Submitted version of: J. Rossouw van der Merwe, Alexander Rügamer, Alejandro Fernández-Dans Goicoechea, and Wolfgang Felber, "Blind spoofing detection using a multi-antenna snapshot receiver," International Conference on Localization and GNSS (ICL-GNSS), submitted February 2019, accepted March 2019.

DOI: 10.1109/ICL-GNSS.2019.8752840

Blind spoofing detection using a multi-antenna snapshot receiver

J. Rossouw van der Merwe, Alexander Rügamer, Alejandro Fernández-Dans Goicoechea, Wolfgang Felber
Fraunhofer IIS, Nuremberg, Germany
johannes.roussouw.vandermerwe@iis.fraunhofer.de

***Abstract*— Spatial processing methods that utilize an array of antennas can be used to detect spoofing signals e.g. due to their typical, common spatial origin. A multi-antenna snapshot receiver that utilizes multi-channel processing is used to estimate the beamforming steering vector to each acquired satellite in a constellation. A detector based on steering vector correlation is presented, analyzed and tested. The detection performance is evaluated using a laboratory setup for spoofing, whereas the false detection rate is evaluated using an open-sky recording with an antenna array. The detector has shown good performance to detect spoofing signals in these controlled spoofing scenarios.**

***Index Terms*—Global navigation satellite system (GNSS), beamforming, server based processing, antenna array.**

I. Introduction

Spoofing, the transmission of false signals to manipulate a receiver, is a significant threat to global navigation satellite system (GNSS) users [1], [2]. A spoofer aims to manipulate the position, velocity, and time (PVT) solution of the receiver, therefore, it is considered an attack. Transmitting, and by extension spoofing, in unowned radio-frequency (RF) spectrum is illegal. There are many anti-spoofing methods and schemes to detect it [2]–[5]; however, many of these fail when a spoofing attack is more sophisticated (e.g. a synchronized attack) or cooperative (i.e. the owner of the receiver assists with the attack). A transmitter in a spoofing attack is usually terrestrial, hence, the spatial distribution over the open-sky of real GNSS signals are not emulated. Therefore, spatial detection methods have proven to be very successful, independent of the spoofing method used [6]. Spatial detection methods require either the utilization of an array of antennas, or a highly directional antenna [7]. Most commonly, an array of antennas that is time and frequency-synchronized is required such that detection methods like direction-of-arrival (DOA) estimation can be applied.

Server-based GNSS processing allows for the remote evaluation of GNSS signals, from a recording made by a receiver. As the processing is done remotely, is is also referred to as cloud GNSS [8]. More often it is commonly referred to as snapshot processing, as a small snapshot of data is sent from the receiver to the server for processing [9], [10]. The server will then compute the PVT solution of the snapshot. One aim of this technique is to remove processing burden from the receiver and transfer it to a server.

Server-based processing can be applied to low-power devices [11], [12] which cannot afford a full GNSS receiver for positioning. This saves on power and weight requirements for the receiver as well as the associated system, hence, it is often used for low size, weight, and power (SWAP) devices. Applications such as remote sensing and animal tracking can benefit from this technique. Mobile devices can also profit from this approach [13]. Another application for server-based processing is the verification of a receiver's position using encrypted GNSS signals [14], [15]. Especially inexpensive receivers do not have the required security module for cryptographically protected GNSS signals on-board, but a central server having this outsourced security module may be used instead. A snapshot of data may be sent to this server for authentication.

This paper presents a spoofing-detection method using an antenna array and a snapshot receiver. The snapshot-concept aims to transfer the processing load to the servers, and to maintain receiver complexity and requirements as low as possible. Therefore, the aim is that the benefits of array processing can be applied to SWAP devices. The drawback of using multiple antennas is that it requires multiple synchronized receiver channels. This increases system complexity and cost which makes this technique counter productive for low SWAP devices. However, it can be argued that this is a necessity for reliable spoofing detection. For DOA based detection the array is required to be calibrated which further increases cost and complexity to the system. The focus of this paper is to develop and assess a blind detection method which does not require DOA, thereby, reducing receiver complexity and cost.

A background on snapshot receivers, server-based processing and the implementation of beamforming to improve performance is provided in Section II. The spoofing detection algorithm is presented in Section III, with additional theoretical analysis to support the expected performance. The experimental setup is introduced in Section IV, and results are presented in Section V. Finally, conclusions are drawn in Section VI.

