Interference and Spoofing Detection for GNSS Maritime Applications
using Direction of Arrival and Conformal Antenna Array

E. Pérez Marcos[1,2], A. Konovaltsev[1], S. Caizzone[1], M. Cuntz[1,2], K. Yinusa[1], W. Elmarissi[1], M. Meurer[1,2]

[1]*Institute of Communications and Navigation, German Aerospace Center (DLR)*
Oberpfaffenhofen-Wessling, Germany
[2]*RWTH Aachen University, Chair of Navigation, Germany*
Emilio.PerezMarcos@dlr.de

BIOGRAPHIES

Emilio Pérez Marcos studied Electrical Engineering at Valladolid University, Spain. From 2006 to 2008 he was granted a young research position within the Electronics Department at the same university. From 2009 to 2014 he worked as Research Engineer in the Medical Technology Industry in Jena, Germany. Since 2014 he has been working within the Algorithms and End-Devices group in the Institute of Communications and Navigation at DLR Oberpfaffenhofen. His current research topics include signal disturbances, interferences and cybersecurity in real time GNSS receivers and Spatial-Temporal Adaptive Processing techniques for multi-antenna systems.

Andriy Konovaltsev received his engineer diploma and the Ph.D. degree in electrical engineering from Kharkov State Technical University of Radio Electronics, Ukraine in 1993 and 1996, respectively. He joined the Institute of Communications and Navigation of DLR in 2001. His main research interest is in application of antenna array signal processing for improving performance of satellite navigation systems in challenging signal environments.

Stefano Caizzone received the M.Sc. in Telecommunications Engineering and the Ph.D. degree in Geoinformation from the University of Rome "Tor Vergata", Italy, in 2009 and 2015, respectively. Since 2010, he is with the German Aerospace Center (DLR), Oberpfaffenhofen, Germany, where he is responsible for the development of innovative miniaturized antennas. His main research interests concern small antennas for RFIDs and satellite navigation, antenna arrays and grids with enhanced sensing capabilities, controlled radiation pattern antennas for robust satellite navigation and high-performance antenna design for precise satellite navigation.

Manuel Cuntz received the diploma in electrical engineering degree in 2005 from the Technical University of Kaiserslautern. He joined the Institute of Communications and Navigation of DLR Oberpfaffenhofen, in June 2006. His fields of research are multi-antenna satellite navigation receivers.

Kazeem Yinusa obtained his BSc in electronics and communications engineering from the Arab Academy for Science and Technology in Cairo in 2009. From 2009 till 2015, he studied at the Technical University Munich where he obtained his MSc in communications engineering and his PhD in electrical engineering based on his dissertation on echo suppression techniques for near-field antenna measurements. He joined the Institute of Communications and Navigation at DLR in March 2015 as a researcher with main interest in antenna technologies for satellite navigation.

Wahid Elmarissi received the B.Sc. in Physics from the University of Sciences "Mohammed V", Rabat, Morocco, in 1992 and the Dipl. Ing. (FH) in Electrical Engineering from the University of Applied Sciences, Kiel, Germany, in 2003. In 2003, he joined the Institute of Communications and Navigation of the German Aerospace Center (DLR), where is responsible for measurement and manufacturing of antennas and antenna electronics.

Michael Meurer received the diploma in electrical engineering and the Ph.D. degree from the University of Kaiserslautern, Germany. After graduation, he joined the Research Group for Radio Communications at the Technical University of Kaiserslautern, Germany, as a senior key researcher, where he was involved in various projects in the field of communications and navigation both as project coordinator and as technical contributor. From 2003 till 2013, Dr. Meurer was a senior lecturer and Associate Professor at the same university. Since 2006 Dr. Meurer is with the German Aerospace Centre (DLR, where he is the director of the Department of Navigation and of the center of excellence for satellite navigation. In addition, since 2013 he is a professor of electrical engineering and director of the Chair of Navigation at the RWTH Aachen University. His current

research interests include GNSS signals, GNSS receivers, interference and spoofing mitigation and navigation for safety-critical applications.

ABSTRACT

An international maritime measurement campaign was done to detect and record radio frequency interferences in the Satellite Navigation frequency bands. The system, installed on a large container ship, consists of a conformal seven elements antenna array, an ad-hoc data recorder system and a multi-antenna navigation receiver prototype. In this paper, the system is briefly presented, together with the proposed detection and analysis methodology. Pertinent results of measurements are shown, including detected radio frequency interferences, its characterization, impact on the receiver performance and the localization of the ship during the time. In addition an on-line calibration scheme is used to correct channel differences, hence allowing Direction of Arrival estimation of the mentioned interferences with the conformal antenna array. Moreover, a Spoofing / Repeater data analysis has been performed over some of the recorded data.

INTRODUCTION

Global Navigation Satellite Systems (GNSS) have become the main technology to provide position and timing services in the world. This increasing dependency on GNSS across many application fields has raised concerns about the vulnerability of the same. As a matter of fact, GNSS signals have very low power when they arrive at the receiver, due to long propagation path from the satellites and low power emitted at transmission. Such situation makes the service vulnerable to interfering signals. The power requirements of such interference signals are not very demanding and therefore they can easily block the reception of satellite signals. These radio frequency interferences are usually of unintentional nature, but they can also be deliberately produced. Unintentional and deliberate interference signals constitute a challenging problem in many Safety of Life applications and in Liability Critical applications.

Whereas in other application domains, such as aeronautics, researches about radio frequency interference (RFI) signals in the operation environment are available [1], the maritime domain is, only recently, paying attention to this threat [2] [3] [4]. Also the International Maritime Organization (IMO) clearly expressed its concern, by including it as part of its e-Navigation plan [5].

While the referenced previous work reported incidents in some harbors, the information is far from offering a complete global picture. In order to provide some more insight into the topic, the Institute of Communications and Navigation of the German Aerospace Center (DLR) conducted an international maritime RFI measurement campaign, included dense traffic maritime routes and harbors around the world.

The main objective of the measurement campaign was to detect, observe and record radio frequency interference events in the GPS and Galileo Open Service frequency bands. Therefore signals in L1/E1 and L5/E5a frequency bands are the objective of the measurement campaign. It is worth to mention that both, L1 and L5, bands are strictly regulated. L1 band being actually reserved for radio navigation services, while L5 band allows coexistence of some other services.

Moreover, as important increment to the previously published work in [6][7], for the first time results regarding the Direction of Arrival (DoA) of the recorded signals will be presented. Also, the main findings from the analysis of the third set of measurements collected between September 2017 and January 2018 are introduced.

MEASUREMENT SYSTEM

A vessel from the company Hapag-Lloyd, specifically a large container ship of the Hamburg Express class (366 meters length, beam (width) of 48 meters and a gross tonnage of 142,292 tons), serves as mobile measurement platform. The vessel travels in a route from Europe to Asia, covering very different regions and docking in several countries. This makes it a very interesting choice for the purposes of the measurement campaign.

On-board two independent systems run in parallel. One system is a DLR in house developed multichannel, multiband RFI data recorder, whose function is to detect and record time snapshots of interference signals. This system will be from now on called either Data Recorder or Snapshot Recorder. Additionally, also a DLR proprietary GNSS multi-antenna navigation receiver prototype is installed for comparison and verification. This system will be called in the following DLR GNSS receiver. Both systems are simultaneously fed by a seven elements conformal antenna array. A functional diagram of the whole measurement system installed onboard can be seen in Figure 1. A communications satellite link is being used for the control and monitoring tasks. Following a very brief description of the respective subsystems is presented. More details of the measurement system can be found in [6] [7].

a. Conformal Antenna Array

An antenna array is used in this project, as it allows the spatial domain characterization of the received signals, both for navigation signals and interferences. That enables digital beamforming for navigation signals together with Direction of Arrival (DoA) on both navigation and RFI signals.

The installed antenna array has been developed for the specific application: the various antennas are placed on a hemispherical support, such as to increase the received energy from signals impinging with low elevation angles and hence gain maximum information from signals of all possible receiving directions. The array antenna is mounted above the navigation bridge, at a height of almost 50 meters above sea level.

The array consists of seven elements arranged on a spherical cap with an equatorial diameter of 24 cm. Coverage of the upper hemisphere is achieved by placing one element (element number 7) on the top of the hemispherical cap. The remaining six elements are uniformly arranged on a ring below the top element and are radially directed at an angle of 58 degrees from zenith (see Figure 2). During installation antenna element 1 was mounted with 100° offset to the vessel moving vector, as pictured in Figure 2 and Figure 3.The green arrow represents the x axis of the hemispherical cap and the dashed orange line the vessel moving vector.
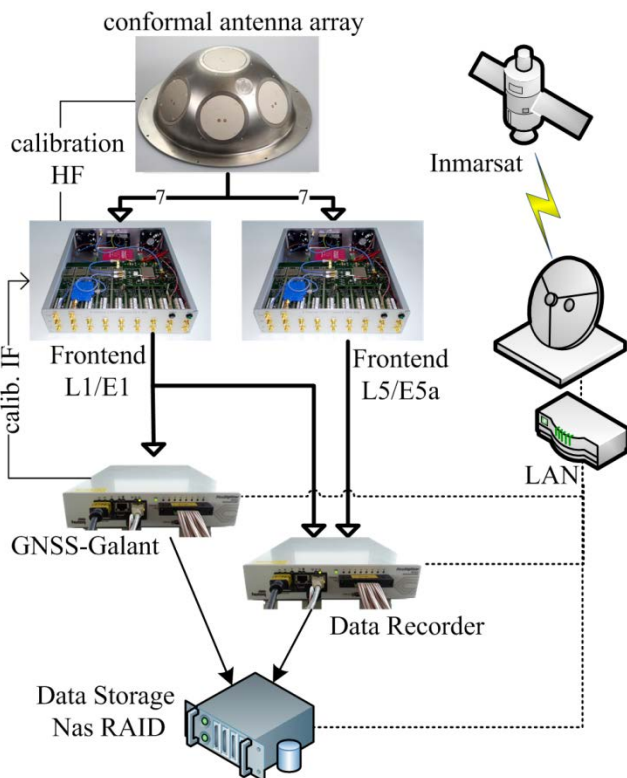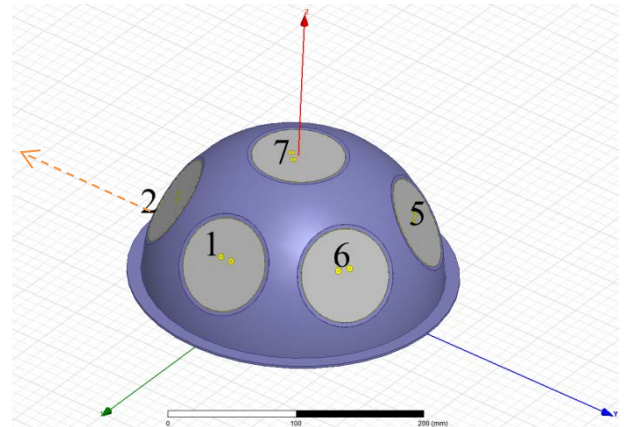

