An Algorithm for Finding the Direction of Arrival of Counterfeit GNSS Signals on a Civil Aircraft

Gianluca Falco, LINKS Foundation, Torino, Italy
Mario Nicola, LINKS Foundation, Torino, Italy
Emanuela Falletti, LINKS Foundation, Torino, Italy
Marco Pini, LINKS Foundation, Torino, Italy

BIOGRAPHIES

Gianluca Falco received the M.S. degree in Communications Engineering from Politecnico di Torino, Italy, in 2007 and the Ph.D. degree in Electronics and Communications Engineering in 2011. He is currently a Communication Engineer with the Space & Navigation Technologies area, LINKS Foundation, Turin, Italy. His research interest focuses on multi-sensors fusion, particularly between GPS and inertial navigation systems, and on advanced processing techniques for dual frequency and multi-constellation GNSS receivers.

Mario Nicola received the M.S. in Computer Science Engineering and a Ph.D. degree in Electronics and Communications Engineering from Politecnico di Torino. He is a researcher in the Space & Navigation Technologies area, LINKS Foundation, Torino. His main activity is the design and implementation of algorithms for software radio GPS/Galileo receivers.

Emanuela Falletti received the M.Sc. and Ph.D. degrees in Telecommunications Engineering from Politecnico di Torino (Italy). She is team leader in the Space & Navigation Technologies area of the LINKS Foundation. Her research interests include digital signal processing algorithms for advanced GNSS software receivers, interference detection and mitigation, multi-antenna processing, and signal simulation.

Marco Pini received the M.Sc. and Ph.D. degrees in Telecommunications Engineering from Politecnico di Torino (Italy), in 2003 and 2006, respectively. He heads the Space & Navigation Technologies area of the LINKS Foundation. His research interests include the field of baseband signal processing of new GNSS signals, multi-frequency RF front-end design, and software radio receivers.

ABSTRACT

The purpose of this paper is to present and discuss the results of a Spoofing Detection and Direction Finding procedure usable for GNSS spoofing monitoring on board of a commercial aircraft. The targeted use case is an evolution of the GNSS equipment used on board of civil aircrafts, characterized by the availability of more GNSS constellations (multi-constellation) and two carrier frequencies (dual-frequency). The GNSS evolution in the civil aviation domain also foresees the progressive acquisition of a prominent role for GNSS in the aircraft navigation system, while today this role is taken by the traditional terrestrial NavAids. In such a scenario, the safe management of the Radio Frequency (RF) interference risk on GNSS becomes a primary task; nonetheless, the strict regulatory and certification procedures of the civil aviation domain impose a smooth technological evolution for the on-board avionic systems and consequent constraints in the design of new functionalities.

The Spoofing Detection and Direction Finding procedure presented in this paper has been developed in this context. It consists of a detection module that employs the Dispersion of Double Difference ($D^3$) algorithm to identify which signals tracked by the receiver are counterfeit, if any; the detection module is followed by a direction finding module that implements an efficient Direction-Of-Arrival estimator, with the purpose of providing information to a ground control center for the localization of the spoofing source (this ground segment is out of the scope of the paper). The necessary on board equipment consists in three GNSS antennas and the same number of receivers, time-synchronized with a common clock, plus a signal processor that implements the detection and DOA estimation algorithms.

The paper presents the design of the chain of algorithms and their preliminary tests in a laboratory setup, with the simulation of a number of spoofing attacks, assumed realistic in a civil aviation scenario. The obtained results confirm the reliability of the spoofing
detection and direction finding procedure, in terms of both correct detection rate and DOA estimate accuracy. They also show that the quality of the carrier phase measurements is a key element of the whole procedure, therefore an interesting indication we obtain is that the choice of the on-board multi-constellation GNSS receivers should take into account also the accuracy and continuity of the provided carrier phase measurements.

INTRODUCTION

The SESAR (Single European Sky Air traffic management Research) Joint Undertaking has financed an initiative under its Exploratory Research framework aimed at proving a novel concept for the integrated management of the two major known threats to GNSS-based air navigation: RF jamming and spoofing [1][2]. The implementation of the initiative is a research project [3] focused on the study, development and assessment of algorithms for the aircraft autonomous detection of malicious RF transmissions that interfere with the correct reception of the GNSS signals. Beyond detection, such algorithms are expected to provide also an indication of the Direction Of Arrival (DOA) of the interfering signals, in order to enable, as ultimate step, a rough localization of the transmitting source. The chain detection–direction finding–source localization is what the project intends for GNSS threats management.

