

Article

A Multi-Antenna Scheme for Early Detection and Mitigation of Intermediate GNSS Spoofing

Jaroslav Magiera 

Faculty of Electronics, Telecommunications and Informatics, Gdansk University of Technology,
ul. G. Narutowicza 11/12, 80-233 Gdansk, Poland; jaroslav.magiera@eti.pg.edu.pl

Received: 13 April 2019; Accepted: 24 May 2019; Published: 27 May 2019



Abstract: This article presents a method for detecting and mitigating intermediate GNSS spoofing. In this type of attack, at its early stage, a spoofer transmits counterfeit signals which have slight time offsets compared to true signals arriving from satellites. The anti-spoofing method proposed in this article fuses antenna array processing techniques with a multipath detection algorithm. The latter is necessary to separate highly correlated true and counterfeit GNSS signals. Spoofing detection is based on comparison of steering vectors related to received spatial components. Whereas mitigation is achieved by means of adaptive beamforming which excises interferences arriving from common direction and preserves undistorted signals from GNSS satellites. Performance of proposed method is evaluated through simulations, results of which prove the usefulness of this method for protecting GNSS receivers from intermediate spoofing interference.

Keywords: GNSS spoofing; spoofing detection; spoofing mitigation; array processing; beamforming; multipath detection

1. Introduction

Spoofing attacks are a well-known threat to the security of civilian GNSS receivers. This malicious interference resembles a bundle of genuine signals arriving from navigation satellites, yet with changed relative delays or carrying modified navigation messages. Spoofing is aimed to force target receiver to indicate incorrect position, velocity and time (PVT) information [1].

Due to low power of spoofing signals and their similarity to true signals, spoofing is far more difficult to detect than jamming. Numerous GNSS spoofing countermeasures have been proposed so far, varying in robustness and complexity [2–4]. Effectiveness of various spoofing detection algorithms depends on how sophisticated is the spoofing device (spoofer). Simplistic spoofing attacks may be conducted using an off-the-shelf GNSS constellation simulator connected to a power amplifier with a transmit antenna [5]. In this case target receiver is expected to lock to strong falsified signals while weaker genuine ones are jammed. This type of spoofing may be detected using relatively simple methods which usually require only modifications of receiver’s software.

In more advanced spoofing scenario, called intermediate spoofing or carry-off attack, spoofer is directly connected with own GNSS receiver which provides current information about parameters of genuine signals [6]. It initially transmits signals which are precisely synchronized with signals arriving from navigation satellites to target receiver. Power of transmitted signals is gradually increased in order to take control over receiver’s tracking loops [7]. After that, relative delays between component signals are manipulated, resulting in calculated position drifting away from the true one. This kind of attack, if conducted properly, will be imperceptible to most of currently used civilian receivers. This means that, unlike in simplistic spoofing scenario, there will be no discontinuities in providing PVT information. Detection of such attack using methods restricted to receiver’s software is in most cases not effective. Multi-antenna signal processing is found to be the most robust approach among spoofing

detection methods which do not employ cryptography nor require additional sensors such as inertial measurement units [8].

Multi-antenna receivers may still be spoofed in the case of coordinated transmission through a distributed network of antennas, when each component signal has a different direction of arrival (DOA) [6]. This scenario, called sophisticated spoofing, is however very unlikely to happen in practice since it is extremely difficult to conduct as long as receiver is not exposed to spoofing on purpose.

Various spatial processing methods for GNSS spoofing detection and mitigation have been proposed in the last several years. In [9,10] authors use a single moving antenna, which corresponds to synthetic antenna array, to analyze spatial patterns of received GNSS signals. Still, it is more often preferred to use a physical antenna array due to better performance and independence from antenna motion. In [11,12] dual-antenna carrier phase measurements are used for purpose of spoofing detection. In [13] an adaptive antenna array is used to both detect and mitigate spoofing basing on DOA analysis, incorporating receiver's antenna attitude estimation. However, estimating actual DOA requires precise array calibration which may be cumbersome. In [14,15] the authors propose GNSS spoofing countermeasures based on analysis of signals' steering vectors, assuming that these vectors may be estimated independently for authentic and spoofing signals. It may not be achieved if these signals are correlated as in case of early stage of intermediate spoofing.

In [16,17] our multi-antenna approach to detection and mitigation of GPS spoofing was presented. However, it was intended for scenarios where spoofing signals are significantly stronger than true signals and there is a relatively large time offset between them. This situation corresponds to either simplistic spoofing or late stage of intermediate spoofing. It is highly desirable that intermediate spoofing is mitigated before it introduces a significant error in position indicated by GNSS receiver. In this paper, a novel version of multi-antenna anti-spoofing scheme is presented, which allows to detect and filter out falsified GNSS signals at early stage of intermediate spoofing, i.e., in the beginning of carry-off phase.

The remainder of this paper is organized as follows: the second part describes the mathematical model of GNSS signals in the presence of intermediate spoofing. Next, the proposed methods for spoofing detection and mitigation are described. The fourth part presents results of simulations which were conducted to validate the anti-spoofing algorithms. The final part presents the conclusions.

2. Intermediate GNSS spoofing Signal Model

In normal conditions (i.e., without spoofing) K_{sat} signals arriving from GNSS satellites are present at receiver's antenna input. Baseband equivalent of a single signal incoming from k -th satellite may be written as:

$$s_{sat}^k(t) = \sqrt{2P_{sat}^k} \times D^k(t - \tau_{sat}^k) \times C^k(t - \tau_{sat}^k) \times e^{i2\pi f_D^k(t - \tau_{sat}^k)}, \quad (1)$$

where D^k represents navigation data component, C^k —pseudorandom (PRN) code component, P_{sat}^k —received power of k -th signal, f_D^k —carrier Doppler shift and τ_{sat}^k —propagation delay from k -th satellite to receiver's antenna phase centre.

In case of spoofing attack, a bundle of $K_{spoofer}$ GNSS signals is transmitted by spoofer. Each of spoofing signal's components at receiver's antenna input is described as:

$$s_{spoofer}^k(t) = \sqrt{2P_{spoofer}^k} \times D^k(t - \tau_{sat}^k - \tau_{spoofer}^k) \times C^k(t - \tau_{sat}^k - \tau_{spoofer}^k) \times e^{i2\pi f_D^k(t - \tau_{sat}^k - \tau_{spoofer}^k)} \quad (2)$$

where $\tau_{spoofer}^k$ is an additional signal delay introduced by spoofer. It is assumed that spoofer has knowledge about receiver's true position so it may calculate accurate τ_{sat}^k values basing on current GNSS ephemeris data. Moreover, spoofer disciplined by GPS clock can reproduce carrier Doppler shifts of genuine signal as observed by the target receiver.

In the first stage of intermediate spoofing, τ_{spoof}^k for each signal is set to zero, thus genuine and falsified signals arriving to receiver are time-aligned. After increasing P_{spoof}^k to be greater than respective P_{sat}^k , τ_{spoof}^k values are modified to shift pseudorange measurements and, in consequence, affect indicated position information. The correlator output during consecutive carry-off spoofing phases is shown in Figure 1.