II. Snapshot receivers and beamforming

A snapshot receiver operates with only a few milliseconds of raw data obtained by the analog-to-digital converter (ADC) output following the RF front-end [9]. This raw data snapshot is sent to a server for processing. As there is limited data available the server can only achieve signal acquisition: there are not enough data available for a tracking process, nor sufficient data to obtain any information from the navigation message. Since the ephemeris data cannot be decoded, this

information is obtained from a secondary source. A direct pseudorange cannot be derived from the acquisition results since the transmission time of the satellite is not available. However, given a rough receiver position and time estimate together with the ephemeris data, the pseudorange reconstruction can be reconstructed by estimating another unknown [16]. Once the PVT has been calculated and verified, the result might be sent back to the receiver, depending on the actual use case.

As acquisition forms the base of the entire processing chain (not just for initialization like with a conventional receiver), it is important to have high performance during this stage. Since the transport channel between receiver and server is often limited the snapshot size is reduced to satisfy data transmission requirements. This is a trade-off for the receiver, since the smaller the snapshot is (due to length, sample rate and quantization reduction), the poorer the acquisition performance [17].

Acquisition performance with snapshot receivers using multiple antennas has been investigated [18]. This method has shown good performance in previous studies. Fig. 1 shows the method that is used for acquisition and to estimate the beamforming steering vector. This method is completely blind, as no DOA is done. Consequently, no calibration or information about the array configuration or orientation is required. The acquisition method first applies incoherent spatial acquisition, followed by coherent spatial acquisition with estimated array steering vector to improve the performance. As this application focuses primarily on beamforming, the array steering vector is also referred to as the beamforming steering vector or the beamforming weights. Hence these terms are used interchangeably.

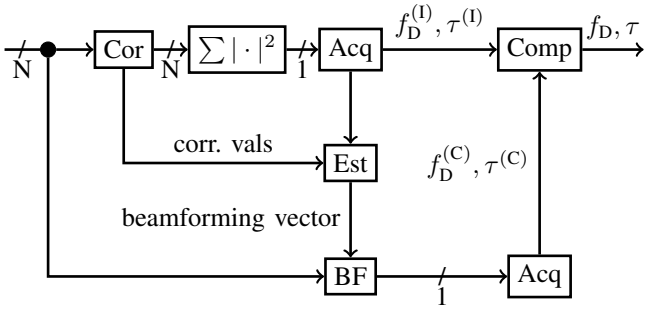


Fig. 1: Block diagram for the used acquisition

At first, a blind incoherent acquisition is carried out for every receiver channel. The signals from every array element are correlated with the replica of each satellite (denoted by "Cor"). The absolute squared values of the correlations are added ("$\sum|\cdot|^2$") in order to estimate the code phase $\tau^{(\mathrm{I})}$ and carrier Doppler $f_{\mathrm{D}}^{(\mathrm{I})}$ in acquisition stage ("Acq"). If the satellite is acquired, then the beamstforming steering vector is estimated ("Est") with the code phase $\tau^{(\mathrm{I})}$ and carrier Doppler $f_{\mathrm{D}}^{(\mathrm{I})}$ from the incoherent acquisition. Once the vector is estimated, the receiver channels are weighted accordingly (denoted by "BF") and a second acquisition takes place. This time the coherent $\tau^{(\mathrm{C})}$ and carrier Doppler $f_{\mathrm{D}}^{(\mathrm{C})}$ are determined. After the second acquisition, the code phases and Doppler frequencies from the first (incoherent), and the second (coherent) one are compared. If these differ too much the satellite is discarded. This allows a secondary test to remove false positives from the acquisition process.

A limitation of this method is that the estimation of the beamforming steering vector is based upon the incoherent results. These values may contain multipath or cross-correlation components from other signals which can obscure the estimation process. In turn, the erroneous array steering vector may form a beam that does not sufficiently suppress these unwanted signal components. This could be an issue especially in harsh environments with significant multipath components.

III. Spoofing detection algorithm

Spoofing detection with an array of antennas has already been proven successful [6], [19], [20]. However, this requires a calibrated array with known receiver phase offsets and antenna orientation. These methods are DOA based, and estimate the direction to each satellite. As the snapshot-concept aims to outsource the processing to the server it implicitly shifts the cost of the system away from the receiver. However, all calibrations required for array processing would increase cost and complexity to the receivers, therefore, working against the snapshot concept. This emphasizes the need for blind methods.

A drawback of blind methods is that the detection is relative. Therefore, should only a single signal be originating from the wrong direction, it cannot be detected. If multiple signals are from the same direction, it can be detected. As a constellation of signals are usually spoofed, this should not be an issue in practice. However, in the case of distributed spoofing attacks (i.e. multiple spoofing transmitters) [21], this could be significantly more difficult to detect.

