Experimental Testing and Impact Analysis of Jamming and Spoofing Attacks on Professional GNSS Receivers

Sanja Miljanovic[a], Francesco Ardizzon[a], Laura Crosara[a], Nicola Laurenti[a], Luca Canzian[b], Enrico Lovisotto[b], Nicola Montini[b], Oscar Pozzobon[b,c] and Rigas T. Ioannides[d]

[a]*Department of Information Engineering, Università degli Studi di Padova, Padova, Italy*
[b]*Qascom, Via Marinali 87, Bassano del Grappa, Italy*
[c]*European Space Research and Technology Centre (ESTEC), Keplerlaan 1, Noordwijk, the Netherlands*

Abstract

In recent years, global navigation satellite systems (GNSSs) have become crucial for many applications; however, GNSS receivers are susceptible to attacks such as jamming and spoofing. As a result, evaluating the impact of these attacks on real receivers is critical in order to develop effective defense strategies. In this paper we propose an evaluation mechanism and also set up an analysis platform to assess and classify impacts of attacks on the position velocity and time (PVT) solution computed by GNSS receivers. We carried out tests of jamming and spoofing attack scenarios employing mass market GNSS receivers in order to validate our procedure. Results obtained for reference scenarios are presented and discussed in the paper, also considering the cooperative action of jamming and spoofing, demonstrating the applicability of the developed tool to evaluate impacts of different attacks on GNSS receivers.

Keywords

GNSS, Spoofing, Jamming

1. Introduction

Global navigation satellite system (GNSS) technology provides real-time positioning and timing for various civil and military applications. GNSS signals are particularly susceptible to both inadvertent and intentional interference due to their low received power (from −163 dBW to −152 dBW). Furthermore, civilian GNSS signal and modulation formats are open to the public. For these reasons, a wide range of attacks are viable. In the field of GNSS security, the major threats considered are jamming and spoofing [1]. Jamming is a denial of service attack where the adversary overshadows the received GNSS signals with a higher power noise-like signal to make the victim receiver unable to acquire or track the satellite signal, affecting system availability [1, 2]. Jammers can disrupt GNSS-based services in wide geographical areas with radii of several kilometers [3, 4]. With a spoofing attack, the attacker produces counterfeit GNSS signals that are similar to authentic ones, by modifying the original satellite signals in order to manipulate the victim receiver's estimated position [1] and/or timing. This attack

ICL-GNSS 2022 WiP, June 07–09, 2022, Tampere, Finland
sanja.miljanovic@studenti.unipd.it (S. Miljanovic); ardizzonfr@dei.unipd.it (F. Ardizzon); crosaralau@dei.unipd.it (L. Crosara); nil@dei.unipd.it (N. Laurenti); luca.canzian@qascom.it (L. Canzian); enrico.lovisotto@qascom.it (E. Lovisotto); nicola.montini@qascom.it (N. Montini); oscar.pozzobon@qascom.it (O. Pozzobon); rigas.ioannides@esa.int (R.T. Ioannides)
0000-0001-6066-7550 (F. Ardizzon); 0000-0002-5996-2074 (L. Crosara); 0000-0001-7592-1929 (N. Laurenti)

is particularly dangerous because it may succeed without the victim being aware of being attacked.

Modern GNSS receivers are equipped with interference mitigation methods, e.g., Receiver Autonomous Integrity Monitoring (RAIM), and even spoofing detection mechanisms such as Galileo OS-NMA [5], GPS CHIMERA [6]. Because of the presence of these defense mechanisms, analyzing the impact of common attacks on real receivers is critical for developing increasingly effective defense methods. A first discussion of jamming impact on commercial GNSS receivers is provided in [2], while analysis and evaluation of spoofing effects was proposed in [7, 8]. In [9, 10, 11] the authors investigate the repercussions of spoofing attacks on mass-market positioning and navigation units integrated in modern day smartphones, while a comparative analysis of GPS receivers resilience to software attacks can be found in [12].

In this paper we propose an evaluation mechanism and set up an analysis platform to classify attack impacts on GNSS receivers by analyzing the computed position velocity and time (PVT) solution. In order to validate our procedure, we present the results obtained for some reference scenarios, considering also a hybrid attack where jamming and spoofing act cooperatively. The developed tool could be employed to assess the performance of existing GNSS interference mitigation and anti-spoofing techniques, as well as a platform to design and test new defence mechanisms. The work was developed in the context of the position, navigation and timing cyber response centre (PNT-CRC) project, that will provide a GNSS vulnerability assessment service to industries, as well as mitigation solutions to enhance robustness of GNSS receivers. The paper illustrates impact classification methodologies together with examples of metrics and attack scenarios.

The reminder of this paper is organized as follows. Section 2 introduces the security model and metrics that will be taken into consideration for impact classification. Section 3 describes the methodology for the experimental setup and test, while results and impact analysis are provided in Section 4. Finally, Section 5 draws the conclusions and presents future developments of our work.

2. Security Model and Measures

In order to analyze the attack impact on a specific scenario we need to examine the PVT solution computed by the GNSS receiver. For this purpose, it is sufficient to process the receiver output obtaining the information needed for our analysis, specifically: position information (latitude, longitude, altitude, referred to as LLA), time and fix quality indicator (i.e. "fix" or "no fix"). This gives us the receiver status and the provided service, meaning PVT, at a typical time rate of 1Hz. Therefore, we can build a timed list of points that represents the reported positions of the receiver as a trajectory. The measured trajectory can be compared with the true one and the spoofing target, if present. Hence, we introduce the following trajectories as 3D LLA coordinates vectors varying along time t

authentic trajectory $\boldsymbol{p}_{\mathrm{a}}(t)$, associated with the legitimate signals;

spoofing trajectory $\boldsymbol{p}_{\mathrm{s}}(t)$, associated with the spoofing signals;

measured trajectory $\boldsymbol{p}_{\mathrm{r}}(t)$, measured by the receiver.

