Joint Antenna Array Attitude Tracking and Spoofing Detection based on Phase Difference Measurements

Manuel Appel*†, Andriy Konovaltsev*, Michael Meurer *†
* Institute of Communications and Navigation, German Aerospace Center (DLR), Oberpfaffenhofen, Germany
manuel.appel@dlr.de † Chair of Navigation, RWTH Aachen University, Germany

BIOGRAPHY

Manuel Appel received his diploma degree in electrical engineering from the university of applied science Ingolstadt, Germany in 2008. Additionally he received a M.Sc. degree from Technical University Munich in 2013 after working at Fraunhofer Institute for Integrated Circuits in Erlangen. He joined the Institute for Communication and Navigation of DLR in January 2014. His main research interest is in development of signal processing algorithms for robust GNSS receivers with the main focus on spoofing detection and mitigation.

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.

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 international and national projects in the field of communications and navigation both as project coordinator and as technical contributor. From 2003 till 2013, Dr. Meurer was active as a senior lecturer and Associate Professor (PD) at the same university. Since 2006 Dr. Meurer is with the German Aerospace Centre (DLR), Institute of Communications and Navigation, 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.

INTRODUCTION

Spoofing attacks are a serious problem for civil GNSS applications with safety content, such as airplane landing or maritime navigation in harbors. Also many strategically important infrastructures, such as electric power grids or mobile communications networks, are becoming increasingly dependent on GNSS services. Military GNSS users solve that problem by signal encryption at chip level. This reduces the threat to only allow for meaconing, i.e. retransmitting the GNSS signals from a certain location, since the exact waveform is unpredictable. Civil users cannot rely on encryption at the moment and most likely in the near future. They must be protected by additional techniques, which are able to detect and mitigate spoofing attacks.

A number of receiver-autonomous solutions for the spoofing problem have been proposed in the last decade. For single antenna receivers the detection of spoofing attacks can rely on the observation of the time evolution of different signal parameters such as power and Doppler frequency shift, the PRN code delay and its rates, the correlation function shape as well as the cross-correlation of the signal components at different carrier frequencies. However, the most advanced protection against the sophisticated spoofing attacks can be provided by utilizing the spatial domain for signal processing available by using antenna arrays ([1], [2], [3], [4], [5]). A GNSS receiver with an antenna array is able to estimate the directions of arrival of the impinging waveforms and so to discriminate between the authentic and counterfeit signals. Moreover the malicious signals can be mitigated by generating a spatial zero into the array antenna reception pattern in the direction of the spoofing source(s).

The use of the array-aided joint estimation of the array attitude and spoofing detection was investigated by the authors in [1], [3], [5]. A post-correlation estimation of the signal direction of arrival (DOA) was utilized as the first step of the corresponding signal processing chain. This approach however still suffers from the effects of short-term distortions in the receiver tracking loops and the resulting unavailability of the DOA estimations during the spoofing attack. Two approaches have been identified to overcome this effect. On the one hand, a more accurate direction of arrival detection and antenna calibration can be used. On the other hand, the attitude estimation can be made more robust by skipping the DOA estimation step and using instead directly the post-correlation array outputs in the underlining measurement model, similar to method 2 in [6]. The latter possibility will be exploited throughout the current paper. One of the main challenges here is to design robust and computationally effective attitude estimation when the post-correlation array outputs consist of the superposition of the authentic and counterfeit signals. This problem, for example, is not adequately handled in [6] and [7].

In the aforementioned approaches, the estimation of the actual direction of arrival in terms of (antenna local) azimuth and elevation was done explicitly before the attitude was estimated. The approach presented in the paper will avoid this (computationally expensive) step, by introducing an adequate measurement model. This model connects the measured relative phases between the antennas elements (spatial signature) to the ones expected from the almanac. This interconnection involves the receiver attitude, which is the state to be estimated.

In a second step, the model fit (i.e. residuals of least square fit) is used to detect anomalies. Further processing is done by comparing the spatial signature for different satellites. Contrary to using the cyclic nature of PRN codes to detect the direction in the pre-correlation domain as described in [2], the spatial signature in the post-correlation domain is used. If one dominant direction is present, the likelihood of spoofing or meaconing is considered high. If detected, a second processing stage is triggered, capable of spatially filtering out the spoofers signature (post-correlation nulling). Finally a second run of the aforementioned procedure is done to estimate the antennas attitude using a spatially filtered signal. Theoretical results as well as hardware simulations ([8]) show, that if a GPS/CA or Galileo receiver already tracks a certain PRN, the likelihood of success is very low for an unsynchronized spoofer. In this context (un)synchronized is related to the PRNs current frequency shift (caused by the Doppler Effect), as well as code delay. The code delay error should not be larger than one chip in general. The tolerable frequency mismatch however, highly depends on the receivers implementation (i.e. FLL and PLL parameters and stages), but should not be bigger than a few multiples of 50 Hz. A synchronized spoofer or meaconing signal which is turned on when the receiver already tracks the corresponding PRN will be considered in the context of the paper. The described methods will be evaluated using software simulations. Scenarios without spoofing or meaconing are used to demonstrate the attitude estimation. Scenarios with repeaters will be used to demonstrate the two-stage approach with spatial filtering.

