17th International Conference on Space Operations, Dubai, United Arab Emirates, 6 - 10 March 2023.
Please input the preferred copyright option as mentioned in the attached "*SpaceOps-2023 Copyright Policy for Manuscripts and Presentations*"
e.g. "Copyright ©2023 by the Mohammed Bin Rashid Space Centre (MBRSC) on behalf of SpaceOps. All rights reserved."

SpaceOps-2023, ID # 224

Towards a Worldwide Monitoring System Against GNSS Spoofing and Jamming Based on LEO Constellations and ML/AI

Francisco Gallardo[ab]*, Antonio Pérez [a], David Sánchez [b], Nil Angli[c]

[a] DLR GfR, Weßling Bavaria, Germany
[b] UPM Universidad Politécnica de Madrid, Madrid, Spain.
[c] ESA, Didcot Harwell, United Kingdom.
* Corresponding Author: francisco.gallardo@dlr-gfr.com

Abstract

The recent rising international tensions and conflicts have shown once again the relevance of electronic warfare, and how GNSS Jamming and Spoofing represent a severe threat to systems and societies relying on GNSS for their underlying infrastructure and services. This paper presents the system design and application of the CMCU (Central Machine Learning Computation Unit) to Space data and space assets, focusing on LEO constellations. This will enable the creation of a worldwide network for monitoring GNSS Spoofers and Jammers. The present work discusses the preliminary results obtained under the IAP.FS.OT.003 RF ANALYTICS APPLICATIONS contract with ESA, funding a feasibility study in order to understand the system design, ground/space segments integration with the archiving, Data Mining facilities and dissemination platforms.

Keywords: GNSS, Spoofing, Machine Learning, Jamming, satellites, LEO

Acronyms/Abbreviations

GNSS: Global Navigation Satellite System
ML: Machine Learning
IF: Intermediate Frequency
CMCU: Central Machine Learning Computation Unit
TDOA: Time Difference Of Arrival
FDOA: Frequency Difference Of Arrival
RESIST : RF analytical Evaluation of Signal Is Space Threats.
ICD: Interface Control Document

1. Introduction

The recent rising international tensions and conflicts make protecting critical infrastructure essential. A wide range of subsystems belonging to such critical infrastructures rely to some extent on GNSS for their nominal operations, i.e. GNSS is used as a source for calculating positions, velocity and/or time. Several incidents related to GNSS and Spoofing and Jamming have recently raised some public attention. Incidents (intentional or not) like a recent one in Dallas airport [1] or many of the ones recently reported over Ukraine (as reported by EUROCONTROL and EASA [2]), or the so-called "Spoofing crop circles" in Shanghai [3], are examples of the importance of protecting GNSS services.

Thus, there is a clear need for GNSS Jamming and Spoofing protection systems. Due to this need, DLR GfR mbH and the Technical University of Madrid (UPM) developed the CMCU [4][5] algorithm, which is based on Machine Learning (ML), and can detect GNSS Jamming and Spoofing attacks by applying ML techniques on a set of novel features extracted from raw GNSS IF (Intermediate Frequency) signals. This system was designed to protect relatively wide geographical areas, and is based on ground front-ends providing IF signals to the CMCU core unit.

This paper presents the results currently achieved from the ESA-funded project (IAP.FS.OT.003 RF ANALYTICS APPLICATIONS) "RESIST" (RF analytical Evaluation of Signal Is Space Threats). The project is a feasibility study to provide a worldwide GNSS Jamming and Spoofing detection system based on injecting raw IF signals recorded by LEO (Low Earth Orbit) constellations into the CMCU. Two specific use cases are under study: the service provision to maritime users/markets and the service provision to companies that provide added value

Please input the preferred copyright option as mentioned in the attached "*SpaceOps-2023 Copyright Policy for Manuscripts and Presentations*"
e.g. "Copyright ©2023 by the Mohammed Bin Rashid Space Centre (MBRSC) on behalf of SpaceOps. All rights reserved."

services based on GNSS (e.g. GNSS corrections services or the Global Navigation Satellite Systems themselves). Different workshops with key industry players are being held to discuss the use cases and the system requirements.

A system integrating the CMCU is being designed, and a proof of concept is being conducted, implementing a considerable amount of the system baseline requirements.

2. CMCU

The Central ML Computation Unit (CMCU) is the core algorithm of the system. It was originally designed [4] [5] to detect GNSS Jamming and Spoofing attacks in ground signals. In the original system design a network of GNSS ground station receivers provides the core unit with Intermediate Frequency (IF) signals. The CMCU performs a proprietary feature extraction process on such GNSS signals. The features are then fed into different Machine Learning (ML) algorithms, which flag the presence of GNSS Jamming or Spoofing signals.

The legacy CMCU was developed to work with ground reference station signals only. Hence, the protection of a geographical area depended on the deployment of reference stations over the area of interest.