In order to evaluate the effect of an attack on the tested receiver, we compare the receiver measurements in nominal conditions and under attack. Thus, we specialize the definition of

$\boldsymbol{p}_{\mathrm{r}}(t)$ into $\boldsymbol{p}_{\mathrm{r}}^{N}(t)$, the trajectory measured by the receiver in the nominal scenario, and $\boldsymbol{p}_{\mathrm{r}}^{A}(t)$, the trajectory measured by the receiver under attack. This allows us to compute the positioning error respectively in the the nominal and under-attack scenarios as

$$e_{\mathrm{r}}^{\mathrm{N}}(t) = \|\boldsymbol{p}_{\mathrm{r}}^{\mathrm{N}}(t) - \boldsymbol{p}_{\mathrm{a}}(t)\|, \tag{1}$$

$$e_{\mathrm{r}}^{\mathrm{A}}(t) = \|\boldsymbol{p}_{\mathrm{r}}^{\mathrm{A}}(t) - \boldsymbol{p}_{\mathrm{a}}(t)\|. \tag{2}$$

2.1. Metrics

Following the recommendations in [13], we evaluate the attack impact on the receiver under the test scenario by choosing as metrics the average, standard deviation, and 95-th percentile of the position error, represented as mean, std and 95th, respectively. All these statistical quantities will be estimated over a time window $W = (t_W - \Delta/2, t_W + \Delta/2)$, centred around t_W and with duration Δ. From them we compute four performance degradation metrics, that will be later used in section 2.2.4 for classification of the PVT degradation

$$\alpha_{\Delta}(t_W) = \mathrm{mean}_W(e_{\mathrm{r}}^{\mathrm{A}})/\mathrm{mean}_W(e_{\mathrm{r}}^{\mathrm{N}}) \tag{3}$$

$$\beta_{\Delta}(t_W) = \mathrm{std}_W(e_{\mathrm{r}}^{\mathrm{A}})/\mathrm{std}_W(e_{\mathrm{r}}^{\mathrm{N}}) \tag{4}$$

$$\gamma_{\Delta}(t_W) = 95\mathrm{th}_W(e_{\mathrm{r}}^{\mathrm{A}})/95\mathrm{th}_W(e_{\mathrm{r}}^{\mathrm{N}}) \tag{5}$$

$$\sigma_{\mathrm{r}}^{\mathrm{N}}(t_W) = \mathrm{std}_W(e_{\mathrm{r}}^{\mathrm{N}}) \tag{6}$$

2.2. Impact classification

This section lists possible impact classes in terms of the resulting receiver condition which shall be evaluated in sequence.

2.2.1. Failure

This is the condition when receiver firmware crashes. The receiver status, if still reported from the device, is not nominal but unexpected. Our proposal is to report and investigate for a failure when the receiver output simply stops coming.

2.2.2. Denial of Service (DoS)

This conditions is declared when PVT solution cannot be computed for a continuous time window longer than 5 seconds. Three things can happen for the tested receiver:

- Receiver stops sending log data (provided this is not due to a software crash and only the PVT service is lost);
- Log files from the receiver are incomplete, missing some fields;
- Fix quality indicator is set to "no fix".

If any of these is met, a DoS event is declared.

2.2.3. Trajectory spoofing

This condition causes the receiver to report a different position (or trajectory) from the authentic one. This impact is evaluated only when spoofing attack is active and requires to jointly monitor the authentic and spoofing trajectory, as well as the position reported by the receiver. Considering a sequence of time windows W_i, $i = 1, 2, \ldots$, of constant width Δ and center points t_i spaced of T seconds, a trajectory spoofing is reported if all these conditions are met

- receiver's output is nominal, i.e. neither failure nor DoS events are reported;
- $\mathrm{mean}_{W_i}(\|\boldsymbol{p}_\mathrm{s}(t) - \boldsymbol{p}_\mathrm{a}(t)\|) > 3\,\sigma_\mathrm{r}^\mathrm{N}(t_i)$, meaning authentic and spoofing trajectory differ significantly, i.e. with a 3-sigma confidence level;
- $\mathrm{mean}_{W_i}(\|\boldsymbol{p}_\mathrm{r}^\mathrm{A}(t) - \boldsymbol{p}_\mathrm{s}(t)\|) < \mathrm{mean}_{W_i}(\|\boldsymbol{p}_\mathrm{r}^\mathrm{A}(t) - \boldsymbol{p}_\mathrm{a}(t)\|)$, meaning reported position is closer to the spoofing trajectory than the authentic one.

On the contrary, if any of the above condition is not met, the following impact classes shall be considered.