Figure 1 Measurement System

Figure 2 3D model of the antenna array on the hemispherical cap.
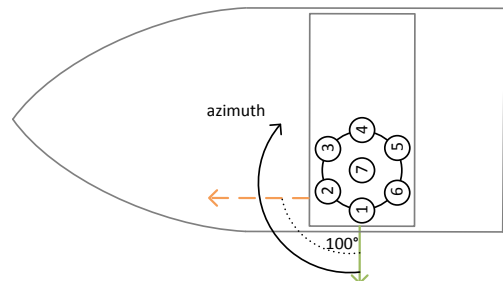

Figure 3. Schematic position of the antenna array.

One known issue related to antenna array systems is the different characteristics of the discrete elements within the several signal paths. The antenna elements, the frontend channels, the analogue to digital converters, etc. all show differences that can be explained by: manufacturing tolerances, electrical tolerances, temperature changes, aging, etc.

Calibration can be used to tackle those differences. The basic idea is to generate a known signal and inject it into the antenna electronics, right after each antenna element. This signal will follow all the parallel data paths and can be therefore used to calculate the variations between them.

In this particular case, the so called live or online calibration is used. In contrast with the one-time calibration commonly used, where the differences are measured and corrected once, usually during the system manufacturing, the online calibration is active for the whole operation time of the system, correcting the deviations on real time.

b. Frontends for the L1/E1 and L5/E5a frequencies

After the antenna array, each of the seven channels is split in order to feed two frontends: a L1/E1 Frontend and a L5/E5a Frontend. Both analogue Frontends perform three main tasks: signal filtering, frequency translation or down-conversion to an intermediate frequency (IF), and amplification.

A detailed description of the Frontends can be found here [8] and here [9].

c. ***GNSS multi-antenna navigation receiver prototype***

During the last years DLR has been developing a flexible receiver prototype for antenna array robust GNSS navigation, with emphasis in Safety of Life applications. A customized version of the prototype, able to accommodate seven antennas and with the ability to run autonomously (with a remote control and monitoring via satellite communication), has been developed for the campaign. DLR's prototype (more details can be found here [9]) is based on a combination of hardware, firmware and software (see [6] for details).

It is worthwhile noticing that, thanks to the use of a seven elements array and the post-correlation beamforming, DLR's GNSS Receiver has higher interference robustness than single antenna receivers: this feature enables the receiver to still provide a PVT solution in case of weak interferences and hence enable a more detailed analysis of the interference effects.

For the sake of in-depth analysis in post-processing, several extra logging functionalities were developed, specifically: tracking tables of space vehicles, tracking of the self-generated calibration signal, position velocity and time (PVT), and the time (UTC) of the local platform. All of them are logged every 20 seconds.

d. ***Snapshot Recorder***

The hardware used for the Snapshot Recorder is identical to the one used for the GNSS multi-antenna navigation receiver. The only difference is that here the seven IF L1/E1 and the seven IF L5/E5a are digitized (14 ADCs are used).

The ADCs sample the IF signals coming from the frontends (both L1 and L5) and map the data into a portion of memory that is shared with the software. The amount of available shared memory constraint the possible record time.

A snapshot is defined as a block of 50 ms or 30 ms, of seven elements of two frequency bands sampled at 100 MHz with two bytes per sample.

The software developed for the project reads the shared memory and evaluates the snapshot trying to find an RFI event. If the snapshot contains interference information, it is saved. In case no interference traces are found, it will be discarded or saved for control purposes. Configurable timers are programmed to manage the time lapses between saved snapshots.

The real-time detection algorithm is based on the amplitude of the digitized IF samples. The model assumes ADC samples with a Gaussian distribution, i.e. $x[n] \sim N(\mu, \sigma)$. With the first run the detection algorithm needs to estimate the mean μ and standard deviation σ in an interference-free case. Once the Gaussian distribution is characterized an M-of-N search algorithm [10] is used to detect the interferences. Within a snapshot, if M of the total N samples fulfil the interference hypothesis, then the snapshot is declared to contain interference. In terms of statistical tests it can be described as:

$$H_0 \text{ (no interference): } x[n] \in [Thr_-, Thr_+]$$
$$H_1 \text{ (interference): } \quad x[n] < Thr_- \text{ or } x[n] > Thr_+$$

(1)

where Thr_- and Thr_+, are the detection thresholds. They are defined for the left and right sides of the Gaussian distribution. These thresholds can be computed using the inverse cumulative distribution function, $\Phi^{-1}(\mu, \sigma, P)$, of the Gaussian distribution and the value of target false alarm probability $P_{fa,single}$:

$$Thr = \Phi^{-1}(0, \sigma, 1 - P_{fa,single}/2)$$
$$Thr_- = -Thr + \mu$$
$$Thr_+ = \quad Thr + \mu$$

(2)

The current implementation uses the following settings: $P_{fa,single}$ = 10%, N = 1500 and M = 300. The detection algorithm declares an RFI event if at least two array elements generate corresponding test statistics.

e. ***Data Storage***

All the collected snapshots from the Snapshot Recorder and all the logs generated by the GNSS Receiver need to be saved for posterior analysis. The risk of losing data had to be minimized as much as possible. A network attached storage (NAS) redundant array of independent disks (RAID) was chosen for the specific application. The RAID was filled with Solid-State Drives (SSDs) to increase the resistance to environment vibrations. The use of SSDs and the redundancy of the RAID improve reliability, but limit the storage capability: as a matter of fact, only 4 TB of data storage are available. For comparison, a 50 ms snapshot takes up to 160 MB, a 30 ms snapshot takes up to 96 MB. Those figures have forced to meet a trade-off among the interest in recording as much information as possible and the limited storage capability.

METHODOLOGY

The collected data is evaluated in post-processing, with the aim of characterizing and cataloguing the detected interferences. This task is accomplished by concurrently using data from the recorded RFI snapshots and the real time GNSS receiver prototype, and also allows assessing the impact of the recorded interference on the received GNSS signal. Also the real-time GNSS positioning information is used, when available, to geographically situate the recorded event.

As required by the project, the M-of-N real time detection algorithm is the principal tool for interference event detection. For each RFI event, it is possible to observe different metrics derived from the data saved in the Snapshot Saver:

- The Estimated Power received at the ADCs over time: this metric is proportional to the power received at the antenna elements. Variations of the input power over time are indicative of possible RFI events.
- The spectrum of the data within the snapshot: also in this case, variations (e.g. abrupt peaks in frequency) in the spectrum are hints for interference events. The kind of variation observed in the spectrum also helps in characterizing the RFI event, for instance by distinguishing Continuous Wave (CW) from Wideband (WB) interferences.

The metrics taken into consideration from the receiver prototype are:
- The calibration signal level:

    As explained before, the GNSS receiver generates an antenna array calibration signal, which is injected into the antenna electronics. The signal is a Gold code number 160, BPSK modulated that the receiver processes. It is therefore tracked as any other valid PRN impinging signals. Such property of the calibration signal proves very useful, e.g. in case of obstructions, such as bridges. In case of a strong interference, GNSS signals and calibration signals are disturbed. Under a bridge, GNSS signals are blocked, whereas the calibration signal is continuously tracked.
- The spread of eigenvalues of the pre-correlation covariance matrix:

    In the absence of radio frequency interference, the elements of the spatial pre-correlation covariance matrix are dominated by the noise contribution; hence the spread of the eigenvalues is small. The presence of a strong interference is manifested by one or more eigenvalues being significantly larger than the rest.

Having the whole list of above mentioned metrics to look at, the data analysis will be performed according to the following steps:

i. Evaluation of the snapshots power over time, to firstly identify interference events (analogously to the generation of "interference flags" by the snapshot recorder in case the M-of-N thresholds are surpassed).

ii. In parallel the receiver pre-correlation eigenvalues over time is looked into, to verify the actual presence of RFIs in the spatial eigenvalues domain.

iii. Also in parallel the Carrier to Noise ratio (C/N0) of the GNSS Receiver calibration signal is looked into, e.g. to disregard obstruction events.

iv. Spectral information of the data within the snapshots are analyzed and compared with data from interference-free snapshots.

v. The performance of the GNSS Receiver PVT solution is analyzed. The aim is to assess the impact of the RFI on the receiver.

DIRECTION OF ARRIVAL

With the measurement platform mounted at around 50 m above the sea level, it is expected to receive interference and spoofing signals mostly with relative low elevation angles. For that matter the Direction of Arrival (DoA) estimation is supported by the semi-spherical design of the seven elements conformal antenna array.

The DoA estimation for conformal arrays is a challenging topic with relevant differences from canonical DoA applied to planar arrays. Many of the normal simplifications and assumptions are not met, for example the array is not easily subdivided into arrays that meet the displacement invariance property required by algorithms like ESPRIT.