Since the GNSS jamming and spoofing are so different in their nature, their detection and consequent processing require different approaches, based on different principles [1][2][4]. While jamming is typically an “unstructured” interference incoming at high RF power with respect to the satellite signals, degrading but also detectable and manageable with standard methods, spoofing exploits the known structure of the GNSS signals themselves, with power levels more comparable with those of the authentic signals it wants to mimic. In this case, detection is the major issue and the DOA estimation of the counterfeit signals ensemble requires specific post-correlation processing.

Although recognized cases of spoofing targeted to civil aircraft have never been reported in the public literature so far, the risk of facing this kind of situations cannot be considered negligible at all [5][6]. On the contrary, the number of reported GPS outage cases, likely caused by jamming, is increasing worldwide [7][8]. In addition, the role of satellite navigation in the civil aviation domain is evolving from a secondary position toward a prominent one, in which legacy terrestrial NavAids will be likely relegated to a role of backup in case of GNSS outages [9][10][11]. This perspective further pushes towards an integrated management of the GNSS interference risk in the evolution of the civil aviation safety, including both structured and unstructured interference. The basic step of such risk management is the timely detection and identification of interference events, for which appropriate signal processing algorithms are necessary. Consequently, the studies conducted in the project have been steered in the direction of investigating signal-processing algorithms suitable for early detection and identification of interference events on board of a commercial aircraft.

This paper reports the principal results of the study, design, in-lab prototyping and in-lab testing of the signal processing algorithms for the detection of counterfeit GNSS signals (‘spoofing’) and the estimation of the direction of arrival of such signals with respect to the aircraft. The key driver for the project was to leverage on the existing aircraft equipment with as minor modifications as possible; this requirement has bounded the technological scope of the project to the best possible exploitation of simple architectures. Thus, the design leverages on the availability of two GNSS antennas and two receivers on board of the aircraft, plus the installation of a third antenna-receiver chain. The clock synchronization among the three GNSS receivers is in this case a technological requirement, necessary to guarantee consistency among the phase measurements used by the DOA estimation algorithm.

The presence of more than one antenna (and associated receiving chains) is a decisive factor for the design and performance of the algorithms. Multi-antenna processing is recognized as one of the most powerful approaches for spoofing detection [2][12][13], thanks to the ability of discriminating the DOA of the received signals: if the DOA is not compatible with the expected satellite positions, then the existence of a counterfeit transmission is detected. Considering the scenario of a spoofing attack hitting an aircraft either intentionally or not, the likelihood of a sophisticated multidirectional attack [1][4] appears very low today. On the contrary, a single source of a false ensemble of GNSS signals is considered a more realistic situation [4][13][17] and is the target scenario also for this work.

The algorithm for spoofing detection is based on the idea of the Sum of Squares (SoS) detector [16][17], further elaborated in order to cope with working conditions not covered by the original detector. The resulting algorithm employed hereafter is the Dispersion of Double Differences (D2) detector [18]. The principal feature of the SoS/D2 approach is the fact that it does not impose any requirement on the control of the clock bias between the receiving chains and, in principle, can work with only two antennas; additional antenna is useful to increase the robustness of the detection, reducing false detections [18]. For this reason this detection approach wins over others [13][19] in terms of equipment complexity and therefore is particularly suitable for the constraints posed by the project.

On the other hand, the SoS/D3 approach does not explicitly quantify the value of the geometrical term within the received signal, which is a function of the DOA. To quantify it, a more complex algorithm is necessary, which imposes some technological
constraints: the first one is the presence of at least three non-collinear antennas; the second one is the synchronization of the receiving chains, whose clock drifts must be kept aligned along the time and the clock biases must be estimated and compensated. The algorithm chosen for direction finding is a robust and problem-specific implementation of the “Precise And Fast GNSS signal DOA estimator” (PAF hereafter, for conciseness) [20], an algorithm originally presented in the literature for the DOA determination of genuine GNSS signals, able to efficiently resolve the problem of determining the direction of arrival of a GNSS signal along a generic array of antennas. The reason for the choice of this algorithm lays in its relatively low computational complexity, if compared with other approaches [21][22][23]; although the resolution of the integer phase ambiguity between pairs of antennas is mandatory and is a computationally demanding task, the PAF estimator proposed in [20] adopts an efficient strategy to reduce the search space in the integer domain and resolve the integer search problem in a few iterations [24].