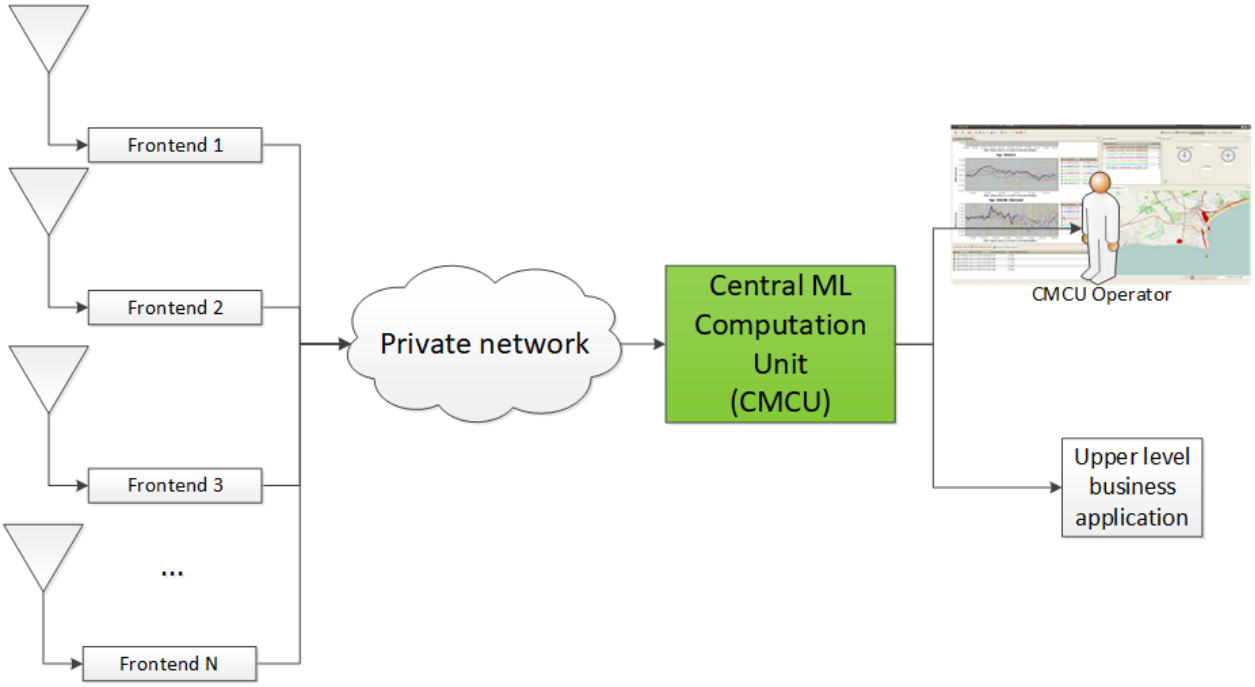

Figure 1 Geographical protection with the original CMCU

As the CMCU relies on ML algorithms, it can be trained to create evolving ML models capable of detecting changing GNSS Jamming and Spoofing scenarios. It is possible to generate a new protection system by updating a single Configuration Item (CI) to the trained ML model.

As described in [5] two separate instances are needed for the proper operation: the operational system and the training and maintenance system.

The training and maintenance system is used to evaluate underperformances of the operational system (allowing the investigation of anomalies, if any) and to develop new trained ML algorithms, allowing the derivation of the expected performance. As with any operational ML system, the management and ingestion of curated data is key for the CMCU, as it allows continuous monitoring of the protection performance, along with its evolution to cope with new types of attacks.

Please input the preferred copyright option as mentioned in the attached "*SpaceOps-2023 Copyright Policy for Manuscripts and Presentations*"
e.g. "Copyright ©2023 by the Mohammed Bin Rashid Space Centre (MBRSC) on behalf of SpaceOps. All rights reserved."