The spoofing detection algorithm present in this paper uses the beamforming steering vector obtained in acquisition (see Section. II). The array steering vector is tested for similarity, by correlating each pair of vectors with each other. If the signals originate from the same direction, then they have similar vectors and have a high correlation value. The detector is based on this correlation value.

The detector implements a detection for each pair of steering vectors, hence, a system of detections is developed. This makes the detection process more efficient. First, all the estimated array steering vectors are stacked in a matrix $\mathbf{B}$:

$$\mathbf{B} = [\mathbf{b}_1, \mathbf{b}_2, ..., \mathbf{b}_{N_\mathrm{w}}] \ , \tag{1}$$

where $\mathbf{b}_n$ is a column vector containing the coefficients for the n-th satellite. The constellation consists of a total of N_w satellites. $\mathbf{B}$ is a number of elements N_e by the number of estimated steering vectors N_w sized matrix. The matrix is correlated to get a non-normalized correlation matrix $\mathbf{C}$:

$$\mathbf{C} = \mathbf{B}^H \times \mathbf{B} \ , \tag{2}$$

where $(\cdot)^H$ is the Hermitian transpose of the signal, and $\times$ is a matrix multiplication. Each element in the matrix is equivalent to the dot product between each pair of steering vectors. $\mathbf{C}$ is N_w by N_w Hermitian matrix. To normalize the matrix, the magnitude of the auto-correlations need to be determined:

$$\mathbf{c} = \sqrt{\text{diag}\left(\mathbf{C}\right)}\,, \tag{3}$$

where $\mathbf{c}$ is a column vector containing the magnitude values, and diag $(\cdot)$ takes the diagonal of a matrix. The normalized correlation matrix $\mathbf{C}_\text{norm}$ is calculated as:

$$\mathbf{C}_\text{norm} = \Re\left\{\mathbf{C}\right\} \circ \left(\mathbf{c} \times \mathbf{c}^T\right)^{\circ -1}\,, \tag{4}$$

where $\Re\{\cdot\}$ takes the real component of the correlation, $\circ$ is the Hadamard product, and $(\cdot)^{\circ -1}$ is the Hadamard inverse. $\mathbf{C}_\text{norm}$ is also an Hermitian matrix. Each element of this matrix has the form:

$$C_\text{norm}(n,m) = \frac{\Re\left\{\mathbf{b}_n^* \cdot \mathbf{b}_m\right\}}{\|\mathbf{b}_n\|\,\|\mathbf{b}_m\|} = \cos\left(\xi_{n,m}\right)\,, \tag{5}$$

where $\|\mathbf{b}_n\|$ is the magnitude of the n-th beamforming vector. Each correlation can be regarded as the cosine of the angle $\xi_{n,m}$ between two vectors. This is not the spatial angle of the DOA between two satellites (also referred to as the incident angle of the array), but a measure of how similar the two steering vectors are. For the remainder of this paper, this will be referred to as the steering vector angle.

As an example, a uniform linear array (ULA) with an inter-element spacing of half a wavelength has beamfroming steering vectors in the form of:

$$\mathbf{b} = \left[\mathrm{e}^{\mathrm{j}\pi\cdot 1\cdot\sin\theta}, \mathrm{e}^{\mathrm{j}\pi\cdot 2\cdot\sin\theta}, ..., \mathrm{e}^{\mathrm{j}\pi\cdot N_\text{e}\cdot\sin\theta}\right]^T\,, \tag{6}$$

where θ is the spatial angle (incident angle) to the broadside of the array. For a two-element array the steering vector can be proven to have the form:

$$\cos\left(\xi_{1,2}\right) = \cos\left(\xi_{2,1}\right) = \cos^2\left(\frac{\pi}{2}\sin\theta\right)\,. \tag{7}$$

In this case the steering vector angle $\xi_{2,1}$ diverges rapidly from the spatial angle θ (array incident angle).

Fig. 2 shows the expected behavior for ULAs with different number of elements. As the number of elements increase, the beamforming angle separates quicker with smaller spatial angles. Consequently, with more elements the increased diversity can be exploited for detection.

ULAs are simple to be used for analysis; however, they are not suitable for GNSS applications as these antenna arrays only have beamforming capabilities in a single dimension. GNSS signals can originate from any direction above the horizon, hence, two-dimensional beamforming capabilities are required. Therefore, uniform circular arrays (UCAs) are often used for GNSS receivers. As the beamforming properties of arrays are dependent on the array configuration, the performance of this method will be fundamentally different. Fig. 3 shows the expected behavior for a UCA under similar circumstances.

