GNSS Navigation Threats Management on-Board of Aircraft

Elena Simona LOHAN*[,1], Ruben Morales FERRE[1], Philipp RICHTER[1],
Emanuela FALLETTI[2], Gianluca FALCO[2], Alberto DE LA FUENTE[3]

*Corresponding author
[1]Tampere University, Finland,
elena-simona.lohan@tuni.fi*, ruben.moralesferre@tuni.fi, Philipp.richter@tuni.fi
[2]Links Foundation, Italy,
emanuela.falletti@linksfoundation.com, gianluca.falco@linksfoundation.com
[3]GMV, Spain,
afuente@gmv.com

DOI: 10.13111/2066-8201.2019.11.3.10

Received: 12 July 2019/ Accepted:12 August 2019/ Published: September 2019

TandemAEROdays19.20 – Bucharest event
Category: D. AIR TRAFFIC MANAGEMENT, Session: D4. Enabling aviation infrastructure
May 27-30, 2019 – Romanian Palace of Parliament

Abstract: *This paper proposes low-complexity measures to be deployed on most aircraft to enable the management of Global Navigation Satellite Systems (GNSS) interference, and in particularly of jamming and spoofing threats, in order to reach the Flightpath2050 safety and security targets. It is known that, if there is a jamming interference and GNSS navigation is lost, a disruption will be caused, requiring the likely intervention of Air Traffic Control. Also, the presence of a spoofing signal is a serious security threat with a potentially catastrophic impact on the safety of the aircraft and on any other ground infrastructure. Through our jamming and spoofing detection and localization stages, based on minimal additional infrastructure, we will reduce the time required to detect and localize an interfering source and, therefore, the time required to mitigate it and restore the nominal traffic operations. Our solutions will also improve the safety of the Air Traffic Management system. Moreover, the deployment of our solution, with its capability of localizing an interfering device, could be a deterrent to any agent interested in intentionally generating a jamming or spoofing signal, and so will reduce the likelihood of this type of interference events.*

Key Words: *Air Traffic Management (ATM), aviation infrastructure, Global Navigation Satellite Systems (GNSS), interference management, jamming, spoofing, commercial aircraft*

1. INTRODUCTION

GNSS are currently the most precise outdoor localization and navigation systems with global coverage, even if they have not been adopted yet as the main navigation instruments in aviation domain.

The aircraft navigation still relies on traditional navigational aids, such as Distance Measuring Equipment (DME), Instrument Landing Systems (ILS), or Tactical Air Navigation System (TACAN), but there have been already discussions and proposals by the

International Civil Aviation Organization (ICAO) to adopt GNSS in aviation as main navigation tool in the not-too-distant future.

With the increasing importance of GNSS in many safety-critical domains, such as the aviation domain, the amount of interference, and in particular the intentional or malicious interference in GNSS bands is also on the rise [7], [31].

Currently, there are four GNSS systems, partially or fully functional, and they operate in the frequency bands shown in Table 1.

Table 1. Frequency bands used in current GNSS systems

GNSS system (Country)	**Status**	**Used frequency band terminology and corresponding carrier frequency[GHz]**
GPS (US)	Fully operational, 31 satellites on sky	L1: 1.57542 L2: 1.22760 L5: 1.17645
Galileo (EU)	Partially functional, 22 satellites on sky	E1: 1.57542 E5a: 1.17645 E5b: 1.20714 E6: 1.27875
Glonass (Russia)	Fully operational, 24 satellites on sky	G1[1]: 1.59806 − 1.60931 G2:1.24293 − 1.25168 G3:1.189 − 1.214
Beidou (China)	Partially functional, 33 satellites on sky	B1: 1.561098 B2: 1.20714 B3: 1.26852

The goal of this paper is to propose a novel concept for GNSS interferences management, including the detection and localization of jamming and spoofing on-board the aircraft, based on existing aircraft equipment, with the target of minimizing the aircraft retrofit.

The on-board GNSS antennas are assumed to be placed on top of the aircraft fuselage and we will rely on the assumption that maximum three GNSS antennas are to be used to deal with interferences.

The considered scenario is depicted in Fig. 1, where we assume a single source of interference which is static or quasi-static.

The affected airplanes can be at ground (taxiing, parking), or in-flight mode (landing, taking off, in-cruise).

The scenario of main interest focuses on commercial airplanes, however the addressed solutions apply also to other aviation areas such as Unmanned Aerial Vehicles (popularly known as drones) or other aircraft types (helicopters, flying taxis, etc.).

The Air Traffic Control (ATC) in Fig.1 is the decisional-making unit with respect to the subsequent actions to the interference detection or localization.

The ground interferer can affect both landed planes or flying planes (approaching airport, in-cruise, or taking off).

[1] For Glonass, the carrier frequencies are given as an interval because Glonass relies on Frequency Division Multiple Access (FDMA) to separate the satellites on sky; all other GNSS system use Code Division Multiple Access (CDMA) and thus have a single carrier/center frequency.