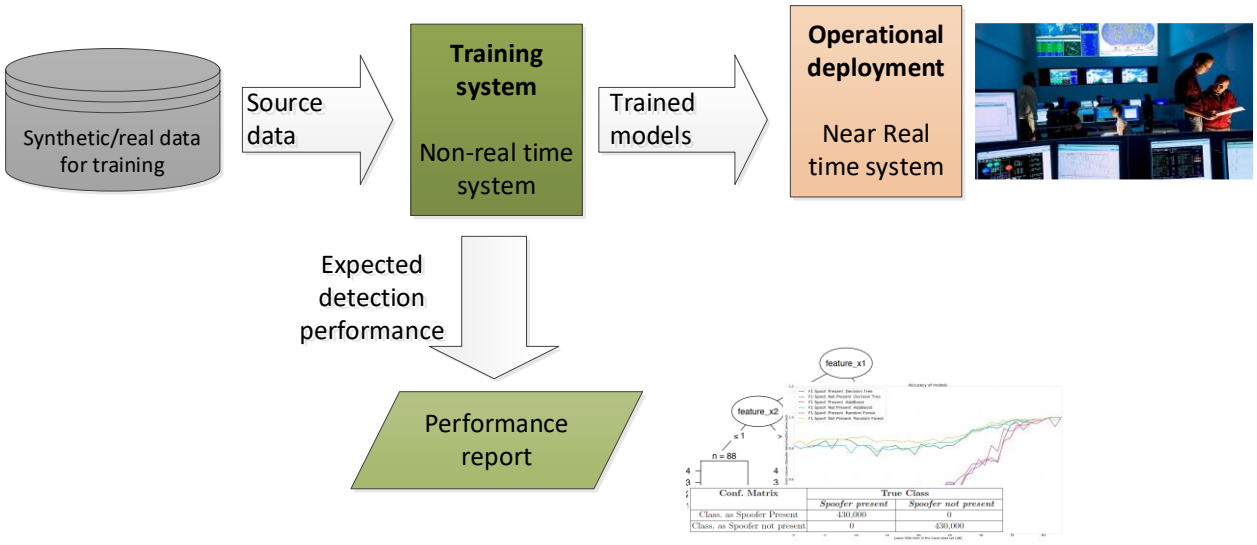

Figure 2 Operational and training instances of CMCU for Operational deployment of the Machine Learning based CMCU

3. Global protection against GNSS Jamming and Spoofing

Based on the CMCU concept, the protection can be extended by the usage of space data, which allows for the coverage of wider geographical areas, allowing the provision of a global service of GNSS Jamming and Spoofing detection.

Several LEO constellations are used to record GNSS signals and jamming signals in the GNSS band originating from Earth. Such raw signals are transmitted to ground, where the CMCU is fed with them. The CMCU is then able to flag the presence of complicated scenarios with Jamming and Spoofing signals.

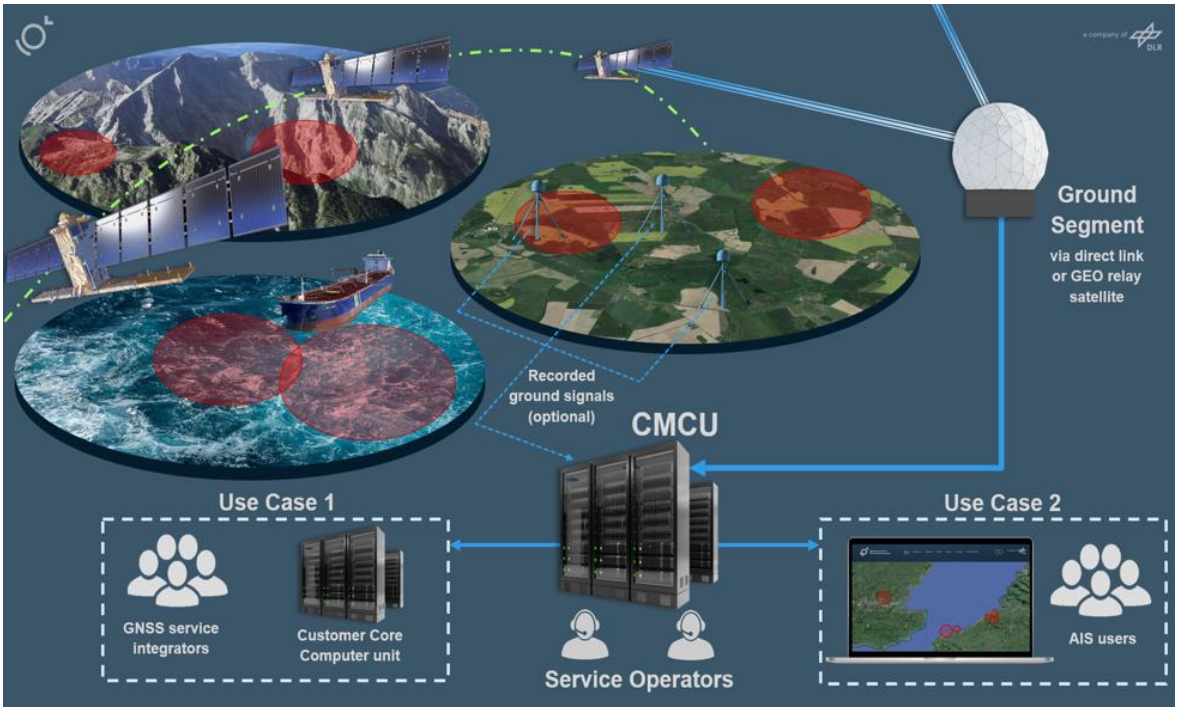

Figure 3 RESIST overall concept

Please input the preferred copyright option as mentioned in the attached "*SpaceOps-2023 Copyright Policy for Manuscripts and Presentations*"
e.g. "Copyright ©2023 by the Mohammed Bin Rashid Space Centre (MBRSC) on behalf of SpaceOps. All rights reserved."

Although the injection of satellite data allows for a wider geographical coverage, it also brings with it some limitations that need to be considered, namely the reception sensitivity from LEO orbit, and the geographical accuracy of the location.

3.1 Reception Sensitivity from LEO orbits

One of the main challenges in the case of satellite detection, originates from the power of the received signals. The long distances travelled by the signals highly attenuate them. The free space loss attenuation is estimated as per equation **Error! Reference source not found.**.