The previous two pictures only show the ideal case of one signal being on the broadside of the antenna array and the other signal moving relative to it. ULAs and UCAs have ambiguities: two satellites at different locations can have similar steering vectors. The result is that these signals would seem to be originating from the same direction and would be detected and classified as being spoofed ones. In order to reduce the false detections probability due to array ambiguities the cumulative distribution function (CDF) for all difference angles are calculated. Fig. 4 shows the CDF function of the steering vector angle for a UCA consisting of six elements. The test angles are for a single cross-section consisting of all elevation angles and a single azimuth value. The angles to which the CDF first achieves a value of one follows the ideal case as shown in Fig. 3. However, it can also be seen that there are many cases where the steering vector angle is spread which may result in poor performance in these cases.

This analysis shows, that the separation can be used as a good detector to determine how similar the origins of two signals are. The detector threshold is tuned according to a symbolic steering vector separation angle. This is the steering vector angular threshold ξ_Th:

$$\lambda_\text{Th} = \cos\left(\xi_\text{Th}\right)\,. \tag{8}$$

This symbolic angle, provides an intuitive understanding how

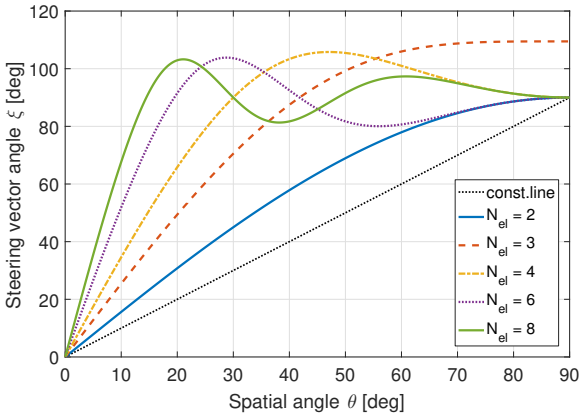


Fig. 2: Spatial angle θ vs. steering vector angle $\xi_{m,n}$ for a ULA

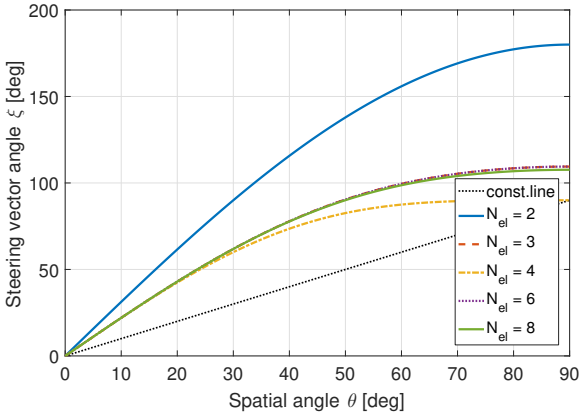


Fig. 3: Spatial angle θ vs. steering vector angle $\xi_{m,n}$ for a UCA

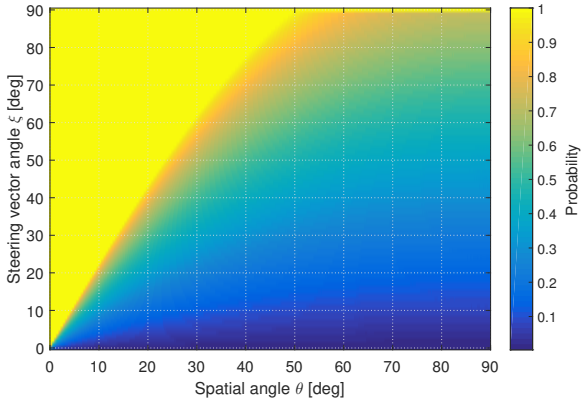


Fig. 4: CDF of spatial angle θ vs. the steering vector angle $\xi_{m,n}$ for a UCA

the detector works as opposed to merely setting an arbitrary threshold value. The threshold is used to detect each value in the matrix $\mathbf{C}_{\text{norm}}$. If the value is lower than the threshold then the null-hypothesis H_0 of no spoofing is accepted. Otherwise, the alternate hypothesis H_1, where the signals have similar origins and are considered spoofed, is accepted:

$$C_{\text{norm}}(n,m) = \cos\left(\xi_{n,m}\right) \underset{H_1}{\overset{H_0}{\gtrless}} \lambda_{\text{Th}} \,. \tag{9}$$

A method to further improve the algorithm is to remove false-detections by using the ephemeris data of the satellites and the approximate position of the receiver. A similar matrix to $\mathbf{B}$ is generated; however, each vector is the unit vector from the receiver to the satellite. A similar detection procedure is followed. The separation angle between these vectors is equivalent to their spatial angle. The detection is used to flag any satellites which have similar directions. These detections are then used to remove false positives of signals which are close to each other.