The remainder of the paper is organized as follows: First a physical model of the array based receiver is described to justify the assumptions made. A signal model using the adopted assumptions is presented, before an algorithm for estimating the antenna arrays attitude and detecting a (spatially spread) spoofer/meaconer is developed. Finally the performance is evaluated using simulated data.

NOTATION

The following notation is used throughout the paper:

- $\boldsymbol{x}$: Bold face lower letters denote column vectors
- $\boldsymbol{X}$: Bold face capital letters denote matrices
- $\mathcal{X}$: Calligraphic letters denote sets
- $|\mathcal{X}|$: The number of elements contained in a set
- $(\cdot)^T, (\cdot)^H$: The transpose and conjugate transpose of a vector or matrix
- $(\cdot)^*$: The complex conjugate
- $\odot$: The Hadamard product (elementwise product)
- $*$: The convolution operation

PHYSICAL MODEL

The purpose of this chapter is to state a physical model of the receiver which allows justifying the assumptions made throughout the paper. The complex baseband representation of the received signal of the array GNSS receiver (see Fig. 1) with M antenna elements for the nominal interference-free signal conditions with signals received from a GNSS constellation can be modeled with the following baseband model (see for comparison [7] and [9]):

$$\boldsymbol{x}(t) = \sum_{l \in \mathcal{L}} \boldsymbol{s}_l(t) + \boldsymbol{n}(t) \tag{1}$$

$\mathcal{L}$ denotes the set of nominal PRN sequences received. The overall number of GNSS satellites tracked

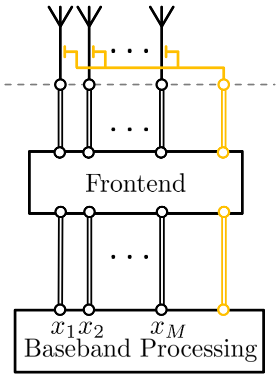

Fig. 1: Receiver setup including calibration to measure and compensate for front-end and cable effects (i.e. delays of the channels).

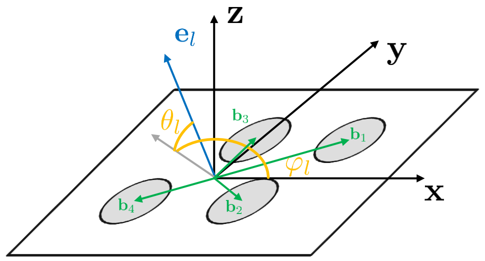

Fig. 2: Antenna coordinate frame with 4 elements, baselines and one incoming signal from direction $\boldsymbol{e}_l$ represented as vector with length 1.

by a receiver is $N = |\mathcal{L}|$. $\boldsymbol{x}(t) \in \mathbb{C}^M$ represent the arrays baseband measurements over time. $\boldsymbol{n}(t)$ denotes the baseband representation of the receiver noise. It is assumed to be band-limited, circularly-symmetric, spatially and temporally white Gaussian noise (WGN) with power spectral density N_0 over a bandwidth B. $s_l(t) \in \mathbb{C}$ denotes a scalar signal received at the antennas reference point (origin of the coordinate frame in which the base vectors of the elements $\boldsymbol{b}_m$ are measured). The term $\boldsymbol{s}_l(t) \in \mathbb{C}^M$ is the signal received from the l-th satellite which can be written as:

$$\boldsymbol{s}_l(t) = \boldsymbol{a}(\boldsymbol{e}_l) \odot \boldsymbol{h}(\boldsymbol{e}_l, t) * \underbrace{\sqrt{P_l} d_l(t-\tau_l) c_l(t-\tau_l) \mathrm{e}^{j(2\pi f_{D,l} t + \theta_l)}}_{s_l(t)} \quad (2)$$

$\boldsymbol{e}_l = [\cos(\varphi_l)\cos(\theta_l), \sin(\varphi_l)\cos(\theta_l), \sin(\theta_l)]^T \in \mathbb{R}^3$ is a unit vector pointing in the direction given by the elevation θ_l and azimuth φ_l. $\boldsymbol{a}(\Theta_l, \varphi_l) = \boldsymbol{a}(\boldsymbol{e}_l) \in \mathbb{C}^M$ is the array steering vector that accounts for the geometrical distribution of the antenna elements in the array grid and is defined as (see [10], Eq. (2.28)):

$$\boldsymbol{a}(\boldsymbol{e}_l) = \begin{pmatrix} \mathrm{e}^{jk\boldsymbol{e}_l^T \boldsymbol{b}_1} \\ \mathrm{e}^{jk\boldsymbol{e}_l^T \boldsymbol{b}_2} \\ \cdots \\ \mathrm{e}^{jk\boldsymbol{e}_l^T \boldsymbol{b}_M} \end{pmatrix} \quad (3)$$

$k = \frac{2\pi}{\lambda}$ is the wavenumber corresponding to the frequency $f = \frac{c}{\lambda}$ and $\boldsymbol{b}_m$ is the vector from the origin of coordinates to the m-th array element (see Fig. 2). The vector $\boldsymbol{h}(\boldsymbol{e}_l, t) \in \mathbb{C}^M$ in Eq. (3) describes the impulse responses of the individual array elements with the RF front-ends attached to them:

$$\boldsymbol{h}(\boldsymbol{e}_l, t) = \begin{pmatrix} h_{\text{ant},1}(\boldsymbol{e}_l, t) * h_{\text{FE},1}(t) \\ h_{\text{ant},2}(\boldsymbol{e}_l, t) * h_{\text{FE},2}(t) \\ \cdots \\ h_{\text{ant},M}(\boldsymbol{e}_l, t) * h_{\text{FE},M}(t) \end{pmatrix} \quad (4)$$

