TRANSACTIONS ON ELECTROMAGNETIC SPECTRUM

# Characterization and Early Awareness of Interference in GNSS L1/E1 Band using an Outlier Detection Algorithm

**Hamid Kavousi Ghafi [1*], Roman Lesjak[1], Günther Obertaxer [1], Michael Schönhuber [1]**
**Alexander Falk [1], Holger Arthaber [2]**

[1]Institute for Information and Communication Technologies, Joanneum Research, Graz, Austria
[2]Institute of Electrodynamics, Microwave and Circuit Engineering, TU Wien, Vienna, Austria

*** Corresponding author's e-mail address:** hamid.kavousighafi@joanneum.at

**Received:** 1 November 2022
**Revised:** 19 November 2022
**Accepted:** 7 December 2022

**Research Article**
**Vol.2 / No.1 / 2023**
**Doi:** 10.5281/zenodo.7700070

**Abstract:** One of the emerging challenges in the Global Navigation Satellite System (GNSS) is the vulnerability to radio frequency interference (RFI). The first step to deal with this problem is to identify and characterize the interference signals. In this work, we propose a combination of an outlier detection method and a time duration threshold checking to effectively detect and characterize RFIs in the GNSS L1/E1 band. The method is applied to the data recorded from a measurement campaign near the A9 highway in the southern part of Graz, Austria. During 6 hours of recording, three moving interference sources are identified and their average speeds, directions, and time-frequency characteristics are reported.

**Keywords:** GNSS, Interference, Outlier detection.

**Cite this paper as:** Ghafi H.K., Lesjak R., Obertaxer R., Schönhuber M., Falk A., ArthaberH. Characterization and Early Awareness of Interference in GNSS L1/E1 Band using an Outlier Detection Algorithm. Transactions On Electromagnetic Spectrum. 2023; 2(1): 19-24, Doi: 10.5281/zenodo.7700070

## 1. INTRODUCTION

Over the past decades, GNSS has become a vital part of many applications. The increase of dependency to this technology has raised concerns about its reliability. The weak signals reaching the GNSS receivers make the system vulnerable to RFI. The RFI can cause by intentional and unintentional sources. Consequently, the detection and characterization of RFI in GNSS systems is a crucial task to extend the application of GNSS.

The detection and localization of different types of interference are addressed in the literature. In [1, 2], the changes in Automatic gain control (AGC) values are used to detect interference. In a wide range of research activities, a combination of metrics such as carrier to noise ratio (C/N0), AGC, spectrum data, and receiver quality of service are used to ensure that an event is an RFI [3, 4, 5]. These approaches require a large computational and processing capacity.

In this work, a two-level algorithm is used to detect and characterize interference using spectrum data. The first level is an outlier detection algorithm. The second is a verification check that defines if the detected outlier has a minimum time duration so that it can be considered as an RFI. As an RFI is identified, its time-frequency characteristics are derived. The spectrum data is recorded in the field using a measurement setup.

The rest of this paper is organized as follows. In section 2, the measurement setup to record spectrum data in the field is presented. Section 3 describes the algorithm that is used to detect and characterize RFIs. The detected RFIs throughout the measurement campaign data is provided in section 4. Finally, section 5 gives the conclusion.

## 2. MEASUREMENT SETUP

The block diagram of the measurement setup is illustrated in Figure 1.

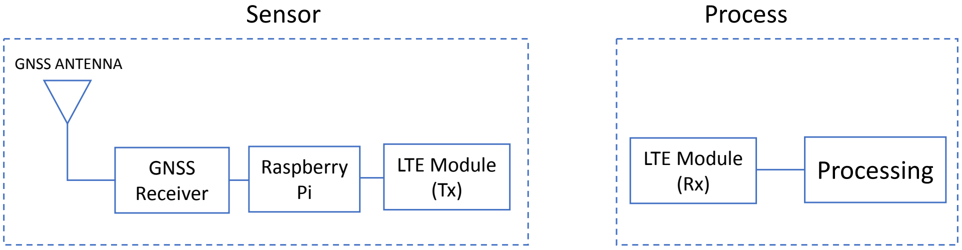

**Figure 1.** Structure of setup to record GNSS L1/E1 band data.

An active GNSS antenna captures signals in GNSS L1/E1 band and sends them to the receiver. The International Telegraph Unit (ITU) defines the GNSS L1/E1 band as the frequency range from 1599 MHz to 1591 MHz centered at 1575.42 MHz [6]. The receiver, u-blox ZED-F9P, processes the GNSS signals and outputs UBX format messages including Position, Velocity, and Time (PVT), AGC values, spectrum data, and etc. This is done using a Raspberry Pi as a host computer. The messages are sent to a central unit in the lab for processing steps, using LTE modules with an internet connection. As shown in Figure 1, the GNSS antenna, the GNSS receiver, a Raspberry Pi 4, and the LTE module compose the sensor block. In this work, two sensors are installed close to the A9 highway in the southern part of Graz, Austria, as shown in Figure 2. The distance between the two sensors is about 4 km.

