An Experimental Evaluation of the GNSS Jamming Threat

Daniele Borio[1], **Ciro Gioia**[2], **Franc Dimc**[3], **Matej Bažec**[3], **Joaquim Fortuny**[1],
Gianmarco Baldini[1] **and Marco Basso**[1]

1) European Commission, Joint Research Centre (JRC),
2)Piksel S.p.A.
3) University of Ljubljana, Faculty of Maritime Studies and Transport, Portorož
1) name.surname@jrc.ec.europa.eu, 2) ciro.gioia@ext.jrc.ec.europa.eu, 3) name.surname@fpp.uni-lj.si

Abstract

Jamming is the act of intentionally directing a disturbing electromagnetic wave towards a communication system in order to disrupt or prevent signal reception. Jamming is becoming a serious threat for several services including Global Navigation Satellite System (GNSS) where it is used to prevent the computation of the user position.

This paper describes the joint efforts of the European Commission (EC) Joint Research Centre (JRC) and of the Faculty of Maritime Studies and Transport of the University of Ljubljana to experimentally evaluate the GNSS jamming threat. In particular several experiments have been conducted in order to build a library of scenarios for the evaluation of jamming detection and mitigation techniques. Data containing jamming signals have been collected in the JRC anechoic chamber and different approaches have been compared for the detection of jamming signals. The analysis shows a good coherence among the different detection metrics considered.

1 Introduction

Good performance and ease of operations make Global Navigation Satellite System (GNSS)-based navigation widely used in several applications and in different fields such as avionic, Location Based Service (LBS) and road transportation. Several infrastructures rely on GNSS-based positioning, hence GNSS should provide reliable and continuous services.

GNSS receivers are able to compute their Position Velocity and Time (PVT) solution using the trilateration technique and exploiting the signals transmitted by different satellites. The distance between receiver and satellite antennas is usually in the order of 20000 km, hence the received signals are very weak and they are vulnerable to different sources of interference. Such interference can be natural, such as that due to atmospheric effects, or malicious such as spoofing and jamming attacks [1]. GNSS threats, such as spoofing and jamming, are attracting increasing interest among the navigation community and several studies have been carried out in order to detect and mitigate GNSS threats. In particular, considerable efforts from the research community have been invested to investigate the impact of jammers [2]. From the studies conducted, it emerges that GNSS jammers can interfere with GNSS signals over wide geographical areas. GNSS jammers can significantly effect on GPS and Galileo receivers which can be however protected using several countermeasures such as adaptive notch filters [3].

In this paper, the joint efforts of the European Commission (EC) Joint Research Centre (JRC) and of Faculty of Maritime Studies and Transport of the University of Ljubljana are described. The experiments conducted have the goal to experimentally evaluate the GNSS jamming threat. In particular, several tests have been conducted in order to build a library of scenarios for the evaluation of jamming detection and mitigation techniques. Data containing jamming signals have been collected in the JRC anechoic chamber. The tests have been carried out in different scenarios including static and kinematic jammer with and without attenuation. Moreover, different approaches have been compared for the detection of jamming signals. The analysis shows the advantages and drawbacks of the different techniques considered. A second series of tests have been conducted in the Slovenian countryside including vehicular tests. The analysis of the data collected will be presented in a separate publication.

The remainder of the paper is organized as follows: in Section 2 the measurement unit adopted for the data collection is described. In Section 3 the experimental setup is shown, then the experimental results are analyzed in Section 4. Finally Section 5 concludes the paper.