$h_{\text{ant},m}(\boldsymbol{e}_l, t)$ is the impulse response of the m-th array element in the direction given by $\boldsymbol{e}_l$, and $h_{\text{FE},m}(t)$ is the impulse response of the RF front-end-channel connected to the m-th array element. Please note that the resulting term of the elementwise product $\boldsymbol{a}(\boldsymbol{e}_l) \odot \boldsymbol{h}(\boldsymbol{e}_l, t)$ describes the complex array response in the direction of the l-th satellite.

For simplicity in the framework of this study it is assumed that only the line-of-sight component of the satellite signal can be observed and that multipath effects can be neglected. In view of this the contribution due to the l-th satellite in Eq. (2) is defined by the following set of parameters:

- P_l is nominal received power corresponding to the isotropic antenna with unity antenna gain.
- $c_l(t-\tau_l)$ is the pseudorandom noise (PRN) spreading sequence used by the satellite.
- $d_l(t-\tau_l)$ is the data modulation.
- τ_l is the propagation delay of the satellite signal, assuming that group and phase delay are equal, i.e. neglecting the dispersive properties of the ionospheric delay.
- $f_{D,l}$ is the Doppler frequency offset resulted from the satellite and user motion, $f_{D,l} = -\frac{\dot{r}}{\lambda}$, where $\dot{r}$ denotes the rate of the LOS range (see e.g. [11], Eq. (1.4)).
- φ_l is the nominal received phase of the carrier, this terms also accounts for the carrier phase shift resulted from the propagation delay.

In case of a spatially distributed spoofing attack, the spoofer is allowed to use up to N_{Tx} transmit antennas. The i-th spoofer station transmits a certain PRN sequences that belongs to the set $\mathcal{K}_i$. The overall set of spoofing counterfeit signals is given by $\mathcal{K} = \cup_{i=1}^{N_{\text{Tx}}} \mathcal{K}_i$.

Every fake PRN sequence is generated by at most one spoofing/meaconing station, i.e. $\mathcal{K}_i \cap \mathcal{K}_j = \emptyset \quad \forall i \neq j$.

Every station is characterized by its direction w.r.t. the victim. These directions are given by the corresponding azimuth and elevation $\{(\Theta_i^s, \varphi_i^s)\}_{i=1}^{N_{\text{Tx}}}$. This also implies, that the spatial signature vector $\boldsymbol{a}(\boldsymbol{e}_i^s)$ is common for all PRNs in $k_i \in \mathcal{K}_i$, i.e. for all PRNs transmitted by station i.

A short remark about notation seems necessary: The scheme uses index sets, which adds one layer of indirection for identifying the PRN numbers. This seems necessary to describe scenarios as precise as possible, since the PRN sequences received in real scenarios are not ordered. The split of PRN sequences generated from certain spoofer location may also be almost arbitrary with just the one restriction (every PRN sequence is transmitted from at most one location) mentioned before.

A superposition of all nominal and counterfeit signals is given by $\boldsymbol{x}(t)$ in complex baseband representation before the correlation:

$$\begin{aligned}\boldsymbol{x}(t) = &\sum_{l\in\mathcal{L}} \boldsymbol{s}_l(t) + \boldsymbol{n}(t) + \\ &\sum_{i=1}^{N_{\text{Tx}}} \boldsymbol{a}(\boldsymbol{e}_i^s)\Big[\sum_{k\in\mathcal{K}_i} s_k^s(t) + \eta_i(t)\Big] \end{aligned} \tag{5}$$

$\eta_i(t)$ is additive noise received from the i-th spoofing source and $s_k^s(t)$ is the counterfeit PRN k transmitted from station i, for which $k \cap \mathcal{K}_i \neq \emptyset$. In order to obtain a clear simple signal model, the array elements are assumed to be isotropic at first and the effect of the RF front ends negligible, i.e. $\boldsymbol{h}(\boldsymbol{e}_l, t) = (\delta(t), \delta(t), ..., \delta(t))^T$, where $\delta(t)$ denotes the Dirac delta distribution. This is to a great extend justified by utilizing an online calibration (see Fig. 1). Also, by neglecting the effect of data modulation, the signal model of Eq. (2) can be stated as:

$$\begin{aligned}\boldsymbol{x}(t) = &\sum_{l\in\mathcal{L}} \boldsymbol{a}(\boldsymbol{e}_l)\sqrt{P_l} c_l(t-\tau_l) \mathrm{e}^{j(2\pi f_{D,l} t + \varphi_l)} + \boldsymbol{n}(t) + \\ &\sum_{i=1}^{N_{\text{Tx}}} \boldsymbol{a}(\boldsymbol{e}_i^s)\Big[\sum_{k\in\mathcal{K}} \sqrt{P_k^s} c_k^s(t-\tau_j)\mathrm{e}^{j(2\pi f_{D,k}^s t + \varphi_k^s)} + \eta_i(t)\Big]\end{aligned} \tag{6}$$