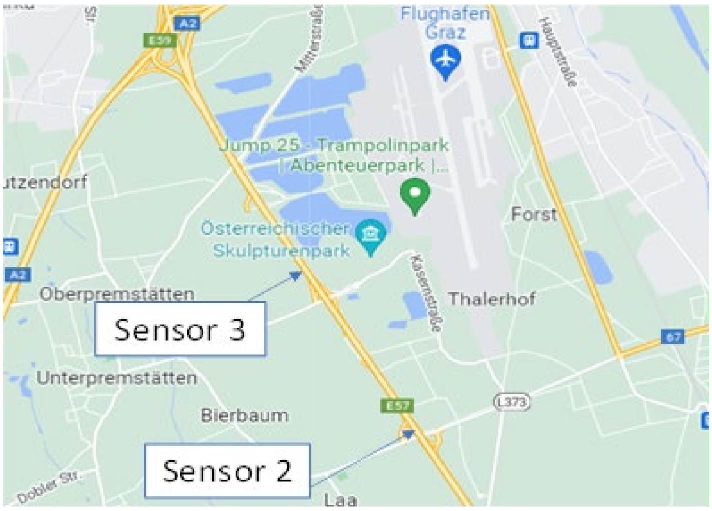

**Figure 2.** Approximate location of sensors.

## 3. DETECTION ALGORITHM

In the process section, the transmitted messages are received and processed. In the first step, the messages are parsed to extract the spectrum data from the binary messages. The receiver provides spectrum data with a span of 128 MHz. However, we only analyze 32 MHz of that, covering L1/G1 band. Then, the detection algorithm is applied to find RFI events in the spectrum data. In this step, a certain number of first received traces are used as the training data set. The detection algorithm is comprised of an outlier detection method and a verification step. Finally, we compare detected RFIs to find out if there are events that appear in both sensors. In these cases, an approximate speed of the source is provided. All processing steps are implemented in the Python programming language. Within the next sections, the approach is explained in more detail**.**

### 3.1. Outlier Detection Algorithm

Outlier detection is an algorithm of defining anomalies in a data set. Outlier detection finds a region (a shape) where the training data is highly concentrated [8]. Inliers exist inside this region while the outliers lie outside of the region.

In this work, we use the "covariance.EllipticEnvelope" object from the "scikit-learn" library. The elliptical envelope method finds an imaginary N-dimensional ellipsoid around the training dataset, where N is the number of frequency bins. In other words, each frequency bin of spectrum data is considered a characteristic feature of the input. In our analysis, N is 64 as the receiver captures the spectrum with a bin width of 0.5 MHz. Figure 3 presents the conceptual presentation of the two-dimensional elliptical envelope algorithm.

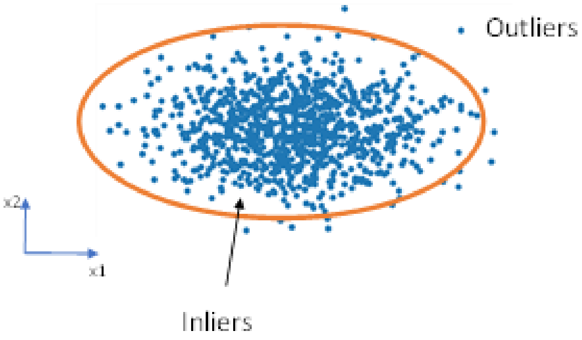

**Figure 3.** Conceptual presentation of the elliptical envelope algorithm.

The object has an argument called contamination, indicating the proportion of outliers in the training dataset. As the object is trained and the ellipsoid is derived, the next spectrum trace is categorized as an outlier if it lies outside the ellipsoid. Otherwise, it is considered normal data. An outlier is categorized as a potential RFI candidate which will be verified in the next step.