2.2.4. PVT degradation

PVT accuracy degrades when the receiver reports a position which is different than the real one. PVT degradation is measured for each receiver with respect to nominal conditions. Let $\alpha_\Delta(t_i), \beta_\Delta(t_i), \gamma_\Delta(t_i)$ denote the performance degradation metrics measured in a sequence of time windows of span Δ and center points $t_i = iT$. Then, we define three degradation levels, as well as a no-degradation status, based on preset threshold values α_j, β_j and γ_j, $j = 1, 2, 3$, such that $\alpha_1 < \alpha_2 < \alpha_3$, $\beta_1 < \beta_2 < \beta_3$ and $\gamma_1 < \gamma_2 < \gamma_3$. Thus, with $\times$ denoting the Cartesian product and $S_j = (0, \alpha_j) \times (0, \beta_j) \times (0, \gamma_j) \subset \mathbb{R}^3$, we have $S_1 \subset S_2 \subset S_3$:

1. no-degradation: $(\alpha_\Delta(t_i), \beta_\Delta(t_i), \gamma_\Delta(t_i)) \in S_1$,
2. minor degradation: $(\alpha_\Delta(t_i), \beta_\Delta(t_i), \gamma_\Delta(t_i)) \in S_2 \setminus S_1$,
3. major degradation: $(\alpha_\Delta(t_i), \beta_\Delta(t_i), \gamma_\Delta(t_i)) \in S_3 \setminus S_2$,
4. severe degradation: $(\alpha_\Delta(t_i), \beta_\Delta(t_i), \gamma_\Delta(t_i)) \in \mathbb{R}^3 \setminus S_3$,

where $A \setminus B$ denotes the set difference. When evaluating the receiver condition in the above classification, comparison shall be done against the thresholds in sequence from case 1 to 4.

For greater clarity, in Figure 1 we have reported three different trajectories, where the authentic one is represented by the blue line. In our model, the trajectory in black is classified as "trajectory spoofing", as it appears to be far from the legitimate trajectory and therefore cannot represent a degradation of the PVT solution. Instead, the red trajectory initially coincides with the authentic trajectory , before deviating from it. Therefore, the red trajectory is first classified as no-degradation and subsequently as minor, major and severe PVT degradation as the gap between the red and the blue trajectories increases.

3. Experimental setup and attack scenarios

In this section a methodology for the experimental setup and test is provided, together with the description of attack scenarios and testing parameters.

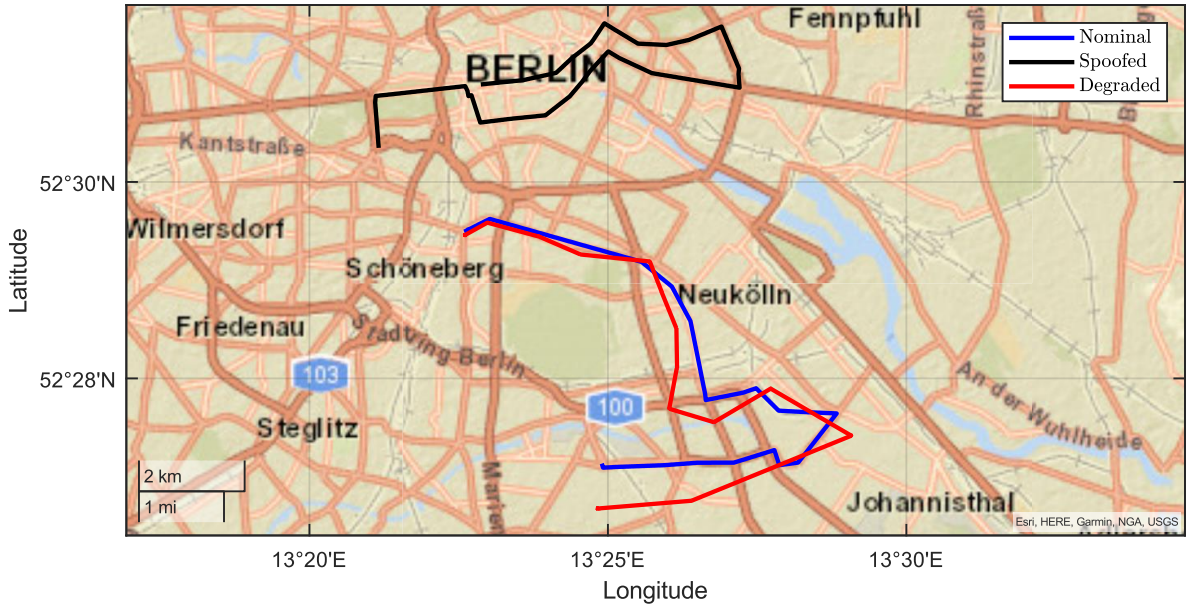

Figure 1: Examples of impact classification on different trajectories: in blue the authentic trajectory, in black a target trajectory for spoofing attack and in red a trajectory subject to PVT degradation.

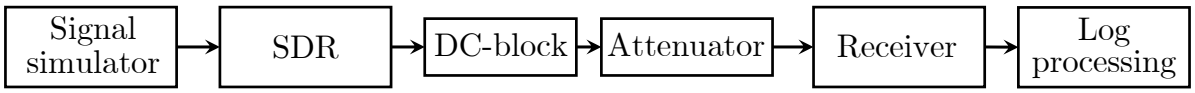

Figure 2: Block scheme of the experimental setup

3.1. Experimental setup

For simulation of scenarios we used QA707 software signal simulator by Qascom [14], that is used to generate both authentic signal and possible interference or attack signals, all at the same time. To perform the various tests needed we had to prepare the equipment as illustrated by the diagram in Figure 2. QA707 simulates the signals (i.e. GNSS and interference), combines them and stores the resulting composite signal in a single binary file which is fed to the USRP X300 software-defined radio (SDR). In order to prevent the flow of direct current frequencies going back into the SDR, potentially damaging the instrumentation, the use of a DC blocker is advised. As GNSS receiver we used a Septentrio PolaRx5 [15]. The output of the receiver was logged using the national marine electronics association (NMEA) standard [16], since it offers a common output interface across many vendors and receiver models. Moreover, we will focus on the GPS fix data (GGA) message since it provides all the data needed for the analysis described in Section 2. Still, notice that the very same procedure can be performed starting from different logging formats, e.g., the Septentrio binary format (SBF). The obtained experimental setup is depicted in Figure 3.