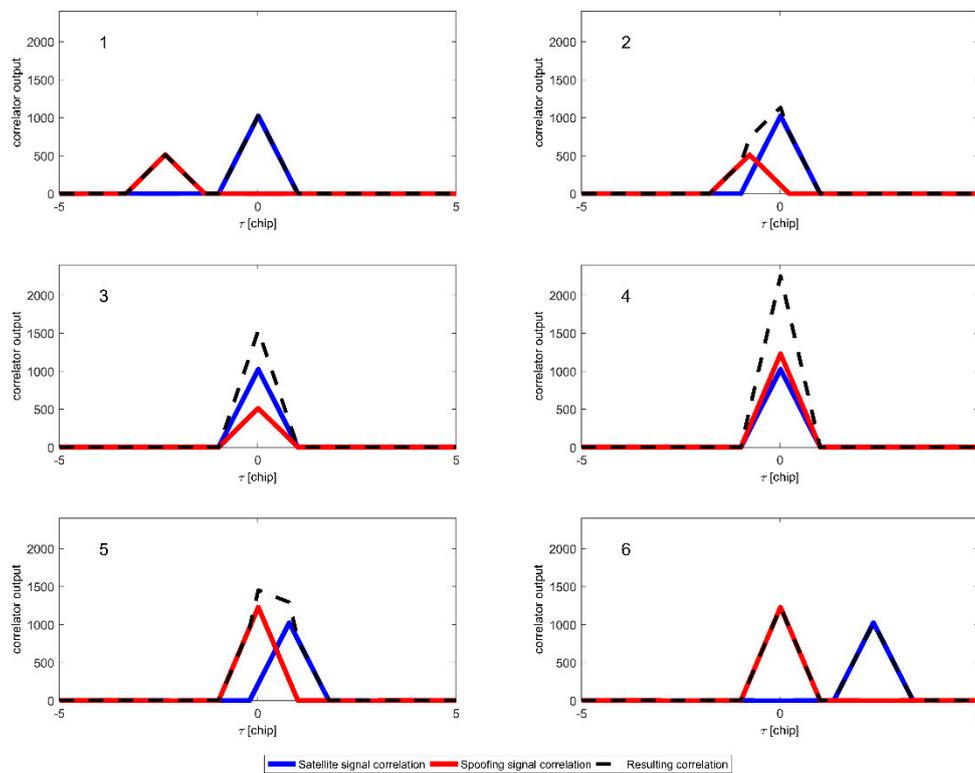


Figure 1. Correlator output during early phase of intermediate spoofing: code phase alignment (1–3), taking control over code tracking loops (4), carry-off—moving the correlation peak away from the true position (5,6).

For a multi-antenna receiver, any component GNSS signal, either true or spoofing, in m -th receive chain is given by following formula:

$$s_{sat(spoof)}^{m,k}(t) = s_{sat(spoof)}^k(t) \times a_{sat(spoof)}^{m,k} \times e^{i\phi_m} \quad (3)$$

where $a_{sat(spoof)}^{m,k}$ is a complex coefficient representing shift in signal's amplitude and phase between m -th antenna element and array reference point. ϕ_m symbol represents signal phase shift introduced in m -th chain between receive antenna and ADC. This phase shift is equal for all received GNSS signals.

A set of all coefficients a of k -th signal received using M -element antenna array form a steering vector:

$$\mathbf{a}_{sat(spoof)}^k = \begin{bmatrix} a_{sat(spoof)}^{1,k} & a_{sat(spoof)}^{2,k} & \cdots & a_{sat(spoof)}^{M,k} \end{bmatrix}^T \quad (4)$$

For a fixed antenna array geometry, the steering vector is related to the incoming signal's direction-of-arrival. Thus, knowing that all falsified signals arrive from the same direction, it is possible to detect GNSS spoofing by comparing steering vectors of received signals. Evaluated values of common steering vector related to falsified signals are then used to control an adaptive spatial filter which excises the adverse spoofing component. Procedures for early detection and mitigation of intermediate GNSS spoofing are described in next section.

3. Early Detection and Mitigation of Spoofing

Assuming that each GNSS signal arrives to target receiver along a single path, composite signal received through m -th sensor of antenna array may be described as:

$$s^m(t) = \sum_{k=1}^{K_{sat}} s_{sat}^{m,k}(t) + \sum_{k=1}^{K_{spoo}} s_{spoo}^{m,k}(t) + \eta_m(t) \quad (5)$$

where $\eta_m(t)$ represents additive noise which is uncorrelated between any pair of antennas.

In concept shown in Figure 2, signal (5) impinges on the receive antenna array. Output signals from all array sensors are shifted to lower frequency band and converted to digital form (these steps were not shown for brevity). Next, signal from a single sensor is processed in acquisition block which determines the indices of received GNSS signals, their carrier Doppler shifts and PRN code phase shifts. While signal acquisition is inherent to any GNSS receiver, remaining blocks in Figure 2 are specific to proposed anti-spoofing scheme. The procedure consists of three stages described in the following subsections.

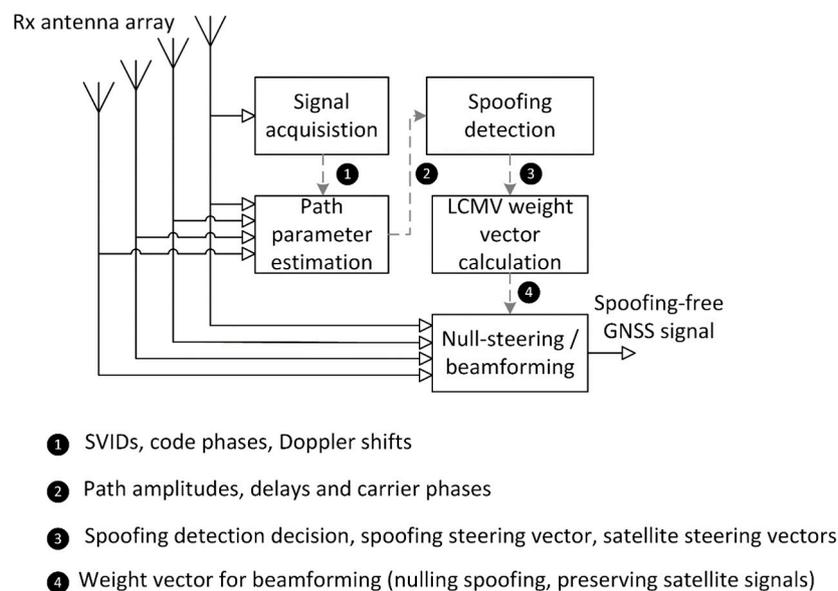


Figure 2. Scheme for detecting and mitigating intermediate GNSS spoofing.

3.1. Steering Vector Estimation

Prior to actual spoofing detection, individual steering vectors need to be estimated. Determining them requires all component signals in (5) to be separated. In absence of spoofing, particular signals may be extracted basing on their unique spreading codes (CDMA – GPS, Galileo) or occupied frequency channel (FDMA - GLONASS). However, when spoofing signals interfere with true signals, estimation of steering vectors is not straightforward. Both signals assigned to the same space vehicle ID (SVID) may be tracked separately if their relative delay is large enough so that they are represented as distinguishable peaks in correlation function. Minimum required delay is equal to one chip duration, which in case of GPS L1 signals is 1 microsecond that corresponds to 300 m of pseudorange difference. In early phase of intermediate spoofing, relative delays between genuine signals and respective falsified signals are much smaller.

In order to detect signals with similar code delays, methods may be adopted which are already used for multipath detection in GNSS receivers. Majority of them is based on multiple correlator architecture, on successive multipath component cancellation or on maximum likelihood (ML) principle.

In this article the last option was chosen as it employs optimum algorithm which provides most accurate parameter estimation.