2 Data Collection System

The measurement unit adopted for the reception of GNSS and jamming signals was made of a Realtek RTL2832U front-end and a ublox LEA-6T receiver connected to the same GPS patch antenna. A schematic representation of the measurement unit used for data collections is shown in Fig. 1. The Realtek RTL2832U device was configured to operate according to the settings reported in Table 1 and it was adopted to collect raw In-phase/Quadraphase (I/Q) GPS and jamming signals. A custom software, the JRC Interference Monitor (JIM), was developed and interfaced to the Realtek RTL2832U device to collect I/Q samples and monitor the histogram and Power Spectral Density (PSD) of the data. The ublox LEA-6T receiver was adopted to collect raw GPS measurements such as pseudoranges, Doppler shifts, carrier phases and Carrier-to-Noise power spectral density ratio (C/N_0) val-

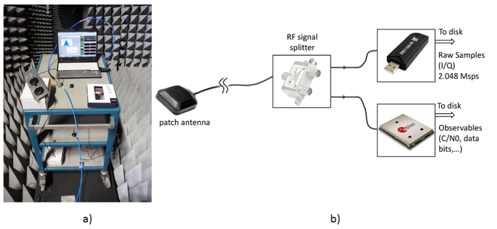
patch antenna
RF signal splitter
To disk
Raw Samples (I/Q) 2.048 Msps
To disk
Observables (C/N0, data bits,...)
a)
b)

Figure 1: Measurement unit used for the data collection. a) Photo of the instrumented cart used in the anechoic chamber. b) Schematic representation of the data collection unit.

Table 1: Settings adopted for the Realtek RTL2832U device used as a GNSS data grabber.

Parameter	Value
Sampling frequency	$f_s = 2.048$ MHz
Centre frequency	1575.42 MHz
Sampling Type	Complex I/Q
No. of bits	8

ues. Moreover, the ublox receiver provides several metrics related to the receiver status such as the Automatic Gain Control (AGC) count. These metrics can be used for jamming detection. The Realtek RTL2832U device and ublox LEA-6T receiver were directly powered through the USB ports of the laptop and no additional power supply was required. Fig. 1 shows a view of the instrumented cart equipped with the Realtek RTL2832U device and the ublox LEA-6T receiver.

3 Experimental Setup

Several experiments were conducted in order to build a library of scenarios for jamming detection. The first set of experiments was conducted inside the anechoic chamber of the JRC. The anechoic chamber is equipped with a Spirent 9000 GNSS simulator. Moreover, it is possible to rebroadcast inside the chamber live GNSS signals collected by a wideband antenna mounted on roof of the building hosting the chamber.

A schematic representation of the experimental setup prepared inside the JRC anechoic chamber is provided in Fig. 2. The floor and the walls of the chamber are covered by Radio Frequency (RF) absorbers which confine electromagnetic signals inside the chamber. For the experiments, a pedestrian path was prepared by removing some absorbing units from the floor and data recording/detection units were installed in the bottom left corner of the chamber as highlighted in Fig. 2. By walking along the pedestrian path, a user carrying a jammer was able to simulate different distances between the detection units and the jamming device. It is noted that the diameter of the chamber is 20 meters and thus its was possible to introduce significant changes in the distance between the jammer and the detection units. Moreover, the chamber is equipped with a central cylinder which is generally used to hold cars and other devices to be characterized from an electromagnetic standpoint. For the experiments, it was decided to leave the central cylinder in order to introduce obstacles between the recording/detection units and the jammer. In this way, different reception conditions were simulated. Finally, power attenuators were used to reduce the power transmitted by the jammer.

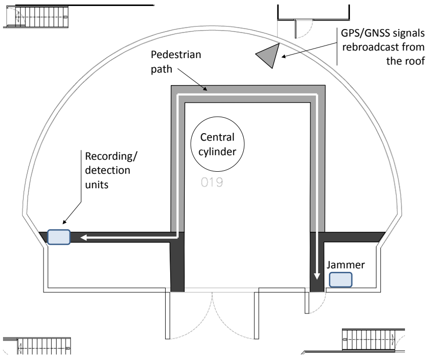
GPS/GNSS signals rebroadcast from the roof
Pedestrian path
Central cylinder
019
Recording/ detection units
Jammer

Figure 2: Schematic representation of the experimental setup prepared inside the JRC anechoic chamber. Different tests were conducted with the jammer static in the right bottom corner of the chamber or carried by a pedestrian user moving along the pedestrian path.