The signal $\boldsymbol{x}(t)$ is used for correlation with a common replica for all array elements in a given satellite channel of the receiver. After correlating with the lth PRN code, the output $\boldsymbol{y}_l(t)$ reads:

$$\begin{aligned}\boldsymbol{y}_l(t) = &\frac{1}{\sqrt{N_0 T}} \int_0^T \boldsymbol{x}(t)^* c_l(t-\hat{\tau}_l) \mathrm{e}^{j(2\pi \hat{f}_{D,l} t + \hat{\varphi}_l)} dt = \\ &\boldsymbol{a}(\boldsymbol{e}_l)\sqrt{\frac{P_l T}{N_0}} R(\epsilon_{\tau,l}) \mathrm{sinc}(\epsilon_{f_{D,l}} \tau_l) \mathrm{e}^{j\epsilon_{\varphi_l}} + \\ &\boldsymbol{a}(\boldsymbol{e}_j^s)\sqrt{\frac{P_l^s T}{N_0}} R(\epsilon_{\tau,k}^s) \mathrm{sinc}(\epsilon_{f_{D,k}^s} \tau_k^s) \mathrm{e}^{j\epsilon_{\varphi_k}^s} + \\ &\sum_{i=1}^{N_{\text{Tx}}} \boldsymbol{a}(\boldsymbol{e}_i^s)\xi_i + \boldsymbol{\nu}_l\end{aligned} \tag{7}$$

The assumption that every PRN is only transmitted once was used by computing the second summand. The index j which was assigned to the spoofers direction is chosen such that $l \in \mathcal{K}_j$. Since the sets are disjoint, this is only possible for at most one set $\mathcal{K}_j$. ξ_i models the post correlation noise term due to the transmission of noise by every source in addition the corresponding PRN sequence assigned to it. $\boldsymbol{\nu}_l$ models the uncorrelated part received by every antenna. T is the correlators integration time. $\epsilon_{\tau,l}, \epsilon_{f_D,l}$ and $\epsilon_{\varphi,l}$ are the tracking errors for the code delay, Doppler frequency and carrier phase. Correspondingly, $\epsilon_{\tau,l}^s, \epsilon_{f_D,l}^s$ and $\epsilon_{\varphi,l}^s$ are the values for the spoofers signal w.r.t. currently used replica, which was parametrized with $\hat{\tau}_l$, $\hat{f}_{D,l}$ and $\hat{\varphi}_l$.

Assumptions and Estimation Problem

A shortcut notation for complex factors of the antenna steering vectors is introduced:

$$\begin{aligned} g_l &= \sqrt{\frac{P_l T}{N_0}} R(\epsilon_{\tau,l}) \mathrm{sinc}(\epsilon_{f_{D,l}} \tau_l) \mathrm{e}^{j\epsilon_{\varphi_l}} \\ g_l^s &= \sqrt{\frac{P_l^s T}{N_0}} R(\epsilon_{\tau,k}^s) \mathrm{sinc}(\epsilon_{f_{D,k}^s} \tau_k^s) \mathrm{e}^{j\epsilon_{\varphi_k}^s}\end{aligned} \tag{8}$$

After developing a physical model for the spoofer/repeater in the previous section, some assumptions for simplification are introduced:

1) The noise transmitted by the spoofing antennas is assumed to be zero.
2) The receivers loops are assumed to be in a steady state, i.e. the magnitude and phase of both nominal and spoofing signal are considered to be constant.
3) Tracking of the nominal signal is perfect and prompt corrector output is used. Previous estimates are used to normalize the nominal output, i.e. $g_l = 1$.

The nominal PRNs are assumed to be ordered, i.e. $\mathcal{L} = \{1, .., N\}$.

Nominal Case

For the nominal case, the correlator output reads:

$$\boldsymbol{y}_l(t) = \boldsymbol{a}(\boldsymbol{e}_l) + \boldsymbol{\nu}_l \tag{9}$$

To describe the antennas attitude w.r.t. to the local ENU-Frame in terms of roll, pitch and yaw, a rotation matrix $\boldsymbol{R} \in \mathcal{SO}(3)$ is introduced. Further details can be found in [4]. The corresponding directional cosine vectors in both frames are connected via $\mathbf{e}_{\text{loc}} = \boldsymbol{R}\mathbf{e}_{\text{enu}}$. The subscript "loc" and "enu" will be dropped in the remainder of the paper (i.e. $\mathbf{e}_{\text{enu}}$ for satellite l is denoted by $\mathbf{e}_l$).

Assuming identical independently distributed (iid) Gaussian noise in each tracking channel, the joint probability density function (pdf) of the correlator output given the attitude is the product of the single pdfs:

$$p(\boldsymbol{\nu}_1..\boldsymbol{\nu}_N) = \prod_{l=1}^{N} p(\boldsymbol{\nu}_l)$$
$$p(\boldsymbol{\nu}_l) \sim \exp((\boldsymbol{y}_l - \boldsymbol{a}(\boldsymbol{e}_l))^H \boldsymbol{C}_N^{-1} (\boldsymbol{y}_l - \boldsymbol{a}(\boldsymbol{e}_l))) \tag{10}$$