Considering reception period without 180-degree phase transitions related to navigation data, baseband equivalent of received multipath signal received through m -th antenna may be presented in the following way [18]:

$$s^{m,k}(t) = \sum_{l=1}^{L^k} A_l^{m,k} \times C^k(t - \tau_l^k) \times e^{i\phi_l^{m,k}} + \eta^m(t) \quad (6)$$

assuming that the carrier Doppler shift is compensated in the receiver. L^k symbol in (6) represents the number of multipath components in signal from the k -th satellite. Each component is characterized by parameters $A_l^{m,k}$, τ_l^k and $\phi_l^{m,k}$ representing its amplitude, delay and phase shift at m -th array sensor. In ML approach such values of these parameters are sought, which minimize loss function Γ defined as square error between received multipath signal $s^{m,k}$ and its estimate:

$$\Gamma(\hat{\mathbf{A}}^{m,k}, \hat{\boldsymbol{\tau}}^k, \hat{\boldsymbol{\phi}}^{m,k}) = \int \left| s^{m,k}(t) - \sum_{l=1}^{L^k} \hat{A}_l^{m,k} \times C^k(t - \hat{\tau}_l^k) \times e^{i\hat{\phi}_l^{m,k}} \right|^2 dt \quad (7)$$

where $\hat{\mathbf{A}}^{m,k}$, $\hat{\boldsymbol{\tau}}^k$, $\hat{\boldsymbol{\phi}}^{m,k}$ represent L^k -element vectors of respective parameter estimates for k -th GNSS signal. Under assumption that each received signal has only two components, i.e., a true one and the spoofing one, Equation (7) may be written as:

$$\begin{aligned} & \Gamma(\hat{\mathbf{A}}^{m,k}, \hat{\boldsymbol{\tau}}^k, \hat{\boldsymbol{\phi}}^{m,k}) \\ &= \int \left| s^{m,k}(t) - \hat{A}_{sat}^{m,k} \times C^k(t - \hat{\tau}_{sat}^k) \times e^{i\hat{\phi}_{sat}^{m,k}} - \hat{A}_{spoo}^{m,k} \times C^k(t - \hat{\tau}_{spoo}^k) \times e^{i\hat{\phi}_{spoo}^{m,k}} \right|^2 dt \end{aligned} \quad (8)$$

The major disadvantage of the ML approach is its high computational complexity, which often prevents its practical application. In a multipath scenario, complexity grows exponentially with the number of spatial components. Even when there are only two spatial paths, ML procedure involves searching for optimal solution in a six-dimensional space $[\hat{A}_1^{m,k}, \hat{A}_2^{m,k}, \hat{\tau}_1^k, \hat{\tau}_2^k, \hat{\phi}_1^{m,k}, \hat{\phi}_2^{m,k}]$, which is challenging for real-time implementation. However, in such case it is possible to apply an estimator called MMT (*Multipath Mitigation Technology*), which substantially reduces computational complexity [19]. The principle of MMT is to transform the vector of unknown parameters in such way that scanning is performed only in two-dimensional space, while optimal values of remaining four parameters are calculated using closed-form formulas. The loss function is decomposed to a sum of in-phase (I) and quadrature (Q) components. For k -th GNSS signal impinging on m -th element of antenna array it may be written as:

$$\begin{aligned} \Gamma(\hat{\mathbf{A}}^{m,k}, \hat{\boldsymbol{\tau}}^k, \hat{\boldsymbol{\phi}}^{m,k}) &= \int [I^m(t) - a \times C^k(t - \hat{\tau}_1^k) - b \times C^k(t - \hat{\tau}_2^k)]^2 dt + \\ & \int [Q^m(t) - c \times C^k(t - \hat{\tau}_1^k) - d \times C^k(t - \hat{\tau}_2^k)]^2 dt, \end{aligned} \quad (9)$$

where I^m and $Q^m(t)$ are real and imaginary parts of the overall signal received through the m -th antenna, and:

$$\begin{aligned} a &= \hat{A}_1^{m,k} \times \cos(\hat{\phi}_1^{m,k}), \quad b = \hat{A}_2^{m,k} \times \cos(\hat{\phi}_2^{m,k}), \\ c &= \hat{A}_1^{m,k} \times \sin(\hat{\phi}_1^{m,k}), \quad d = \hat{A}_2^{m,k} \times \sin(\hat{\phi}_2^{m,k}). \end{aligned} \quad (10)$$

It should be noted that $\hat{\boldsymbol{\tau}}^k$ is considered to be independent from m , since relative delays of signal propagation between array sensors introduce negligibly small shifts in code phase. On the other hand, amplitudes and carrier phase shifts for different antennas may vary significantly.

The optimum solution is sought within $\hat{\tau}^k = [\hat{\tau}_1^k, \hat{\tau}_2^k]$ space, where, for each considered pair of code delays, values of parameters a , b , c and d are evaluated which locally minimize the loss function. These are obtained by solving following equations:

$$\frac{\partial \Gamma}{\partial a} = 0 \quad \frac{\partial \Gamma}{\partial b} = 0 \quad \frac{\partial \Gamma}{\partial c} = 0 \quad \frac{\partial \Gamma}{\partial d} = 0 \quad (11)$$

Once the global minimum of loss function is found, values of $[\hat{A}_1^{m,k}, \hat{A}_2^{m,k}, \hat{\phi}_1^{m,k}, \hat{\phi}_2^{m,k}]$ may be calculated by solving set of equations (10). Next, for each spatial path, a steering vector is created in the following form:

$$\mathbf{a}_p^k = \left[\hat{A}_p^{1,k} \times e^{i\hat{\phi}_p^{1,k}} \quad \hat{A}_p^{2,k} \times e^{i\hat{\phi}_p^{2,k}} \quad \dots \quad \hat{A}_p^{M,k} \times e^{i\hat{\phi}_p^{M,k}} \right]^T \quad (12)$$

3.2. Spoofing Detection

Respective steering vectors are related to signals' directions of arrival, thus they may be used for detecting multiple signals originating from a single antenna. In proposed method, spoofing is detected when four or more GNSS signals arrive from the same direction. This assumption is based on the fact that at least four falsified signals are required to induce incorrect position. It is expected that in real spoofing scenarios the number of counterfeit signals will be similar to the number of visible satellites. Less than four spoofing signals could be possibly discarded by RAIM algorithm [20], as they would be considered inconsistent with majority of received genuine signals.

In order to assess whether two spatial components arrive from the same direction, their steering vectors are compared. Since a spoofer may transmit signals with different amplitudes and carrier phase shifts, it is necessary to normalize steering vectors before comparing them. It is performed by simply dividing all components of vector by the value of its first component:

$$\check{\mathbf{a}}_p^k = \frac{\mathbf{a}_p^k}{\hat{A}_p^{1,k} \times e^{i\hat{\phi}_p^{1,k}}} \quad (13)$$

The distance between any two steering vectors is defined as a complex norm of their difference:

$$\Delta \mathbf{a}_{i,j} = \|\mathbf{a}_i - \mathbf{a}_j\| \quad (14)$$

When steering vectors for all received spatial components are determined, spoofing detection is performed, following the algorithm presented in Figure 3.