The post-processing computed DoA is estimated using the recorded signals after the Frontend, that is, before the PRN-code correlation process. For multichannel antenna array systems, the differences in the several parallel channels along the data paths (electromagnetic elements forming the array, cabling, analogue discrete components in the Frontend, etc.) manifest themselves as errors in the DoA estimations.

The self-generated calibration signal plays a fundamental role in order to provide DoA estimations without the above mentioned errors. By providing the phase differences between each of the different channels, the IF data can be corrected before computing the DoA. Without the corrections provided by the calibration process the DoA results will contain an inherent error due to the different signal pathways.

Before the PRN correlation process, the navigation signals ought to be buried below the noise level, the only signals clearly visible above the noise are interference signals, its reflections and maybe some higher power repeater/spoofer.

The following assumption is made: by estimating the DoA of all visible signals before the correlation, we are indeed estimating the DoA of all received interfering signals. In order to do that, the snapshots marked as containing RFIs are reprocessed. Firstly an estimation of the number of signals D, is performed by using the Akaike [11] and the Minimum Descriptive Length (MDL) [12] methods. Both methods try to estimate the number of signals D, from a family $d \in \{0,1,...,N_{ant} - 1\}$, as the value that minimized the Akaike criteria Eq. (3) and MDL criteria Eq. (4). The eigenvalues, λ_i, are obtained performing the Eigen decomposition from the estimated covariance matrix, calculated as

$$\boldsymbol{R}_{xx} = \frac{1}{N}\sum_{k=0}^{N-1} \boldsymbol{x}\boldsymbol{x}^{H},$$

(3)

where $\mathbf{x} \in \mathbb{C}$, is the vector of size $N_{ant} \times 1$ of IF samples contained in a snapshot after a Hilbert transformation.

The Akaike and MDL methods are not always precise; therefore manual modifications using the other available metrics (received power at each element, and snapshot spectrum) are used for corrections.

$$AIC(d) = -\log \left\{ \frac{\prod_{i=d+1}^{N_{ant}} \lambda_i^{\frac{1}{N_{ant}-d}}}{\frac{1}{N_{ant}-d}\sum_{i=d+1}^{N_{ant}} \lambda_i} \right\}^{(N_{ant}-d)N} + d(2N_{ant}-d) \quad (4) \qquad MDL(d) = -\log \left\{ \frac{\prod_{i=d+1}^{N_{ant}} \lambda_i^{\frac{1}{N_{ant}-d}}}{\frac{1}{N_{ant}-d}\sum_{i=d+1}^{N_{ant}} \lambda_i} \right\}^{(N_{ant}-d)N} + \frac{1}{2}d(2N_{ant}-d)\log N \quad (5)$$

The obtained number of estimated sources (for the pre-correlation case: the impinging RFIs) served as input parameter for the DoA algorithm. For the DoA the well-known MUltiple SIgnal Classification (MUSIC) algorithm has been chosen [13]. As mentioned, the conformal antenna is not very well suited to be used with more efficient algorithms that perform well with planar symmetric arrays.

The MUSIC algorithm can be understood as the search performed through all possible array steering vectors, $\boldsymbol{a}(\theta, \varphi)$, to find those which are perpendicular to the space spanned by the non-principal, i.e. noise, eigenvectors. That is, to search, in the noise subspaces signal components which are orthonormal.

By applying the Eigen decomposition to the estimated covariance matrix, noise eigenvectors are obtained:

$$\boldsymbol{R}_{xx} \boldsymbol{V} = \boldsymbol{V}\boldsymbol{D}, \qquad (6)$$

where $\boldsymbol{R}_{xx}$ is the estimated covariance matrix, $\boldsymbol{D} = diag\{\lambda_0, \lambda_1, \dots, \lambda_{Nant-1}\}$ are the eigenvalues shorted in descending order, and $\boldsymbol{V} = [\boldsymbol{q}_0, \boldsymbol{q}_1, \dots, \boldsymbol{q}_{Nant-1}]$ are the corresponding eigenvectors. From those, only the ones belonging to the noise subspaces, that are the ones not belonging to all the d signals, D to $N_{ant}-1$, shall be used:

$$\boldsymbol{V}_n = [\boldsymbol{q}_D, \boldsymbol{q}_{D+1}, \dots, \boldsymbol{q}_{Nant-1}]. \qquad (7)$$

The orthonormal property of the signal steering vector in a noise subspace can be written as:

$$\boldsymbol{a}^H(\theta, \varphi)\boldsymbol{V}_n \boldsymbol{V}_n^H \boldsymbol{a}(\theta, \varphi) = 0. \qquad (8)$$

Then, the DoAs of the impinging signals are found locating the largest peaks in the known MUSIC spatial spectrum:

$$P_{MUSIC}(\theta, \varphi) = \frac{\boldsymbol{a}^H(\theta, \varphi)\boldsymbol{a}(\theta, \varphi)}{\boldsymbol{a}^H(\theta, \varphi)\boldsymbol{V}_n \boldsymbol{V}_n^H \boldsymbol{a}(\theta, \varphi)} \qquad (9)$$

SPOOFING / REPEATER DETECTION

The detection of counterfeit GNSS signals, which could be due to a non-properly installed GNSS repeater or to an intentional spoofing attack, is based on the approach introduced in [14]. The detection test metric is the ratio between the two largest eigenvalues of a combined post-correlation array covariance matrix. Since this information was not recorded by DLR's multi-antenna receiver during the measurement campaign, the corresponding signal processing was performed using the recorded snapshots of IF samples. The implemented post-processing signal chain is shown in Figure 4. First, the coarse and fine acquisition stages are performed to find GNSS signals in the snapshot. In the absence of strong radio frequency interference the signal acquisition delivers the estimated PRN code-phase and Doppler frequency for all visible, N_{sat}, GNSS signals. These estimations are typically sufficient to obtain stable strong correlation results over the entire length of the snapshot (30 ms or 50 ms). Each correlation result contains an in-phase, I, and a quadrature, Q, components. Both form a complex correlator output, $I + jQ$, for every l-th satellite signal in the n-th correlation epoch. The vector $\boldsymbol{x}_{l,n} \in \mathbb{C}$ of size $N_{ant} \times 1$ represents the combination of those correlator outputs. Then the post-correlation array covariance matrix for each acquired GNSS satellite, $\mathbf{R}_{xx,l}$, is computed by using the correlation results from all epochs, $\boldsymbol{x}_{l,n}, n = 1 \dots N_{corr}$, according to Eq. (3).
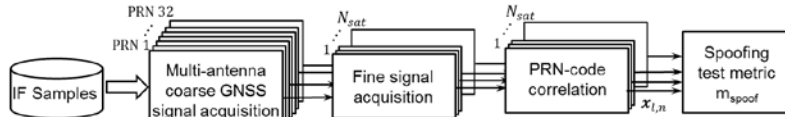

Figure 4. Block diagram of signal processing to obtain spoofing test metric.

The proposed spoofing detection metric is computed as:

$$m_{spoof} = \lambda_1 / \lambda_2 , \qquad (10)$$

where λ_1 and λ_2 are the largest and second largest eigenvalues of the combined array post-correlation covariance matrix:

$$\mathbf{R}_\Sigma = \sum_{l=1}^{N_{sat}} \mathbf{R}_{\mathbf{xx},l} \qquad (11)$$

As shown in [14], in the presence of a single spoofing or repeater source, the counterfeit signals appears in each satellite channel with the same spatial signature. Since the spatial signatures of the authentic satellite signals are significantly different, the signature of the spoofing/repeater signal dominates in the combined array covariance matrix, and hence a large eigenvalue is observed. However, also a RFI signal -not strong enough to block the signal acquisition- can be observed with the same spatial signature in all satellite channels. Distinguishing between the spoofing/repeater and RFI can be achieved by monitoring the estimated signal to noise ratios of GNSS signals during tracking. In this work the C/N0 value of the self-generated calibration signal has been used for this purpose.

RESULTS OF DETECTED INTERFERENCES

The presented results are mainly focused on the collected data from September 2017 to January 2018, which is the third and last phase of the measurement campaign. The data is analyzed following the proposed methodology, taking into account the metrics provided by both systems: the Snapshot Recorder and the GNSS Receiver prototype. For previous results please consult [6] and [7]. Due to space limitations not all results will be shown here, specifically: full month data is not going to be fully reported (only September, November and January). Also the L5/E5a band results are not shown, but they are counted in the classification.

During this phase the vessel has followed a route (see Figure 5) from the Andaman Sea, Sri Lanka, Arabian Sea, Red Sea (Jeddah), Suez Canal, Mediterranean sea (Italy, Spain), Suez Canal, Arabian Sea, Andaman Sea, Singapore, South China Sea (Hong Kong), East China Sea (Busan, Shanghai), Sea of Japan (Nakhodka), East China Sea (Qingdao, Shanghai), South China Sea (Hong Kong), Singapore, Sri Lanka, Arabian Sea (Jebel Ali), Andaman Sea and South China Sea.

Figure 5. Vessel route from September 2017 to January 2018 recorded by DLR's GNSS receiver prototype.

During this travel 39,045 snapshots were recorded, each one of them containing intermediate frequency samples of the L1/E1 and L5/E5a bands.

To assess the effects of the interferences on a non-multi-antenna receiver the estimated input power (obtained from the ADC snapshots values) on the 7th antenna element is used, because element number 7 is located flat on the top of the conformal array (see Figure 2). Moreover, it is assumed that the ADC power increments are due to interferences and they have a negative impact on the C/N0 of the tracked space vehicle (SV) signals.

As defined in previous work [6] [7] the detected RFI events in the reference element are grouped, according to its power, into three categories: weak, medium and strong. Weak RFIs are received with a power between 1 dB and 3 dB more than the interference-free signal; medium RFIs are received with between 3 dB and 5 dB more; finally strong interferences are received with more than 5 dB respect to the non-interference case. The complete summary of the detected RFIs along the 3rd phase of the campaign are summarized in Table 1. As it will be shown, 95% of the strong RFIs are due events occurring on January.