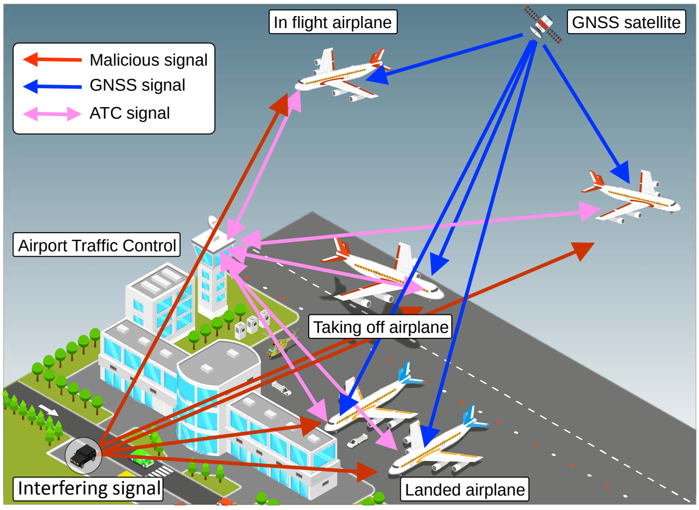


Fig. 1 Illustration of interference scenarios in an aviation application

The novelty of our approach comes from several angles: (i) proposing a three-step interference management solution relying in interference detection and direction finding algorithms; (ii) selecting and analyzing several interference detectors, namely three jamming detectors and two spoofing detectors, in order to offer a good tradeoff between complexity of implementation/minimal retrofit and detection performance; (iii) selecting and analyzing angle-of-arrival-based approaches for jamming and spoofing direction finding; and (iv) in-lab validation of the considered algorithms. The rest of the paper is organized as follows: Section 2 gives a brief overview of the considered interference types and their mathematical models; Section 3 presents our proposed three-step concept for interference management; Section 4 explains the considered interference management solutions and their placement with respect to the GNSS receiver chain blocks; Sections 5 and 6 present the studied detection and direction finding algorithms against jamming and spoofing, respectively; simulation results and in-lab validation results are supporting the discussions in these sections 5 and 6; Section 7 focuses on open challenges and future directions in this research field, and Section 8 summarizes the findings and presents the conclusions of this work.

2. INTERFERENCE TYPES

Interferences that can affect the frequency bands shown in Table 1 fall mainly in two categories:

- **Jamming**, i.e., intentional or unintentional Radio Frequency Interference (RFI), typically narrowband, sent on one or several of the carrier frequencies shown in Table 1. The jammers are typically located on ground, but aerial jammers are also possible [25]. Jammers can be divided into several classes, as detailed for example in [6]. The most common types of jammers are the amplitude-modulated (AM) single or multi-tone jammers (stationary, with constant single or multiple carrier frequencies) and the chirp jammers (non-stationary, with sweeping carrier frequency). Both AM and chirp jammers will be investigated in our studies.
- **Spoofing**, i.e., intentional fake GNSS-like signals interfering with the GNSS signals of interest. One particular category of spoofing is the meaconing-type of interference, which refers to the re-transmission of a GNSS signal captured from one or several GNSS

satellites in view; this re-transmission occurs with a delay and typically at a higher power (e.g., using an amplifier or a repeater) than the genuine GNSS signal. Spoofers can also be of several types, namely simplistic, intermediate, or sophisticated spoofers, as described in detail for example in [8] [27]. A meaconer or a repeater is one example of a simplistic spoofing attack, where a genuine GNSS signal is re-transmitted in the air, typically from a ground transmitter, at a higher power than the normal GNSS signal.

A generic mathematical modeling for an AM multi-tone jammer with K tones is given below

$$j(t)=\sum_{k=1}^{K}\sqrt{P_{J_k}}\exp\left(2\pi f_{J_k}t+\theta_{J_k}\right) \tag{1}$$

where $j(t)$ is the jamming signal, P_{J_k} is the power of the *k*-th jamming tone, *k=1, …K,* f_{J_k} is the frequency of the *k*-th jamming tone, and θ_{J_k} is the phase of the *k*-th jamming tone.

A generic mathematical modeling for the multi-chirp jammer is shown in eq. (2)

$$j(t)=\sum_{k=1}^{K}\sqrt{P_{J_k}}\exp\left(2\pi f_{J_k}t+\pi b_{J_k}\frac{f_{\max_k}-f_{\min_k}}{T_{sweep_k}}t^2+\theta_{J_k}\right) \tag{2}$$

with the additional parameters: b_{J_k} - a 0/1 flag indicated a downwards or upwards chirp for the *k*-th chirp, $f_{\min_k}/f_{\max_k}$ - the minimum and maximum sweeping frequency ranges for the *k*-th chirp, respectively, and T_{sweep_k} the *k*-th chirp sweeping period.

The single chirp (*K=1*) is typically the most encountered one in practice. The chirp bandwidth *B* is computed as $B=f_{\max_k}-f_{\min_k}$.

Regarding the simplistic spoofer and meaconer's models, as the spoofing cases of interest in this paper, eq. (3) reflects them

$$s(t)=\sqrt{P_S}\sum_{n}d_n c_n(t-\tau_{sp})\exp\left(2\pi\Delta f_S t+\theta_S\right) \tag{3}$$

where $s(t)$ is the spoofing/meaconer signal, P_S is the power of the spoofer, *n* is the navigation data bit index, d_n is the *n*-th data bit of the spoofer, $c_n(\bullet)$ is the pseudo-random code corresponding to the spoofed satellite and to the *n*-th data bit, τ_{sp} is the spoofer time delay, Δf_S is the spoofer Doppler shift, and θ_S is the spoofer carrier phase offset.

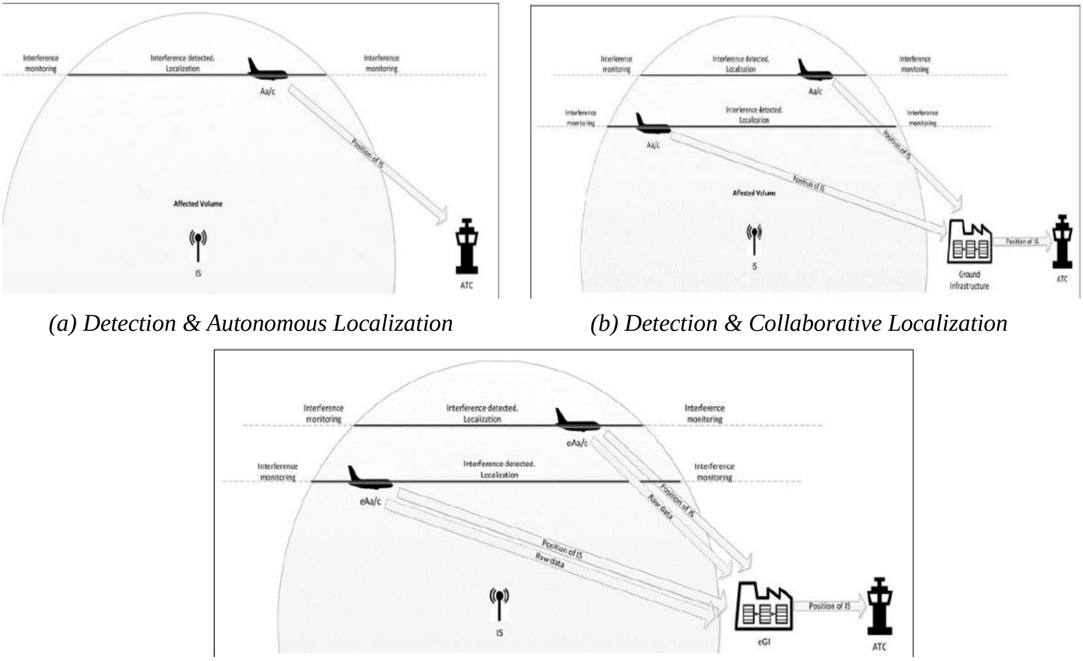
3. PROPOSED CONCEPT FOR INTERFERENCE MANAGEMENT

Our proposed three-step concept for interference management is depicted in Fig. 2:

1. *Detection & Autonomous Localization* step: this is the simplest and lowest complexity method to deal with an Interference Source (IS), as it is fully done at the Affected Aircraft (Aa/c) side. The on-board GNSS receiver endorsed with interference detection and localization engine reports the IS position to the Air Traffic Control (ATC), and the ATC takes further action regarding the interference management (e.g., sending warnings to aircraft in the affected areas, informing the aircraft to move to alternative or complementary localization/navigation solution or to send beam-steering nulls in the

direction or interferer, sending human force to disable the localized IS, etc.). This mode is completely autonomous, in the sense that the aircraft relies only on the data recorded on-board to localize the IS.

2. *Detection & Collaborative Localization* step: this is an intermediary-complexity action, involving at least two aircraft exchanging wireless information and being affected by the interference source. Both aircraft can detect and localize the interference source and the estimated locations are sent to the ATC for further consistency checks. The main difference of this mode of operation with respect to the previous step (Detection & Autonomous Localization) is the need of a ground infrastructure. The IS locations estimated by each aircraft are transmitted to the ground infrastructure, which may improve the estimate of the interference location thanks to the multiple sources of information (i.e. multiple aircrafts affected by the interference). The amount of data exchanged between the aircraft and the ground infrastructure is expected to be very small, thus the bandwidth required for data transmission is not very demanding.
3. *Detection & Enhanced Collaborative Localization* step: in this step, which also involves the highest complexity and the highest data transfer among the three considered steps, two or several affected aircraft send to ATC not only the estimated IS location, but also additional IS-related measurements, such as pre-correlation or post-correlation GNSS samples, pseudoranges, etc.). In this step, an enhanced IS detection and localization is done by the ground infrastructure. Due to the higher amount of measurements transmitted between the aircraft and ground infrastructure, a higher bandwidth is needed for this step compared to the first two steps. Also, due to the transmission delays, this step may not be done in real-time and the initial IS detection might need still to rely on the estimates done at steps 1 and 2.



(a) Detection & Autonomous Localization

(b) Detection & Collaborative Localization

(c) Detection & Enhanced Collaborative Localization

Fig. 2 Proposed concepts from interference management, from the lowest complexity/ full on-board processing in (a) to the highest complexity highest performance in (c)

The next section discusses various interference management solutions, with a focus on the interference detection and direction finding/ localization and presents our investigated solutions in more detail.

4. STUDIED INTERFERENCE MANAGEMENT SOLUTIONS

The algorithms existing in the literature for the interference detection and direction finding for both jamming and spoofing can be mainly grouped according to the receiver stages depicted in Fig. 3.

The front-end and pre-correlation techniques from Fig. 3 rely on Radio frequency (RF) or Intermediate Frequency (IF) samples, before or after the Analog-to-Digital Converter (ADC) from the RF chain. Examples of such techniques include the Automatic Gain Control (AGC) detector and time and frequency power detectors, which are investigated in more detail in the next section.

The post-correlation techniques rely on the outputs of the tracking channel in a GNSS receiver and they are typically more suited for interference mitigation than for interference detection. The last category of interference management methods are those at system-level or navigation domain, which rely on the pseudoranges computed by a GNSS receiver and on the signal from multiple satellites on sky. Examples from this category are the Sum-of-Squares detector and the Dispersion of Double Differences detector analyzed in more detail in Section 6.

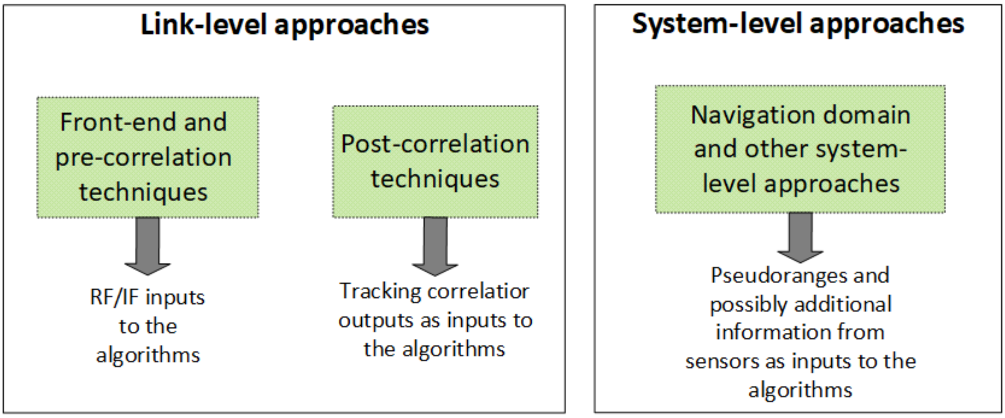

Link-level approaches
Front-end and pre-correlation techniques
RF/IF inputs to the algorithms
Post-correlation techniques
Tracking correlatior outputs as inputs to the algorithms
System-level approaches
Navigation domain and other system-level approaches
Pseudoranges and possibly additional information from sensors as inputs to the algorithms

Fig. 3 The three classes of the interference management methods

As mentioned in Section 3, the adopted interference management methods to support the three-step solution of Fig. 2 rely on interference detection and interference direction finding, assuming a minimal infrastructure on-board of aircraft (i.e., up to three GNSS antennas). The processing can be done either on the aircraft or at the ground infrastructure side, as depicted in Fig. 2.

First, based on literature studies, it has been observed that jamming detection algorithms are not efficient for spoofing detection and vice-versa, thus different approaches must be used to detect the jammers and the spoofers. Secondly, it has been also observed that in terms of interference localization, the best approaches for both jammer and spoofing direction finding are those based on angle of arrival measurements from at least three on-board antennas. Results are presented in the next two sections for jamming and spoofing, respectively.