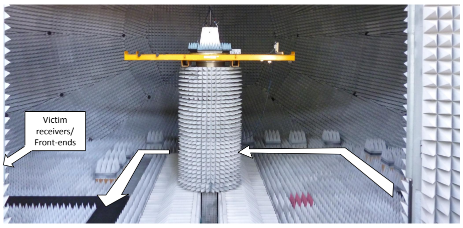

Figure 3: View of the experimental setup used for the anechoic chamber tests.

In addition to the experiments involving a pedestrian user, a second set of tests were performed with a static jammer. The jammer was left in the bottom right corner of the chamber. A programmable attenuator was used to vary the power transmitted by the jammer. In this case, the distance between the recording/detection units and the jammer was 11.78 metres. A view of the experimental setup used for the anechoic chamber tests is provided in Fig. 3.

4 Experimental Analysis

In this section, the results obtained using different measurement units adopted for the reception of GNSS and jamming signals, specifically the Realtek RTL2832U front-end and the ublox LEA-6T GPS receiver, are analysed. The devices provide different types of measurements which can be used to demonstrate different techniques for jamming detection.

As a first step, the data collected using the Realtek RTL2832U front-end are analysed. The metrics computed using the I/Q data from the front-end can be divided in direct and derived metrics. Examples of direct metrics are the time-varying histogram and the time-varying PSD. Metrics derived from the histogram are the mean, variance and kur-

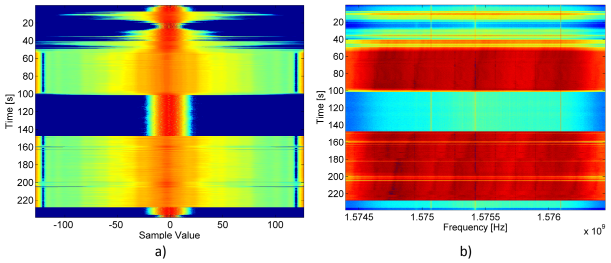

Figure 4: a) Time evolution of the histograms of the samples collected using the RTL2832U receiver. b) Time evolution of the PSDs of the samples collected using the RTL2832U receiver. Battery-powered jammer test.

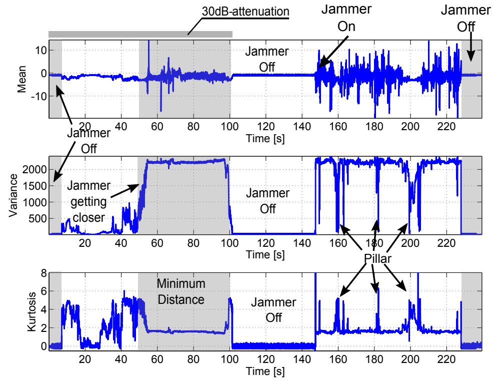

Figure 5: The derived metrics are plotted as a function of the time. Specifically the mean (in the upper box) the variance (in the central box) and Kurtosis (in the lower box) are represented as a function of time.

tosis whereas metrics derived from the PSD are the total power and the PSD entropy.