In order to perform meaningful tests in an indoor laboratory scenario with wired connection, we have to adjust the generated signal power to a realistic level. To this purpose, we started by observing the automatic gain control (AGC) level at the receiver using a Spirent GSS9000

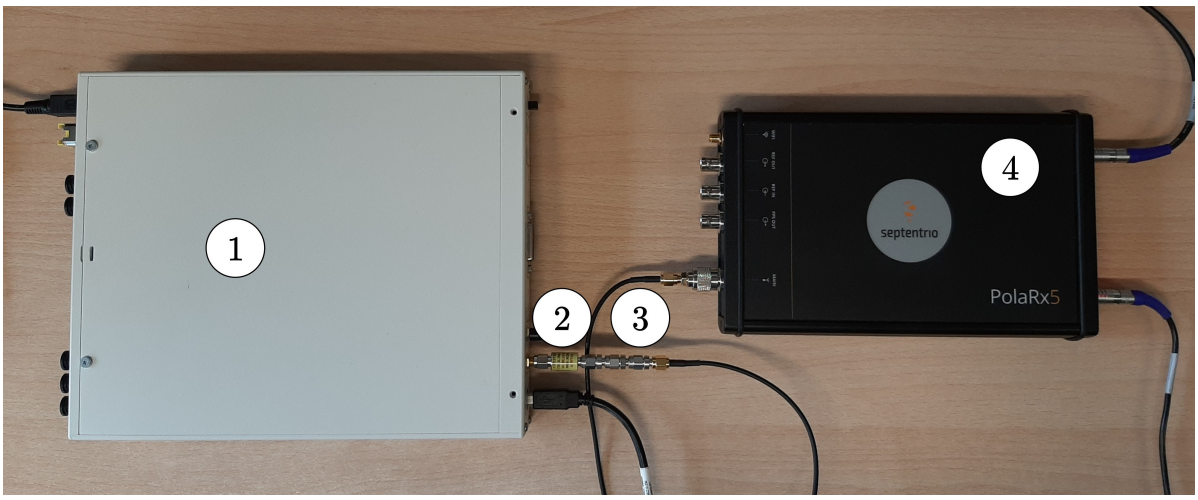

Figure 3: Experimental setup consisting of (1) USRP X300 SDR, (2) DC-block, (3) attenuators, (4) Septentrio PolaRx5 GNSS receiver.

Table 1
AGC levels measured by the Septentrio during the calibration phase, obtained using different signal generators. The AGC is not reported if the receiver was not able to acquire the signal.

Attenuation [dB]	0	10	20	30	40	50
AGC using Spirent [dB]	62	62	-	-	-	-
AGC using USRP X300 [dB]	-	-	-	57	61	61

signal simulator, which had been previously calibrated so its output can be assumed reliable. Then, we observed the AGC value measured by the Septentrio using the USRP X300; finally, we added signal attenuators in order to achieve the same AGC level observed with the Spirent. Results are reported in Table 1. In order to obtain similar conditions with respect to nominal (Spirent) ones, we need to pick an attenuation in the range [40 dB,50 dB] while using USRP X300 + QA707. Therefore, in the following experiments we picked an attenuation value of 50 dB.

3.2. Scenario configuration

The QA707 software allows the setup of several configuration parameters that allow to model several nominal and under attack scenarios.

A first batch of settings identifies the *navigation scenario* and includes all the parameters needed to characterize the navigation simulation, i.e., user position or trajectory, simulation start time and duration, channel impairments, and number of generated channels. A second group of settings characterizes the generation of jamming and spoofing attacks. Concerning jamming attacks, the user can set the jamming power (which can possibly vary during the attack simulation), central frequency, bandwidth and frequency modulation type (e.g., simple narrow-band, frequency hopping or chirp).

Regarding signal-level spoofing attacks, the QA707 allows two types of attack simulations. The former, referred to as *channel spoofing*, allows the operator to configure pseudoranges and Doppler frequency associated to each spoofed channel (i.e. a specific satellite). This type

of simulation can, for example, prevent the PVT algorithm from converging to any position, setting pseudorange values that do not correspond to any physical point in space. However, in the channel spoofing mode it is difficult to configure a spoofing attack that is consistent with a specific spoofing trajectory. Instead, the second attack simulation, called *trajectory spoofing*, allows the operator to configure a spoofing trajectory, so that the spoofing signals associated to all channels are generated consistently with it. The spoofing trajectory can be both static (i.e., a fixed position) or dynamic and is fed to QA707 software as an input. For both attack types, user can define the spoofer transmitting power.

4. Experimental Results

The results discussed in this section have been obtained through experimental tests using the setup depicted in Figure 3. The goal of these tests is to recognize the impacts of different types of jamming and spoofing attacks on commercial GNSS receivers, according to the metrics and the classification method outlined in Section 2. By way of example, we will discuss three different attack scenarios, namely a jamming scenario, a spoofing scenario and, finally, a scenario were jamming and spoofing act cooperatively. The trajectories used for the dynamic scenarios are those reported in Figure 1: the blue one represents the authentic trajectory $\boldsymbol{p}_{\mathrm{a}}(t)$ for all scenarios while the black one is the target trajectory for the spoofing attack $\boldsymbol{p}_{\mathrm{s}}(t)$.