First, for all pairs of steering vectors, their distances are calculated. For K steering vectors there are $K(K-1)/2$ unique distances $\Delta \mathbf{a}_{i,j}$. Next, distances are compared against the threshold value $\Delta \mathbf{a}_{thr}$. The ones which are above this threshold are discarded as they are considered too large for signals arriving from the same direction. Initially, a hypothetical number of spoofing signals K_{spoof} is set to four as a minimum number of signals required to estimate receiver's position. Then, all possible K_{spoof} -combinations of steering vectors are analyzed. For each combination of vectors it is checked whether all of their distances are included in the set of remaining $\Delta \mathbf{a}_{i,j}$ (i.e., not greater than $\Delta \mathbf{a}_{thr}$). If the test result is positive, K_{spoof} is increased by one and the check is repeated. Otherwise, $K_{spoof} - 1$ spoofing signals are detected if K_{spoof} is greater than four. In other case, the algorithm ends without spoofing detection.

In the case of positive spoofing detection, an alarm should be raised to warn the user that the indicated position or time information may not be correct. Apart from that, steering vectors are divided into two groups—one group contains steering vectors related to genuine signals, while the other one contains steering vectors related to counterfeit signals. This information is passed to spoofing mitigation block.

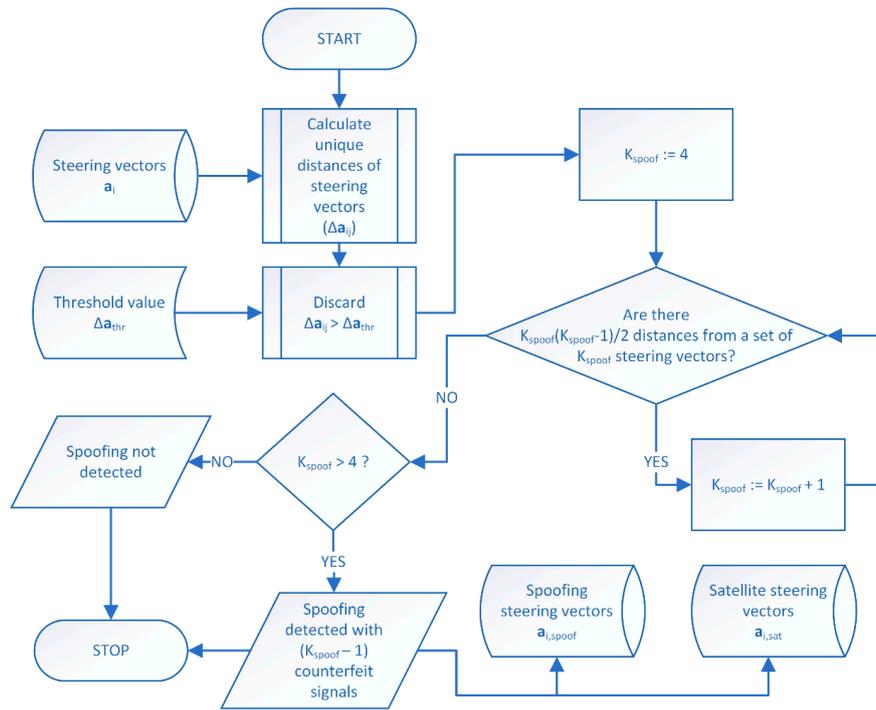


Figure 3. GNSS spoofing detection algorithm.

3.3. Determining Optimal Spoofing Detection Threshold

In the spoofing detection procedure, a threshold Δa_{thr} is set which is used to distinguish pairs of spoofing steering vectors from other pairs of steering vectors. It is required to evaluate optimal threshold which will maximize the probability of spoofing detection with acceptably small probability of false alarm. A false alarm is considered as a situation when spoofing signals are not present, but detection is positive since for K_{sat} signals received from satellites there are $[K_{sat} \times (K_{sat} - 1)/2]$ distances of steering vectors which do not exceed Δa_{thr} . It may occur when noisy steering vectors are evaluated for satellite signals which arrive from narrow spatial sector.

Probability of spoofing detection may be estimated using the following formula:

$$P_d = P \left[\forall_{1 \leq i < K} \forall_{j > i} (\Delta a_{ij} \leq \Delta a_{thr}) \right] = \prod_{i=1}^{K-1} \prod_{j=i+1}^K \int_0^{\Delta a_{thr}} \{p(\Delta a_{ij})\} d\Delta a_{ij} \quad (15)$$

where $p(\Delta a_{ij})$ is the probability density function (PDF) of the distance between i -th and j -th steering vectors. When signals arrive from the same direction, as in spoofing case, $p(\Delta a_{ij})$ depends only on C/N_0 values of components related to particular SVs. On the other hand, when no-spoofing case is considered, $p(\Delta a_{ij})$ is also a function of true non-zero distance between given pair of steering vectors. Thus, in order to evaluate the threshold value for which acceptable probability of false alarm is not exceeded, the worst case no-spoofing scenario should be analyzed with smallest nominal distances Δa_{ij} observed in practice. When maximum threshold value is found, probability of spoofing detection may be evaluated using (15).

3.4. Spoofing Mitigation

Basically, spoofing is mitigated by means of adaptive control of the antenna reception pattern. When using an antenna array consisting of M sensors, $M-1$ degrees of freedom are available for steering spatial nulls or pointing beams towards particular directions. If a composite spoofing signal arrives

from only one direction (or it has a dominant line-of-sight component), a single spatial null will suffice to remove this undesired component before it is passed to the GNSS receiver's input. However, setting a single null without any other constraints may lead to a significant SNR decrease of desired signals from GNSS satellites as well. This is because a null exploiting only a single degree of freedom is spread over a range of directions which contain DOA of spoofing component, but may also include DOAs of genuine signals. It is possible to make use of all available degrees of freedom to establish a deep and spatially narrow null. However, in such case it is still not possible to control the distortion of signals from GNSS satellites. The better approach is to use each of remaining $M-2$ degrees of freedom to put a constraint setting 0 dB gain for given genuine signal. Minimum Variance Distortionless Response (MVDR) is a beamforming scheme which minimizes the output power while preserving a component arriving from desired direction [21]. Here, a modified version of MVDR is used, called Linearly Constrained Minimum Variance (LCMV) which allows for more than one constraint [22]. In this case, one constraint places a null for undesired spoofing components while other ones assure undistorted reception of signals from satellites. It should be noted that the main optimization criterion for both MVDR and LCMV beamforming algorithms is minimizing the power at the output of the antenna array. This means that, apart from spoofing mitigation, strong interference such as jamming will be removed as well, as long as its DOA does not coincide with DOA of acquired satellite signal.

In practice, due to noise and mutual interference between GNSS signals, steering vectors estimated for every spoofing component are not exactly the same. Because of that, it is recommended to place a spatial null for each spoofing steering vector instead of a single null which could provide insufficient mitigation performance.

Furthermore, at most $M-K_{spoof} - 1$ steering vectors of true GNSS signals are selected. These signals will be protected from distortion caused by array processing.

A steering matrix \mathbf{A} is created, composed of steering vectors as its columns. The first K_{spoof} columns are the steering vectors of spoofing components, while remaining columns are steering vectors of genuine signals' components:

$$\mathbf{A} = \left[\begin{array}{cccc} \mathbf{a}_{spoof}^1 & \dots & \mathbf{a}_{spoof}^{K_{spoof}} & \mathbf{a}_{sat}^1 & \dots & \mathbf{a}_{sat}^{M-K_{spoof}-1} \end{array} \right] \quad (16)$$

If number of satellite steering vectors is smaller than $M-K_{spoof} - 1$, number of columns in matrix \mathbf{A} is reduced respectively.