5. JAMMING DETECTION AND DIRECTION FINDING RESULTS

The following simulation scenarios have been analyzed, as given in Table 1. We are focusing on the European GNSS system, Galileo, but similar results have been obtained also with GPS signals. The considered jamming types fall into the multi-tone and chirp jammer categories, as described in eqs. (1)-(2), as these jammer types are the most encountered in practice and also in research papers [14][22]

Table 2. Simulation scenarios for the jammer detection and direction finding algorithms

Scenario Number	Scenario Name	GNSS signal	Jammer Signal
#1	GAL E1 + Chirp 1 MHz	Galileo E1	Chirp 1 MHz, see eq. (2) with K=1 and B=1 MHz
#2	GAL E1+ Chirp 40 MHz	Galileo E1	Chirp 40 MHz, see eq. (2) with K=1 and B=40 MHz
#3	GAL E1+ Dual-chirp 10 MHz & 20 MHz	Galileo E1	Dual Chirp (10 MHz up-chirp and 20 MHz down-chirp), see eq. (2) with K=2
#4	GAL E1 + Triple AM-tone	Galileo E1	Triple AM tone, see eq. (1) with K=3
#5	GAL E5 + Chirp 1 MHz	Galileo E5	Chirp 1 MHz, see eq. (2) with K=1 and B=1 MHz
#6	GAL E5+ Chirp 40 MHz	Galileo E5	Chirp 40 MHz, see eq. (2) with K=1 and B=40 MHz
#7	GAL E5+ Dual-chirp 10 MHz & 20 MHz	Galileo E5	Dual Chirp (10 MHz up-chirp and 20 MHz down-chirp), , see eq. (2) with K=2
#8	GAL E5 + Triple AM-tone	Galileo E5	Triple AM tone, see eq. (1) with K=3

Fig. 4 shows a comparison of the effective Carrier-to-Noise ratio (CN0) for Galileo E1 and E5 frequency bands for different jammer types. The real CN0 (i.e., in the absence of jamming) is also shown for comparison purposes. Clearly, when the jammers are present, the effective CN0 is decreased considerably. As can be noticed looking at Fig. 4, Galileo E5 signals deal better with the considered interferences than Galileo E1 signals. Considering the same level of Jammer-to-Signal Ratio (JSR), Galileo E5 shows about 10 dB of higher effective CN0 during the whole set of simulated JSR. If we compare the different jammer types, no significant differences are seen.

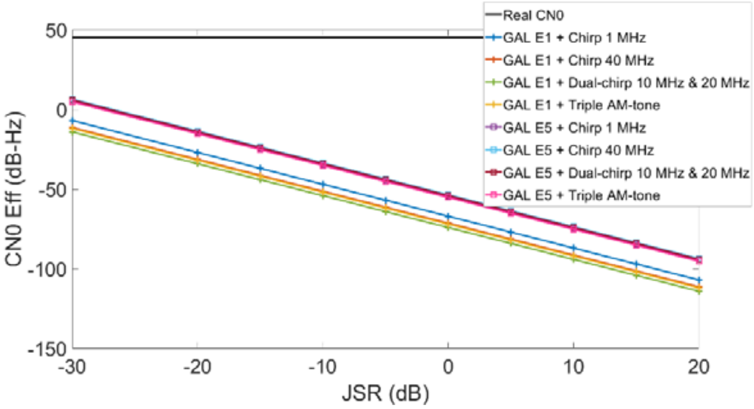


Fig. 4 Effective CN0 for different GNSS + jammer combination at different JSR. The set real CN0 is 45 dB-Hz

Fig. 5 shows the performance of the three considered jammer detectors in terms of the detection probability (P_d) versus the JSR level:

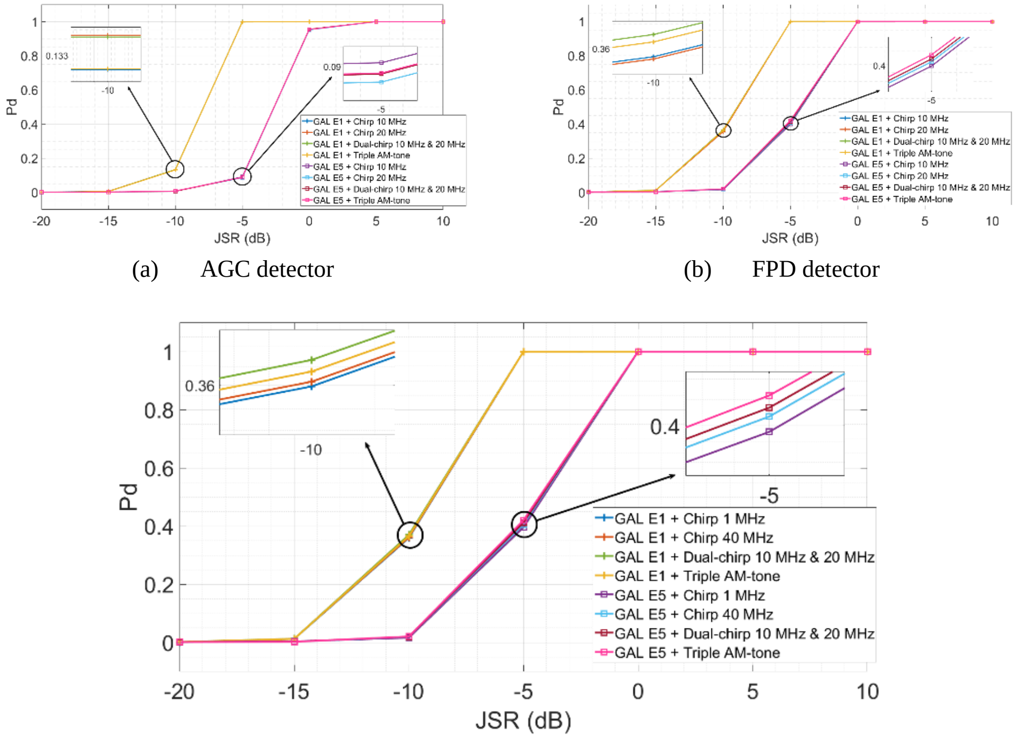
- the Automatic Gain Detection (AGC), e.g., described e.g., in [8][17]
- the Frequency Power detector (FPD), e.g., described e.g., in [15][18][13]
- the Time Power Detector (TPD), e.g., described e.g., in [18]

These three detectors have been selected based on literature studies, as the ones most promising in terms of jamming detection. They are all based on pre-correlation domain (see Fig. 3).