Although several tests were conducted, a single experiment is presented here due to space limitations. The total duration of the test was of almost 4 minutes. In the first part of the test the jammer position was fixed and the jamming power was attenuated using a 30 dB attenuator. The user then started to move along the path described in Fig. 3. The first part of the test was concluded by turning off the jammer and removing the attenuator. The second part of the test was performed similarly to the first one but without attenuating the jammer power. In Fig. 4 a), the time evolution of the histogram of the samples collected is shown. During the initial phase of the test (5 sec), when the jammer was off, the samples follow a Gaussian distribution. When the jammer was turned on and the user started to walk along the path described in Fig. 3, the distribution of the samples started to change; in particular when the user reached the minimum distance from the receiving equipment, the maximum deviation from the Gaussian distribution appeared in the histogram. Specifically, a saturation of the device can be noted: this appears as the concentration of the samples in the tails of the histograms. When the jammer was turned off, the sample distribution came back to Gaussian. In the second phase (i.e., without attenuation) of the test the impact of the jammer clearly emerges, and is even more evident than in the previous case. This is due to the higher power transmitted by the jammer. In Fig. 4 b), the time evolution of the PSDs of the samples collected using the RTL2832U receiver is shown. The analysis of the PSD evolution provides similar findings to that obtained from the histogram analysis. At the beginning of the test, almost no power can be detected at the different frequencies. When the jammer was turned on and the user stared to move, the presence of the jammer can be clearly identified, in both phases of the test (i.e., without and with attenuation).

In Fig. 5, the derived metrics are plotted as a function of time. Specifically, the mean (in the upper box), the variance (in the central box) and excess kurtosis (in the lower box) are represented. From the analysis of the mean, it can be noted that when the jammer was activated a high frequency noise is present, this phenomena is more evident when the user is closer to the receiving device and when the attenuator is removed as highlighted in the grey boxes. From the central box, it can be noted that the variance of the samples increases when the jammer was activated, in particular a ramp can be appreciated when the user was moving towards the receiver device. In the second part of the test, such behaviour is not detected because of the removal of the attenuator and of the limited walking distance available in the anechoic chamber. However it is possible to identify the passages of the user behind the central pillar which strongly attenuates the jammer power. Also from the lower box of Fig. 5, where the kurtosis is plotted as a function of the time, it is possible to identify the presence of jamming effects. When the jammer is turned on, the parameter is higher than in the other case. Also in this case it is possible to identify the shielding effect of the central pillar.

In Fig. 6 the received power (upper box) and entropy (lower box) are plotted as a function of time. From the upper box, the presence of the jammer and the user moving can be clearly identified; the power grew when the jammer was turned on and a ramp can be identified due to the approaching of the jammer to the receiver. Also in this case the presence of the central cylinder can be noted. From the lower box, the activation of the jammer is clearly indicated by the entropy behaviour. Also in this case the results are consistent with that obtained from the other metrics used for the jamming detection.

The ublox receiver does not provide I/Q samples and alternative metrics have been used for jamming detection. Specifically, the authors used the C/N_0 measurements provided by the device. The C/N_0 of the signals received by the ublox receiver are plotted as a function of time in Fig. 7. From the figure, the impact of the jammer on the C/N_0 measurements clearly emerges; in the first part of the test (with the 30 dB attenuation), a slight reduction of the C/N_0 values can be noted when the jammer was turned on. When the user started moving towards the receiver all the C/N_0 values were reduced reaching the minimum value when the user, with the jammer, approached the receiver. In the second phase of the test (without attenuation) the jammer effect is more evident. In this case, it is not possible to identify the ap-

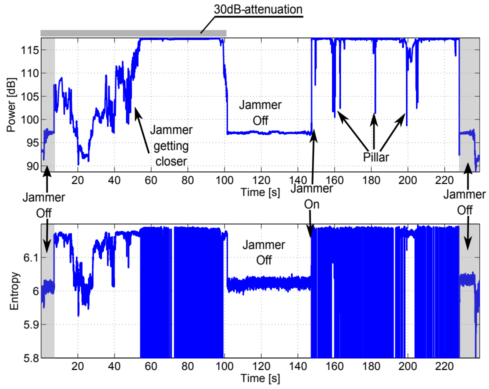

Figure 6: Received power (upper box) and entropy (lower box) computed using the PSD of the samples collected using the RTL2832U receiver, as a function of time.