Next, constraints vector \mathbf{g} is created in the following form:

$$\mathbf{g} = \left[\begin{array}{cc} \underbrace{0 \ \dots \ 0}_{K_{spoof}} & \underbrace{1 \ \dots \ 1}_{M-K_{spoof}-1} \end{array} \right]^T \quad (17)$$

where zeros correspond to the spatial null constraints and ones represent the non-distortion constraints. Number of elements in vector \mathbf{g} is the same as the number of columns in matrix \mathbf{A} .

Signal y at the output of the adaptive antenna array is a linear combination of array inputs forming vector \mathbf{x} multiplied by weight coefficients forming a weight vector \mathbf{w} .

$$y[n] = \mathbf{w}^H \mathbf{x}[n] \quad (18)$$

where n is the index of time instant and H represents the Hermitian transpose. Weight vector for LCMV beamforming must fulfil the following equation:

$$\mathbf{A}^H \mathbf{w} = \mathbf{g} \quad (19)$$

There may be many solutions of Equation (19), but there is only one which also minimizes the output power. It is calculated using Equation (20):

$$\mathbf{w}_{LCMV} = \hat{\mathbf{R}}_{xx}^{-1} \mathbf{A} (\mathbf{A}^H \hat{\mathbf{R}}_{xx}^{-1} \mathbf{A})^{-1} \mathbf{g} \quad (20)$$

where $\hat{\mathbf{R}}_{xx}$ is the array input covariance matrix estimate based on N snapshots:

$$\hat{\mathbf{R}}_{xx} = \frac{1}{N} \sum_{n=1}^N \mathbf{x}[n] \mathbf{x}^H[n] \quad (21)$$

Output from the LCMV beamformer, being a digital waveform without components caused by spoofing or jamming, may be reconstructed in the analog domain and upconverted to its original frequency band. In such form it may be passed to RF input of GNSS receiver which is supposed to be protected from intentional interference.

When neither spoofing nor jamming are present, weight vector corresponding to single antenna reception should be applied:

$$\mathbf{w} = [1 \ 0 \ \dots \ 0]^T \quad (22)$$

Another possibility is to use a \mathbf{g} vector with all ones, when number of array sensors is at least one more than number of visible satellites.

4. Simulation Results

Performance of the proposed anti-spoofing method was evaluated through computer simulations. These include: a) evaluation of optimum threshold for steering vector distances and b) verification of spoofing detection and mitigation in two spoofing scenarios.

Signal processing procedure was implemented in accordance with scheme presented in Figure 2. Ten-millisecond waveforms of signals received through array sensors were generated, following the formula (5). GPS L1 C/A signal structure was used, but it should be noted that presented approach generally applies to all GNSS signals based on spread spectrum technique. Additive noise components were uncorrelated between array sensors. A uniform rectangular antenna array (URA) model was applied, consisting of sixteen sensors arranged as shown in Figure 4. The XY plane is assumed to be parallel to the ground with Z axis pointing upwards. The distance between closest sensors is equal to one half of the wavelength at L1 carrier frequency.

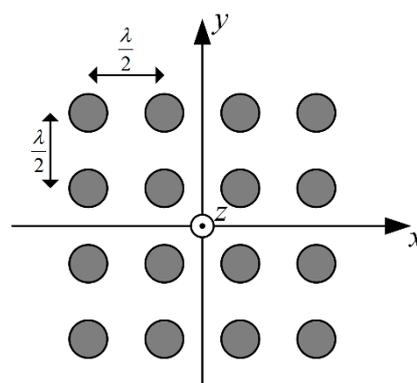


Figure 4. Arrangement of sensors in simulated model of antenna array.

The MMT algorithm was applied to estimate parameters of spatial components. Delay of the first path was sought in range ± 0.5 microseconds around the correlation peak obtained from acquisition stage. This search span corresponds to duration of a single chip in GPS C/A code, whereas the relative delay of the second path from the first path was sought in range from 0 to 100 nanoseconds.

4.1. Evaluation of Detection Threshold

It is assumed that probability of false alarm P_{fa} should not exceed 10^{-2} . The worst-case scenario, where P_{fa} is highest, is when four genuine signals arrive from similar directions resulting in small distances between steering vectors. In order to determine such conditions, GPS satellite trajectories were analyzed within 24-h period with 1-min step. Steering vectors were calculated corresponding to azimuth and elevation angles of signals arriving to a fixed location at 54° N latitude. It was found that for four signals arriving from directions $[146^\circ, 35^\circ]$, $[143^\circ, 19^\circ]$, $[150^\circ, 5^\circ]$, $[126^\circ, 59^\circ]$ a set of smallest true distances between steering vector is obtained, $\Delta \mathbf{a}_{ij} \in \{0.87, 0.95, 1.31, 2.54, 3.15, 3.67\}$. PDFs of $\Delta \mathbf{a}_{ij}$ were estimated for integer values of C/N_0 in range from 45 dBHz to 55 dBHz. For each value, Monte Carlo trials were conducted, assuming that C/N_0 was equal for each of arriving spatial components. Empirical PDFs were derived from histograms of 1000 simulated output values. Using formula (15), maximum threshold values were estimated for which $P_{fa} < 10^{-2}$. Results are shown in Table 1. As may be seen, thresholds are lower for smaller C/N_0 values because then PDFs are spread over a range of larger values of $\Delta \mathbf{a}_{ij}$. According to Table 1, threshold value of 3.6 should be used in spoofing detection procedure as it constrains P_{fa} for all C/N_0 values in the analyzed range.

Table 1. Maximum $\Delta \mathbf{a}$ threshold satisfying condition $P_{fa} < 10^{-2}$.

C/N_0	$\Delta \mathbf{a}_{thr,max}$	C/N_0	$\Delta \mathbf{a}_{thr,max}$
45	3.6	51	3.7
46	3.6	52	3.8
47	3.6	53	3.8
48	3.6	54	4.0
49	3.6	55	4.0
50	3.6		

Once the optimum threshold value was found, next simulations were conducted to evaluate the probability of spoofing detection. Another series of 1000 Monte Carlo trials were conducted to estimate the PDFs of $\Delta \mathbf{a}_{ij}$ for signals arriving from the same direction with the same C/N_0 in range from 45 to 55 dBHz. PDFs obtained for C/N_0 values of 45, 50 and 55 dBHz are shown in Figure 5.

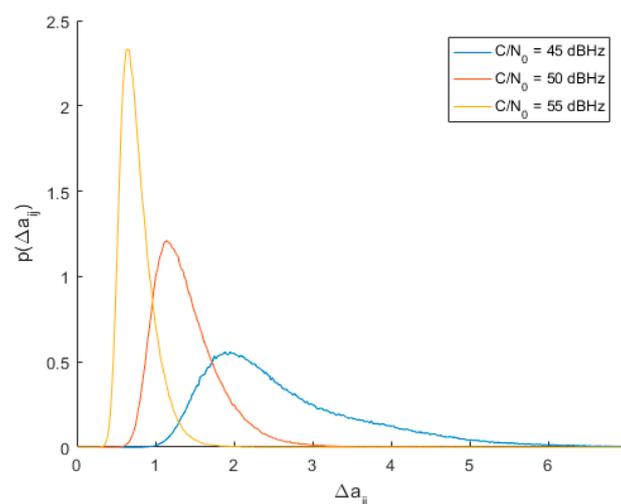


Figure 5. Empirical PDFs of spoofing steering vector distance for different C/N_0 values.

