propag Lett. 2020;19:482–6.

35. Osechas O, Fohlmeister F, Dautermann T, Felux M. Impact of GNSS-band radio interference on operational avionics. Navigation. 2022;69:navi.516.

36. Le Roy F, Roland C, Le Jeune D, Diquet JP. Risk assessment of SDR-based attacks with UAVs. In: Proceedings of the 16th International Symposium on Wireless Communication Systems, Oulu, Finland; 2019. p. 222–6.

37. Huang L, Lu Z, Xiao Z, Ren C, Song J, Li B. Suppression of jammer multipath in GNSS antenna array receiver. Remote Sens. 2022;14:350.

38. Su XL, Zhan X, Tu J. GNSS constellation integrity evaluation based on quality control. J Aeronaut Astronaut Aviat. 2016;48:37–46.

39. Spens N, Lee DK, Nedelkov F, Akos D. Detecting GNSS jamming and spoofing on Android devices. Navigation. 2022;69:navi.537.

40. Sharifi-Tehrani O, Sabahi MF, Danaee MR. Low-complexity framework for GNSS jamming and spoofing detection on moving platforms. IET Radar Sonar Navig. 2020;14:2027–38.

41. Falletti E, Gamba MT, Pini M. Design and analysis of activation strategies for adaptive notch filters to suppress GNSS jamming. IEEE Trans Aerosp Electron Syst. 2020;56:3718–34.

42. Bažec M, Dimc F, Pavlovčič-Prešeren P. Evaluating the vulnerability of several geodetic GNSS receivers under chirp signal L1/E1 jamming. Sensors. 2020;20:814.

43. Zhang J, Cui X, Xu H, Lu M. A two-stage interference suppression scheme based on antenna array for GNSS jamming and spoofing. Sensors. 2019;19:3870.

44. Li J, Zhu X, Ouyang M, Li W, Chen Z, Fu Q. GNSS spoofing jamming detection based on generative adversarial network. IEEE Sens J. 2021;21:22823–32.

45. Meng L, Yang L, Yang W, Zhang L. A survey of GNSS spoofing and anti-spoofing technology. Remote Sens. 2022;14:4826.

© 2024 The Author(s). | Published by Agro Intelligence Research Press

46. Khan SZ, Mohsin M, Iqbal W. On GPS spoofing of aerial platforms: A review of threats, challenges, methodologies, and future research directions. PeerJ Comput Sci. 2021;7:e507.

47. Gaspar J, Ferreira R, Sebastião P, Souto N. Capture of UAVs through GPS spoofing using low-cost SDR platforms. Wirel Pers Commun. 2020;115:2729–54.

48. Haljaková P, Novák A, Žižka J. Monitoring GNSS signal quality at Žilina airport. In: Proceedings of the 19th International Conference on New Trends in Civil Aviation, Prague, Czech Republic; 2017. p. 289–93.

49. Van Rychlicki M, Kasprzyk Z, Rosiński A. Analysis of accuracy and reliability of different types of GPS receivers. Sensors. 2020;20:6498.

50. Gúcky J, Kováčiková K, Novák A, Bugaj M. Analysis of the introduction of artificial intelligence in the control of UAV. In: Proceedings of the New Trends in Aviation Development 2022, Novy Smokovec, Slovakia; 2022. p. 67–70.

51. Kerns AK, Shepard DP, Bhatti JA, Humphreys TE. Unmanned aircraft capture and control via GPS spoofing. J Field Robot. 2014;31:617–36.

52. Terris-Gallego R, López-Salcedo JA, Seco-Granados G, Fernandez-Hernandez I. Preliminary evaluation of Galileo ACAS using existing E1-E6 open signals and a low-cost SDR platform. In: Proceedings of the 36th International Technical Meeting of the Satellite Division of the Institute of Navigation, Denver, CO, USA; 2023. p. 1388–402.

53. Nayfeh M, Li Y, Shamaileh KA, Devabhaktuni V, Kaabouch N. Machine learning modeling of GPS features with applications to UAV location spoofing detection and classification. Comput Secur. 2023;126:103085.

54. Bi S, Li K, Hu S, Ni W, Wang C, Wang X. Detection and mitigation of position spoofing attacks on cooperative UAV swarm formations. IEEE Trans Inf Forensics Secur. 2024;19:1883–95.

55. Martinez Quintero JC, Estupiñan Cuesta EP, Ramirez Lopez LJ. A new method for the detection and identification of the replay attack on cars using SDR technology and classification algorithms. Results Eng. 2023;19:101243.