Further improvements also include comparing the multiple detections with each other. For example, if $\mathbf{b}_1$ and $\mathbf{b}_2$ are detected as coming from the same origin, and satellite $\mathbf{b}_1$ and $\mathbf{b}_3$ are also detected, but $\mathbf{b}_2$ and $\mathbf{b}_3$ are not, then the first two detections can be used to remove the missed detection of the last one. Such system level sensing can be used to improve spoofing detection as well as enhance the grouping of spoofed and real satellites. These analysis methods are considered outside the scope of this paper.

IV. Experimental set-up

Two experimental setups are used. The first one uses a six element circular array. The array is connected to a six channel receiver, which consists of two synchronized three-channel Flexiband front-ends [22], synchronized with a 10 MHz clock and triggered simultaneously. These front-ends have a maximum sample-rate of 81 MHz at 8 bit I/Q; however, for this experiment only 10.125 MHz was used. A recording of 1 min was made, and saved to be used in post-processing. A picture of the system is shown in Fig. 5. The recording is made under open-sky conditions with the purpose to determine the probability of false alarm for the used detector.

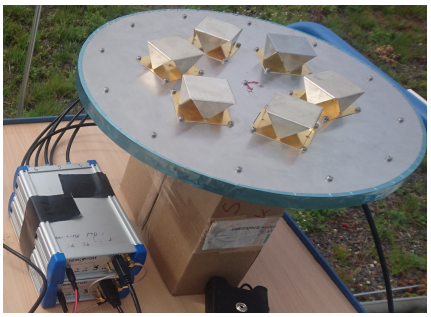


Fig. 5: Photo of the measurement system

The second setup uses a single antenna connected to each channel of the receiver via a splitter. For this recording, all signals will have similar and static beamforming steering vector. Therefore, this is considered as a spoofing simulation without the need for an anechoic chamber or a live setup. With this recording the probability of detection is derived.

Only Global Positioning System (GPS) L1 C/A signals are considered in this experiment. A total of 1000 snapshots are taken and evaluated for each test. Snapshots of length 2, 3, 6 and 10 ms are extracted from the recordings. In the acquisition a coherent integration of 1 ms is selected, and 1, 2, 5 and 10 epochs are added incoherently, respectively. The integration time significantly influences the performance of acquisition and the accuracy of the estimation for the beamforming steering vector. Acquisition is done on each snapshot and the beamforming steering vector for each acquired satellite are then estimated. Lastly, the detector is run on each set of the resulted beamforming steering vectors.

V. Results

The detectors are evaluated at different values for the steering vector angular threshold ξ_{Th}. This allows the performance of the detector to be determined for different thresholds. First, the open-sky real world recordings using the array are used. The sky-plot with the visible GPS satellites is shown in Fig. 6.