$\boldsymbol{C}_N$ is denoting the covariance of the noise, which is given by $\sigma_N^2 \boldsymbol{I}$. Using a maximum likelihood approach evaluating the aforementioned pdf of the tracking channels, a minimization of the sum of exponents (see Eq. (10)) is done, yielding the following optimization for $\boldsymbol{R}$ ($(\cdot)^*$ denotes the estimate of the optimal value):

$$\boldsymbol{R}^* = \arg \min_{\boldsymbol{R} \in \mathcal{SO}(3)} \underbrace{\sum_{l=1}^{N} \|\boldsymbol{y}_l - \boldsymbol{a}_l(\boldsymbol{R})\|^2}_{:= f(\boldsymbol{R}; \boldsymbol{Y}, \boldsymbol{B}, \boldsymbol{E})} \tag{11}$$

This problem is equivalent to the following:

$$\boldsymbol{R}^* = \arg \max_{\boldsymbol{R} \in \mathcal{SO}(3)} \sum_{l=1}^{N} \text{Re}\{\boldsymbol{y}_l^H \boldsymbol{a}_l(\boldsymbol{R})\} \tag{12}$$

The structure of this optimization problem does not allow for a straightforward solution for the following reasons:

1) No closed form solution is available.
2) The cost function $f(\cdot)$ is none-convex in $\boldsymbol{R}$, meaning several maxima exist.
3) The restriction to orthogonal matrices forces special manifold optimization techniques.

To deal with these effects, an iterative approach with a starting point close to the maximum is implemented. Details on how to deal with the manifold structure can be found in [12] and especially for the orthogonal manifold in [13]. A steepest ascend line search algorithm on that manifold is used. The involved Euclidean gradient needed reads:

$$\nabla_{\boldsymbol{R}} f(\boldsymbol{R}; \boldsymbol{B}, \boldsymbol{E}, \boldsymbol{Y}) = \sum_{m=1}^{M} \sum_{l=1}^{N} y_{m,l}^* j 2\pi e^{j2\pi \boldsymbol{b}_m^T \boldsymbol{R} \boldsymbol{e}_l} \boldsymbol{b}_m \boldsymbol{e}_l^T \tag{13}$$

The following parametrization for the cost function is used:

$$\begin{aligned} \boldsymbol{B} &= [\boldsymbol{b}_1, .., \boldsymbol{b}_M] \\ \boldsymbol{E} &= [\boldsymbol{e}_1, .., \boldsymbol{e}_N] \\ \boldsymbol{Y} &= [\boldsymbol{y}_1, .., \boldsymbol{y}_N] \end{aligned} \tag{14}$$

Without considering the restriction of the feasible set $\mathcal{SO}(3)$, the convergence properties of the algorithm are very poor, i.e. a starting point $\mathbf{R}_0$ has to be chosen, which is very near the optimal value. However, this can be dropped, if a successive estimation over time ("tracking") is considered. The estimate of the last epoch is used to initialize the estimation of the current epoch. The assumption here is, that the starting for the first iterate is not "to far" away from the optimal point. The maximum distance mainly depends on the current constellation and the geometry (i.e. baseline vectors) of the antenna elements.

Spoofing Detection

If the residual of the attitude estimation problem is larger than a certain threshold ϵ, the presence of a spoofer is detected. If detected, the model stated in in Eq. (9) is rejected. The following is assumed instead:

$$\boldsymbol{y}_l(t) = \boldsymbol{a}(\boldsymbol{e}_l) + \boldsymbol{a}(\boldsymbol{e}_i) g_l^s + \boldsymbol{\nu}_l \tag{15}$$

The steering vector $\boldsymbol{a}(\boldsymbol{e}_i)$ is assumed to be observed at the correlator output of more than one satellite channel of the receiver. If it can be found, a projection into this orthogonal subspace is performed, redoing the process of finding the direction. This naturally corresponds to a mitigation of the spoofer.

The direction finding process is repeated taking the projection into account. This is repeated at most $L - 1$ times, yielding a succesive cancellation of the spoofers DoA.

Mitigation

If a spoofer was detected, the fundamental assumption is the presence of the corresponding steering vector in several satellite channels of the multi-antenna correlator outputs. The correlation matrix of a corresponding tracking channel l reads:

$$C_l^y \approx a_l a_l^H + |g_l^s|^2 a_i^s a_i^{H,s} + 2\mathrm{Re}\{g_l^s a_i^s a_l^H\} \quad (16)$$

This is an approximation since the noise is considered small compared to the signal. The span of the correlation matrices is caused by the steering vector of the nominal signal and the steering vector of the spoofers direction i, from which the "fake" PRN l is transmitted. Summing up the available correlation matrices will (according) to the spoofers parameters emphasize this steering vector in the final span of C_l^y.

$$C^y = \frac{1}{N}\sum_{l=1}^{N} C_l^y \quad (17)$$

Under the assumption that the spoofing steering vector spans the dominant space of the correlation, it's estimate is given by:

$$\hat{a}_i(e^s) = \arg\max_{a} a^H C^y a \quad \text{s.t.} \quad \|a\| = 1 \quad (18)$$

The solution is given by choosing the eigenvector corresponding to the strongest eigenvalue of C^y.