The purpose of this paper is to present and discuss the results of a Spoofing Detection and Direction Finding (SpDDF) approach for an aircraft GNSS user equipment, consisting in the D3 detection algorithm followed by the PAF DOA estimator retailed to work for that specific scenario. The assumption of knowing the number and Pseudo-Random Noise (PRN) codes of the counterfeit signals is satisfied by the presence of the D3 detection algorithm in the processing chain, which is used to activate the PAF algorithm. The results are promising, in that the implementation of the procedure is robust and gives accurate enough estimates of the DOA of the spoofing source.

The paper content is organized in the following four sections: ‘Reference signal model and SpDDF functional architecture’ presents the signal model and the logical architecture of the SpDDF procedure; section ‘Mathematical formulations’ summarizes the mathematical formulation of the D3 and robust PAF implementation; section ‘In-lab test and performance assessment’ presents some of the in-lab functional tests executed to verify the capability of the SpDDF algorithms to produce the expected output under working conditions of interest; finally, section ‘Conclusions and further perspectives’ concludes the work and gives some further investigation perspectives.

**REFERENCE SIGNAL MODEL AND SPDDF FUNCTIONAL ARCHITECTURE**

When a GNSS receiver is under spoofing attack, it is generally exposed at the same time to the genuine satellite signals and to satellite-like signals, likely but counterfeit, generated by a non-GNSS source; if the receiver locks on a consistent set of counterfeit signals, these can induce deviations of receiver Position, Velocity, and Time (PVT) solution from the true one. The effects of this superposition of genuine and counterfeit signals are detectable at different stages of the receiving chain with appropriate signal processing [1][4][25][26][27]. However, if only the standard receiver outputs are available, as in the considered use case in which the receiving chain cannot be accessed for safety and certification reasons, the number of available algorithms reduces. The receiver observables used in the proposed SpDDF architecture are, for each signal band, the code and carrier phase pseudoranges produced by the receiver for each PRN code in view, at the output of the tracking stage, differenced over each antenna pair (i, j):

\[
\begin{align*}
\Delta\rho_{ij}^{(m)} &= \Delta r_{ij}^{(m)} + c \Delta T_{ij} + \Delta \epsilon_{\rho,ij}^{(m)} \\
\Delta\phi_{ij}^{(m)} &= \Delta \phi_{ij}^{(m)} + c \Delta T_{ij} + \lambda_f \Delta N_{\phi,ij}^{(m)} + \Delta \epsilon_{\phi,ij}^{(m)}
\end{align*}
\]

where \(\Delta\rho_{ij}^{(m)}, \Delta\phi_{ij}^{(m)}\) denote the Single Difference (SD) code and carrier phase pseudoranges in meters for the \(m\)-th source, \(\Delta r_{ij}^{(m)}\) is the SD \(i\)-\(j\) geometric range, \(c\) is the speed of the light, \(\Delta T_{ij}\) is the SD \(i\)-\(j\) clock error, \(\lambda_f\) is the wavelength, \(\Delta N_{\phi,ij}^{(m)}\) is the SD \(i\)-\(j\) carrier phase integer ambiguity, \(\Delta \epsilon_{\rho,ij}^{(m)}, \Delta \epsilon_{\phi,ij}^{(m)}\) are differential noise terms accounting for residual un-modeled errors, including thermal noise and multipath [17][18][20]. The geometric range difference between the satellite and the receivers \(\Delta r_{ij}^{(m)}\) contains a geometrical term, which depends on the DOA of the \(m\)-th source with respect to the antennas position; it is the component, along the \(ij\) baseline, of the orthogonal projection of the unitary vector \(\mathbf{x}^{(m)}\) representing the signal DOA:

\[
\Delta r_{ij}^{(m)} = \mathbf{g}_{ij}^T \mathbf{x}^{(m)}
\]

where \(\mathbf{g}_{ij}\) is the geometrical vector describing the relative position of the antenna \(j\) with respect to the antenna \(i\) (baseline \(ij\)). This geometrical term is the basis of the SpDDF algorithm addressed in this paper [18][20], because:

a) If more signals share the same geometrical term, they are likely produced by the same source, so they are not genuine (detection);

b) The common DOA of such counterfeit signals can be extracted from the common geometrical term (direction finding).