Estimated probabilities of spoofing detection, calculated using Equation (15), are given in Table 2. As may be seen, best performance is observed for C/N_0 not smaller than 50 dBHz, but even for smaller values P_d is much greater than P_{fa} .

Table 2. Probability of spoofing detection with $\Delta\mathbf{a}_{thr} = 3.6$.

C/N_0	P_d	C/N_0	P_d
45	46.9%	51	99.9%
46	57.9%	52	> 99.9%
47	74.4%	53	> 99.9%
48	83.5%	54	> 99.9%
49	97.2%	55	> 99.9%
50	99.2%		

4.2. Spoofing Scenario 1

In the first scenario six GPS satellite signals were received and each of these signals had a spoofing counterpart. All spoofing components arrived from direction $[\phi_{spoof}, \theta_{spoof}] = \{50^\circ, 20^\circ\}$, where ϕ and θ represent azimuth angle and elevation angle respectively. DOAs of genuine signals and their C/N_0 values are given in Table 3.

Table 3. Parameters of simulated genuine GPS signals.

SVID	ϕ_{sat} [°]	θ_{sat} [°]	C/N_0 [dBHz]
1	300	35	47
2	0	45	48
3	200	50	49
4	100	60	50
5	120	80	51
6	10	30	52

Each signal from GPS satellite had a different code phase and Doppler shift. Simulated spoofing signals arriving to receiver were the delayed copies of true signals with twice greater power (3 dB higher C/N_0). Introduced delays did not exceed 50 nanoseconds. It corresponds to the early stage of carry-off spoofing phase with relative pseudorange differences not greater than 15 m. In this scenario the actual pseudorange differences between counterfeit and true signals were set to: 3 m, 5 m, 10 m, 7, 8 and 9 m for SVIDs 1 to 6 respectively. Figure 6 presents the results of multipath detection procedure using MMT algorithm. For each SVID, estimated multipath bins are shown along with their relative pseudorange ΔPR and amplitude ratio A_2/A_1 . All pseudorange differences between multipath bins were estimated correctly, while amplitude ratios varied from the true value of 1.41 (3 dB power ratio).

Table 4 and Figure 7 present values of distances between steering vectors of all 12 detected spatial components. As may be seen from Table 4, there were 16 distances which were smaller than $\Delta\mathbf{a}_{thr} = 3.6$ (highlighted cells). Assuming that K_{spoof} is equal to 6, the spoofing detection checks if there are 15 distances related to 6 components. It is visible that there was a set of 15 distances related to components 2, 4, 6, 8, 10 and 12. In result, spoofing was detected and counterfeit signals were identified as even spatial components, which is correct.

Two six-element sets of steering vectors of true and counterfeit signals were passed to weight calculation block, where optimal weight vector was determined using LCMV method.

The resulting pattern of antenna array with optimum set of weights applied is shown in Figure 8. The green diamond symbols indicate the DOAs of true signals according to Table 3, while the red circle symbol marks the DOA of composite spoofing signal. As may be seen, there is a deep null (over -30 dB) including direction of spoofing interference while preserving unity gains (0 dB) towards GPS satellites.

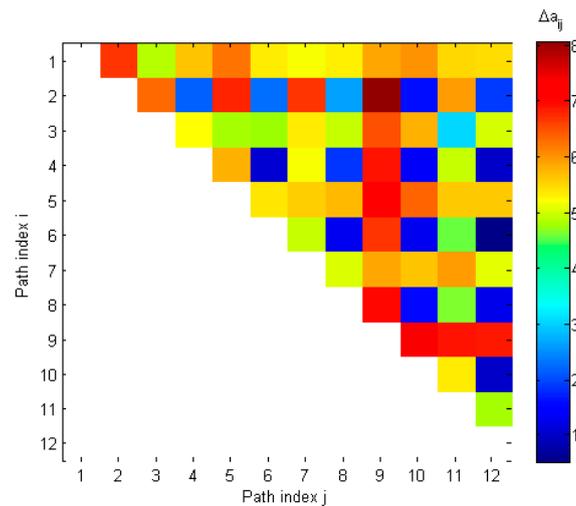


Figure 7. Distances between steering vectors in spoofing scenario 1.

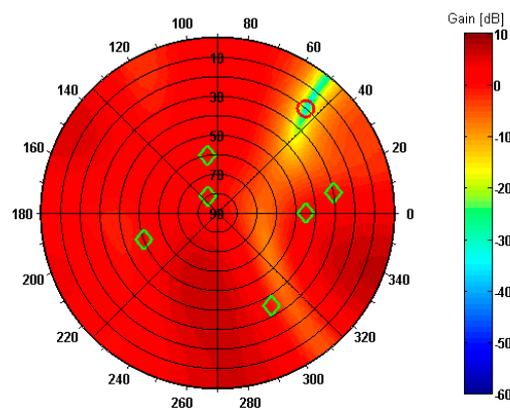


Figure 8. Reception pattern of antenna array in spoofing scenario 1.

4.3. Spoofing Scenario 2

This simulation was conducted to prove the effectiveness of proposed method when the number of spoofing components is not equal to the number of visible satellites. In addition, the DOA of the spoofing signal was set to coincide with the DOA of one of satellite signals. These conditions may represent the situation where a spoofer is located on an aircraft, helicopter, unmanned aerial vehicle or on a high-altitude platform.

In this scenario the number of satellite signals, their DOAs and C/N_0 values were the same as shown in Table 3. On the other hand, there were only four spoofing components imitating satellites with SVIDs from 1 to 4. These components were arriving from direction $[\phi_{spoof}, \theta_{spoof}] = \{100^\circ, 60^\circ\}$, which is the same as DOA of satellite with SVID 4.

Again, the MMT method was used to detect the spatial components. The results are presented in Figure 9. For SVIDs from 1 to 4 estimated bins are similar to the ones shown in Figure 6, except for SVID 3, where relative pseudorange ΔPR of spoofing component was found to be 9 m instead of actual 10 m. Also, estimated amplitude ratios do not differ significantly from the true value of 1.41. The results for SVIDs 5 and 6 expose one dominant bin as expected. Even if only a single spatial component is present, MMT returns two bins where one of them has much smaller amplitude than the other one.

During the spoofing detection procedure, assuming that K_{spoof} is equal to 5, then 10 distances between steering vectors are selected. From Figure 10 and Table 5 it may be seen that there are fourteen distances smaller than Δa_{thr} . However, it is visible that a full set of steering vector distances occurs for the combination of components 2, 4, 6, 8 and 7, i.e., four spoofing components and one true signal.