To mitigate the effect of the spoofer, the output of the correlation process is projected (i.e. spatially filtered) in the orthogonal subspace spanned by the estimated spoofing direction, which is given by:

$$P_\perp(\hat{a}_i(e^s)) = I - \frac{1}{\|\hat{a}_i(e^s)\|^2}\hat{a}_i(e^s)\hat{a}_i(e^s)^H \quad (19)$$

When considering eigenvectors directly, the normalization can be dropped by definition, yielding:

$$P_\perp(\hat{a}_i(e^s)) = I - \hat{a}_i(e^s)\hat{a}_i(e^s)^H \quad (20)$$

The attitude estimation process is repeated by solving the optimization problem stated in Eq. (12) in the projected subspace:

$$R^* = \arg\max_{R\in\mathcal{SO}(3)} \underbrace{\sum_{l=1}^{N} \|y_l^H P_\perp a_l(R)\|^2}_{:=f(R;P,Y,B,E)} \quad (21)$$

Final Algorithm

The final algorithm is depicted in Fig. 3:

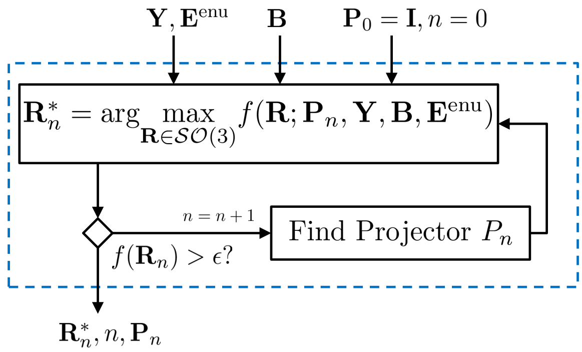

Fig. 3: Simultaneous attitude estimation and spoofing detection algorithm. $f(R) = f(R; P, Y, B, E)$ is used as a short cut in the block diagram.

The estimation process is performed initially under the assumption, that no spoofer is present. If a spoofer is detected by inspecting the cost function using the optimal estimate for the attitude, a dominant direction using all estimates for the correlations is searched for constructing the projector. This process is repeated by continuously searching for dominant subspaces if the residual is to large.

Simulation Results

Software simulations have been performed to test the performance of the proposed algorithm before processing real data. Several scenarios have been set up using different parameters.

Scenario 1

The first scenario consists of a random constellation using 5 nominal signals with randomly chosen elevation and azimuth angles. The array consists of a 2×2 uniform rectangular array (URA) with baseline vectors spaced by $\frac{\lambda}{2}$. The center of the antenna coordinate frame is chosen as the center of point symmetry of this configuration, yielding the following baseline vectors:

$$B = [b_1, b_2, b_3, b_4] = \frac{\lambda}{4}\begin{pmatrix} 1 & 1 & -1 & -1 \\ 1 & -1 & 1 & -1 \\ 0 & 0 & 0 & 0 \end{pmatrix} \quad (22)$$

The starting point R_0 to initialize the line search algorithm was chosen to have a difference in pitch, roll and yaw of each 40 degree from the true attitude. This value was used for all simulations performed.

Fig. 4 shows the outcome of the attitude estimation using algorithm depicted in Fig. 3. A noise variance of 0.01 was chosen. This corresponds to a signal to noise ratio in the post-correlation domain of about 40dB. 100 successive simulation runs have been performed.

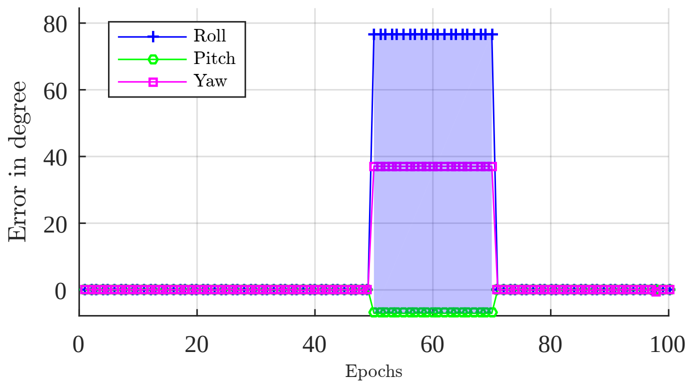

Fig. 4: Quality of estimated attitude compared to ground truth used for simulation.

For simulation run 50 to 70 a spoofer coming in from a randomly chosen direction was added on all 5 signals, with an amplitude of 2 for all signals. Fig. 5 shows the corresponding residual of the cost function with and without performing the mitigation strategy described in the previous sections.

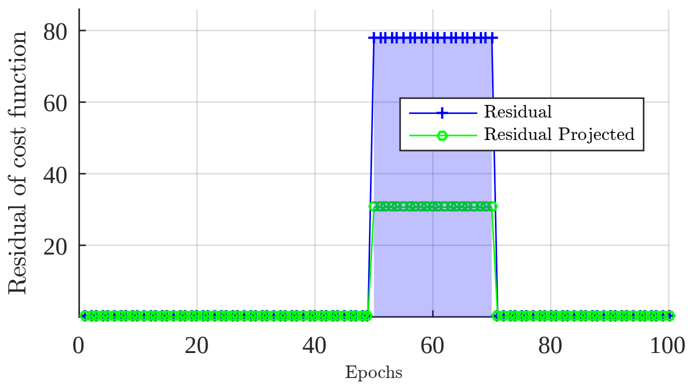

Fig. 5: Residual of optimization cost function.