The functional logic of the overall SpDDF procedure is depicted in Figure 1 and summarized in the following points:
1. the carrier phase observables produced at each epoch by three receivers, connected to three antennas properly spaced each other, enter the detection module;
2. the detection algorithm forms the SDs and Double Differences (DDs) for each antenna and signal pair at each measurement epoch; it monitors its detection metric computed from the DD measurements and then it identifies the set of tracked signals that are recognized as spoofed. Such set can be:
   a. empty: if all the signals are genuine
   b. full: if all the signals are spoofed;
   c. partially full (subset): if only a set of signals are spoofed.
3. if a subset of signals is declared ‘spoofed’, then the Direction Finding (DF) algorithm is activated on the SD code and carrier phase measurements for the current epoch and the DOA is estimated;
4. the SpDDF procedure continues to the next epoch.

It is worth noticing here that the D^3 detector is able to detect also spoofing attacks that are not 100% successful, as in the case where the receiver locks onto both actual and spoofed signals.

**Figure 1. Principle of the Spoofing Detection and Direction Finding (SpDDF) procedure.**

**MATHEMATICAL FORMULATIONS**

The equipment setup assumed for this work includes three antennas placed on board of the aircraft; if they are not co-linear, they define a plane, which is taken as the \( z = 0 \) plane of the Cartesian coordinate reference frame used hereafter (antenna frame). The origin of such reference frame is placed on the reference antenna, the \( x \) axis is along the aircraft body and the \( y \) axis is in the direction of the left wing. With these assumptions the baseline vectors \( g_{ij} \) simplify to be bi-dimensional, as well as the DOAs \( \mathbf{x}^{(m)} \). Thus, the DOA estimation capability of the robust PAF algorithm is limited to the azimuth angle in the antenna reference frame, which is sufficient for the purpose of the project and reduces the computational complexity.

**Detection**

The principle of the SoS spoofing detection algorithm [16][17], reused in the D^3 formulation [18], is that the geometrical terms \( \Delta r_{ij}^{(m)} \), \( \Delta r_{ij}^{(r)} \) of two signals coming from two different satellites are different, while if the signal source is the same, the two terms are equal and their difference is 0. Thus, to observe the difference of the geometrical terms, the detector forms the Double Differences (DDs) of pairs of carrier phase measurements, along the \( ij \) baseline:

\[
\nabla \Delta \phi_{ij}^{(m)} = \frac{1}{\lambda_f} (\Delta \phi_{ij}^{(m)} - \Delta \phi_{ij}^{(r)}) = \frac{1}{\lambda_f} g_{ij}^{T}(x^{(m)} - x^{(r)}) + \nabla \Delta N_{ij}^{(m)} + \nabla \Delta \epsilon_{ij} \tag{3}
\]

expressed in number of cycles, where the superscript \(^{(r)}\) indicates the signal taken as a reference (possibly the one with the most stable tracking). In the bi-dimensional geometry. The geometrical term for the baseline \( ij \) can be written as:
\[
\Delta r_{ij}^{(m)} = D \cos(\theta^{(m)})
\]  
(4)

where \(D = |g_{ij}|\) and \(\theta^{(m)}\) is the angle of arrival of the \(m\)-signal with respect to the considered baseline.

In order to remove the effect of the DD integer ambiguity \(\nabla \Delta N_{ij}^{(m)}\), the fractional part only of (3) is considered, i.e.:  
\[
\mu^{(m)} = \nabla \Delta \phi^{(m)} - \text{round}(\nabla \Delta \phi^{(m)}) = \frac{D}{\lambda_f} (\cos(\theta^{(m)}) - \cos(\theta^{(r)})) + \nabla \Delta \epsilon \phi
\]  
(5)

At this point, the \(D^3\) algorithm differs from the SoS in that it admits that not all the tracked signals are simultaneously spoofed (in fact small differences in the receiver manager scheduling, the time of acquisition and small scale fading effect may be the reasons why the receiver locks onto both the actual and spoofed signal), then the expected value of \(\mu^{(m)}\) is not necessarily equal to zero if the \(m\)-th signal is spoofed (it is 0 only if \(\theta^{(m)} = \theta^{(r)}\)). However, the subset of spoofed signals “cluster” their fractional DDs around a certain value proportional to \((\cos(\theta^{(m)}) - \cos(\theta^{(r)}))/\lambda_f\), therefore it is possible to decide for the presence of spoofed signals if at least three fractional DDs on the same baseline are “close enough”, or, to follow [18], they belong to the same cluster or region of similarity. This means that there exist at least one triplet of signals \((m,n,k)\) such that
\[
|\bar{\mu}^{(m)} - \bar{\mu}^{(k)}|^2 \leq \xi^{(k)} \quad \text{and} \quad |\bar{\mu}^{(m)} - \bar{\mu}^{(k)}|^2 \leq \xi^{(k)}
\]  
(6)