Therefore, the attenuation is calculated as in (1).

$$Atenuation = \left(\frac{4\pi LEO freq}{c}\right)^2 = 4{,}36085E + 15 \cong 154\ dB \qquad (1)$$

By considering:

- Freq is the L band frequency used by Galileo. E1 Galileo signals (1572,42 MHz)
- LEO is the communication distance. To simplify the problem, a fixed distance of 819 km has been chosen.

The signal to noise ratio (SNR) determines the final errors in communications, in this case this will allow estimating the geolocation of the Jammer or Spoofer. The SNR is determined as per *(2)*. Note in this case we are not accounting for the receiving satellite antenna, nor other losses like the feeder losses.

$$SNR = 10\log\frac{ptx}{Atenuation} + G - N \qquad (2)$$

Where:

- Ptx/alpha is the received power in the satellite
- G is the gain of the satellite's antenna
- N is the noise introduced by the received antenna
    - Being the equivalent noise temperature at the satellite input level, accounting for the receiver noise temperature and the antenna noise temperature (for a captured bandwidth of 500 KHz and assuming a noise figure of 7 dB):

$$T = 290 + 290 * (10^{\frac{7}{10}} - 1) \qquad (3)$$

$$N = TkB = T * 1{,}38 * 10^{-23} * 500 * 10^3 = 2{,}070 * 10^{-17}\ W/Hz \qquad (4)$$

It is assumed the satellite antenna is pointing towards Earth.

Note that the antenna gain is assumed to be 0 dBi in this estimation, when calculating the SNR (otherwise the SNR would be higher in the satellite receiver end). Therefore, by analysing the link to the given features mentioned before, it is expected that a -44,51 dB SNR is obtained by the satellite receiver given by a 1mW GNSS spoofer transmission on the Earth's surface.

3.2 Geolocation accuracy from LEO orbits

The next challenge for the system design is estimating the geolocation accuracy of the emitter. The proposed solution for determining the location of the attack signal source is the combination of the Time Difference Of Arrival (TDOA) and Frequency Difference Of Arrival (FDOA).

As described in [6], the TDOA (which requires at least three receivers) measurement is defined as:

Please input the preferred copyright option as mentioned in the attached "*SpaceOps-2023 Copyright Policy for Manuscripts and Presentations*"
e.g. "Copyright ©2023 by the Mohammed Bin Rashid Space Centre (MBRSC) on behalf of SpaceOps. All rights reserved."

$$\tau = \frac{r_2 - r_1}{c} \quad (5)$$

Being:

- Ri the distance from the emitter to the i receiver.
- c the speed of light

On the other hand, the FDOA follows[6]:

$$f_{av} = f_c - \left(\frac{r_{12} - r_{11}}{\lambda T}\right) \quad (6)$$

$$\Delta f^{1,2} = \frac{f_0}{c} \times ((i^1)^T(\dot{x}^1 - \dot{x}) - (i^2)^T(\dot{x}^2 - \dot{x})) \quad (7)$$

Where:

$f_0 \rightarrow signal\ carrier\ frequency$
$i^i = \frac{r^i}{\|r^i\|} \rightarrow radial\ component\ of\ the\ emitter\ relative\ velocity$
$\dot{x}^i \rightarrow sensor\ i\ velocity$
$\dot{x} \rightarrow emitter\ velocity$

From [7], the TDOA accuracy follows:

$$\sigma^2_{w,\tau_{ij}} > \frac{3\, N_{0,i} N_{0,j}}{2\pi^2 T S_i S_j \Delta f^3} = \frac{3}{\pi^2 SNR_p \Delta f^2} \quad (8)$$

Where:

- $\sigma^2_{w,\tau_{ij}}$ is the error variance of the TDOA estimate under a weak received power assumption: $\bar{\sigma}^2_{w,\tau_{ij}}$
- T is the integration time
- $S_s(f)$ is the emitter signal power spectral power
- $N_{0,i}\ and\ N_{0,j}$ are the noise power density

This provides the results shown in Figure 5, both for 1mW and 10W spoofer on Earth surface.

Please input the preferred copyright option as mentioned in the attached "*SpaceOps-2023 Copyright Policy for Manuscripts and Presentations*"
e.g. "Copyright ©2023 by the Mohammed Bin Rashid Space Centre (MBRSC) on behalf of SpaceOps. All rights reserved."