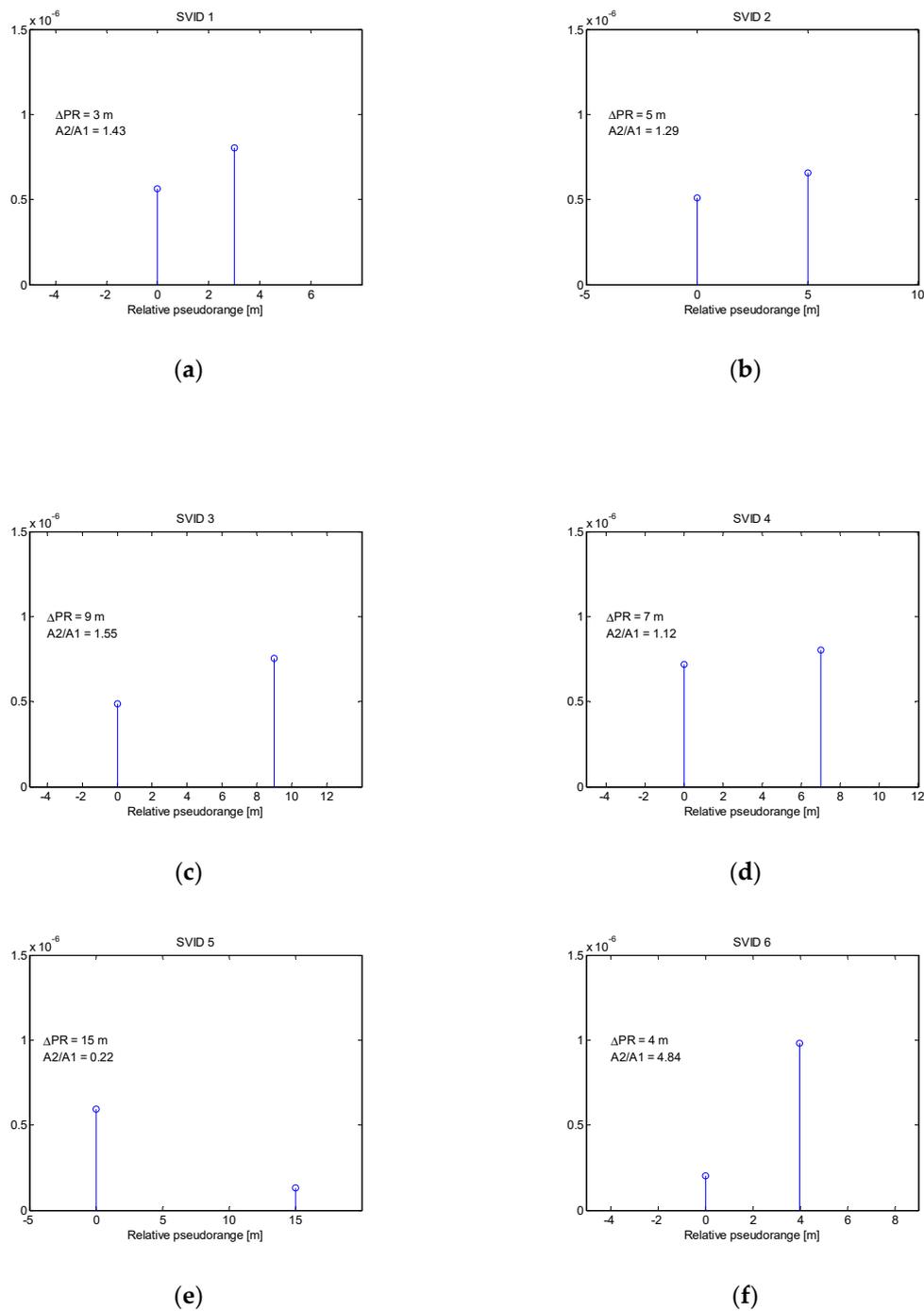


Figure 9. Multipath bins estimated in spoofing scenario 2 for signals related to SVIDs 1-6 (a–f).

In this case, one of true signals from GPS satellites is incorrectly classified as spoofing signal. However, since proposed anti-spoofing method is based solely on analysis of signals' spatial signatures, it is not possible to decide which signal with SVID 4 is the true one and which is counterfeit.

The antenna array reception pattern evaluated for spoofing scenario 2 is presented in Figure 11. It is visible that a spatial null is formed in common DOA of spoofing components and one of true signals. For DOAs of other five true signals, unity gain is provided, as in scenario 1. This means that in this case spoofing is successfully mitigated at the cost of not receiving one of the true signals. If signals from at least four satellites remain, it will still be possible for the GPS receiver to estimate the 3D position.

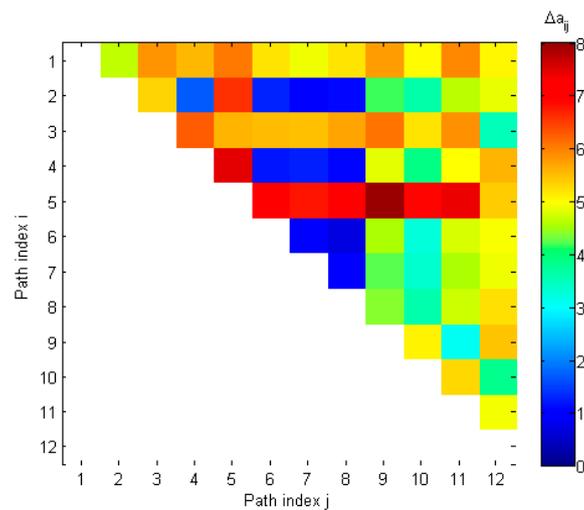


Figure 10. Distances between steering vectors in spoofing scenario 2.

Table 5. Distances between steering vectors in spoofing scenario 2.

i,j	2	3	4	5	6	7	8	9	10	11	12
1	4.64	5.82	5.54	6.05	5.19	4.88	5.20	5.76	5.00	5.91	5.05
2		5.34	1.69	6.58	1.30	1.01	1.11	4.18	3.64	4.61	4.86
3			6.25	5.57	5.52	5.49	5.72	6.06	5.20	5.85	3.52
4				7.45	1.21	1.26	1.07	4.82	3.90	4.99	5.58
5					7.09	6.77	7.20	7.97	6.90	7.39	5.39
6						1.00	0.70	4.54	3.26	4.77	4.96
7							0.98	4.22	3.37	4.56	4.89
8								4.40	3.62	4.69	5.22
9									5.08	3.07	5.46
10										5.29	3.82
11											4.92

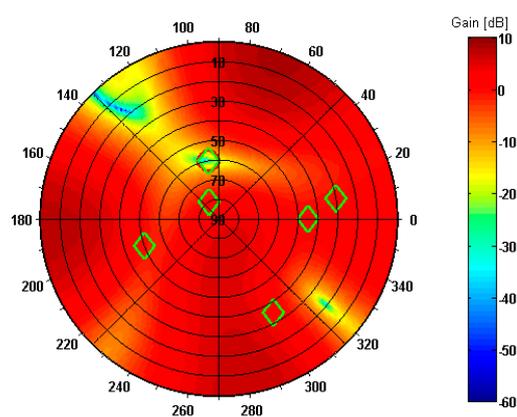


Figure 11. Reception pattern of antenna array in spoofing scenario 2.

5. Conclusions

The shown simulation results above prove the usefulness of the proposed method of detecting and mitigating intermediate GNSS spoofing at its early stage, which is a major advantage over other multi-antenna anti-spoofing solutions presented so far. Previously proposed methods could be still applied when spoofing signals are offset by more than one chip from respective true signals. Then

it is not necessary to apply multipath detection technique, since these components may be acquired separately as their correlation peaks do not overlap.

Another asset is that proposed method combines spoofing detection and mitigation. When compared to [13,14], exploiting all spoofing and satellite steering vectors in LCMV beamforming provides greater control over antenna array pattern. Specifically, all spoofing components are nulled independently while genuine signals are preserved undistorted.

It should be also noted that described spoofing detection and spoofing mitigation methods both rely on knowledge about signals' steering vectors. This is a substantial advantage over methods based on actual DOAs, like [13], as it eliminates the necessity to maintain local oscillator phase coherence between receive chains. This means that no phase calibration is necessary before using this anti-spoofing system, i.e., phase shifts ϕ_m in (3) may have arbitrary values. Still, it is required to maintain time and frequency synchronization between receive chains to avoid time-varying steering vectors.