where \(\bar{\mu}^{(m)}, \bar{\mu}^{(n)}, \bar{\mu}^{(k)}\) are short time estimates of the mean value. \(\xi^{(k)}\) is a detection threshold that counts for the noise terms of the DDs and therefore depends on the \(C/N_0\) ratio of the received signals. It can be set either empirically, as in [18], or using a formal approach guided by the decision theory, currently under development. In particular, the evaluation of the test metric as defined in (6) is prone to detection errors due to the presence of the noise component \(\nabla \Delta \epsilon \phi\). Although the cycle slips are removed from the observations using the strategy described before, the residual noise and the possible presence of fading effects may affect the single metrics so as to possibly determine a wrong decision in (6). In order to increase the robustness of the detection against the noise effect, one possible option is that the fractional DDs are averaged for short windows (e.g. 5 seconds) before taking the decision. However, in aviation applications where the target user moves at high speed (>250 km/h), an average window of even only 5 seconds can be too long to localize the direction of arrival of the spoofing attack. Therefore, a second option, which we adopted in this paper, is to use more than one baseline. The DDs formed on each of these baselines are not the same because the relative position of the antennas is different as well as the received carrier phases on them. Thus, the spoofed detection algorithm is run in parallel on each baseline. We declare spoofing only when both the baselines detect a spoofing attack.

It is interesting to notice that the original detector [16] is developed for a single baseline only (two antennas), but the presence of the second baseline can be very fruitfully used for confirmation and redundancy [18].

### Direction finding

Once the subset of counterfeit signals is identified, then an adaptation and redundant implementation of the PAF algorithm shown in [20] is employed to estimate the azimuth of the spoofing source with respect to the antenna frame. The formulation adopted here employs the SD code and carrier phase equations of all the same-source signals along the two baselines (1,2) and (1,3): such measurements share the same DOA \(x^{(m)} = x\).

\[
\begin{bmatrix}
\Delta \rho_{12}^{(m)} \\
\Delta \rho_{13}^{(m)} \\
\Delta \phi_{12}^{(m)} \\
\Delta \phi_{13}^{(m)}
\end{bmatrix} =
\begin{bmatrix}
\mathbf{g}_{12}^T \\
\mathbf{g}_{13}^T \\
\mathbf{g}_{12}^T \\
\mathbf{g}_{13}^T
\end{bmatrix} x +
\begin{bmatrix}
\Delta \epsilon_{\rho,12}^{(m)} \\
\Delta \epsilon_{\rho,13}^{(m)} \\
\Delta \epsilon_{\phi,12}^{(m)} \\
\Delta \epsilon_{\phi,13}^{(m)}
\end{bmatrix}
\]  
(7)

for all the signals identified in the detection module, say \(M\) signals \((M \geq 3)\); the vector \(x\) is the common DOA of the counterfeit signals.

The above set of equations (multi-satellite problem) consists in a system of \(4M\) equations and \((2 + 2M)\) unknowns, i.e., the bi-dimensional vector \(x\) and the 2M SD integer ambiguities, from now on indicated with the vector \(\mathbf{a}\) for simplicity of notation. The system has rank equal to the number of unknowns (it is overdetermined but consistent for \(M > 1\) and a Least Squares (LS) float solution exists: \([x^T \quad \mathbf{a}^T]^T\), with associated covariance matrices \(Q_{xx}\) and \(Q_{xx}\). The system can be readily extended to the use of two
GNSS frequencies, by adding a second pair of carrier phase equations for each signal and a second subset of $2M$ unknowns; however this dual-frequency formulation is out of the scope of the current paper.

Once obtained the float solution, the vector $\hat{a}$ can be constrained to integer values using an Integer Least Squares (ILS) approach, resolved via sequential conditional adjustment [24]; the problem can be written in the form
\begin{equation}
\hat{a} = \min_{a \in \mathbb{Z}^{2M}} |\hat{a} - a|^2_{Q_{\hat{a} a}}
\end{equation}
where $\mathbb{Z}^{2M}$ is the space of the integer numbers of dimension $2M$ and the notation $\sim$ indicates a vector after ambiguities fixing. This approach, although precise and highly reliable, can be computationally demanding and time consuming if the space of $a$ is vast. To overcome this aspect, the PAF algorithm [20] employs a numerically efficient procedure for bounding the ambiguity search space of the ILS problem and reducing the adjustment steps; this is obtained exploiting the known constraint on the DOA modulus: $|x| = 1$ (unitary vector).