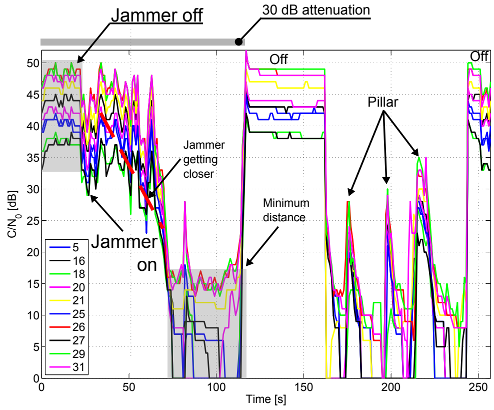

Figure 7: C/N_0 of the signals received by the ublox receiver as a function of time.

proaching movement of the jammer to the receiver, because the C/N_0 values fell down drastically but it is possible to identify the shielding effect of the pillar. As in the previous case, two derived metrics, exploiting the C/N_0 measurements, have been analysed. In Fig. 8, the Sum of Square (SoS) detector (upper box) [4] and the average C/N_0 have been plotted as a function of time. Although no information related to the movement of the jammer can be obtained, the SoS decision metric was able to identify the activation and de-activation of the jammer, exploiting the correlation on the C/N_0s introduced by the jammer; also the presence of the pillar can be noted. From the lower box, it clearly emerges that when the jammer was activated, the average C/N_0 decreases and the approaching movement of the user can be identified. In the second part of the test, the impact of the jammer is more evident and the presence of the central cylinder can be identified. The cylinder limits the jammer power and the observations on the C/N_0 are coherent with the results of the other metrics.

5 Conclusion

In order to evaluate the jammer impact, several experiments have been conducted using a Realtek RTL2832U front-end and a ublox LEA-6T receiver connected to the same GPS patch antenna and different types of jammers. Several tests have been carried out in order to build a library of scenarios for the evaluation of jamming detection and mitigation techniques. The test were performed in the JRC anechoic chamber, using different types of jammers in different configurations including static and kinematic jamming attacks. In addition, different approaches for jamming detection have been implemented exploiting the measurements provided by the two above mentioned receivers. The performance of the algorithms has been compared and the analysis shows that a user equipped with one of the device can clearly identify a jamming attack. The use of different metrics allows one to obtain different types of information such as the approaching of a kinematic jammer or the presence of obstacles in the jamming path which can mitigate the jamming effects. The results show that even a mass-market receiver can detect a jamming attack exploiting the SoS decision or the average C/N_0.

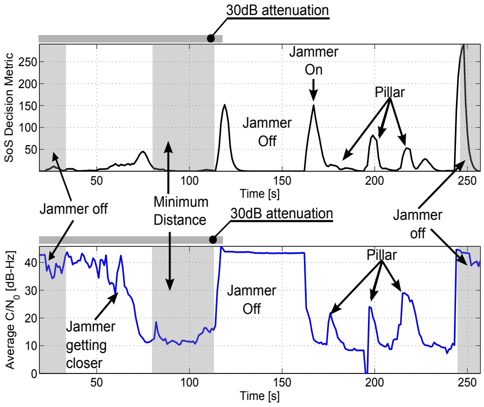

Figure 8: SoS decision metric (upper box) and average C/N_0 as a function of time.

References

[1] T. Economist, "GPS jamming: No jamming tomorrow," *Technology Quartely*, Mar. 2011.

[2] R. H. Mitch, R. C. Dougherty, M. L. Psiaki, S. P. Powell, B. W. O'Hanlon, J. A. Bhatti, and T. E. Humphreys, "Signal characteristics of civil GPS jammers," in *ION GNSS 2011*, 2011.

[3] D. Borio, C. O'Driscoll, and J. Fortuny, "GNSS jammers: Effects and countermeasures," in *Proc. of the 6th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, Dec. 2012, pp. 1–7.

[4] D. Borio and C. Gioia, "Real-time jamming detection using the sum-of-squares paradigm," in *Proc. of International Conference on Localization and GNSS (ICL-GNSS)*, Gothenburg, Sweden, Jun. 2015, pp. 1–6.