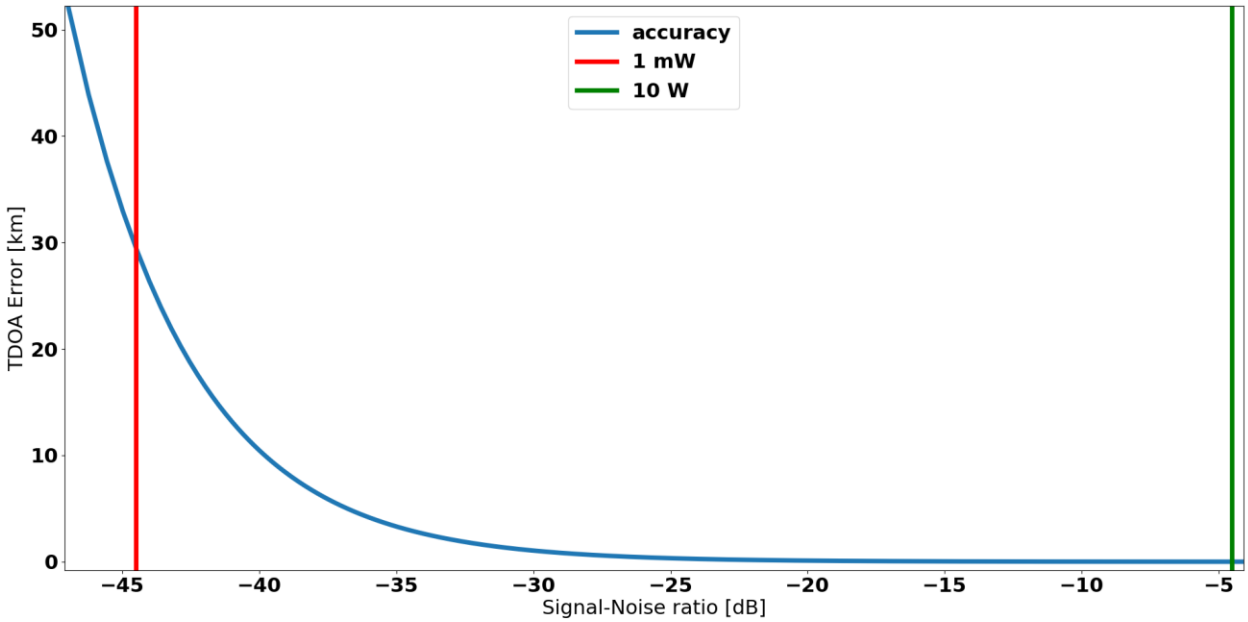

Figure 4 - Accuracy dependence of SNR received in sensors.

4. RESIST System

Following the model-based Systems Engineering Arcadia methodology, a system design is being performed. This methodology is a structured approach to identifying and checking the architecture of complex systems. It promotes collaborative work among all stakeholders during many of the engineering phases of the system around the system model at different levels. It allows iterations during the definition phase that help the architects to converge towards a satisfactory solution to the identified needs.

As a result of applying such Arcadia approach in the ESA feasibility study, a system design with the CMCU at its core was proposed.

During the following sections the system blocks will be introduced.

Please input the preferred copyright option as mentioned in the attached "*SpaceOps-2023 Copyright Policy for Manuscripts and Presentations*"
e.g. "Copyright ©2023 by the Mohammed Bin Rashid Space Centre (MBRSC) on behalf of SpaceOps. All rights reserved."