Table 1. Number of potentially significant intterferences

type	Number of RFI events		
	C/N0 (dB)	L1	L5
weak	$\Delta C/N_0 \in [-1, -3[$	287	380
medium	$\Delta C/N_0 \in [-3, -5[$	191	192
strong	$\Delta C/N_0 \leq -5$	2381	3201

a. September Results

The L1/E1 interference results for September are now shown. Figure 6 displays the estimation of impinging power on the equivalent single element antenna receiver (7th element of the conformal antenna) as recorded by the Snapshot Recorder. Figure 7 confirms the validity of the data, by displaying the pre-correlation eigenvalues obtained with the (parallel system) GNSS receiver.
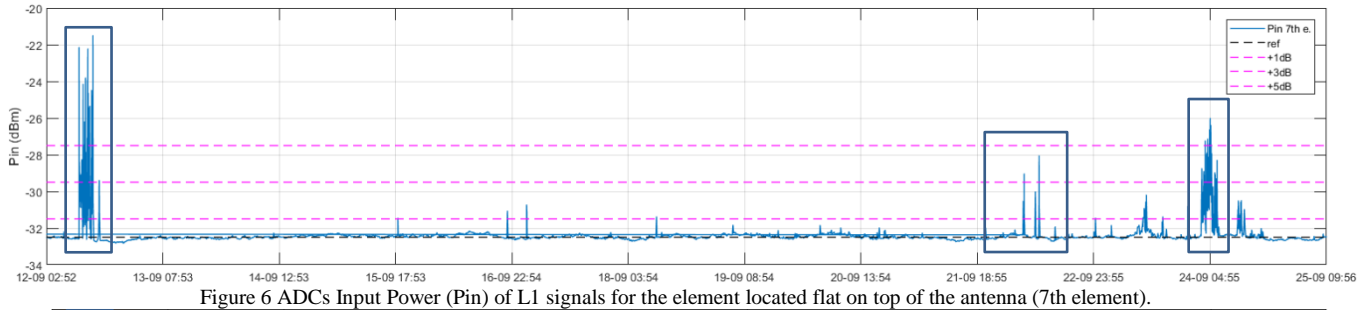

Figure 6 ADCs Input Power (Pin) of L1 signals for the element located flat on top of the antenna (7th element).
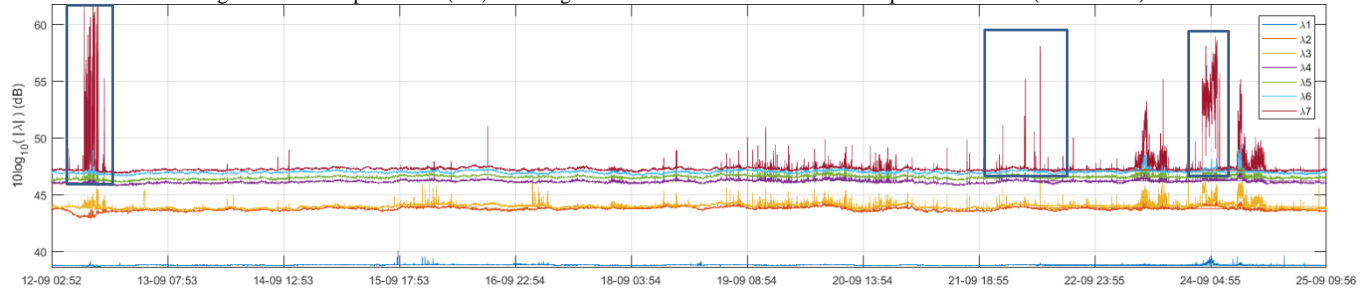
Figure 7 GNSS receiver Eigenvalues for the L1 pre-correlation data.

Three groups of big RFI are clearly visible: September 12th; 22nd, and 24th.

Regarding September 12th some initial discussion was started in [6]. For completeness: Figure 8 shows the RFIs impact on Input Power measured at the reference element. The corresponding Eigenvalues appear in Figure 9.

In [6] it was shown that the big RFI was capable of bringing out of tracking most of the SV (Figure 10), even with the extra protection provided by the post-correlation beamforming, in some cases the receiver stopped providing a valid position (see Figure 12), velocity and time.
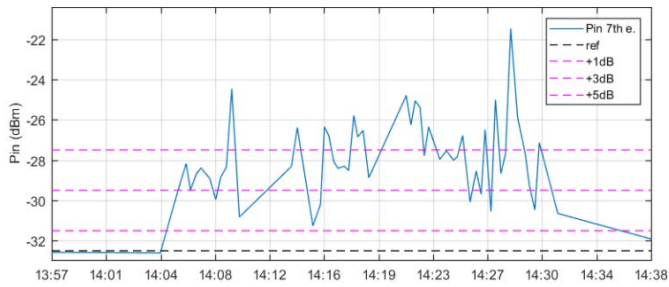
Figure 8. ADC Input Power antenna element #7 (September 12th).
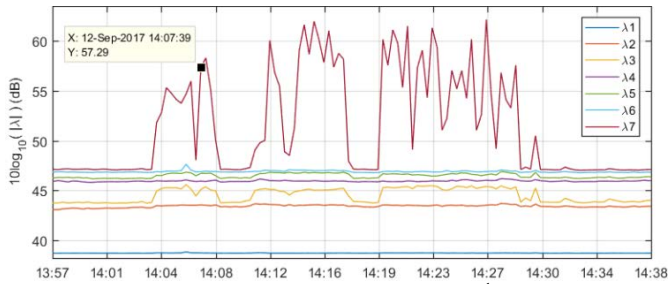
Figure 9. Eigenvalues (September 12th).
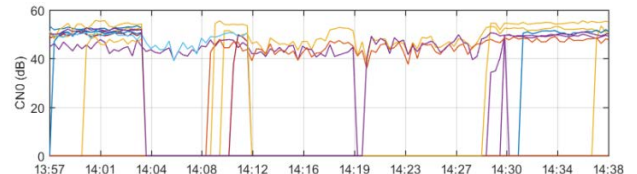
Figure 10. SV tracking.
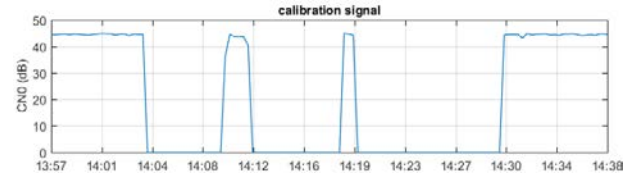
Figure 11. Calibration Signal.
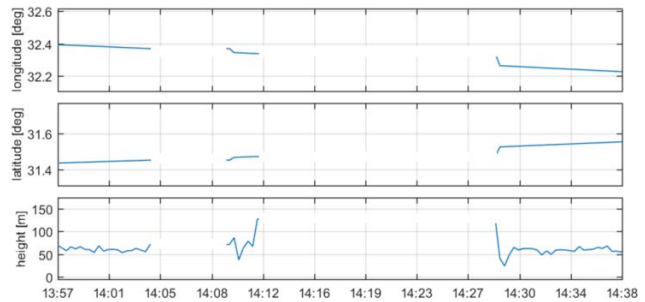
Figure 12. Position provided by the receiver.

Also, the use of the calibration signal as a valid discriminator between interference and obstruction (e.g. bridges) was demonstrated. When the receiver stops tracking the calibration signal (Figure 11), it can be confirmed it is under interference.

The argument of using the tracking of the calibration signal will be later proposed to provide a discriminator between interference and spoofing/repeater.

Regarding the events on September 12th, the power spectral density estimation of a snapshot at 14:07h shows a narrow signal, very alike to be Continuous Wave (CW) interference (see Figure 13). However the direct Fast Fourier Transform (FFT) of the same data displays a narrow Additive White Gaussian Noise (AWGN) signal (see Figure 14). The AWGN signature is not comparable to other detected AWGN RFIs: it spreads its high power in a very narrow frequency band, which is very close to the L1/E1 central frequency.
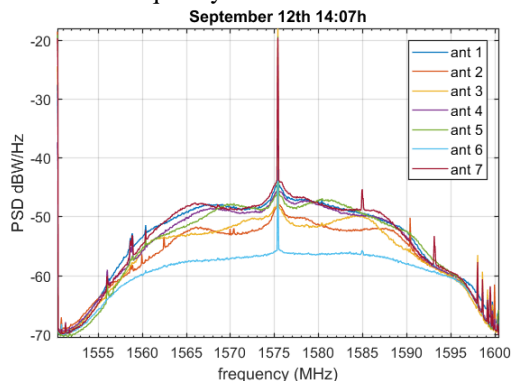
Figure 13. Power Spectral density estimation.
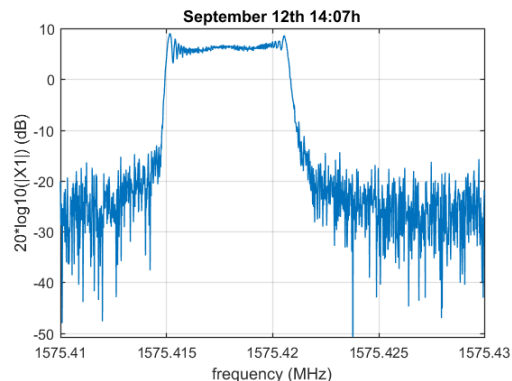
Figure 14. Direct FFT of the snapshot.