All the tests were performed fixing the following parameters:

Simulated time and day : August 01, 2021, 12:00:00;

Duration : 00:10:00;

Visible satellites 17;

Received GNSS signal power : $-158\,\mathrm{dBW}$;

Concerning the parameters discussed in Section 2.2, we decided to keep them constant for all the experiments:

- $\Delta = 30$ seconds, $T = 10$ seconds;
- $\alpha_1 = 2, \quad \alpha_2 = 4, \ \alpha_3 = 8$;
- $\beta_1 = 1.5, \ \beta_2 = 3, \ \beta_3 = 10$;
- $\gamma_1 = 2.5, \ \gamma_2 = 5, \ \gamma_3 = 8.5$.

The threshold values α_j, β_j and γ_j, $j = 1, 2, 3$, were calculated based on testing documents for GNSS receivers released by european telecommunications standards institute (ETSI) [13]. More specifically, in [13] GNSS receivers are discriminated into three categories A, B and C, starting from high-end and loosening the performance requirements to low-end ones, according to vertical precision accuracy (VPA) and horizontal precision accuracy (HPA) levels[1]. In particular, we considered the values regarding the open area scenario which are summarized in Table 2. Note that the performance requirements for moving scenarios specified in [13] are identical to those for static scenarios, for the metrics under consideration. Since we aim to

[1]VPA (HPA) is defined as the difference (error) between the position of the location target reported by the GNSS based location system (GBLS) and its true position projected onto the vertical (horizontal) plane, at a given time (i.e. with a given timestamp). We remark that these are different with respect to the VPA and the HPA as typically used in the literature (e.g., [17]).

Table 2
Performance requirements for vertical and horizontal position accuracy in open area scenarios [13, Tables 3, 6, 9, 12], in nominal conditions.

Reference metric		Max position error [m] Class A (t_A)	Class B (t_B)	Class C (t_C)
mean (α)	HPA	1	4	8
	VPA	2	8	16
std (β)	HPA	0.7	2	7
	VPA	1.5	4	14
95th (γ)	HPA	2	10	17
	VPA	4	20	34

generalize with respect to receiver type and experimental settings, we consider a receiver to always be in class A while in nominal scenario. Then, the relative dropping of class caused by the tested attacks, from class A to B or from class A to C, is interpreted as major or severe degradation, respectively. Therefore, we computed $\alpha_2, \beta_2, \gamma_2$ as t_B/t_A and $\alpha_3, \beta_3, \gamma_3$ as t_C/t_A, rounding to the nearest multiple of 0.5. It is worth noting that we get the same threshold values whether we start with vertical or horizontal position accuracy performance requirements.

Moreover, we introduce the minor degradation category, in order to characterize cases when the PVT degradation is noticeable but not so disrupting to change the receiver relative class. So, the values of α_1, β_1 and γ_1 have been computed halving α_2, β_2 and γ_2, respectively.

4.1. Jamming scenario

We tested a triangular frequency modulation jamming attack in dynamic PVT model, i.e. assuming that the position of the receiver is changing over time. We considered a narrow-band jammer transmitting triangular modulated Gaussian noise with bandwidth 100kHz. We gradually increased the jammer's power over the time interval considered, from -119 dBW to -112 dBW of received power. In Figure 4 we show impact classification results for the jamming scenario, for 5 Hz of frequency variation rate (rate of variation of the frequency modulation) and frequency modulation span (peak-to-peak amplitude of the frequency modulation, across the central frequency) of 200 kHz. DoS status was detected when the jamming signal power exceeded -118 dBW, at 200 seconds of scenario, meaning that the jamming attack was successful. In Figure 4 the red, green and blue curves depict the values of the parameters α, β and γ during the tested scenario. Moreover, Figure 4 exhibits an abrupt degradation behaviour since the receiver status jumps from minor degradation to DoS. This effects is a consequence of the increasing jamming power: first the receiver manages to mitigate jammer's interference but, when the jamming signal power exceeded -118 dBW, it looses the track on the legitimate signal, leading to DoS status.

4.2. Spoofing scenario

We carried out spoofing attack tests both in static (where the authentic and target spoofing trajectories are fixed positions) and dynamic (moving trajectories) scenarios, considering 10 spoofed satellites out of 17. Spoofing attack is successful if the impact classification procedure identifies the receiver status as trajectory spoofing. Impact classification results for the static