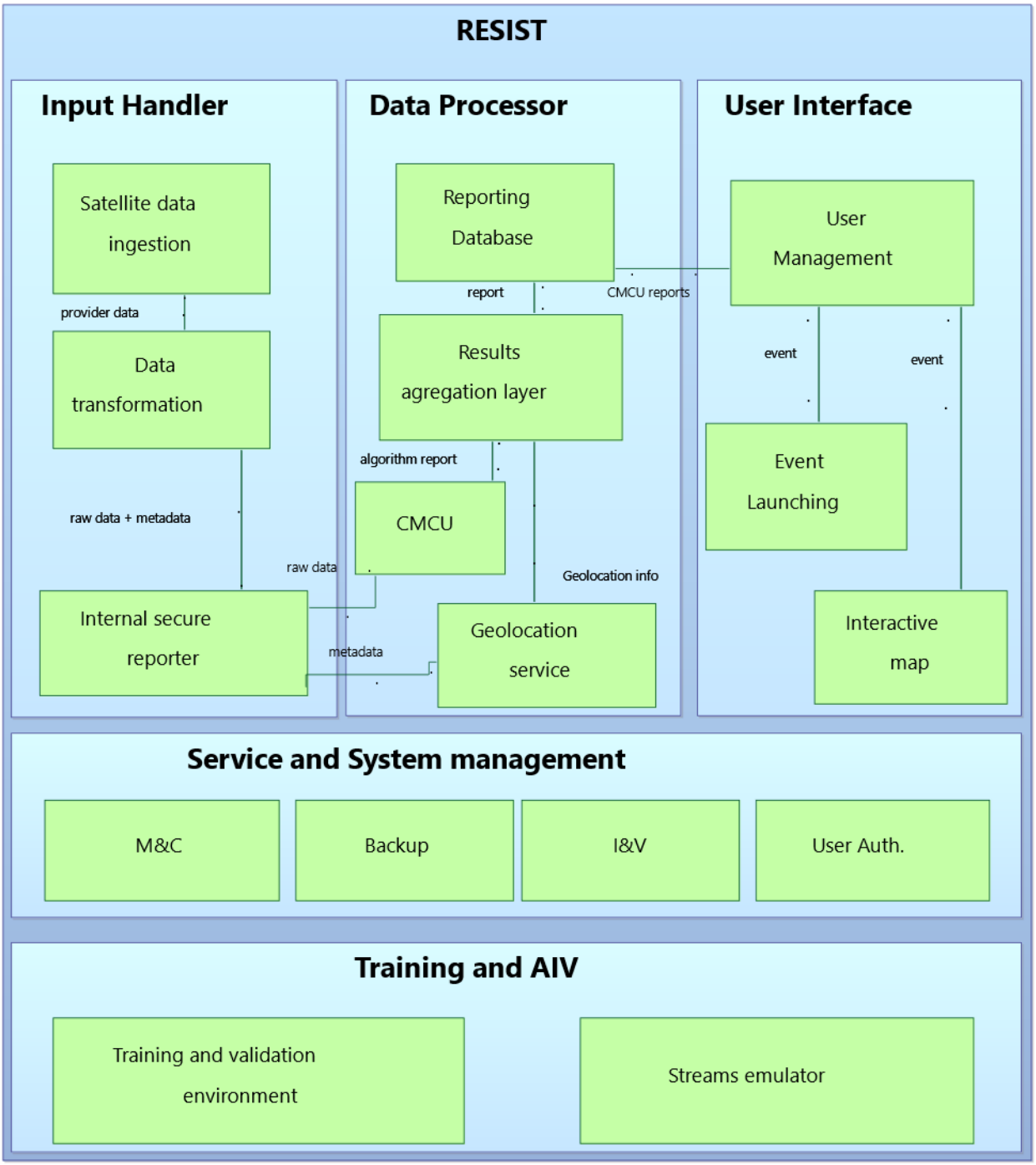

Figure 5 RESIST System diagram

4.1 Input handler

Raw data is collected from the data provider. Signals are recorded from a LEO constellation and given to the core of the RF Analytics to analyse them.

The input handler is composed by:

- **Satellite data ingestion functions**: The data provided by the LEO constellation operators will need to be received and managed by the RF Analytics system. These functionalities will implement the external ICD towards the data provider, as agreed with the different providers.

Please input the preferred copyright option as mentioned in the attached "*SpaceOps-2023 Copyright Policy for Manuscripts and Presentations*"
e.g. "Copyright ©2023 by the Mohammed Bin Rashid Space Centre (MBRSC) on behalf of SpaceOps. All rights reserved."

- **Data Transformation functions**: Depending on the provider, the signal can be formatted in different ways. To be able to perform the evaluation in the Data Processor function an initial pre-processing and format adaptation is required.
- **Internal secure reporter functions**: This function will implement the internal ICDs between the Input Handler functionalities and the data processor. Allowing the reception of the data by the CMCU, along with the distribution of the geolocation data to the next functional blocks. Based on the geolocation, the CMCU processing will be arranged so that those time-critical areas (use case 1) shall be computed with priority against the areas from use case 2.

4.2 Data processor

To evaluate the input data, the processing in this block is split. First, the geographical information relating to the recorded signals needs to be estimated. Next, the raw data is evaluated by the CMCU (the core algorithm of the system), which will analyse the presence of a Jamming/Spoofing attack and report the results in a database.

- **Geolocation service functions**: Groups of functionalities associated to the geolocation estimation of the signal originator.
- **CMCU**: The raw data is evaluated by the CMCU (the main algorithm of the system). It will analyse the presence of a Jamming/Spoofing attack and report the results in a database.
- **Results aggregation layer**: Groups of functionalities responsible for evaluating the output from the CMCU algorithm. This component sorts the data adding metadata to deliver this information to the user.
- **Reporting Database**: Groups of functionalities associated with the storing and transmitting of the aggregated layer information. The information will contain the following:
    - Timestamp: Time when the evaluation is made.
    - Latitude and Longitude: Geographic position of the reporting signal.
    - RFI: Informs about the presence of a Radio Frequency Interference (RFI)
    - Spoofer: Informs about the presence of a spoofer.
    - Affected area: Area or ground recorders affected by the event.
    - Frequency band: Galileo frequency band(s) affected.
    - Attack presence probability: CMCU PFA of the used model.
    - Probability of area affected: pfa_CMCU·error_TDOA
    - SVID: Indicates the satellite on which the evaluation has been made.

4.3 User Interface

Via the User Interface, the user has access to the RF Analytics core algorithm reports. The interface usage depends on the use case and the user's needs.

- **User Management**: A group of functionalities dedicated to communicating with the web interface with the information obtained by the data management.
- **Event Launcher**: In use case 1, when an event is detected for a determined location, then it is reported to the user. Raw data of the event may be stored, for forensic analysis and Machine Learning training.

Please input the preferred copyright option as mentioned in the attached "*SpaceOps-2023 Copyright Policy for Manuscripts and Presentations*"
e.g. "Copyright ©2023 by the Mohammed Bin Rashid Space Centre (MBRSC) on behalf of SpaceOps. All rights reserved."

- **Interactive Map**: In use case 2, the web interface allows searching historical data for reports on the different areas of a map .

4.4 Service and Management System

The support and control functional blocks group the functionalities related with the monitoring and control of the RESIST elements and required support functionalities.