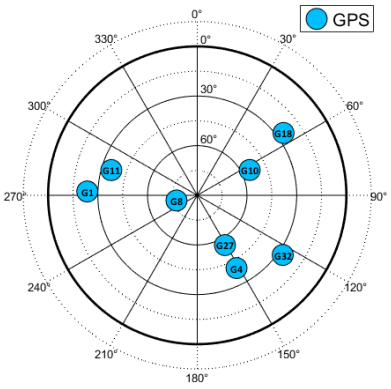
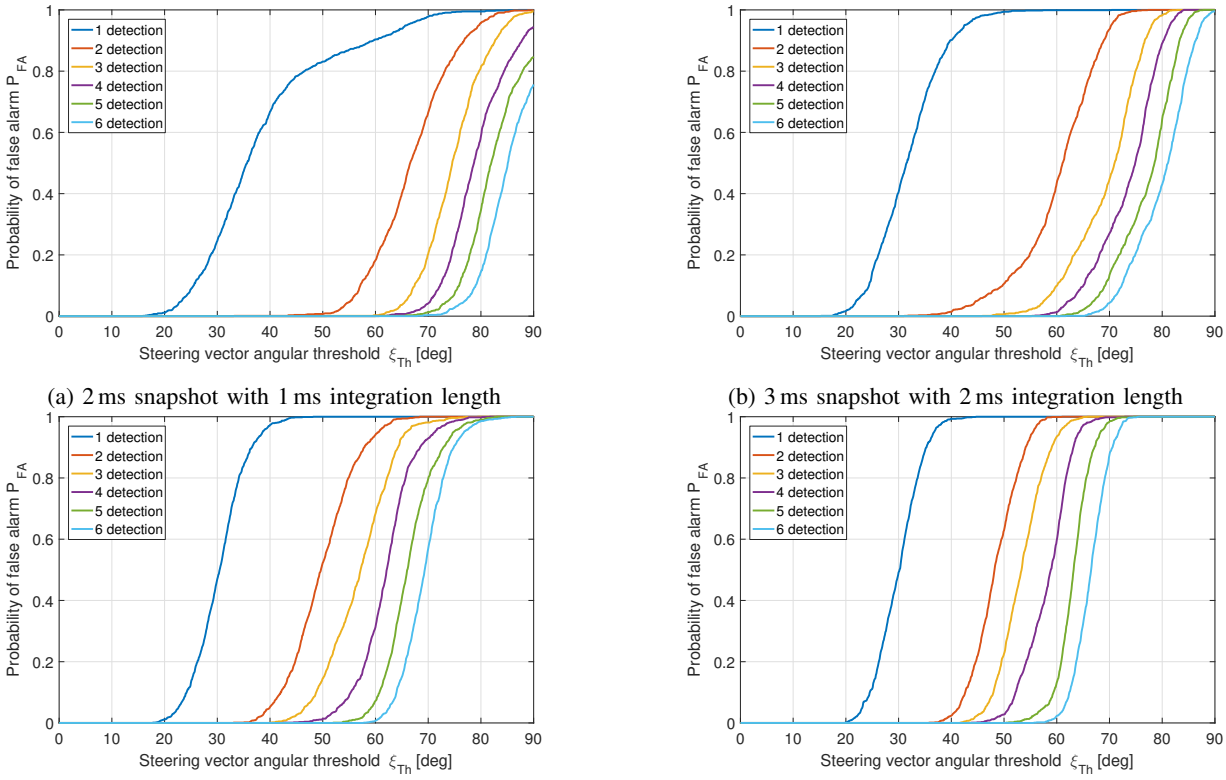


Fig. 6: Sky-plot of the open-sky recording



(a) 2 ms snapshot with 1 ms integration length

(b) 3 ms snapshot with 2 ms integration length

(c) 6 ms snapshot with 5 ms integration length

(d) 10 ms snapshot with 10 ms integration length

Fig. 7: Comparison of the probability of false alarm P_{FA} for different integration lengths

Fig. 7 shows the comparison of the detection results for this recording. As actual data is used, these detections represent the probability of false alarm P_{FA} for the detector as the signals have different DOAs.

In the figures a single detection means that only one pair of satellites were detected in the system. As spoofing usually consists of an entire constellation begin spoofed, this is an unlikely case, and, therefore, a single detection can be ignored. These results demonstrate that even for short integration times false detections only start occurring at moderately high thresholds of higher than 20°. However, the constellation does not consist of near flying satellites. Further, the integration time used in acquisition does not significantly affect the detector results. This is expected, as the variance of the beamforming steering vectors have limited impact in the non-spoofed case.

Fig. 8 shows the comparison for different probabilities of detection P_{D} for the second experiment, where a splitter was used to simulate a spoofing attack to be used to evaluate the detector performance.