The detection probability is the probability to correctly detect the jammer in the scenarios when the jammer is present. The plots in Fig. 5 confirm the observations from Fig. 4, i.e., the fact that Galileo E5 signal is less affected by jammers, and in consequence it is more difficult for the detectors to be able to determine the presence of interference in E5 signal band.

The three considered detectors need a minimum JSR of -10 dB to be able to start detecting the presence of jamming.

When the JSR is about 0 dB, the P_d for the three considered detectors is 1 or close to 1. All three detectors show similar performance dealing with the different set scenarios, thus the jammer type is not especially important as can be observed in Fig. 5.



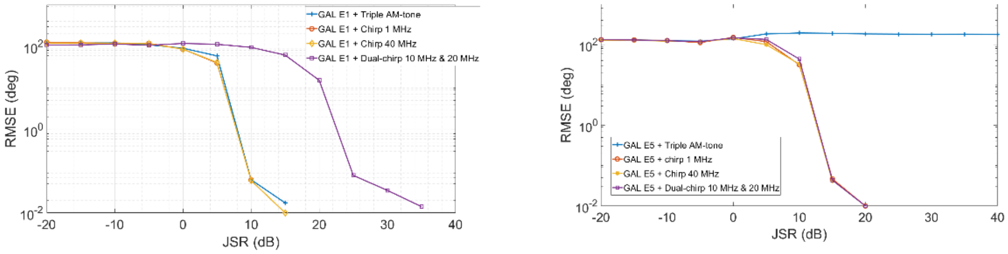
(a) AGC detector

(b) FPD detector

(c) TPD detector

Fig. 5 Jamming detection performance for three detectors: (a) AGC; (b) FPD; and (c) TPD

Regarding the jamming direction finding, after a preliminary investigation of Time-Difference-Of-Arrival (TDoA) and Angle-of-Arrival (AoA) algorithms, we have concluded that AoA direction finding algorithms are more suitable for aviation application (when the spacing between antennas is limited by the aircraft size) than the TDoA algorithms.



(a) Galileo E1 scenarios

(b) Galileo E5 scenarios

Fig. 6 Jammer direction finding performance for AoA direction finding algorithms:
(a) Galileo E1 scenarios; (b) Galileo E5 scenarios

The results are shown in Fig. 6 for the eight considered scenarios from Table 2 (the left-hand plots are for the first four scenarios and the right-hand plots are for the last four scenarios).

The results in Fig. 6 show that jammer localization is possible with small enough error angles only if the jammer is strong enough, i.e., JSR above 10 dB or more.

Unlike the detection results, now the jammer type influences the jammer direction finding performance. For example, the direction finding of triple AM tone jammer was very poor in our tests.

The jamming detection and direction-finding algorithms discussed in Fig. 6 via simulations have also been partially analyzed in an in-lab testing environment shown in Fig. 7. The in-lab environment is composed by a NI Vector Signal Transceiver (VST) PXIe-5645R, a Spectracom GSG-64 GNSS signal generator, an Universal Software Radio Peripheral (USRP), and a computer to control the setup.

The NI VST (in combination with Matlab and the Windows device drivers) generated the baseband jammer signal.

The Spectracom GSG-64 generated the GNSS signals. The USRP recorded both data streams in two separated channels. In order to achieve synchronization between both channels, a pulse-per-second (PPS) signal coming from the GNSS signal generator was connected as input to the USRP.

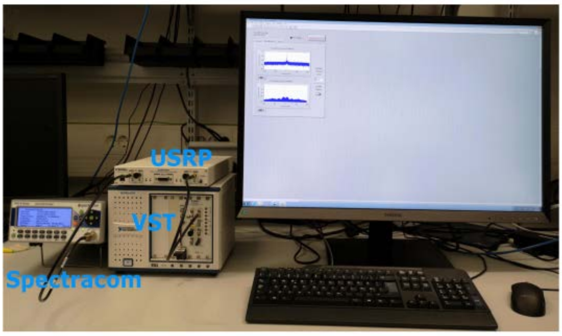
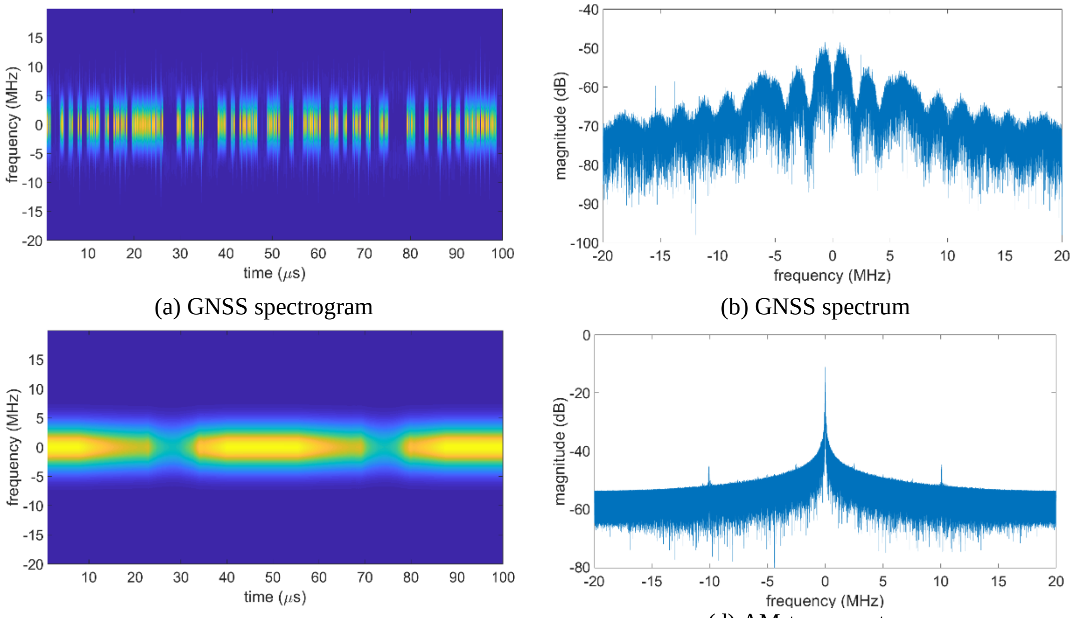


Fig. 7 In-lab validation setup for jamming detection and direction finding

Fig. 8 shows the spectrogram and spectrum for signals recorded using the setup shown in Fig. 7. Fig. 8 (a) and Fig. 8 (b) show the spectrogram and the spectrum for a jammer-free Galileo E1 signal.