The PAF algorithm first divides the float ambiguities to be fixed in two subsets: a primary one, $a_p$, with the same dimension of the DOA unknown $x$, and a secondary one, $a_s$, containing all the other ambiguities, conditioned on the set of candidates for the primary one. The search space for the primary subset is first identified exploiting the constraint on the DOA modulus: writing $x$ as a function of $a_p$, we obtain
\begin{equation}
x(a_p) = G^{-1} \begin{bmatrix} \Delta \phi_{12}^{(m)} \\ \Delta \phi_{13}^{(m)} \end{bmatrix} - \lambda_f a_p,
\end{equation}
with $G = \begin{bmatrix} g_{12} & g_{13} \end{bmatrix}$
then the unitary constraint $|x| = 1$ can be relaxed in the two inequalities
\begin{equation}
1 - \delta \leq |x(a_p)|^2 \leq 1 + \delta
\end{equation}
where $\delta$ is close to 0. The sequential conditional adjustment can be now separately applied to $|x(a_p)|^2 \leq 1 + \delta$ on the search space $\mathbb{Z}^2$ and $|x(a_p)|^2 \leq 1 - \delta$ on the search space $\mathbb{Z}^2$ again, giving the sets of candidates $\Omega_{+\delta}$ and $\Omega_{-\delta}$ respectively. Then, the search space for $a_p$ is reduced to $\mathbb{D}_p = \Omega_{+\delta} \setminus \Omega_{-\delta} \subset \mathbb{Z}^2$, where $\setminus$ indicates a difference in the sets domain. The set of possible vectors $a_p$ can be found via sequential conditional adjustment again, as
\begin{equation}
\Omega_{a_p} = \{ a_p \in \mathbb{D}_p | |\hat{a}_p - a_p|^2_{Q_{a_p a_p}} \leq \chi^2 \}
\end{equation}
which is computationally more convenient and precise than a solution on the whole $\mathbb{Z}^2$. Now the set of candidates for the secondary subset $a_s$ can be determined conditioned to $\Omega_{a_p}$ as
\begin{equation}
\Omega_{a_s|a_p} = \{ a_s \in \mathbb{Z}^{2M-2} | a_p \in \Omega_{a_p}, |\hat{a}_s - a_s|^2_{Q_{a_s a_s}} \leq \chi^2 \}
\end{equation}
Finally, the set of candidates for $a$ is determined as $\mathbb{D}^{2M} = \Omega_{a_p} \cup \Omega_{a_s|a_p} \subset \mathbb{Z}^{2M}$, so that the final ILS problem to be solved is
\begin{equation}
\tilde{a} = \min_{a \in \mathbb{Z}^{2M}} |\hat{a} - a|^2_{Q_{\hat{a} a}}
\end{equation}
where the advantage over (8) is in the reduction of the search space from $\mathbb{Z}^{2M}$ to $\mathbb{D}^{2M}$. The final DOA estimate is then computed with high accuracy as
\begin{equation}
\hat{x}(\tilde{a}) = \hat{x} - Q_{\hat{a} a} Q_{\hat{a} a}^{-1} (\hat{a} - \tilde{a})
\end{equation}
where $Q_{\hat{a} a}$ is the cross-covariance matrix obtained from the LS float solution.

**IN-LAB TEST AND PERFORMANCE ASSESSMENT**

In order to test the performance of the SpDDF procedure, an in-lab test setup was prepared: it employed a hardware generator of GNSS signals to simultaneously simulate both the authentic signals and the counterfeit ones, as received by three antennas placed according to a predefined geometry. The RF signal ensemble was fed to the receivers via RF cables. This approach enables to simulate various kinds of spoofing attack to an array of antennas, without broadcasting the spoofing signal on the air. It also allows simulating different antenna geometries and flight conditions, e.g. different aircraft velocities and trajectories. On the other hand, the injection of the RF signals via cable bypasses any antenna effect, creating a working condition in which the antennas are assumed ’ideal’: however, in practice, the stability of the antenna phase center has a role in the carrier phase measurement noise, as well as its radiation pattern impacts on the power ratio between authentic and spoofed signals. These aspects are out of the scope for the present work.
The receiver model used for processing the simulated signals was a dual-antenna professional receiver (AsteRx4 OEM module produced by Septentrio N. V.); time synchronization was guaranteed via the 1PPS signal.

Hereafter we present the results obtained for two test cases, selected as particularly representative of the overall SpDDF behavior. Their setup is defined in the following table.