Before described method may be applied in practice, it should be verified that antenna array may be located in a multipath-free environment. When the signal from a GNSS satellite or signals from a spoofer travel along more than one spatial channel, the MMT algorithm is not suitable for estimating steering vectors. In such case, other multipath detection methods need to be used, which cannot be based on Maximum Likelihood due to its high computational burden. An example of iterative GNSS multipath mitigation technique is described in [23].

Regarding computational complexity, the most computationally intensive stages of proposed algorithm are the signal acquisition and multipath estimation which are both related to spoofing detection. For a PC with a dual-core CPU running MatLab it took about one second to perform the MMT procedure for a single SVID (a pair of true and spoofing components). It is expected that this time could be significantly reduced if a DSP or FPGA hardware platform was used. Nevertheless, spoofing detection is considered to be not time-critical and may be performed periodically. On the other hand, spoofing mitigation must be done in real-time. It is possible to achieve this, as beamforming spatial filter is basically a linear combiner which exhibits low computational complexity (M complex multiplications and $M - 1$ additions).

Another practical aspect is the optimal number of elements in the antenna array. There is an inherent tradeoff between hardware/DSP complexity and effectiveness. More antennas may improve spoofing detection when C/N_0 is low. Moreover, the number of sensors determines the degrees of freedom for controlling the array reception pattern. Recommended minimum number of antennas is one more than the total number of expected spoofing components and genuine signals from visible satellites.

When spoofing is aimed at GNSS receivers installed in aerial vehicles, it is expected that the spoofer will be located higher than the antenna of the target. Such conditions were assumed in two scenarios described in Section 4. It was proven that spoofing may be mitigated even when counterfeit signals arrive from the same direction as one of the true signals.

Funding: This research received no external funding.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Ioannides, R.T.; Pany, T.; Gibbons, G. Known Vulnerabilities of Global Navigation Satellite Systems, Status, and Potential Mitigation Techniques. *Proc. IEEE* **2016**, *104*, 1174–1194. [[CrossRef](#)]
2. Warner, J.S.; Johnston, R.G. GPS spoofing countermeasures. *Homeland Secur. J.* **2003**, *25*, 19–27.
3. Jafarnia-Jahromi, A.; Broumandan, A.; Nielsen, J.; Lachapelle, G. GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques. *Int. J. Navig. Obs.* **2012**, *2012*, 127072. [[CrossRef](#)]
4. Wen, H.Q.; Huang, P.Y.-R.; Dyer, J.; Archinal, A.; Fagan, J. Countermeasures for GPS Signal Spoofing. In Proceedings of the 18th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2005), Long Beach, CA, USA, 13–16 September 2005.

5. Dampf, J.; Pany, T.; Bär, W.; Winkel, J.; Mervart, L.; Ávila-Rodríguez, J.; Ioannides, R.; Hein, G. Real World Spoofing Trials and Mitigation. *InsideGNSS* **2017**, *12*, 55–65.
6. Humphreys, T.E.; Ledvina, B.M.; Psiaki, M.L.; O'Hanlon, B.W.; Kintner, P.M., Jr. Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer. In Proceedings of the 21st International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2008), Savannah, GA, USA, 16–18 September 2008.
7. Psiaki, M.L.; Humphreys, T.E. GNSS Spoofing and Detection. *Proc. IEEE* **2016**, *104*, 1258–1270. [[CrossRef](#)]
8. Huang, J.; Lo Presti, L.; Motella, B.; Pini, M. GNSS spoofing detection: Theoretical analysis and performance of the Ratio Test metric in open sky. *ICT Express* **2016**, *2*, 37–40. [[CrossRef](#)]
9. Nielsen, J.; Broumandan, A.; Lachapelle, G. Spoofing Detection and Mitigation with a Moving Handheld Receiver. *GPS World* **2010**, *21*, 27–33.
10. Psiaki, M.L.; Powell, S.P.; O'Hanlon, B.W. GNSS Spoofing Detection using High-Frequency Antenna Motion and Carrier-Phase Data. In Proceedings of the 26th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2013), Nashville, TN, USA, 16–20 September 2013; pp. 2949–2991.
11. Psiaki, M.L.; O'Hanlon, B.W.; Powell, S.P.; Bhatti, J.A.; Wesson, K.D.; Humphreys, T.E.; Schofield, A. GNSS Spoofing Detection Using Two-Antenna Differential Carrier Phase. In Proceedings of the 27th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2014), Tampa, FL, USA, 8–12 September 2014; pp. 2776–2800.
12. Borio, D.; Gioia, C. A sum-of-squares approach to GNSS spoofing detection. *IEEE Trans. Aerosp. Electron. Syst.* **2016**, *52*, 1756–1768. [[CrossRef](#)]
13. Konovaltsev, A.; Caizzzone, S.; Cuntz, M.; Meurer, M. Autonomous Spoofing Detection and Mitigation with a Miniaturized Adaptive Antenna Array. In Proceedings of the 27th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+ 2014), Tampa, FL, USA, 8–12 September 2014; pp. 2853–2861.
14. Daneshmand, S.; Jafarnia-Jahromi, A.; Broumandan, A.; Lachapelle, G. 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, USA, 17–21 September 2012; pp. 1233–1243.
15. Daneshmand, S.; Jafarnia-Jahromi, A.; Broumandan, A.; Lachapelle, G. A GNSS structural interference mitigation technique using antenna array processing. In Proceedings of the 2014 IEEE 8th Sensor Array and Multichannel Signal Processing Workshop (SAM), A Coruna, Spain, 22–25 June 2014; pp. 109–112.
16. Magiera, J.; Katulski, R. Accuracy of differential phase delay estimation for GPS spoofing detection. In Proceedings of the 36th International Conference on Telecommunications and Signal Processing (TSP), Rome, Italy, 2–4 July 2013; pp. 695–699.
17. Magiera, J.; Katulski, R. Applicability of Null-Steering for Spoofing Mitigation in Civilian GPS. In Proceedings of the IEEE 79th Vehicular Technology Conference (VTC Spring), Seoul, Korea, 18–21 May 2014.
18. Sahmoudi, M.; Landry, R. Multipath Mitigation Techniques using Maximum-Likelihood Principle. *InsideGNSS* **2008**, *3*, 24–29.
19. Weill, L.R. Multipath Mitigation using Modernized GPS Signals: How Good Can it Get? In Proceedings of the 15th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GPS 2002), Portland, OR, USA, 24–27 September 2002; pp. 493–505.
20. Parkinson, B.W.; Axelrad, P. Autonomous GPS integrity monitoring using the pseudorange residual. *Navigation* **1988**, *35*, 255–274. [[CrossRef](#)]
21. Capon, J. High-resolution frequency-wavenumber spectrum analysis. *Proc. IEEE* **1969**, *57*, 1408–1418. [[CrossRef](#)]
22. Frost, O.L. An algorithm for linearly constrained adaptive array processing. *Proc. IEEE* **1972**, *60*, 926–935. [[CrossRef](#)]
23. Chen, X.; Doyis, F.; Peng, S.; Morton, Y. Comparative Studies of GPS Multipath Mitigation Methods Performance. *IEEE Trans. Aerosp. Electron. Syst.* **2013**, *49*, 1555–1568. [[CrossRef](#)]