By making blocks of samples within the snapshots and looking at several snapshots one after the other, the RFI can be characterized as a frequency sweeping RFI with a triangular or saw-tooth shape (Figure 15). The frequency sweeping RFI varies "slowly" precisely around the L1 center frequency. The displayed bandwidth is around 20 kHz. Unlike known Personal Privacy Devices (PPDs), see Figure 16:

a. it displays a narrower bandwidth;
b. the frequency initialization mechanisms differs: it bounces the frequency while usual PPDs tend to "reset" it;
c. it displays a much slower changing frequency than usual PPDs. In 50 ms of recorded snapshot, it is not possible to visualize a complete period, while for other known PPDs, in that same time hundreds of periods are completed.
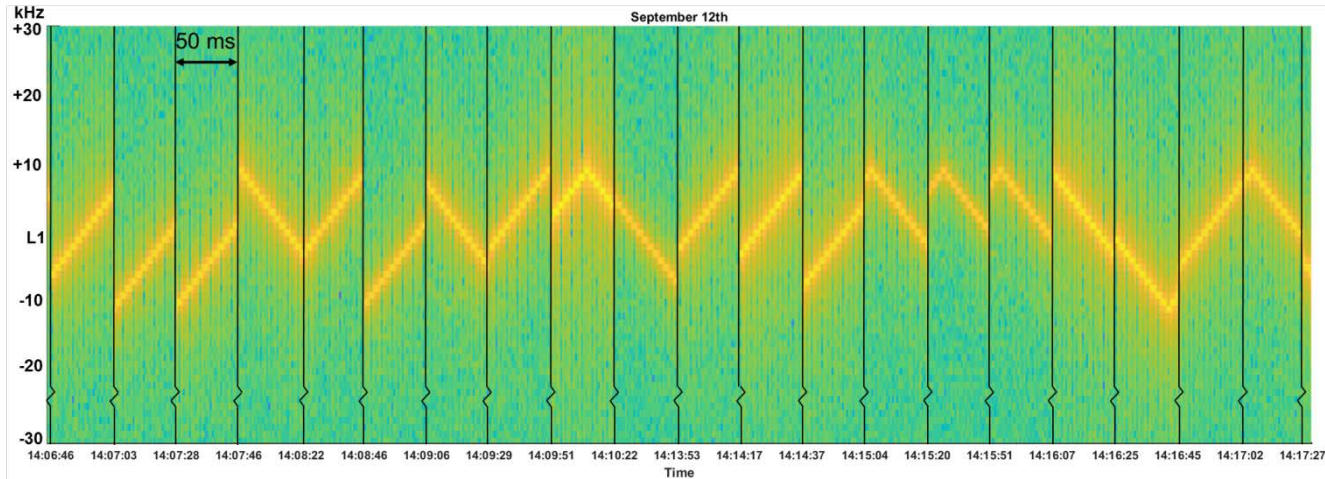
Figure 15. Spectrogram showing a frequency-sweeping RFI, ≈20 kHz bandwidth, exactly around L1.
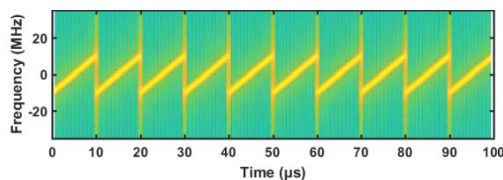
Figure 16. Spectrogram of typical PPD. Note: the bigger bandwidth, the fast frequency change (period of 10us) and the frequency "reset" after each period.

The whole event was present while the vessel was crossing the Suez Canal. It was detectable during approximately 60 km and lasting more than 5 hours.
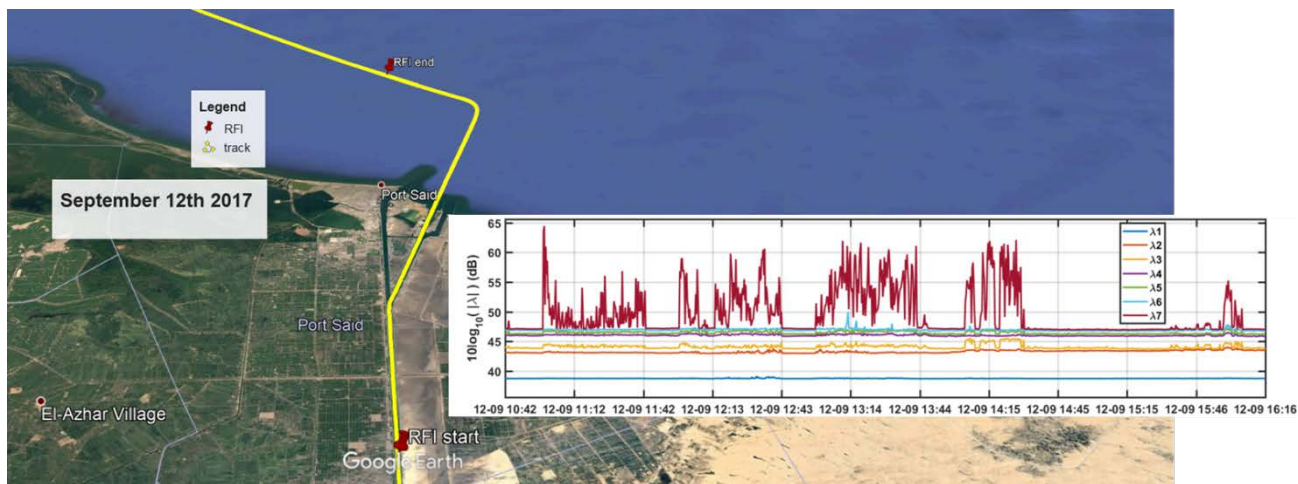
Figure 17. Vessel going north in Suez Canal. RFI detectable during approx. 60 km.
Inset: Eigenvalues during the 5 hours that the RFI was detectable.

Regarding the group of peaks on 22nd (Figure 18) the first remark shall be that it did not affect the robust receiver: PVT solutions were still obtained (Figure 19), yet it can be seen that the height suffered some stronger than normal alterations. From Figure 19 is noticeable that the event took place while the vessel was anchored: latitude, longitude and velocity remained constant.

Figure 18. Power peaks at antenna element #7 on September 22nd.
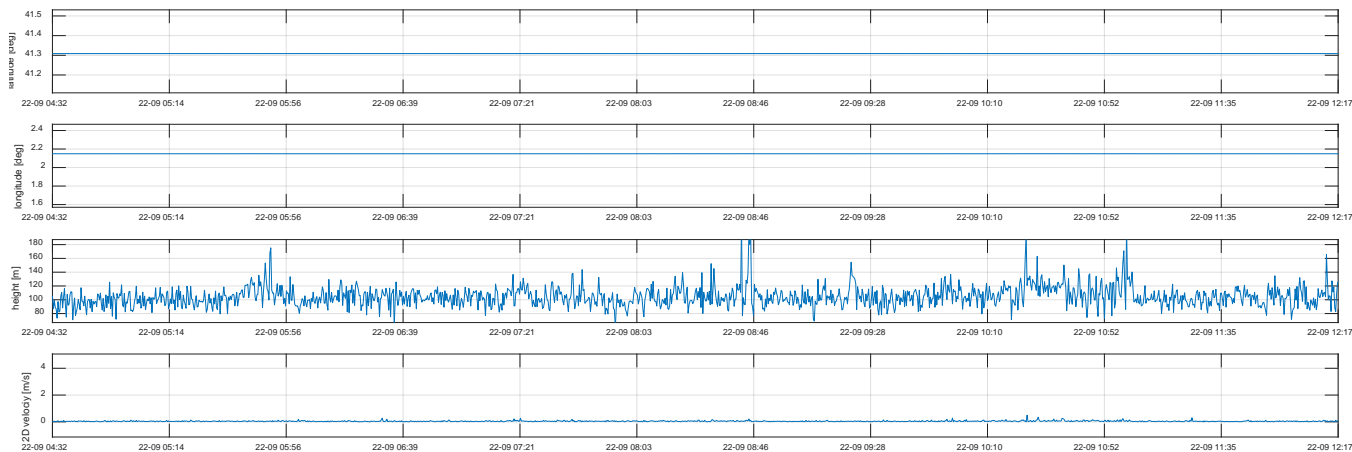
Figure 19. Position and Velocity

Each of the RFI events in Figure 18 feature different characteristics, which can be shown by looking at the recorded snapshots. For the ones happening around 6:35h or 9:21h, the spectral power density estimation (Figure 20) shows a strong CW-like RFI, which is not centered at the L1 band. The spectral analysis of the one recorded at 10:18h (Figure 21) shows a wideband RFI that affects the whole receiver band. To illustrate the effect of the RFI a comparison between an interference-free power spectral density of element 4 at 02:40h is shown versus the same element at 10:18h (Figure 22).

Which bandwidth is affected and how it is affected provide information about the RFI. This information can be corroborated by the eigenvalues (recorded in the Receiver and not the Snapshot Recorder), which show only one affected eigenvalue for the first events; whilst for the wideband RFIs more eigenvalues appear altered.
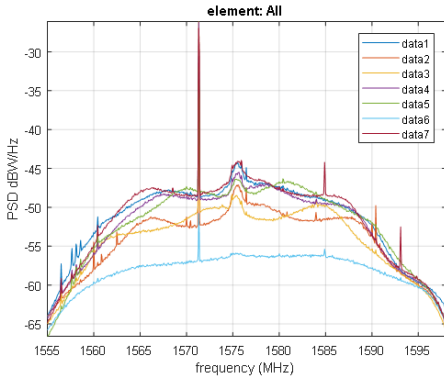
Figure 20. CW-like RFI. Sep 23rd; 6:35h:
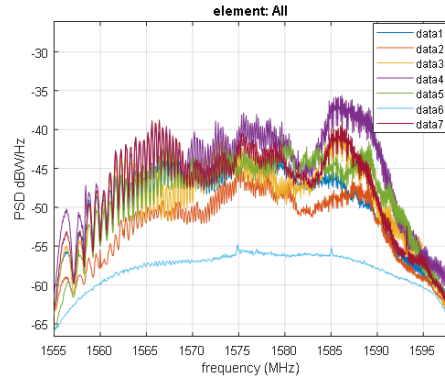
Figure 21. Wideband RFI. Sep 23rd; 10:18h:
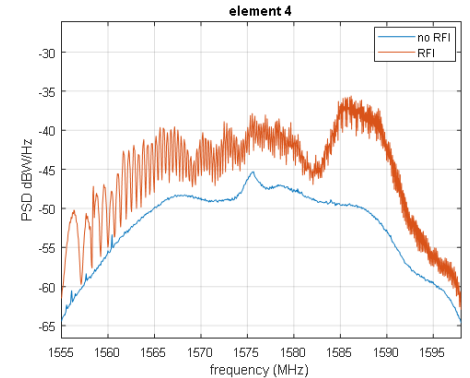
Figure 22. Sep 23rd; no RFI vs WB RFI at 10:18h