<table>
<thead>
<tr>
<th>Test case ID</th>
<th>Test Case 1</th>
<th>Test Case 2</th>
</tr>
</thead>
<tbody>
<tr>
<td>antenna geometry</td>
<td>The system is made of three antennas placed to form two orthogonal baselines. The distance between antennas is chosen to be likely feasible for a civil aircraft scenario, where a long baseline can be placed along the fuselage and a short one across it. The chosen baselines are with: $</td>
<td>\mathbf{g}_{12}</td>
</tr>
<tr>
<td>aircraft trajectory simulated with GNSS generator</td>
<td>Trajectory depicted by Figure 3, with the following parameters Side length $l = 15$ km, turn radius $r = 5$ km. Travelled by the aircraft at 250 km/h</td>
<td>Trajectory depicted by Figure 3, with the following parameters Side length $l = 30$ km, turn radius $r = 10$ km. Travelled by the aircraft at 500 km/h</td>
</tr>
<tr>
<td>authentic GNSS signals simulated</td>
<td>GPS L1 CA (8 satellites) + Galileo E1 B/C (5 satellites)</td>
<td>GPS L1 CA (8 satellites)</td>
</tr>
<tr>
<td>counterfeit GNSS signals simulated</td>
<td>GPS L1 CA (8 satellites)</td>
<td>GPS L1 CA (6 satellites)</td>
</tr>
<tr>
<td>methodology of the attack</td>
<td>Simplistic spoofing: the spoofer tries to gain control over the victim receiver by first jamming it, then injecting the counterfeit signals at higher power level than the authentic ones. In more detail: when the simulation starts, the GNSS signal generator produces only the authentic signals, and no counterfeit signal is present. This initial phase lasts 120 seconds, then a 20-seconds jamming attack is simulated avoiding the reception of any GNSS signals. After the jamming attack ends, the GNSS generator produces simultaneously the authentic and the counterfeit signals; the power advantage of the counterfeit signals w.r.t. the authentic ones is $10$ dB. To simulate the simplistic spoofing attack an initial synchronization error of $3$ $\mu$s is simulated (without this synchronization error, an intermediate spoofing attack would be simulated). The reported parameters are listed as follows: $\bullet$ duration of the initial authentic phase: $120$ s $\bullet$ duration of the jamming attack: $20$ s $\bullet$ time misalignment of the counterfeit signal: $3$ $\mu$s $\bullet$ power advantage of the counterfeit signal: $+10$ dB</td>
<td></td>
</tr>
<tr>
<td>targeted effects of the attack</td>
<td>To hack the estimated altitude: $+300$ meters altitude, varied $+1$ m/s</td>
<td></td>
</tr>
</tbody>
</table>

A couple of additional comments may help in understanding the two test cases.

The GNSS generator simultaneously simulates authentic and counterfeit signals, but the counterfeit signals are not generated for all the visible satellites: for example, in the Test Case 1, the spoofing involves only GPS satellites, leaving unaltered the reception of the Galileo signals. This behavior simulates a partially successful spoofing attack, where the receiver under attack is still able to track some authentic signals. As already assessed in [18], the $D^3$ detection algorithm is able to successfully cope with these mixed conditions.

The simulated trajectory is a square with rounded corners: the choice of a closed loop trajectory leads to two simulation advantages: it is easy to simulate all possible direction of arrival of the spoofing signal with a limited simulation duration and avoids an indefinite growth of the distance between the spoofer and the target receiver, making redundant any consideration about the fluctuations of the power of the spoofing signal available at the target receiver antennas.
Analysis of the detection capabilities

The fractional DD measurements (3) produced by the receivers under attack in the two test cases and employed as metrics in the D³ detection module are shown in Figure 4, where each color refers to a different signal (PRN code). The carrier phase measurements appear highly degraded during the turns at high speeds, likely because the receivers were not configurable for use in aviation; during such turns many cycle slips are detected by the D³ module [18] and spoofing detection is not available. On the other hand, receivers seamlessly continue to produce highly accurate position fixes. Figure 4 highlights also each phase of the simulation as described in Table 1: it can be noticed that, during the simulation of the jamming attack (labelled Receivers under jamming attack in the pictures), receivers are not able to track any signals and, consequently, no DD measurements are available: the missing availability is graphically represented by the absence of markers on the plotted curves.