### 3.2. Verification Algorithm

The detected outliers in the previous block are the input of this section. To consider an outlier as interference, it should last for a predefined time period, further called duration threshold. The time duration of an event can be estimated as the difference between the timestamp of the trace that the given event was detected for the last time and the timestamp of the trace that the given event was detected for the first time. To find an event through several successive traces, their center frequencies and bandwidths (50% occupied bandwidth) are compared. If center frequencies of events in successive traces have less than 1 MHz offset and also their bandwidths have less than 1 MHz difference, we assume that the anomalies in these traces originate from one event [9]. To show the severity of detected RFIs, a power indicator (PI) is used. That is the difference between the peak value of a given event and the mean value of the corresponding bin in the training data.

## 4. RESULTS

The approach introduced in section 3 was applied to the recorded data by sensors 1 and 2. The number of training datasets was set to 2000. The contamination factor of the outlier detection algorithm was set to 0.005. The duration threshold was set to four seconds. The sensors recorded data on 28.04.2022 from about 7:00 AM to 1 PM UTC.

Before analyzing the results, we show that the verification step prevents from false detection of random events. Considering the contamination factor of 0.005 and 6 hours of recorded data, an average of 108 outliers is expected for each sensor. Assuming uniform occurrence over timestamps, the probability of an outcome with 4 successive outliers is 1.18e-7 ($1\times 107/21600\times 106/21600\times 105/21600$). Taking the center frequency and bandwidth distributions into account, this possibility will become even smaller. This indicates that the probability of false detection is negligible. The outlier detection algorithm identifies 126 anomalies in sensor 1, and 64 anomalies in sensor 2. The detected events after applying the verification process are shown in Table 1.

**Table 1.** Detected events in two sensors.

| Sensor | Timestamp (UTC) | Center Frequency (MHz) | Bandwidth (MHz) | Time Duration (s) | PI (dB) |
|---|---|---|---|---|---|
| Sensor 1 | 08:43:29 | 1576.46 | 1.5 | 6 | 20.41 |
| | 10:24:57 | 1566.46 | 0.5 | 6 | 21.31 |
| | 11:20:28 | 1582.96 | 4.5 | 6 | 23.17 |
| | 11:41:54 | 1569.46 | 0.5 | 4 | 17.22 |
| | 11:52:32 | 1588.46 | 2.5 | 11 | 23.01 |
| Sensor 2 | 08:35:43 | 1564.96 | 0.5 | 4 | 16.25 |
| | 08:45:39 | 1575.96 | 0.5 | 4 | 16.20 |
| | 10:22:44 | 1566.96 | 1.5 | 11 | 16.07 |
| | 11:20:10 | 1568.46 | 1.5 | 5 | 19.28 |
| | 11:49:34 | 1588.46 | 3.5 | 23 | 19.63 |

Comparing the characteristics of the detected events that appeared in the two sensors gives the idea that there are some events generated from a common source (moving cars). To consider that, three conditions should be fulfilled.

- The timestamps at two sensors are close enough. Assuming a minimum speed of 50 km/h, the delay between two timestamps should be less than 5 minutes. If the RFI source is moving from south to north, it appears in sensor 1 first. Otherwise, it first appears in sensor 2.
- The center frequencies have less than a 1 MHz shift.
- The bandwidths of the events have less than a 1 MHz difference.

Applying these constraints, the interference sources are identified. The interference characteristics are provided in Table 2.

**Table 2.** Events generated from common sources.

| RFI | Timestamp (UTC) | Average Speed and Direction of Source |
|---|---|---|
| 1 | 08:43:29 in sensor 1<br>08:45:39 in sensor 2 | 110.77 (km/h)<br>from south to north |
| 2 | 10:24:57 in sensor 1<br>10:22:44 in sensor 2 | 108.27 (km/h)<br>from north to south |
| 3 | 11:52:32 in sensor 1<br>11:49:34 in sensor 2 | 80.1 km/h<br>from north to south |

The narrow bandwidth feature of the detected RFIs shows that the major source of interference in our measurement campaign is the harmonic emissions of other radios operating at frequencies close to the GNSS L1/E1 band [10]. As the center frequencies of RFI 2 and 3 are far from the center frequency of the GNSS L1/E1 band, they have a low impact on the receivers operating in this band. However, RFI 1 is centered near the carrier frequency of the GNSS L1/E1 band. Figure 4 shows the spectrum of the RFI 1 in sensor 1 and 2.