Similarly, Fig. 8 (c) and Fig. 8 (d) show the spectrogram and the spectrum for single AM-tone jammer signal.

We have reported our detailed in-lab results in [23]. Similar observations have been drawn from both simulation-based and in-lab based scenarios. Our in-lab data for jamming validation is also available in open-access at [21].



(a) GNSS spectrogram

(b) GNSS spectrum

(c) AM-tone spectrogram

(d) AM-tone spectrum

Fig. 8 Spectrogram and Spectrum for in-lab validation signal for no jammer and single AM-tone scenarios

6. SPOOFING DETECTION AND DIRECTION FINDING RESULTS

Several detection and direction finding/localization algorithms have also been investigated for spoofing [3], [4], [20], [27].

As mentioned in Section 4, the most promising spoofing detection algorithms proved to be:

- the Dispersion of Double Differences (D^3) detector, described e.g., in [20]
- the Sum of Squares (SoS) detector, described e.g., in [20][4][3]

Examples of D^3 and SoS detection metrics are shown in Fig. 9 for a scenario with mixed tracking condition, i.e., when both spoofed and un-spoofed signals co-exist in the tracking stage of the receiver.

In this examples, 3 out of 9 considered signals are counterfeit. The SoS detector is taken as a benchmark and it is plotted with black line.

SoS fails in case of ‘mixed tracking’, because it is not able to discriminate the three counterfeit signals (i.e., its detection metric is significantly higher than 0), but the D^3 detection works (i.e., it is able to “cluster” the detection metrics of all the spoofed signals around the same mean value).

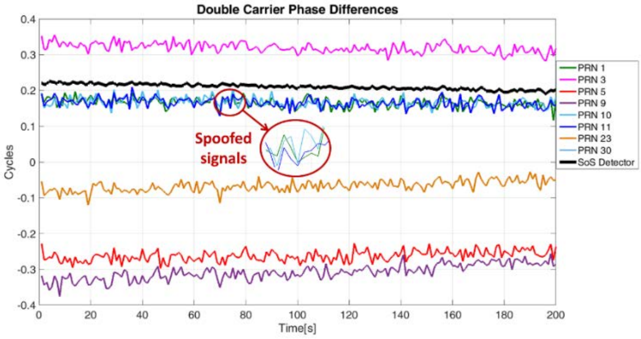


Fig. 9 Example of Dispersion of Double Differences (D^3) and SoS detection in mixed tracking condition (i.e., both spoofed and un-spoofed signals)

An example of spoofing detection performance with Double Carrier Phase Differences is further shown in Fig. 10. As it can be seen there, both the genuine and the spoofed or fake satellites are identified correctly in 100% of the cases: the green dots signify a correct detection of an un-spoofed satellite and the red dots signify a correct detection of a spoofed satellite; the un-spoofed satellites here are the satellites 3,5,6,7,9, 23, and 30, and the spoofed satellites are the satellites 1,2,4,8,10,11,12,13,14.

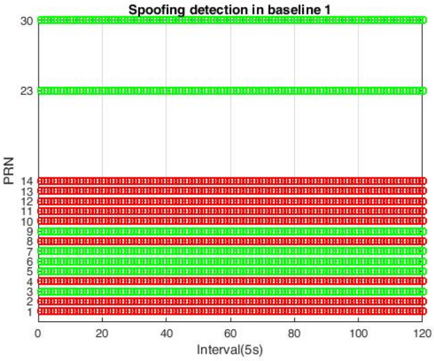


Fig. 10 Example of spoofing detection results (100% detection accuracy) in a mixed environment with both spoofed (red color) and genuine/un-spoofed (green color) satellites.

In terms of spoofing direction finding, also AoA algorithms proved to be the best choices on-board of aircraft. An example of spoofing direction finding performance, based on the algorithm [26], is shown in Fig. 11 for nine test cases listed in Table 3. Performance are measured here in terms of absolute AoA estimation error produced by the on-board algorithm with the use of three antenna-receiver chains [9].

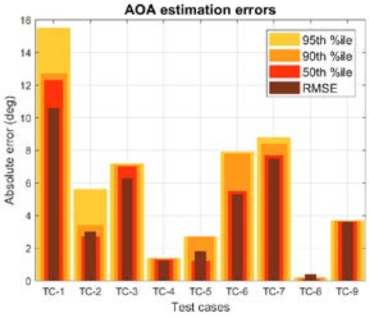


Fig. 11 Examples of spoofing direction finding results via AoA algorithm for 9 test cases (TC)

Table 3. Test scenarios for spoofing detection and direction finding

Test case index	Characteristics
TC-1	Single constellation, all signals spoofed, medium speed, all Angles of Arrival (AoAs)
TC-2	Single constellation, subset of signals spoofed, medium speed, all AoAs
TC-3	Single constellation, all signals spoofed, high speed, all AoAs
TC-4	Single constellation, subset of signals spoofed, high speed, all AoAs
TC-5	Single constellation, all signals spoofed, taxiing speed, all AoAs
TC-6	Double constellation, subset of signals spoofed, medium speed, all AoAs
TC-7	Double constellation, other subset of signals spoofed, medium speed, all AoAs
TC-8	Double constellation, subset of signals spoofed, high speed, all AoAs
TC-9	Double constellation, other subset of signals spoofed, high speed, all AoAs

The spoofing management solutions have also been tested in an in-lab environment depicted in Fig. 12. Our in-lab data for spoofing validation is also available in open-access at [10].