- **Backup management functions**: Groups the required functionalities for information backup and recovery.
- **Monitoring and control functions**: Groups the functionalities associated with the monitoring the RF Analytics operation and performance, modification of the RESIST component variables and configuration, visualization of the different operation and performance variables and operator console.
- **Infrastructure**: Groups the set of functionalities associated with the network elements, analytics operational components user (in opposition to users on web and programmable interfaces) authentication, operational component user management and other RF Analytics operational infrastructure functionalities.
    - Network functions.
    - Authentication functions.
- **Fault detection and isolation**: Groups the set of functionalities which allow detection of failures (very related to monitoring), helping to identify and isolate the failed component.

4.5 Training and AIV

The AIV functional blocks integrate the functionalities associated with the validation of the RF Analytics components and training of operators.

- **Training, verification & validation functions**: Groups the functionalities associated with the training, verification and validation of RESIST and their associated operation.
- **Emulators and verification & validation support functions**: Groups the functionalities associated with the emulation of RF Analytics interfaces for verification, validation and training.

5. Use Cases

As indicated in Section 1, there are two Use Cases considered at the moment for the RESIST system:

5.1 Use case 1

In this case of use, the end-user shall be notified about the presence of a GNSS attack when is detected. Figure 6 – Use case 1 , shows the functioning of this case of use. This service will be provided to those customers whose services are GNSS-dependent.

Therefore, the raw data is analysed to detect the presence of an attack and report the event to the end-user with reduced delay.

Please input the preferred copyright option as mentioned in the attached "*SpaceOps-2023 Copyright Policy for Manuscripts and Presentations*"
e.g. "Copyright ©2023 by the Mohammed Bin Rashid Space Centre (MBRSC) on behalf of SpaceOps. All rights reserved."

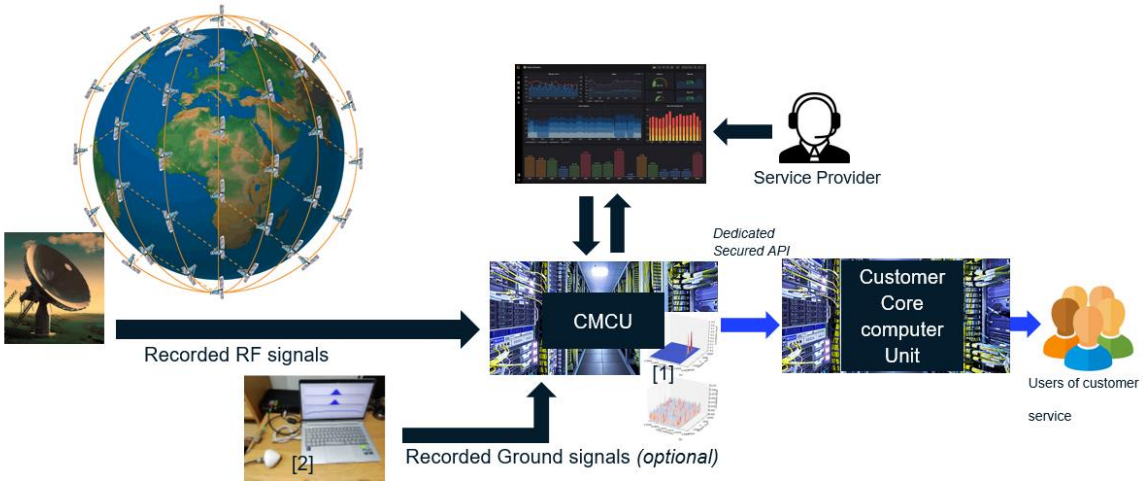

Figure 6 – Use case 1 illustration

5.2 Use case 2

In this case, the customer use of GNSS is not as critical as in use case 1. Thus, the end-user may be only interested in historical data. The functioning is shown in Figure 7.

The end-user will have access to the events historical data for the requested area through a web interface based on an interactive map.