Since the estimation of the underlying rotation alone is not enough to explain the structure of the incoming signal, for periods 50 to 70 the presence of a spoofer is declared (indicated by the blue background).

To investigate the effect of the residual, several parameter variations of the spoofer to nominal signal ratio have been performed. The results are presented in the next chapter.

Residual of Cost function in Presence of Spoofer

Several simulation runs have been performed to determine the effect of spoofer with different spoofer to signal ratio varying from -25 to 15 dB. The result is depicted in Fig. 6:

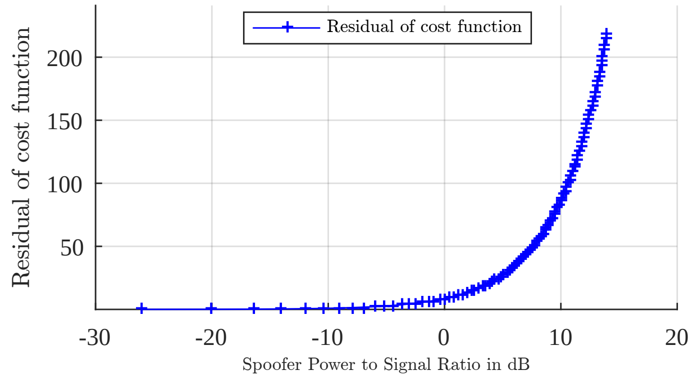

Fig. 6: Residual of optimization cost function depending on spoofers nominal to signal ratio.

Every simulation run was repeated 30 times. The mean value of all runs was chosen as representative value. 10 incoming signals have been used to perform the simulations. The nominal signal to noise ratio was again 40 dB.

Fig. 7 shows the difference of the residual in the cost function for mitigation.

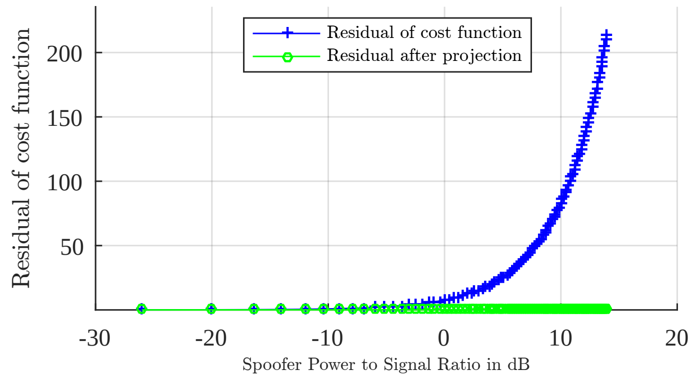

Fig. 7: Residual of optimization cost function dependent on the projected and mitigated case.

Fig. 8 again shows the effect of performing one projection. This time 5 spoofing PRNs are chosen from one direction and the other 5 from an other direction.

The quality of the attitude estimation can be measured in terms of the matrix norm $\|\boldsymbol{R} - \boldsymbol{R}^*\|$. This difference is compared for the unprojected and mitigated case in Fig. 9. It can clearly be seen that a bias is introduced for weak spoofing powers. This is most likely be caused by an error in the estimate of the spoofers direction, i.e. not all contributions of the spoofer are spatially filtered. The stronger the spoofers power is, the better is the estimate. However, a constant bias is introduced.

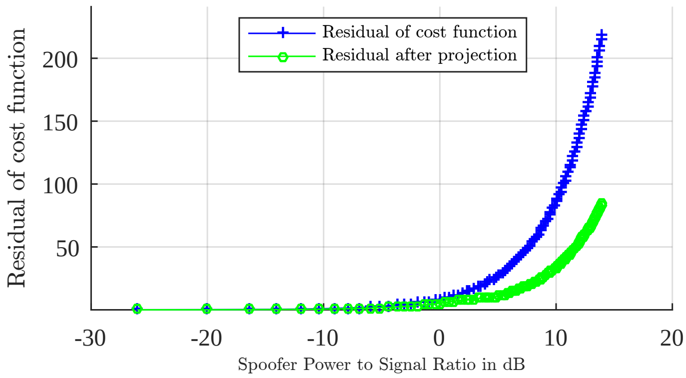

Fig. 8: Residual of optimization cost function.

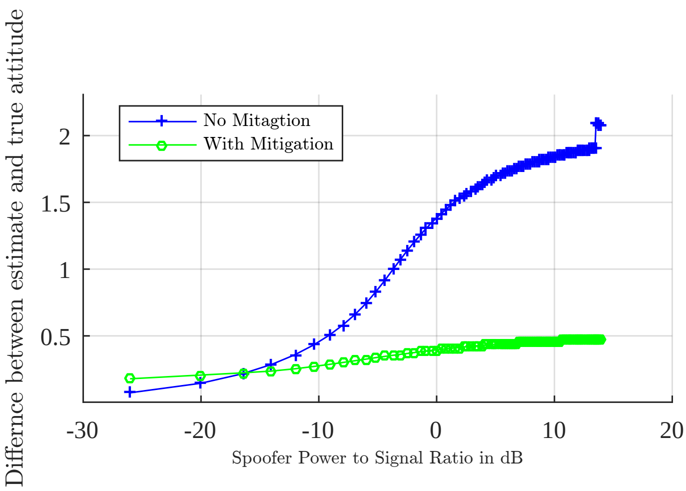

Fig. 9: Residual of optimization cost function.