For evens occurred on 24th no results are going to be presented due to the space limitation. They seem similar to the earlier recorded events on 22nd (Figure 20): the ship was also anchored; some recorded RFI were received with more power; and some have its frequency centered at different locations around L1/E1.

b. November Results

The results obtained for November provide a good basis to start shaping a threat model for the navigation maritime domain. In November the vessel stayed at port near Shanghai, traveled north-east across the Sea of Japan reaching the Gulf of Nakhodka, where it spent some time near the coast. It returned back setting course to Busan, where it arrived on December. This route can be broken, according with the position and velocity (see Figure 23) into 3 regions: I) within Shanghai limits (anchored or moving out); II) traveling to north-east; III) within the Gulf of Nakhodka (not in harbor). By looking at the detected events (Figure 24), each region can be mapped with the detected RFIs. The results represent quite well observations made other months. Region I represents the case of an important harbor, with lot of sea and ground traffic and many detected events. Region II is a sea travel (in this case a very short one) where a few events are detected. Region III covers the case where the vessel in not in a big harbor but near the coast, not so many RFIs as in region I, but still some events are recorded.
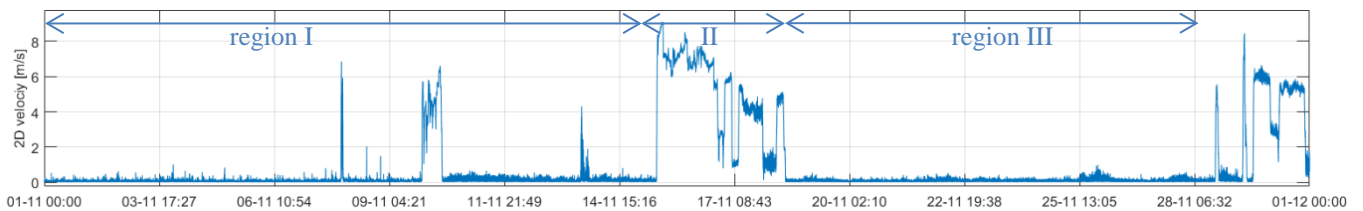
Figure 23.2D velocity of the vessel during November 2017.
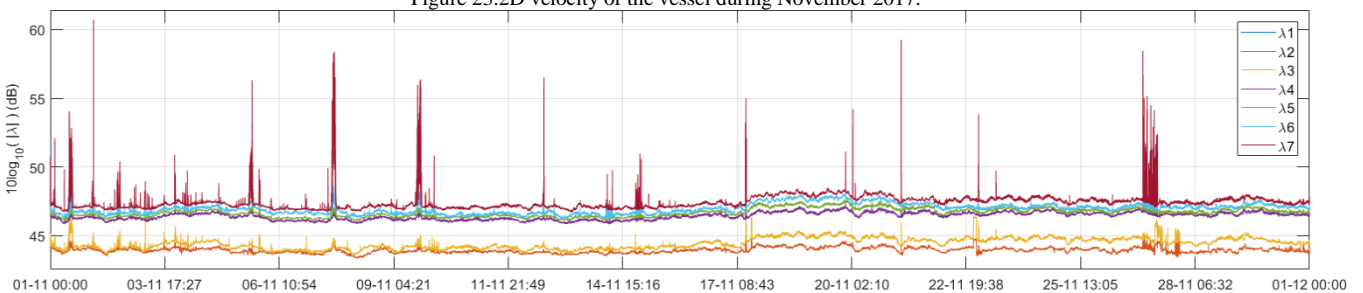
Figure 24 GNSS receiver Eigenvalues for the L1 pre-correlation data over November 2017.

Most of the recorded RFIs fall either into the CW type, like the one displayed in Figure 20, with frequency peaks close to the L1/E1; or the AWGN type, like in Figure 21. Some are, however, quite different. As an example, on 21st and 23rd (Gulf of Nakhodka) two signals that do not fall into those categories were recorded. These signals (Figure 25 and Figure 26) are centered at 1563.5 MHz (11.92 MHz below the L1 central frequency). They are much stronger than the navigation signals: the PSD shows an Interference to Noise ratio (I/N0) of 25 dB. Despite its power the signal is not affecting the DLR's GNSS receiver, but it is still within the L1 band limits. L1 band should be free of such events since it is for navigation use only.

The event duration was recorded for 15 minutes on November 21st and 19 minutes on the 23rd. The occupied bandwidth is difficult to establish, since a single snapshot (30 ms) does not seem to contain any full period. From the current available data, it is assumed to be smaller than 2 MHz.
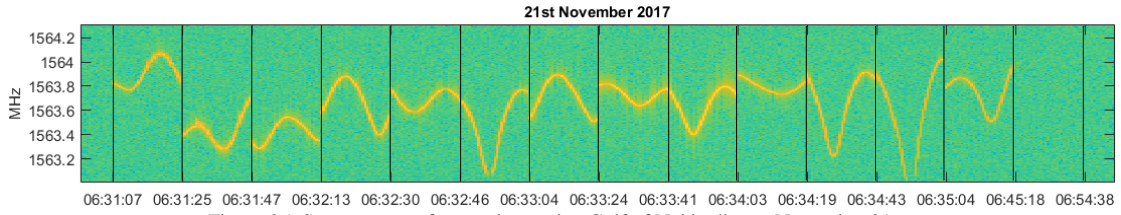
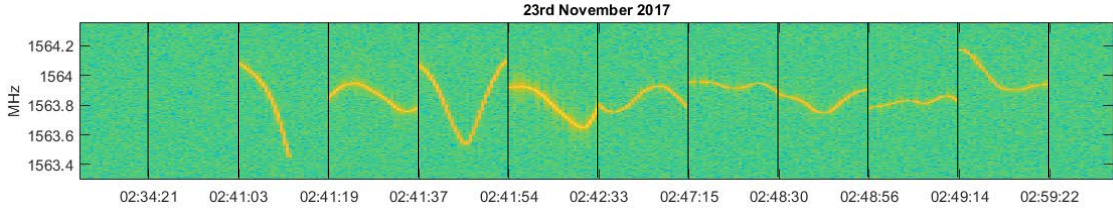Figure 25. Spectrogram of event detected at Gulf of Nakhodka on November 21st.

Figure 26. Spectrogram of event detected at Gulf of Nakhodka on November 23rd.

c. January Results

The results obtained on January 2018 are now broadly described. Specially, from January the 12th on, when a large RFI is detected during more than 6 days (Figure 27). The receiver stopped delivering a valid PVT on 12th at 14:52h (see the calibration tracking metric in Figure 28). Shortly before losing its capabilities, the receiver reported its position entering Jebel Ali port (Dubai, United Arab Emirates). The receiver provided its next valid position on the 23th, at the Laccadive Sea (south of India, close to Sri Lanka), the metrics show strong RFIs and the position was lost again on 27th. The I/N0 is 45 dB, i.e. the interference is 45 dB bigger than the valid navigation signals (see Figure 29). It is composed of four peaks centered on 1585 MHz and another wider RFI around 1588 MHz. The four peaks are always present (see Figure 30) while the wider RFI appears intermittently. For L1, 95% of the strong RFIs reported on Table 1 are due to the January events.
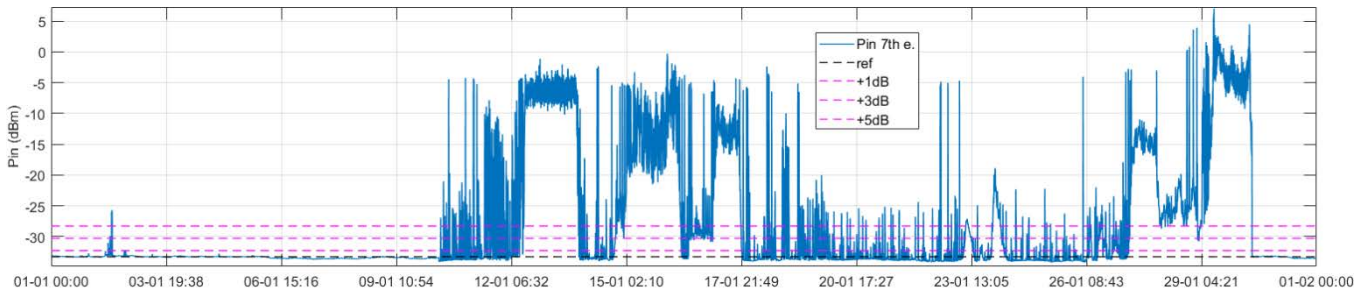
Figure 27. ADCs Input Power (Pin) of L1 signals for the element located flat on top of the antenna (January 2018).
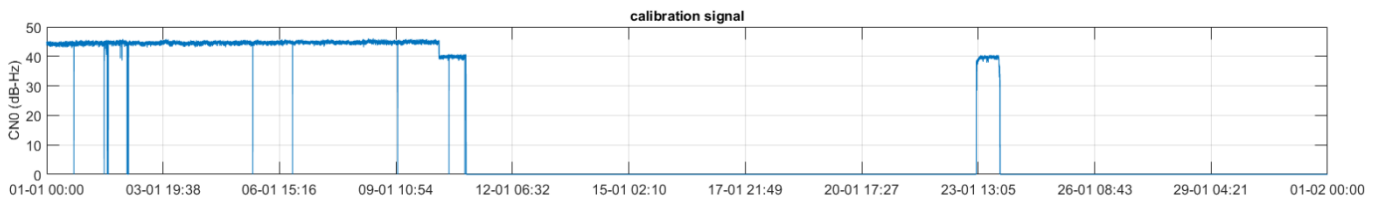
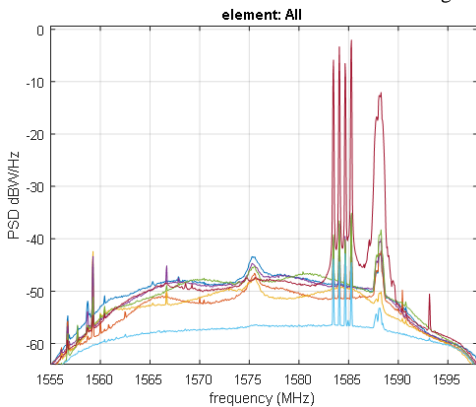Figure 28. Tracking of the calibration signal (January 2018).