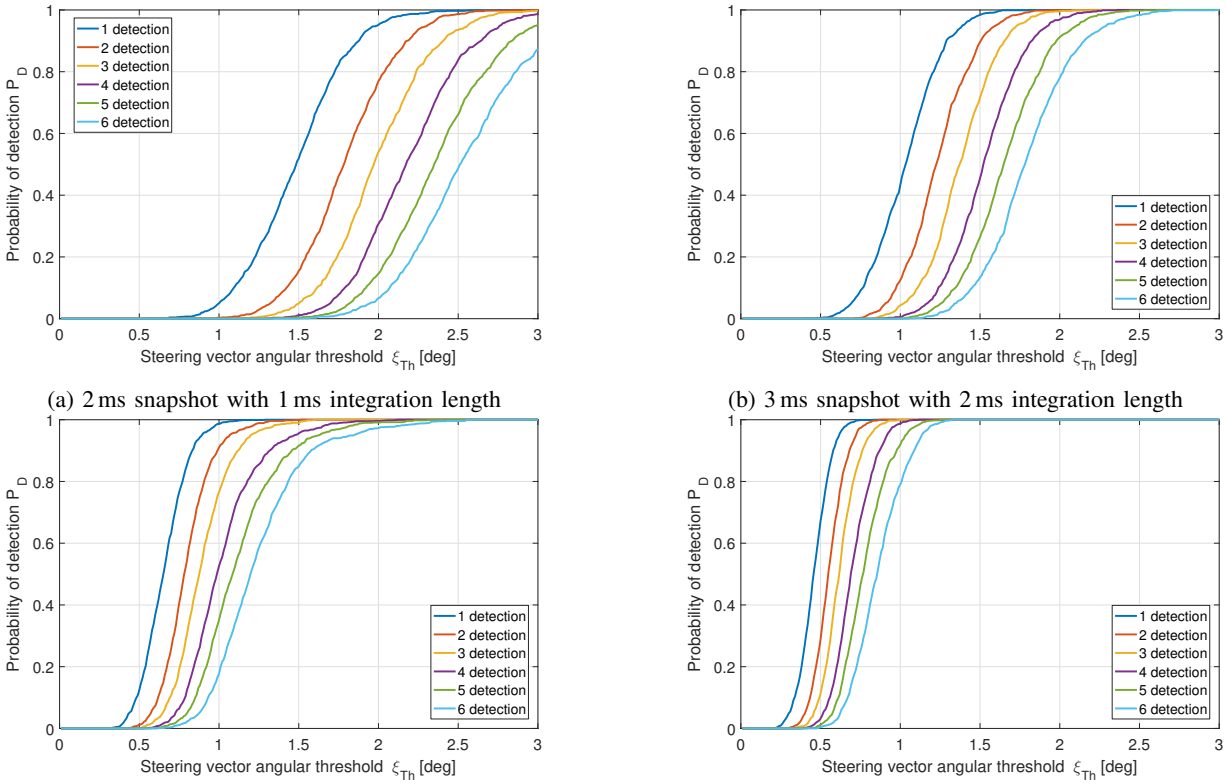
As the integration times increase, the estimation of the beamforming steering vector improves. As such, the beamforming steering vectors are more accurate and more similar for the spoofing signals. This in turn improves the detection performance. For example, the 90 % detection rate for at least 6 detections is approximately halved from 3° for a 1 ms integration time of (Fig. 8a), to 1.7° using a 5 ms integration time (Fig. 8c). This shows that by increasing the integration gain used in the acquisition, the detector is also improved. A snapshot receiver tries to minimize the snapshot size (being proportional to the length) to limit data transmission requirements, therefore, this is an additional design trade-off to consider.

The number of valid detections depend on the number of signals spoofed. In the spoofing simulation data all signals are spoofed. As the threshold increases, one by one the signals are detected. This is depicted for each number of detection in Fig. 8.

Comparing the probabilities of detection (Fig. 8) to the probabilities of false alarm (Fig. 7), a significant difference is evident. All detectors have more than 90 % probability of detection at a detector threshold that relates to a separation angle of 3°. In comparison, the probability of false alarm at this threshold setting is negligible for the test data. Based on these observations, a detector threshold that relates to a steering vector angle 5° is recommended, having a high detection rate to detect multiple spoofing signals, but also having a sufficient low rate of false detections.

VI. Conclusion

In this paper, a blind detection method of spoofing signals is presented exploiting the spatial diversity of an antenna array. The detection method is implemented in a snapshot receiver and evaluated using open-sky data recorded with a six element array as well as in a spoofing attack emulation using a splitter



(a) 2 ms snapshot with 1 ms integration length

(b) 3 ms snapshot with 2 ms integration length

(c) 6 ms snapshot with 5 ms integration length

(d) 10 ms snapshot with 10 ms integration length

Fig. 8: Comparison of the probability of detection P_{D} for different integration lengths

instead of an array. The method shows that the detector is effective, with high detectability rates. Further, this method is blind, hence, no array calibration or additional information is required.

For future research it is suggested to repeat the tests either inside an anechoic chamber or real live tests, as this would further validate the presented algorithm. Another improvement is the use of a system of detectors where the entire detection matrix is considered. Separating a real constellation of satellites from a spoofing constellation is also a possibility.

References

[1] J. A. Volpe, "Vulnerability assessment of the transport infrastructure relying on the global positioning system," *U.S. DoT*, 2001.