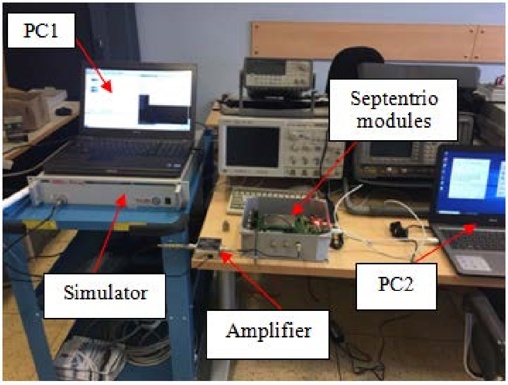


Fig. 12 In-lab validation scenario for spoofing management

7. CHALLENGES AND OPEN DIRECTIONS

The real-field validation of current results raises some issues as the GNSS band is protected and therefore jamming and spoofing are illegal in Europe [16] and special permissions are needed in order to conduct real-field experiments for research purposes. In order to provide efficient interference direction finding and spoofing detection mechanisms, at least three GNSS antennas are needed on-board of aircraft and the possible interference with other wireless on-board equipment, such as used for communication and surveillance purposes, must be taken into account and investigated further.

While our focus has been on interference detection and localization/direction finding, two additional steps in interference management are also open for future research directions, namely the interference classification and interference mitigation. In terms of classifying various interference types present in the GNSS band, there have been very little studies in the present literature to the best of the Authors' knowledge. Machine learning algorithms are promising approaches for the interference classification, but they remain to be further investigated. In terms of GNSS interference mitigation, many approaches have been studied so far in the literature such as notch filters [11], frequency excision filters [28], or pulse blanking methods [5], [2]. However, a comparative analysis of various interference mitigation methods in GNSS is still to be done.

In addition to GNSS as future navigational solution for aircraft, redundant and complementary localization solutions must be found and research, in order to achieve the required levels of reliability and availability of the navigation solution, as well as cm-level accuracy.

Current research directions investigate the use of 5G cellular systems in aviation [19] for both communication and positioning purposes, as well as multi-frequency multi-constellation GNSS receivers [30] on-board of future aircraft.

The GNSS augmentation with satellite and ground infrastructures such as Satellite Based Augmentation Systems (SBAS) and Ground Based Augmentation Systems (GBAS) for increased accuracy and continuity are also upcoming trends in GNSS research [24]. With additional sources of positioning, the verification of the integrity of the navigation solution also becomes a more complex problem to solve, but at the same time it promises additional counter-measures against malicious interference in GNSS bands.

Artificial Intelligence (AI) and Machine Learning (ML) algorithms to support the Communication, Navigation, and Surveillance (CNS) solutions in aviation are also emerging trends [1], [12], [29].

8. CONCLUSIONS

The presence of jammers and spoofers capable of misleading the position, velocity, and timing computations of the GNSS receiver on-board of an aircraft poses serious security threats with potentially catastrophic impacts on the safety of the aircraft, on other traffic, or on any other ground infrastructure.

Therefore, it is critical to endow the future aircraft with the capability to detect the presence of an interferer signal, while at the same time preserving the low-complexity of the equipment required on-board of aircraft.

Our solutions investigated in this paper will reduce the likelihood and impact of this security threat and, consequently, will improve the safety of air traffic management, by astutely incorporating interference detectors and direction finding on the GNSS receivers on-board of future aircraft.

With a minimal number of GNSS antennas, our studies have shown promising results in terms of interference detection and direction finding. Future work is dedicated to collaborative approaches, where more than one aircraft are affected by the interference sources and aircraft communicate with each other in a cooperative manner. In addition, further research is needed towards multiple sources of interferers and towards aerial interferers, such as those placed on-board of a drone.

ACKNOWLEDGMENTS

This work has received funding from the SESAR Joint Undertaking under the European Union’s Horizon 2020 research and innovation programme under grant agreement No 783183. This project is a partnership between GMV Innovating Solutions, Tampere University, and LINKS Foundation. The opinions expressed herein reflect the Authors’ views only. Under no circumstances shall the SESAR Joint Undertaking be responsible for any use that may be made of the information contained herein. The Authors would like to thank Dr. Aleksandr Ometov from Tampere University for his help in the graphical design of the first plot in this paper.

REFERENCES

[1] * * * "Detection, Tracking and Classification of Aircraft and Drones in Digital Towers using Machine Learning on Motion Patterns", 2019 Integrated Communications, Navigation and Surveillance Conference (ICNS), Herndon, VA, USA, 2019, pp. i-xxxvi. doi: 10.1109/ICNSURV.2019.8735238

[2] D. Alonso, *Narrowband interference rejection studies for Galileo signals via Simulink*, MSc thesis, Tampere University of Technology, Apr 2015, https://dspace.cc.tut.fi/dpub/handle/123456789/23215

[3] D. Borio and C. Gioia, *A dual-antenna spoofing detection system using GNSS commercial receivers*, in Proc. of the 28th Inter. Tech. Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2015), Sep. 2015.

[4] D. Borio and C. Gioia, A sum-of-squares approach to GNSS spoofing detection, *IEEE Trans. Aerosp. and Electron. Syst.*, vol. **52**, no. 4, pp. 1756–1768, 2016.

[5] D. Borio and E. Cano, Optimal global navigation satellite system pulse blanking in the presence of signal quantisation, *IET Signal Processing*, vol. **7**, no. 5, pp. 400–410, Jul. 2013.

[6] D. Borio, F. Dovis, H. Kuusniemi, and L. L. Presti, Impact and detection of GNSS jammers on consumer grade satellite navigation receivers, *Proc. IEEE*, vol. **104**, no. 6, pp. 1233–1245, Jun. 2016.

[7] * * * EUROCONTROL, Eurocontrol voluntary ATM incident reporting (EVAIR) bulletin no 19, 2012–2016, EUROCONTROL, Incident Report 19, Apr. 2018.

[8] F. Bastide, D. Akos, C. Macabiau, and B. Roturier, *Automatic gain control (AGC) as an interference assessment tool*, in ION GPS/GNSS 2003, 16th International Technical Meeting of the Satellite Division of The Institute of Navigation, (Portland, OR, pp. 2042–2053), Sep. 2003.