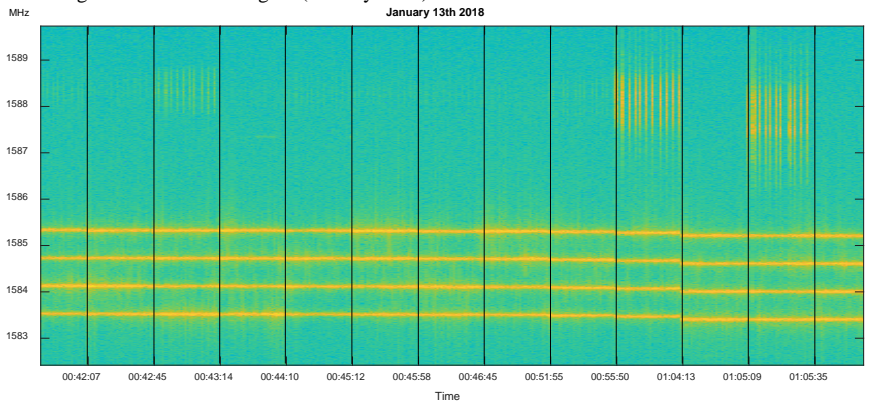Figure 29. PSD on January 13th at 00:55h

Figure 30. Spectrogram extract of RFI detected several days during January 2018.

RESULTS OF DIRECTION OF ARRIVAL

In order to perform a successful DoA with MUSIC at least two issues shall be taken into account: the variation of the elements in the array; and the phase differences from the elements to the ADCs, due to the tolerances of all the components along the parallel data paths (cable, Frontend channels components, etc.).

To correct for antenna elements, the simulated antenna patterns are used. Differences between simulated and measured patterns and the consequently use of measured antenna patterns to compute DoA are an ongoing task.
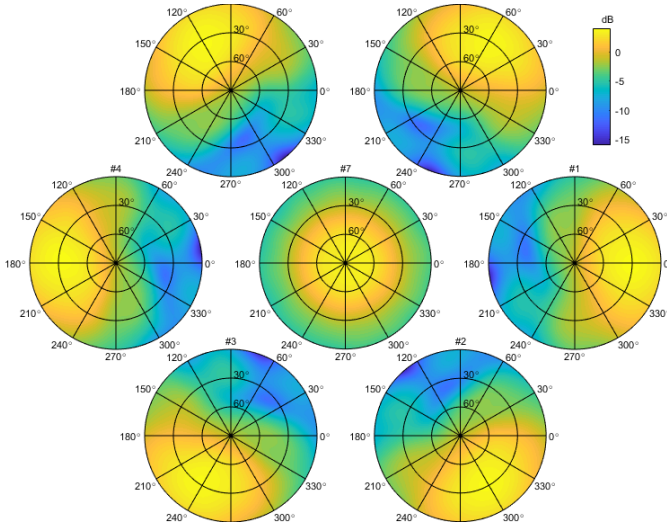
Figure 31. Simulated gain patterns for the conformal array.
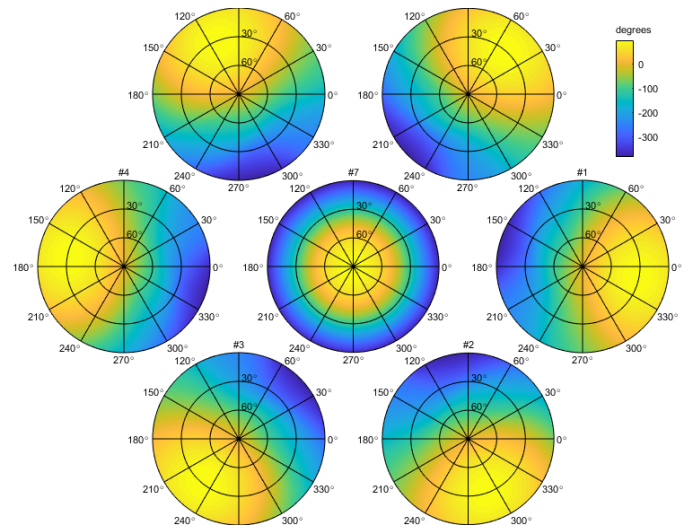
Figure 32. Simulated phase patterns for the conformal array.

To correct the differences in the elements along the data path, the calibration signal is used. Once the self-generated PRN is visible after correlation, the phase differences of all channels with respect to channel 7 are calculated. The phase difference is stable during long periods of time (Figure 33), enabling the use of the calibration values as time independent coefficients.
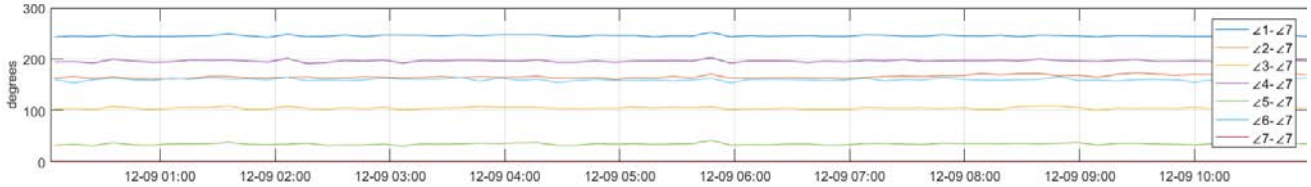

Figure 33 Phase differences (respect to channel 7) provided by the Calibration signal.

With both corrections the MUSIC results at three different times on September 12th (11:00h, 12:37h and 13:11h) are shown (Figure 34, Figure 35 and Figure 36 respectively). Note that, for the first two, a clear signal is detected around 110 degrees elevation (zero degrees represents zenith), or equivalently 25 degrees below the horizon. However the third measurement shows a not very realistic 60 degrees below horizon. It is expected to receive RFI from low elevations, and with the antenna mounted at around 50 meters above the sea level, it can be that the algorithm shows a suboptimal performance. This is still an ongoing work.
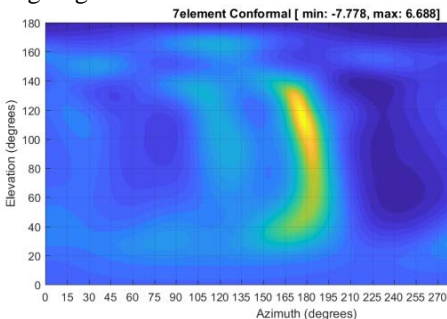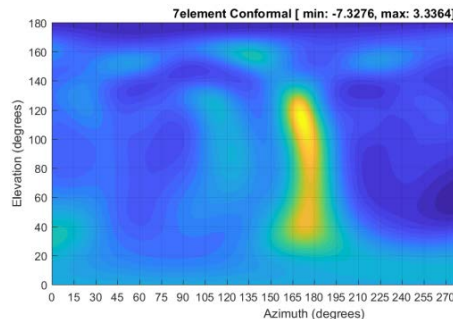

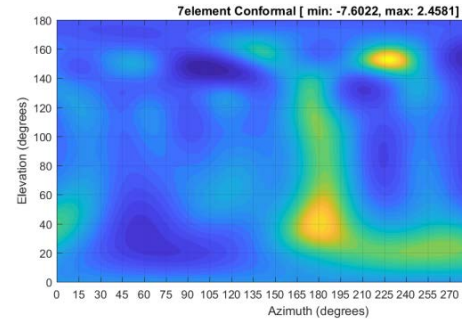Figure 34. (P1) DoA at 11:00h

Figure 35. (P2) DoA at 12:37h

Figure 36. (P3) DoA at 13:11h

For now it makes sense to focus on the azimuth alone. Assuming the source of the RFI is static; a proportional change in azimuth due to the vessel movement is expected. At the referred times the ship course was up north crossing the Suez Canal. In Figure 37 the three evaluated time points are shown along the route. The exactly heading of the vessel is -unfortunately-unknown. However the orientation of the array in the vessel is known. Also the estimated signal impinging power on each

array element is available. Therefore one could try to match the estimated DoA results, with the coarse "direction" indicated by the element on the circular array that receives the highest signal power. The following figures sketch this effort. On then the dashed orange line represents the vessel direction vector; the green line is the x axis of the array; the orange colored element is the one receiving the highest power; and the DoA estimated azimuth is displayed in black with an arc. Figure 38 sketches point one (P1), where the matching between the highest power element, number 4, and the DoA azimuth are quite good. In Figure 39 the second point (P2) shows a suboptimal matching; the highest power is received in element 5, what would indicate that the DoA estimation falls short. In Figure 40 the third point (P3) displays a good matching, both array elements show similar power (element 4 receives slightly more power than 5) and the DoA azimuth estimation seems to agree.