[2] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS vulnerability to spoofing threats and a review of antispoofing techniques," *International Journal of Navigation and Observation*, vol. 2012, pp. 1–16, 2012.

[3] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1258–1270, June 2016.

[4] C. Günther, "A survey of spoofing and counter-measures," *Navigation: Journal of the Institute of Navigation*, vol. 61, no. 3, pp. 159–177, 2014.

[5] A. Rügamer and D. Kowalewski, "Jamming and Spoofing of GNSS Signals - An Underestimated Risk?!" in *Proceedings, FIG Working Week 2015, May 17 - 21, 2015, Sofia, Bulgaria*, 2015.

[6] 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)*, 2013, pp. 2937 – 2948.

[7] E. Tuncer and B. Friedlander, *Classical and Modern Direction-of-Arrival Estimation*. Burlington: Elsevier, 2009.

[8] V. Lucas-Sabola, G. Seco-Granados, J. A. López-Salcedo, J. A. Garcia-Molina, and M. Crisci, "Cloud GNSS receivers: New advanced applications made possible," in *2016 International Conference on Localization and GNSS (ICL-GNSS)*, June 2016, pp. 1–6.

[9] I. Fernández-Hernández and K. Borre, "Snapshot positioning without initial information," *GPS Solutions*, vol. 20, no. 4, pp. 605–616, Oct 2016. [Online]. Available: https://doi.org/10.1007/s10291-016-0530-4

[10] S. V. Shafran, E. A. Gizatulova, and I. A. Kudryavtsev, "Snapshot technology in GNSS receivers," in *2018 25th Saint Petersburg International Conference on Integrated Navigation Systems (ICINS)*, May 2018, pp. 1–3.

[11] T. N. Dinh and V. La The, "A novel design of low power consumption GPS positioning solution based on snapshot technique," in *2017 International Conference on Advanced Technologies for Communications (ATC)*, Oct 2017, pp. 285–290.

[12] B. Wales, L. Tarazona, and M. Bavaro, "Snapshot positioning for low-power miniaturised spaceborne GNSS receivers," in *2010 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC)*, Dec 2010, pp. 1–6.

[13] A. Rügamer, D. Rubino, X. Zubizarreta, W. Felber, J. Wendel, and D. Pfaffelhuber, "Spoofing resistant UAVs," in *Proceedings of the International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2018)*, 2018.

[14] D. Rubino, A. Rügamer, I. Lukčin, S. Taschke, M. Stahl, and W. Felber, "Galileo PRS snapshot receiver with serverside positioning and time verification," in *Proceedings of DGON POSNAV 2016*, 2016.

[15] A. Rügamer, D. Rubino, I. Lukčin, S. Taschke, M. Stahl, and W. Felber, "Secure Position and Time Information by Server Side PRS Snapshot Processing," in *Proceedings of the 29th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2016)*, September 2016, pp. 3002–3017.

[16] F. van Diggelen, *A-GPS: Assisted GPS, GNSS, and SBAS*. Artech House, 2009.

[17] D. Borio, "A statistical theory for GNSS signal acquisition," 2008.

[18] J. R. van der Merwe, A. Fernández-Dans Goicoechea, A. Rügamer, X. Zubizarreta, D. Rubino, and W. Felber, "Multi-antenna snapshot receiver," in *2019 European Navigation Conference (ENC)*, April 2019.

[19] M. Appel, A. Konovaltsev, and M. Meurer, "Joint antenna array attitude tracking and spoofing detection based on phase difference measurements," in *Proceedings of the 29th International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2016) September 12 - 16, 2016*, 2016, pp. 3018 – 3026.

[20] E. Pérez Marcos, A. Konovaltsev, S. Caizzone, M. Cuntz, K. Yinusa, W. Elmarissi, and M. Meurer, "Interference and spoofing detection for GNSS maritime applications using direction of arrival and conformal antenna array," in *Proceedings of the 31st International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2018)*, 2018, pp. 2907 – 2922.

[21] J. R. van der Merwe, X. Zubizarreta, I. Lukčin, A. Rügamer, and W. Felber, "Classification of spoofing attack types," in *2018 European Navigation Conference (ENC)*, May 2018, pp. 91–99.

[22] A. Rügamer, F. Förster, M. Stahl, and G. Rohmer, "A flexible and portable multiband GNSS front-end system," in *Proceedings of the 25th International Technical Meeting of the Satellite Division of the Institute of Navigation, ION GNSS 2012, September 17-21, 2012, Nashville, Tennessee, USA*, September 2012.