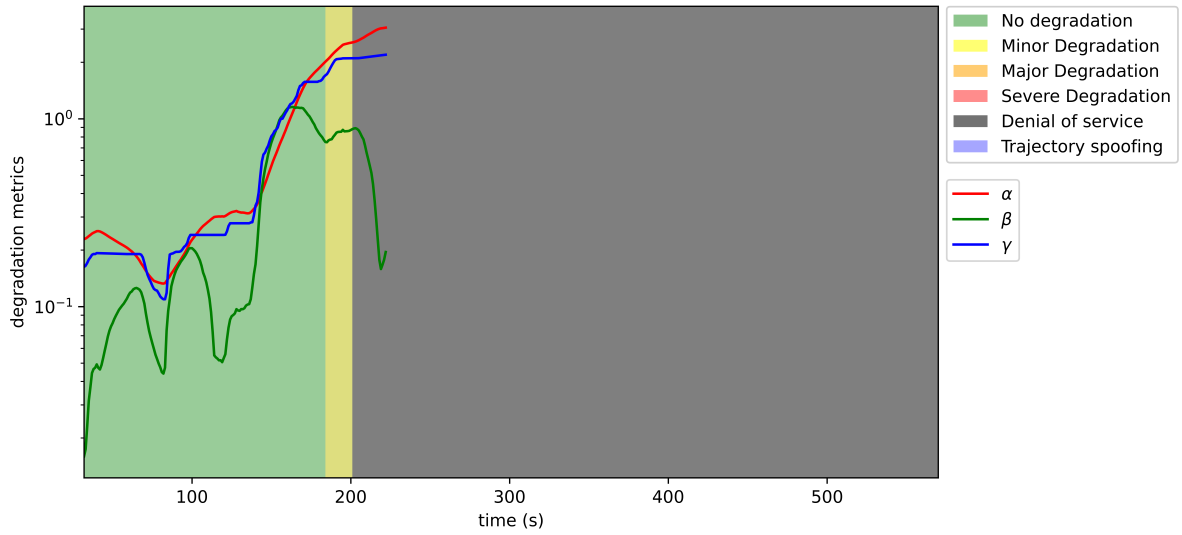

Figure 4: Impact classification results for dynamic narrow-band jamming attack scenario.

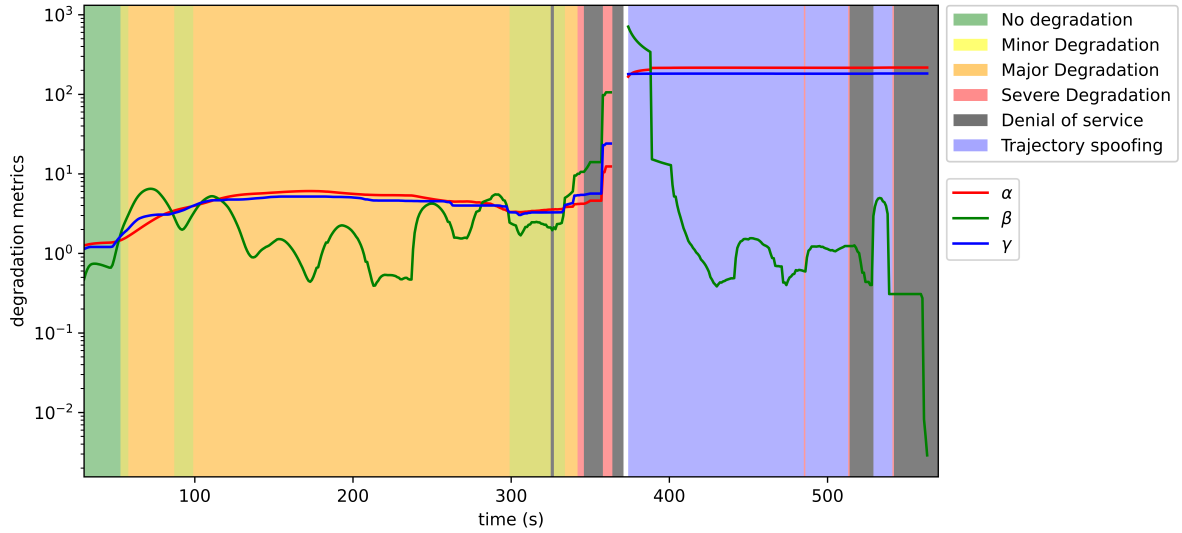

Figure 5: Impact classification results for static spoofing attack scenario.

spoofing scenario are shown in Figure 5, where the power gain of the spoofing signal tested with respect to the legitimate signal increases uniformly from 10 dB to 17 dB in the considered time interval. Fixed position spoofing was successful for spoofing signal gains greater than 14 dB, after 374 seconds since the beginning of the test. The results obtained for the dynamic spoofing attack are shown in Figure 6, for a spoofing signal power uniformly increasing in the considered time interval from 17 dB to 24 dB gain over the authentic signal. The impact of the attack on the receiver was classified as trajectory spoofing at 502 seconds of scenario when the spoofing signal power gain exceeded 23 dB. Therefore, based on the results depicted in Figure 5 and Figure 6 we can conclude that it is easier for attacker to achieve successful trajectory spoofing attack in case of a static spoofing scenario than in a dynamic one. Figure