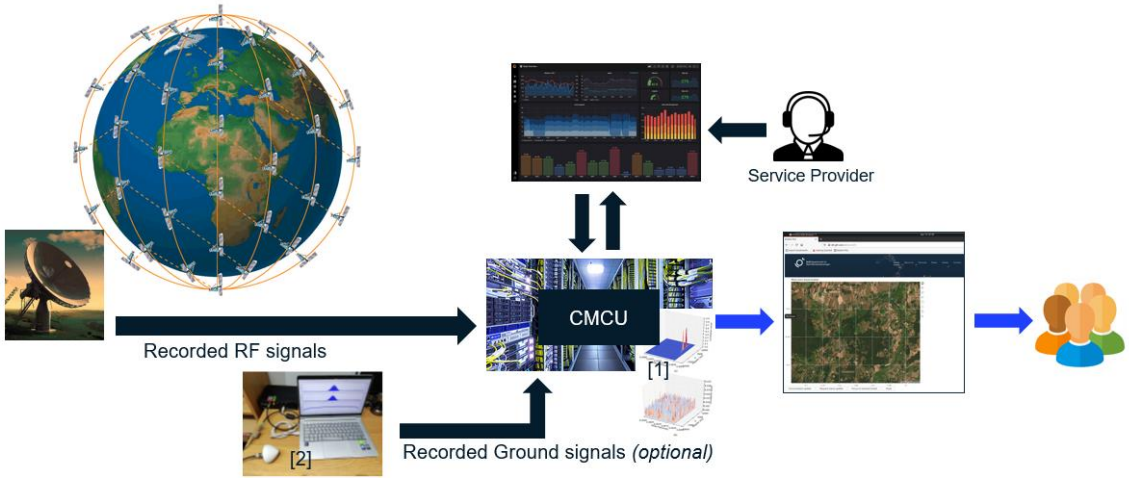

Figure 7 – Use case 2 illustration

6. Results

The RESIST system is set to be a service to add robustness to GNSS services. The system, divided in 5 modules, will be able to acquire and process the information/data collected by the satellite and ground receivers. It is capable of evaluating the GNSS Search Space to apply the CMCU Jamming and Spoofing detection algorithm and report the results. See the RESIST Product Tree in Figure 8Figure 8.

Please input the preferred copyright option as mentioned in the attached "*SpaceOps-2023 Copyright Policy for Manuscripts and Presentations*"
e.g. "Copyright ©2023 by the Mohammed Bin Rashid Space Centre (MBRSC) on behalf of SpaceOps. All rights reserved."

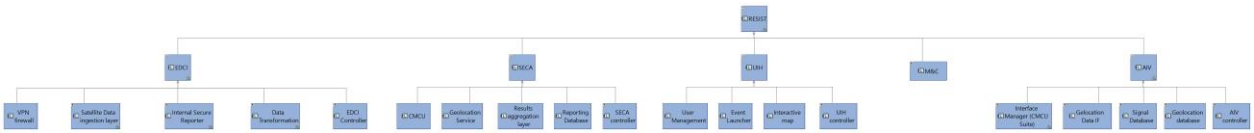

Figure 8 – RESIST Product Tree

As discussed in Section 3.1 and Section 3.2, the main two difficulties for the implementation of the system are the receiver power sensitivity and the geolocation accuracy, associated to TDOA measurements with three or more satellites. The final resolution and accuracy of the system will depend mainly on the transmitted signal power. Therefore, the CMCU evaluation and the interference allocation will increase as the SNR in the satellite receivers does. The emitter location, according to the TDOA/FDOA measurements would describe the next performance of the accuracy for a given interference transmitted power, for 1mW spoofer a theoretical accuracy of ~30Km is to be expected, while for a 10W a 3m accuracy is to be expected. Note that such accuracy estimates don´t account for geometrical errors introduced.

6. Conclusions and next steps

As discussed in Section 6 the main limiting factors, assuming continuous streams of data from satellites are provided, are the satellite receiver sensitivity and the geolocation accuracy.

Nonetheless, the CMCU system is perfect for overcoming such limitations, as the inclusion of a complementary ground network can be used for improving the sensitivity and supporting the fine geolocation after the rough position was determined from the satellite constellation data.

Detecting powerful Spoofing attacks (military grade) based on the performed simulation seems possible, allowing the provision of a world-wide protection systems against advanced GNSS Jamming and Spoofing.

Considering the status of the technical feasibility study and the interest different markets are showing in this type of service, the next step is to perform an end-to-end demonstrator of the service, feeding CMCU with ground and space data at the same time.

References

[1] Bloomber Wire, "Runway at DFW Airport temporarily closes while FAA looks into faulty GPS signals," *The Dallas Morning News*, pp. https://www-dallasnews-com.cdn.ampproject.org/v/s/www.dallasnews.com/business/airlines/2022/10/18/runway-at-dfw-airport-temporarily-closes-while-faa-looks-into-faulty-gps-signals/?amp_gsa=1&amp_js_v=a9&outputType=amp&usqp=mq331AQKKAFQArABIIACAw%3D%3D#amp_, 18 October 2022.
[2] EASA, "Safety Information Bulletin, Global Navigation Satellite System Outage Leading to Navigation/Surveillance Degradatation EASA 2022"
[3] Inside GNSS. Inside GNSS 10 December 2019 (Online) Available: https://insidegnss.com/sinister-spoofing-in-shanghai/ .Last access on: 07 December 2022
[4] F. &. Y. A. Gallardo López, "SCER Spoofing Attacks on the Galileo Open Service and Machine Learning Techniques for End-User Protection," *IEEE Access*, vol. 10.1109/ACCESS.2020.2992119, pp. 1-1, 2020.
[5] F. &. Y. A. Gallardo López, "Operational Deployment of GNSS Anti-spoofing System for Road Vehicles," *Communication Technologies for Vehicles. Nets4Cars/Nets4Trains/Nets4Aircraft 2021. Lecture Notes in Computer Science.*, vol. 13120, 2021.
[6] P. C. Chestnut, "Emitter Location Accuracy Using TDOA and Differential Doppler," *Transactions on Aerospace and Electronic Systems,*, pp. 214-218, 1982.
[7] Jahshan A. Bhatti and Todd E.Humphreys, "Development and Demonstration of a TDOA-Based GNSS Interference Signal Localization System,," *Proceedings of the 2012 IEEE/ION Position,,* pp. 455-469, 2012.