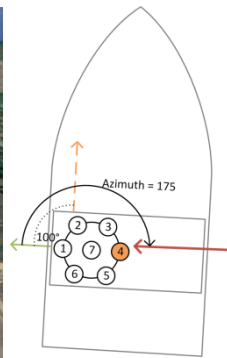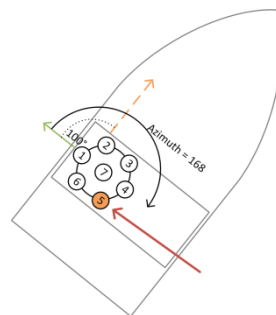Figure 37. RFI DoA analysis at three points in the Suez Canal.   Figure 38. P1 sketch.   Figure 39. P2 sketch.   Figure 40. P3 sketch.
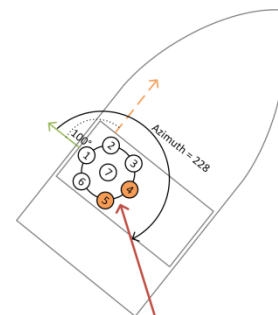
RESULTS OF SPOOFING / REPEATER DETECTION

Figure 41 shows the simulation results for the spoofing detection method. The scenario simulates a single spoofing source, with a power -at the receiver tracking loops- 3 dB higher than the authentic GNSS signals. It can be observed that the proposed test metric (m_{spoof}) significantly changes when the spoofing is active, therefore is suitable to be used as a detection method.
Figure 42 shows how the test metric changes with the increasing relative power of the spoofing signals. Based on these simulation results, the detection threshold was set to a value of 5 in the spoofing analysis tool processing the snapshots.
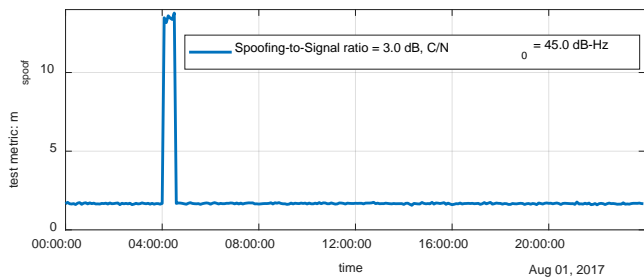

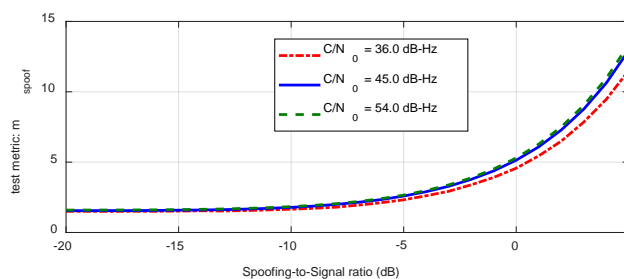Figure 41. Spoofing metric on simulated data.   Figure 42. Spoofing metric variation respect to the Spoofing to Signal ratio.

In the practice, the proposed spoofing test metric should be supported by another metric. That is so because a RFI signal - not strong enough to block the signal acquisition - can also be observed with the same spatial signature in all satellite channels. Distinguishing between the spoofing/repeater and RFI can be achieved by monitoring the estimated C/N0 of the self- generated calibration signal.
Figure 43 shows the results obtained after analyzing two sets of snapshots: August 1st, 2017, an interferences free day; and September 12th of 2017, where a strong RFI is present. It can be observed that the measured C/N0 values of the calibration signal starts do drop at the same time as the proposed detection metric increases. In this case, the degradation of C/N0 values allows to clearly classify the interference occurred on September 12th as RFI and not as spoofing/repeater.
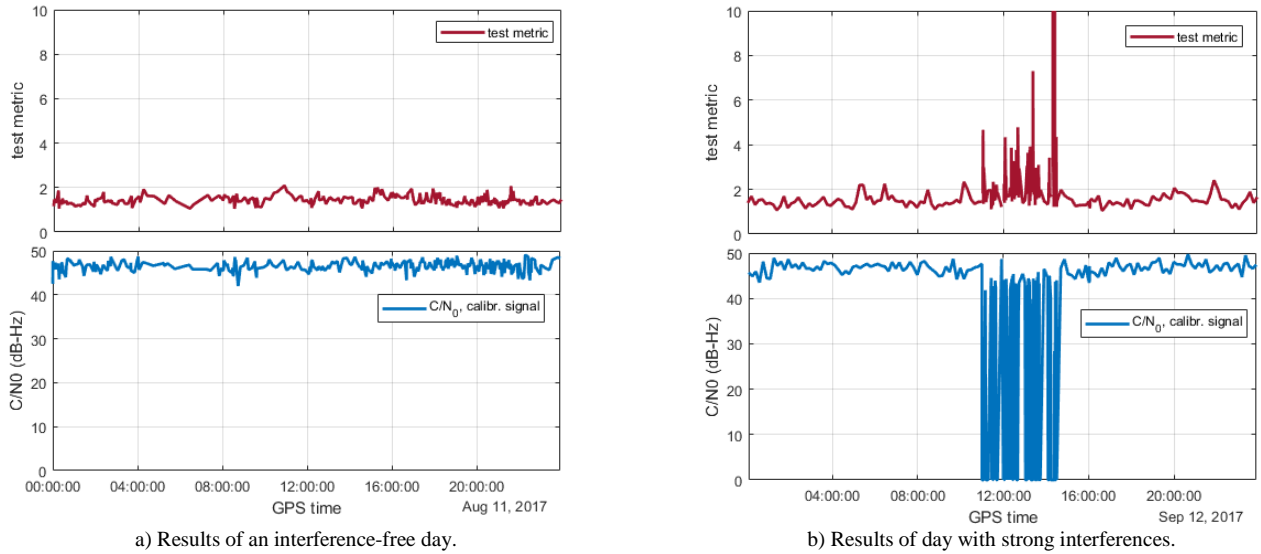
| a) Results of an interference-free day. | b) Results of day with strong interferences. |

Figure 43. Spoofing detection test metric and the corresponding C/N0 of the calibration signal.

DISCUSSION AND CONCLUSIONS

An RFI international maritime measurement campaign has been performed to detect and record snapshots of IF samples, containing representative RFI signals. A post-processing detection and analysis methodology has been presented and its validity has been verified with results. The results contain a big number of detected RFI events, some of them with considerable power values.

In addition, detailed analysis of some exemplar events - occurring in L1/E1 band - have been carried out. Any L1/E1 detected interference deserves particular attention. Such interferences, potentially impacting the GNSS applications, have been recorded and their effects evaluated. It was shown that they can make the GNSS service unavailable even with extra protection measures, like post-correlation beamforming.

In addition a Direction of Arrival technique for conformal arrays, based on MUSIC, has been proposed. Two modifications to the MUSIC algorithm have been applied. First, antenna patterns of each array element are used to correct the gain and phase of the steering vectors. And second, to deal with the phase differences in each parallel data path (from antenna to ADC), a self-generated signal is being injected into the antenna electronics, from there is tracked in the receiver as any other navigation signal. The tracking of the signal enables to compute coefficients to calibrate out the phase differences in the channels. The DoA is still an ongoing work. Some requirements of the DoA, like finding the number of signals to be searched, have been proved to be a challenging task even if recognized source detection tests have been used.

Also a method to detect spoofing/repeater events have been put to test. While no results have been yet obtained from the small part of already processed snapshots, simulation results are encouraging. Hence some results shall be available when the processing advances.

Though not claiming to be an exhaustive analysis of all possible interference events in the maritime domain, the presented work shows however a first world-spanning analysis, a general view including strong and weak signal, and it highlights the most frequently occurring ones, adding the Direction of Arrival information and Spoofing detection. The authors believe this information will be a valuable input for the development of corresponding interference threat models for the maritime GNSS applications and countermeasures.

ACKNOWLEDGMENTS

REFERENCES

[1] "Assessment of Radio Frequency Interference Relevant to the GNSS (RTCA/DO-235A)", RTCA, Inc., 2002.

[2] A. Parkins, A. Grant, and P. Cross, "The impact of new signals on precise marine navigation - initial results from an experiment in Harwich harbour.", 2008.

[3] A. Grant, P. Williams, N. Ward, and S. Basker, "GPS Jamming and the Impact on Maritime Navigation", Journal of. Navigation, vol. 62, no. 2, pp. 173–187, 2009.

[4] J. R. Clynch, A. A. Parker, R. W. Adler, and W. R. Vincent, "System challenge—The hunt for RFI—Unjamming a Coast Harbor", GPS World, pp. 16–22, 2003

[5] "Development of an e-Navigation strategy implementation plan.", IMO Sub-Committee on Safety of Navigation, 2011. And also "MSC 85/26/Add.1 Annex 20".

[6] Emilio. Pérez. Marcos et al., "Interference awareness and characterization for GNSS maritime applications," 2018 IEEE/ION Position, Location and Navigation Symposium (PLANS), Monterey, CA, USA, 2018, pp. 908-919.

[7] A. Konovaltsev, E. Pérez Marcos, et al, "Interference Detection and Characterization with an Array based GNSS Receiver using Conformal Antennas in Maritime Environments", Proc. of ION GNSS+ 2017, Portland, OR, USA, Sept. 2017, pp. 2795-2811.

[8] M. Cuntz, A. Konovaltsev, et al, "Lessons Learnt: The Development of a Robust Multi-Antenna GNSS Receiver," in Proc. of ION GNSS 2010.

[9] M. Cuntz, A. Konovaltsev and M. Meurer, "Concepts, Development, and Validation of Multiantenna GNSS Receivers for Resilient Navigation," in Proceedings of the IEEE, vol. 104, no. 6, pp. 1288-1301, June 2016.

[10] IALA, "IALA Recommendation R-129 on GNSS Vulnerability and mitigation measures." pp. 1–19, 2008.

[11] Stephan V.Schell, William A.Gardner, "High-resolution direction finding", Handbook of Statistics Volume 10, 1993, Pages 755-817.

[12] J.Rissanen, "Modeling by shortest data description", Automatica, Volume 14, Issue 5, September 1978, Pages 465-471.

[13] R. Schmidt, "Multiple emitter location and signal parameter estimation", IEEE Transactions on Antennas and Propagation, vol. 34, no. 3, pp. 276-280, Mar 1986.

[14] M. Appel, A. Konovaltsev, M. Meurer, „Joint Antenna Array Attitude Tracking and Spoofing Detection based on Phase Difference Measurement", ION GNSS+ 2016, Portland, OR, USA, Sept. 12-16, 2016.