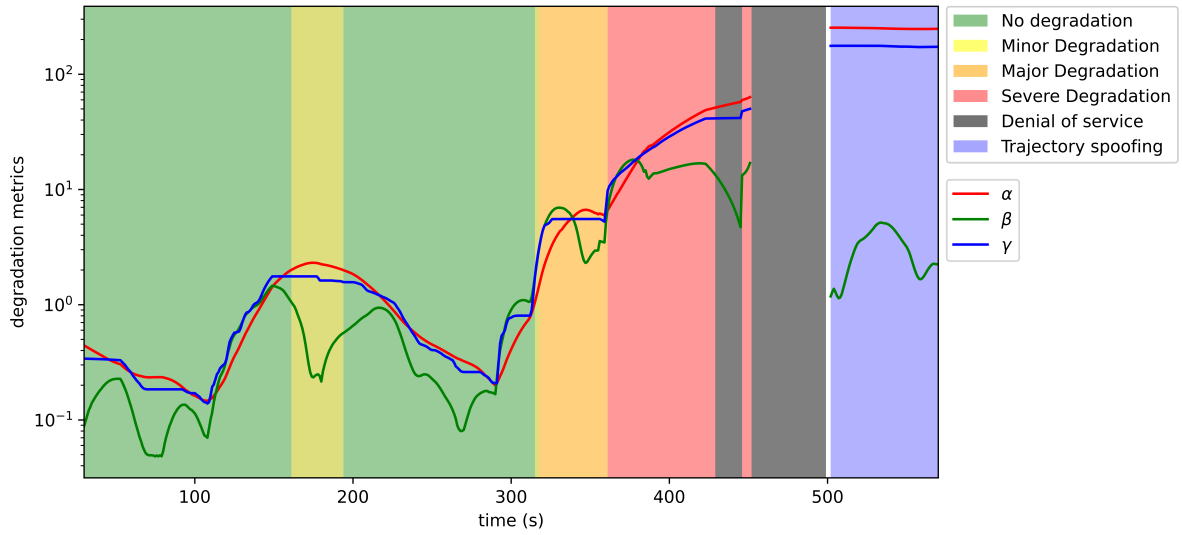

Figure 6: Impact classification results for dynamic spoofing attack scenario.

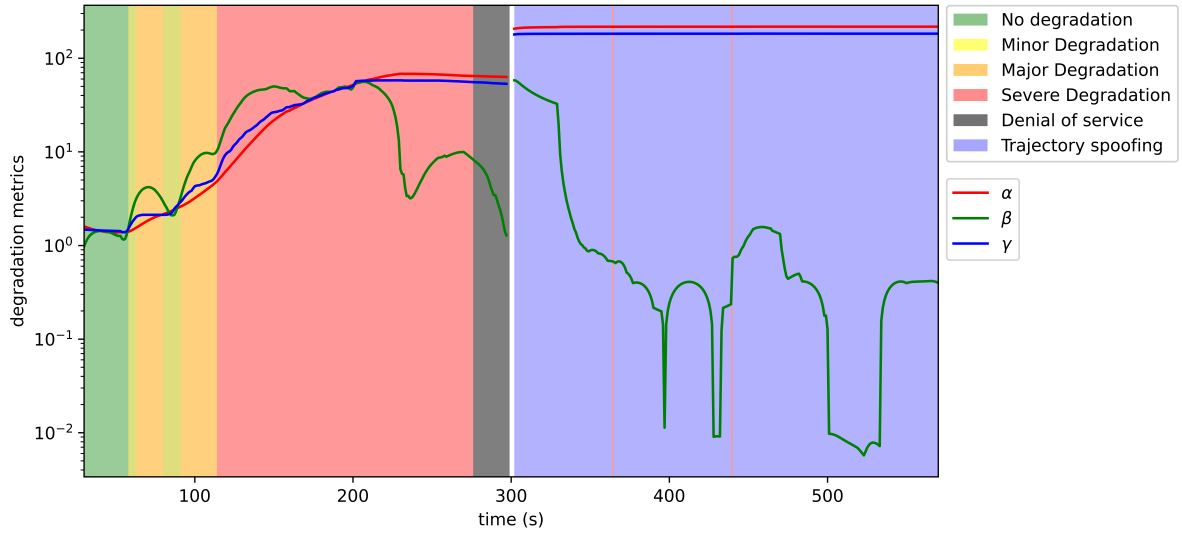

Figure 7: Impact classification results for jamming and spoofing attacks acting cooperatively.

5 and Figure 6 shows also the values of the parameters α, β and γ during the tested scenarios. Moreover, in both figures we can notice a similar behaviour: when the spoofing gain reaches a certain threshold, a DoS status is detected since the receiver stops tracking the legitimate signal. Then, with a further increase of the spoofing power, the receiver locks onto the spoofing signal and falls into the trajectory spoofing status.

4.3. Joint Jamming and Spoofing scenario

We tested the reaction of the receiver to the cooperative action of jamming and fixed position spoofing attacks. We used jamming before the spoofing attack to force the receiver into acqui-

sition mode by inducing loss-of-lock on the legitimate signal, then we turned off the jammer so that the spoofing position could be collected by the receiver and, in case the spoofing attack is successful, recognized as authentic. In Figure 7 we show the impact classification results, for a narrow-band jammer with band of 100 kHz, frequency modulation span equal to 200 kHz and constant jamming signal power equal to −112 dBW. The power gain of the spoofing signal tested with respect to the legitimate signal was uniformly increased from 10 dBW to 17 dBW in the time interval between 300 and 600 seconds. Fixed position spoofing was successful for power gain of 10 dBW. We note that, the cooperative action of jamming and spoofing allows the spoofing attack to be successful with a lower power gain than the one detected when only fixed position spoofing is applied. In fact, as described in Section 4.2, spoofing alone is successful for attack signal power gain with respect to the legitimate signal greater than 14 dB, whereas when the jammer acts before the spoofer, the latter is successful for power gain greater than 10 dB relative to the legitimate signal.

5. Conclusion

In this paper we have built a thorough effectiveness evaluation mechanism and also set up an analysis platform to evaluate and classify attack impacts on GNSS receivers; in the future, it could become a useful tool for assessing the effectiveness of existing defense methods as well as for developing and testing new defense mechanisms. To validate the proposed procedure, we carried out tests on mass market GNSS receivers. In detail, we considered several nominal and under-attack scenarios where the attacker was able to use jamming, spoofing or both: we observed that, by using joint jamming and spoofing it was possible for the attacker to achieve the same impact with a lower power consumption, i.e., when a jamming attack acts before the spoofing, the power required to succeed is lower than the signal power required when the spoofer acts alone. We observed that, for the reference scenarios, by using the proposed model we were able to correctly classify the attacks, successfully distinguishing a legitimate from an under-attack scenario. The proposed method provides a blueprint for impact classification which differs from detection methods present in the literature since it will allow to test receiver performance under attack conditions specifically during the development phase.