Conclusion and Outlook

An approach for solving the joint problem of estimating an antenna arrays attitude and detecting spoofing/meaconing attacks by using the correlator outputs of an GNSS array receiver has been proposed. A physical model of the array receiver has been introduced and used further to formulate the estimation problem and describe the associated assumptions. It has been shown that the resulting optimization problem has no closed-form solution and therefore an iterative algorithm has been proposed (see Fig. 3). The gradients of the optimization cost function required in the iterative algorithm has been derived. In order to evaluate the performance of the proposed solution, numerical simulations, where a 2-by-2 uniform rectangular array with half-wavelength spacing of the antenna elements was used, have been performed. The results of the numerical simulations indicate the ability to reliably detect the simulated spoofing attack and mitigate the interference. In these simulations, an accurate estimation of the array attitude has been delivered under the interference-free conditions while systematic estimation errors on the level of up to 40 degrees (e.g. for yaw angle, see Fig. 4) have been observed.

Future work will focus on the improving of the algorithm performance including the following topics:

- performing more extensive hardware simulations in order to cover a larger scope of possible spoofing/meaconing scenarios
- extension of the proposed approach to the case of sequential estimation
- assessment of the statistical properties of the proposed detection scheme
- evaluating the proposed approach on raw samples collected in field experiments

Acknowledgment

Some parts of the research leading to the results reported in this paper have been funded by the program Research for Civil Security of the Federal Ministry of Education and Research (BMBF) of the Federal Republic of Germany under the grant FKZ 13N12744. Other aspects presented in this paper have been funded within the project KOSERNA by the German Aerospace Center (DLR) on behalf of the German Federal Ministry of Economics and Technology under grant nr 50 NA 1406. This support is greatly acknowledged.

References

[1] M. Meurer, A. Konovaltsev, M. Cuntz, and C. Httich, "Robust Joint Multi-Antenna Spoofing Detection and Attitude Estimation using Direction Assisted Multiple Hypotheses RAIM," in *Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012)*, Nashville, TN, Sep. 2012, pp. 3007–3016.

[2] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandon, and G. Lachapelle, "A Low-Complexity GPS Anti-Spoofing Method Using a Multi-Antenna Array," in *Proceedings of the 25th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012)*, Nashville, TN, Sep. 2012, pp. 1233–1243.

[3] A. Konovaltsev, M. Cuntz, C. Haettich, and M. Meurer, "Autonomous Spoofing Detection and Mitigation in a GNSS Receiver with an Adaptive Antenna Array," in *Proceedings of the 26th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2013)*, Nashville, TN, Sep. 2013, pp. 2937–2948.

[4] M. Appel, A. Konovaltsev, and M. Meurer, “Robust Spoofing Detection and Mitigation based on Direction of Arrival Estimation,” in *Proceedings of the 28th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2015)*, Tampa, Florida, Sep. 2015, pp. 3335–3344.

[5] M. Meurer, A. Konovaltsev, M. Appel, and M. Cuntz, “Direction-of-Arrival Assisted Sequential Spoofing Detection and Mitigation,” in *Proceedings of the 2016 International Technical Meeting of The Institute of Navigation*, Monterey, California, Jan. 2016, pp. 181–192.

[6] M. Markel, E. Sutton, and H. Zmuda, “An antenna array-based approach to attitude determination in a jammed environment,” in *Proceedings of the 14th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GPS 2001)*, vol. 1114, Salt Lake City, UT, USA, 2001.

[7] S. Daneshmand, N. Sokhandan, and G. Lachapelle, “Precise GNSS Attitude Determination Based on Antenna Array Processing,” in *Proceedings of the 27th International Technical Meeting of The Satellite Division of the Institute of Navigation*, vol. 812, Tampa, FL, USA, 2014.

[8] M. Appel, A. Hornbostel, and C. Haettich, “Impact of Meaconing and Spoofing on Galileo Receiver Performance,” in *7th ESA Workshop on Satellite Navigation Technologies NAVITEC*, 2014. [Online]. Available: http://elib.dlr.de/93975/

[9] G. A. McGraw, R. S. Young, K. Reichenauer, J. Stevens, and F. Ventrone, “GPS Multipath Mitigation Assessment of Digital Beam Forming Antenna Technology in a JPALS Dual Frequency Smoothing Architecture,” in *Proceedings of the 2004 National Technical Meeting of The Institute of Navigation*, San Diego, CA, Jan. 2004, pp. 561–572.

[10] H. L. Van Trees, *Optimum Array Processing (Detection, Estimation, and Modulation Theory, Part IV)*, 1st ed. Wiley-Interscience, Mar. 2002, published: Hardcover.

[11] P. Misra and P. Enge, *Global Positioning System: Signals, Measurements and Performance Second Edition*. Lincoln, MA: Ganga-Jamuna Press, 2006.

[12] P.-A. Absil, R. Mahony, and R. Sepulchre, *Optimization Algorithms on Matrix Manifolds*. Princeton, NJ: Princeton University Press, 2008.

[13] A. Edelman, T. A. Arias, and S. T. Smith, “The geometry of algorithms with orthogonality constraints,” *SIAM J. MATRIX ANAL. APPL*, vol. 20, no. 2, pp. 303–353, 1998.