The presence of both authentic and spoofed signals is evident in Figure 4: when the counterfeit signal is not received (label Authentic signal only) the DD measurements exhibit different values, depending on the direction of arrival of the authentic signal. When the jamming attack (label Receivers under jamming attack) ends, both authentic and counterfeit signals are received (label Receivers under spoofing attack): when the receivers still track the authentic signals, the DD measurements continue to have different values; on the contrary, when the receivers track the counterfeit signals, since these fake signals come from the same source, then the DD measurements have the same geometrical term and cluster around the same value. In the reported results, this center value is zero because the reference signal used for the DD computation, indicated with index r in (3), was a counterfeit one. In order to make this analysis more apparent, the DD measurements for the second baseline in the Test Case 2 are depicted as an example in Figure 5, where the DD measurements related to authentic signals are highlighted in green color and the ones for the fake signals are highlighted in red.
Test Case 1 – Correct detection rate: 90.5%  
Test Case 2 – Correct detection rate: 75.0%

Figure 4. Fractional DDs over time from the beginning of the simulation and along the two baselines, for the Test Case 1 (left) and the Test Case 2 (right). The resulting correct detection rate is also reported.

Figure 5. Fractional DDs when receivers track the authentic signals (green) or the counterfeit ones (red).
The DD measurements reported in Figure 4 were fed to the D³ spoofing detection algorithm. The last row of Figure 4 compares the measured correct detection rate for the two cases, defined as the ratio between the number of the successful decisions taken by the algorithm over the total number of executions of the detection algorithm (excluded the epochs in which cycle slips were detected). This result is satisfactory, however it also indicates that further improvements in the detection capabilities could be pursued, for example with an optimized choice of the detection threshold.

**Analysis of the DOA estimation performance**

The DOA estimation performance of the PAF algorithm can be assessed observing the statistics of the azimuth estimation error of the spoofing source. Figure 6 reports the time sequence of the DOA estimation errors for the two test cases and the indication of their Root Mean Square Error (RMSE) and 95th percentile. It is evident that the DOA estimation is not available when the detection algorithm does not provide information (trajectory turns); furthermore, after each turn the PAF algorithm takes time to fix the integer ambiguities again, further reducing the availability. The consequence of this is that the overall DOA availability provided by the SpDDF procedure in the considered test cases is measured in:

| Test Case 1 | SpDDF DOA availability: 63.9% | Test Case 2 | SpDDF DOA availability: 41.3% |

Notice that the SpDDF DOA availability is defined as the ratio between the number of available DOA estimates during the spoofing attack over the total number of measurement epochs from the beginning of the spoofing attack. Other test cases, currently under evaluation, interestingly show more variability on their numerical results, for what concerns correct detection rate, DOA availability and error statistics. This fact confirms the complexity of the interactions inside the receiver of various external factors, such as the simultaneous presence of genuine and counterfeit signals, a strong lateral acceleration, etc.

![Figure 6. DOA estimation errors over time from the beginning of the spoofing attack, for the Test Case 1 (left) and the Test Case 2 (right). The resulting Root Mean Square Error (RMSE) and 95th percentile of the absolute error are also reported.](image)

**CONCLUSIONS AND FURTHER PERSPECTIVES**

TheSpoofing Detection and Direction Finding procedure presented in this paper has been designed for the specific target of a next-generation civil aviation scenario, in which the more central role of the GNSS in the on-board navigation functionality pushes to increase the resilience of the on-board GNSS module to possible spoofing attacks, with a correct management of the situations. The procedure described in this paper is able to detect the presence of counterfeit signals, identify them and determine their direction of
arrival; the DOA information can be used to enable source localization based on the data provided by several aircraft affected by the same spoofing source. This idea is developed in another work package of the project that has supported this research. The algorithms forming the procedure presented in this paper have shown promising results in the in-lab tests, in terms of correct detection rates, DOA estimation availability and accuracy. On-field tests are going to be executed in an authorized location. Further refinements of the procedure will target the optimization of the detection threshold, now selected in an empirical way, and a detailed analysis of performance as a function of some relevant parameters, such as the quality of the carrier phase measurements (residual noise), the number of spoofed signals and the baseline geometry.

ACKNOWLEDGMENTS

This work has received funding from the SESAR Joint Undertaking under the European Union’s Horizon2020 Research and Innovation programme, under Grant Agreement No783183. The opinions expressed herein reflect the author’s view only. Under no circumstances shall the SESAR Joint Undertaking be responsible for any use that may be made of the information contained herein.

REFERENCES

3. GATEMAN, GNSS nAvigation ThrEats MANagement, Grant agreement No 783183 under European Union’s Horizon 2020 research and innovation programme. 2017-2019.
8. EUROCONTROL, Voluntary ATM Incident Reporting (EVAIR) Safety Bulletin No. 19, April 2018.