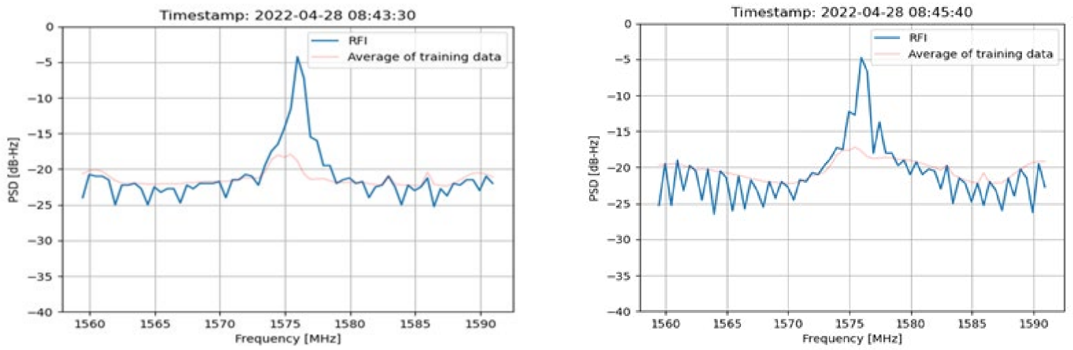

**Figure 4.** A snapshot of the RFI 1 spectrum in sensor 1 (Left) and sensor 2 (Right)

## 5. CONCLUSION

In this paper, the elliptical envelope method was used to detect outliers in the GNSS L1/E1 band. To reduce the chance of positive false detection, the time duration of detected outliers was verified. Two sensors were installed in southern Austria near A9 highway to find and characterize RFI sources. The results of this paper can be used as an early-stage awareness for high-reliability applications

### Acknowledgment

This work was partially executed within the research project Gireko. Gireko has been funded by the Austrian security research program KIRAS of the Federal Ministry of Agriculture, Regions and Tourism (BMLRT).

### REFERENCES

[1] Bastide F., Akos D., Macabiau C., & Roturier B. Automatic gain control (AGC) as an interference assessment tool. In Proceedings of the 16th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS/GNSS 2003), pp. 2042-2053. 2003.

[2] Isoz O., Akos D., Lindgren T., Sun C. C., and Jan S. S. Assessment of GPS L1/Galileo E1 interference monitoring system for the airport environment. In Proceedings of the 24th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2011), pp. 1920-1930. 2011.

[3] Marcos, E. P., Caizzone, S., Konovaltsev, A., Cuntz, M., Elmarissi, W., Yinusa, K., & Meurer, M., Interference awareness and characterization for GNSS maritime applications. In 2018 IEEE/ION Position, Location and Navigation Symposium (PLANS), pp. 908-919. IEEE, 2018.

[4] Thombre S., Bhuiyan M. Z. H., Eliardsson P., Gabrielsson B., Pattinson M., Dumville, M. & Kuusniemi, H. GNSS threat monitoring and reporting: Past, present, and a proposed future. The Journal of Navigation 71, no. 3 (2018): 513-529.

[5] Ying Y., Whitworth T., & Sheridan K. GNSS interference detection with software defined radio. In 2012 IEEE First AESS European Conference on Satellite Telecommunications (ESTEL), pp. 1-6. IEEE, 2012.

[6] Telecommunicaton Standardizaton Sector of ITU. Considerations on the use of GNSS as a primary time reference in telecommunicatons. ITU, 2020.

[7] Google. (2022), Kalsdorf bei Graz, 2022. [Online]. Available: “https://goo.gl/maps/rNssT7SLoWy8GPM77

[8] Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., ... & Duchesnay, E. Scikit-learn: Machine learning in Python. the Journal of machine Learning research 12 (2011): 2825-2830.

[9] Kavousi Ghafi H., Spindelberger C., & Arthaber H. Modeling of co-channel interference in bluetooth low energy based on measurement data. EURASIP Journal on Wireless Communications and Networking 2021, no. 1, 1-17.

[10] Ferrara, N. G., Bhuiyan, M. Z. H., Söderholm, S., Ruotsalainen, L., & Kuusniemi, H. A new implementation of narrowband interference detection, characterization, and mitigation technique for a software-defined multi-GNSS receiver. GPS Solutions 22, no. 4 (2018): 1-15.