The tools developed and the results obtained in this paper are part of the PNT-CRC project, whose purpose is the development of a centre capable of storing, discovering, and distributing security threats, vulnerabilities, and mitigations associated to position navigation and timing (PNT) services, with particular emphasis to the GNSS technology. The PNT-CRC will include both technology and application specific threats, as well as real time location-based threats observed in the territory for context awareness and emergency warning. The PNT-CRC will provide to industries a GNSS vulnerability assessments service as well as mitigation solutions to enhance robustness of GNSS receivers.

Acknowledgments

This work was funded by the European Space Agency under contract n. 4000123484/18/NL/MP: “Position, Navigation and Timing Cyber-Response Center (PNT-CRC)”.

References

[1] Z. Wu, Y. Zhang, Y. Yang, C. Liang, R. Liu, Spoofing and anti-spoofing technologies of global navigation satellite system a survey, IEEE Access 8 (2020) 165444–165496. doi:10.1109ACCESS.2020.3022294.

[2] D. Borio, F. Dovis, H. Kuusniemi, L. Lo Presti, Impact and detection of GNSS jammers on consumer grade satellite navigation receivers, Proceedings of the IEEE 104 (2016) 1233–1245. doi:10.1109JPROC.2016.2543266.

[3] R. H. Mitch, R. C. Dougherty, S. P. Psiaki, Mark L.and Powell, B. W. O'Hanlon, J. A. Bhatti, T. E. Humphreys, Signal characteristics of civil GPS jammers, in: Proceedings of the 24th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2011), Portland, OR, 2011, pp. 1907–1919.

[4] T. Morong, P. Puricer, P. Kovář, Study of the GNSS jamming in real environment, International Journal of Electronics and Telecommunications 65 (2019) 65–70. doi:10.24425ijet.2019.126284.

[5] I. F. Hernández, T. Ashur, V. Rijmen, C. Sarto, S. Cancela, D. Calle, Toward an operational navigation message authentication service proposal and justification of additional OSNMA protocol features, in: European Navigation Conference (ENC), 2019, pp. 1–6. doi:10.1109EURONAV.2019.8714151.

[6] J. Hinks, J. Gillis, P. Loveridge, S. Shawn, G. Myer, J. Rushanan, S. Stoyanov, Signal and data authentication experiments on NTS-3, in: Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021), 2021, pp. 3621–3641. doi:10.330122021.17964.

[7] X. Ouyang, F. Zeng, P. Hou, R. Guo, Analysis and evaluation of spoofing effect on GNSS receiver, in: 2015 IEEE 12th Intl Conf on Ubiquitous Intelligence and Computing and 2015 IEEE 12th Intl Conf on Autonomic and Trusted Computing and 2015 IEEE 15th Intl Conf on Scalable Computing and Communications and Its Associated Workshops (UIC-ATC-ScalCom), 2015, pp. 1388–1392. doi:10.1109UIC-ATC-ScalCom-CBDCom-IoP.2015.250.

[8] L. Perdue, H. Sasaki, G. Boime, E. Sicsik-Paré, Testing GNSS receivers robustness against spoofing attempts, in: etc2016 - 36. European Telemetry and Test Conference, Nürnberg, Germany, 2016, pp. 33 – 39.

[9] A. Rustamov, N. Gogoi, A. Minetto, F. Dovis, Assessment of the vulnerability to spoofing attacks of GNSS receivers integrated in consumer devices, in: 2020 International Conference on Localization and GNSS (ICL-GNSS), 2020, pp. 1–6. doi:10.1109ICL-GNSS49876.2020.9115489.

[10] S. Ceccato, F. Formaggio, G. Caparra, N. Laurenti, S. Tomasin, Exploiting side-information for resilient GNSS positioning in mobile phones, in: 2018 IEEEION Position, Location and Navigation Symposium (PLANS), 2018, pp. 1515–1524. doi:10.1109PLANS.2018.8373546.

[11] N. Spens, D.-K. Lee, D. Akos, An application for detecting GNSS jamming and spoofing, in: Proceedings of the 34th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2021), St. Louis, Missouri, 2021, pp. 1981–1988. doi:10.330122021.18027.

[12] G. Mori Gonzalez, I. Petrunin, R. Zbikowski, K. Voutsis, R. Verdeguer Moreno, Vulnerability analysis of GPS receiver software, in: 2019 International Conference on Localization and GNSS (ICL-GNSS), 2019, pp. 1–6. doi:10.1109ICL-GNSS.2019.8752862.

[13] Satellite Earth Stations and Systems (SES); GNSS based location systems; Part 3 Perfor-

mance requirements, ETSI TS 103 246-3 V1.3.1 (2020-10), 2020.
[14] QA707: GNSS simulator supporting interference and authentication, https://www.qascom.it/GNSS-software-simulation.php, [Online; accessed 03-February-2022].
[15] Septentrio PolaRx5 GNSS receiver, https://www.septentrio.com/en/products/gnss-receivers/reference-receivers/polarx-5, [Online; accessed 03-February-2022].
[16] NMEA 0183 Standard, https://www.nmea.org/content/STANDARDS/NMEA_0183_Standard, [Online; accessed 03-February-2022].
[17] C. Hegarty, E. Kaplan, Understanding GPS Principles and Applications, Second Edition, Artech, 2005.