56. Broadcast Ephemeris Data. National Aeronautics and Space Administration. 2023. https://cddis.nasa.gov/Data_and_Derived_Products/GNSS/broadcast_ephemeris_data.html (accessed on 30 November 2023).

57. Zhang T, Song T, Chen D, Zhang T, Zhuang J. WiGrus: a WiFi-based gesture recognition system using software-defined radio. IEEE Access. 2019;7:131102–13.

58. Borio D, Gioia C. Interference mitigation: impact on GNSS timing. GPS Solut. 2021;25:37.

59. Morong T, Puričer P, Kovář P. Study of the GNSS jamming in real environment. Int J Electron Telecommun. 2019;65:65–70.

60. Specht M. The evaluation of the positioning accuracy of the EGNOS and DGPS systems based on the long-term measurements in the years 2006–2014. Pol Cartogr Rev. 2015;47:99–108.

61. Kalašová A, Faith P, Mikulski J. Telematics applications, an important basis for improving the road safety. Tools Transp Telemat. 2015;531:292–9.

62. Harre I. Navgen-Calculation of Position Errors drms, 2drms, cep95 and of the Error Ellipse for p = 0.95. 2009. http://www.mar-it.com/NavGen/navgen.htm (accessed on 30 November 2023).

63. Closas P, Arribas J, Fernandez-Prades C. Spoofing detection by a reduced acquisition process. In: Proceedings of the 2016 International Technical Meeting of The Institute of Navigation, Monterey, CA, USA; 2016. p. 726–31.

64. Jafarnia-Jahromi A, Daneshmand S, Broumandan A, Nielsen J, Lachapelle G. PVT solution authentication based on monitoring the clock state for a moving GNSS receiver. In: Proceedings of the European Navigation Conference (ENC), Vienna, Austria;

© 2024 The Author(s). | Published by Agro Intelligence Research Press

2013.

65. Jafarnia-Jahromi A, Broumandan A, Nielsen J, Lachapelle G. Pre-despreading authenticity verification for GPS L1 C/A signals. Inst Navig. 2014;61:1–11.

66. Broumandan XA, Jafarnia-Jahromi A, Dehghanian V, Nielsen J, Lachapelle G. GNSS spoofing detection in handheld receivers based on signal spatial correlation. In: Proceedings of the IEEE/ION Position, Location and Navigation Symposium, Myrtle Beach, SC, USA; 2012. p. 479–87.

67. Broumandan A, Jafarnia-Jahromi A, Lachapelle G. Spoofing detection, classification and cancelation (SDCC) receiver architecture for a moving GNSS receiver. GPS Solut. 2014;19:475–87.

68. Psiaki XML, Powell SP, O'Hanlon BW. GNSS spoofing detection using high-frequency antenna motion and carrier-phase data. In: Proceedings of the 26th International Technical Meeting of the Satellite Division of the Institute of Navigation, Nashville, TN, USA; 2013. p. 2949–91.

69. Psiaki XML, O'Hanlon BW, Powell SP, Bhatti JA, Wesson KD, Schofield TE, et al. GNSS spoofing detection using two-antenna differential carrier phase. In: Proceedings of the 27th International Technical Meeting of the Satellite Division of the Institute of Navigation, Tampa, FL, USA; 2014. p. 2776–800.

70. Parro-Jimenez M, Ioannides R, Crisci M, Lopez-Salcedo JA. Signal-level integrity monitoring metric for robust GNSS receivers. In: Proceedings of the 31st AIAA International Communications Satellite Systems Conference, Florence, Italy; 2013. p. 5613.

71. Roberts XJ. Drones Vulnerable to Terrorist Hijacking, Researchers Say. 2012. http://www.foxnews.com/tech/2012/06/25/drones-vulnerable-to-terrorist-hijacking-researchers-say (accessed on 5 March 2024).

72. UT News. The University of Texas at Austin. UT Austin Researchers Successfully Spoof an $80 Million Yacht at Sea. 2013. http://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea (accessed on 5 March 2024).

73. Olson P. Hacking a Phone's GPS May Have Just Got Easier. Forbes. 2013. http://www.forbes.com/sites/parmyolson/2015/08/07/gps-spoofing-hackers-defcon/ (accessed on 5 March 2024).

© 2024 The Author(s). | Published by Agro Intelligence Research Press