[9] G. Falco, M. Nicola, E. Falletti, M. Pini, *An Algorithm for Finding the Direction of Arrival of Counterfeit GNSS Signals on a Civil Aircraft*, ION GNSS+ 2019, Miami, FL, 16-20 September 2019.

[10] G. Falco, E. Falletti, and M. Nicola, *GATEMAN project, GNSS raw data in presence of spoofing* (Version 0.1) [Data set], Zenodo, 2019, http://doi.org/10.5281/zenodo.2537055

[11] G. J. Saulnier and P. Das, Antijam spread spectrum receiver using LMS adaptive filtering techniques, in *IEEE Military Communications Conference (MILCOM)*, vol. **3**, pp. 482–487, 1984.

[12] G. Yang, Y. Zhang, Z. He, J. Wen, Z. Ji and Y. Li, Machine-learning-based prediction methods for path loss and delay spread in air-to-ground millimetre-wave channels, in *IET Microwaves, Antennas & Propagation*, vol. **13**, no. 8, pp. 1113-1121, 3 7 2019. doi: 10.1049/iet-map.2018.6187.

[13] J. Lehtomäki, *Analysis of energy based signal detection*, PhD thesis, University of Oulu, 2005.

[14] J. Querol, A. Camps, E. G. Manfredini and R. Píriz, *An anti-jamming system for GNSS timing applications*, 2018 European Frequency and Time Forum (EFTF), Turin, 2018, pp. 155-158. doi: 10.1109/EFTF.2018.8409021

[15] K. D. Wesson, J. N. Gross, T. E. Humphreys, and B. L. Evans, GNSS signal authentication via power and distortion monitoring, *IEEE Trans. Aerosp. Electron. Syst.*, vol. **54**, no. 2, pp. 739–754, Apr. 2018.

[16] L. Chen et al., Robustness, Security and Privacy in Location-Based Services for Future IoT: A Survey, in *IEEE Access*, vol. **5**, pp. 8956-8977, 2017.doi: 10.1109/ACCESS.2017.2695525

[17] M. Z. H. Bhuiyan, H. Kuusniemi, S. Söderholm, and E. Airos, The impact of interference on GNSS receiver observables – a running digital sum based simple jammer detector, *Radioengineering*, vol. **23**, no. 3, pp. 898–906, Sep. 2014.

[18] N. Fadaei, *Detection, characterization and mitigation of GNSS jamming interference using pre-correlation methods*, Master's thesis University of Calgary, 2016.

[19] N. Hosseini, H. Jamal, J. Haque, T. Magesacher and D. W. Matolak, UAV Command and Control, Navigation and Surveillance: A Review of Potential 5G and Satellite Systems, *2019 IEEE Aerospace Conference*, Big Sky, MT, USA, 2019, pp. 1-10. doi: 10.1109/AERO.2019.8741719

[20] V. H. Nguyen, G. Falco, E. Falletti, M. Nicola, *A dual antenna GNSS spoofing detector based on the dispersion of double difference measurements*, NAVITEC 2018, ESA-ESTEC, Netherlands, 5-7 Dec 2018.

[21] P. Richter, R. Morales Ferre, and E. S. Lohan, *GATEMAN project -- Wide-bandwidth, high-precision GNSS and jammer raw data* [Data set], Zenodo, 2019), http://doi.org/10.5281/zenodo.2654322

[22] P. Wang, Y. Wang, E. Cetin, A. G. Dempster and S. Wu, GNSS Jamming Mitigation Using Adaptive-Partitioned Subspace Projection Technique, in *IEEE Transactions on Aerospace and Electronic Systems*, vol. **55**, no. 1, pp. 343-355, Feb. 2019, doi: 10.1109/TAES.2018.2852199

[23] R. Morales Ferre, P. Richter, A. De La Fuente, and E. S. Lohan, In-lab validation of jammer detection and localisation algorithms for GNSS, in Proc. of *IEEE ICL-GNSS*, Jun 2019, Nuremberg, Germany

[24] R. Sabatini, T. Moore and C. Hill, Avionics-based GNSS integrity augmentation synergies with SBAS and GBAS for safety-critical aviation applications, *2016 IEEE/AIAA 35th Digital Avionics Systems Conference (DASC)*, Sacramento, CA, 2016, pp. 1-10. doi: 10.1109/DASC.2016.7778076

[25] S. Bhattacharya and T. Başar, Game-theoretic analysis of an aerial jamming attack on a UAV communication network, *Proceedings of the 2010 American Control Conference*, Baltimore, MD, 2010, pp. 818-823.

[26] R. Sun, K. O'Keefe, J. Guo and E. Gill, Precise and Fast GNSS Signal Direction of Arrival Estimation, *Journal of Navigation*, Vol. **67**, 2013, pp. 17-35. doi:10.1017/S0373463313000453.

[27] T. E. Humphreys et al., Assessing the spoofing threat, *GPS World*, vol. **20**, no. 1, pp. 28-38, Jan. 2009.

[28] Y. Chien, C.-H. Chen, P.-Y. Chen, and H. Tsao, Impact of jamming excisor on the tracking loops for GPS receivers, in *2014 Proc. of the SICE Annual Conference (SICE)*, Sep. 2014, pp. 383–388

[29] Y. Li, K. Cai and S. Yan, Critical Flight Trajectory Identification via Machine Learning for Large-scale Trajectory Management, *2018 IEEE/AIAA 37th Digital Avionics Systems Conference (DASC)*, London, 2018, pp. 1-7. doi: 10.1109/DASC.2018.8569654

[30] Y. Yang, X. Ba and J. Chen, A Novel VLSI Architecture for Multi-Constellation and Multi-Frequency GNSS Acquisition Engine, in *IEEE Access*, vol. **7**, pp. 655-665, 2019. doi: 10.1109/ACCESS.2018.2885592

[31] * * * Yle Uutiset. (Nov. 2018). Russia suspected of GPS jamming during nato exercises, Yleisradio Oy, [Online]. https://yle.fi/uutiset/osasto/news/russia_suspected_of_gps_jamming_during_nato_exercises/10500210 (active Jul 2019).

The authors declare on their own responsibility that the paper has not been previously published elsewhere.