Autonomous Spoofing Detection and Mitigation with a Miniaturized Adaptive Antenna Array

Andriy Konovaltsev[1], Stefano Caizzone[1], Manuel Cuntz[1], Michael Meurer[1,2]

[1] *Institute of Communications and Navigation, German Aerospace Center (DLR),*
Oberpfaffenhofen, Germany

[2] *Institute of Navigation, RWTH Aachen University, Germany*

BIOGRAPHY

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.

Stefano Caizzone received the M.Sc. degree in Telecommunications Engineering from the University of Rome “Tor Vergata” in 2009. He is now with the Antenna group of the Institute of Communications and Navigation of the German Aerospace Center (DLR), where he is responsible for the development of innovative miniaturized antennas. His main research interests concern small antennas for RFIDs and navigation, antenna arrays and grids with enhanced sensing capabilities.

Manuel Cuntz received the diploma in electrical engineering degree in 2005 from the Technical University of Kaiserslautern. He joined the Institute of Communications and Navigation of DLR in June 2006. His fields of research are multi-antenna satellite navigation receivers.

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 Institute 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.

ABSTRACT

The performance of a spoofing detection and mitigation technique that makes use of the directions of arrival (DOAs) information about the navigation signals has been assessed. The directions of arrival have been estimated by utilizing a miniaturized antenna array developed for the reception of Galileo navigation signals of the public regulated service in E1 and E6 frequency bands. The performance assessment has been performed by using realistic post-correlation data which were collected in field with a multi-antenna receiver tracking GPS L1 signals.

INTRODUCTION

The positioning and timing services provided by global navigation satellite systems (GNSSs), for example by the American NAVSTAR Global Positioning System (GPS), may be strongly affected by the perturbations occurred in the radio propagation channel between a GNSS satellite and the user. Because of their extremely low power the GNSS navigation signals can be easily jammed, on purpose or unintentionally, which poses the problem of radio frequency interference. Moreover, since the structure of the ranging signals and navigation data is open to public, it is not only possible to distort the reception of GNSS signals in a brute-force way but also to counterfeit the signals to make the user’s receiver generating false position and/or time. This kind of interference is commonly referenced in the literature as spoofing. Until recently because of its intentional nature, the spoofing threat was considered as relevant only for the military users of GNSS. However as our dependence on GNSS services in the everyday life continuously grows, it turns out that the spoofing problem is also of concern for the civil users. Especially strategically important infrastructures, such as electric power grids or mobile communications networks, are becoming increasingly dependent on the GNSS services. Spoofing is also an issue for safety-of-life applications like airplane landing or ship navigation in a harbor.

A number of studies have been performed on finding solutions to the problem of GNSS spoofing, see for example [1], [2] and references herein. The most exhaustive solutions based on the cryptographic authentication of GNSS signals were proposed on the system level. These solutions may be introduced in the future as a part of the modernization programs of existing GNSSs.

The solutions at the receiver level are easier to introduce in a short time frame in order to protect the most critical GNSS applications. In the user receiver, the authentic and spoofing signals can be discriminated by examining the signal amplitudes, frequency offsets and times-of-arrival. If the receiver utilizes multiple receive antennas the spatial properties of the signals can be additionally exploited. The typical strategies proposed for the spoofing detection in a multi-antenna receiver are as follows:

- to use carrier phase measurements in order to detect if a signal tracked by the receiver arrives from a different direction as predicted from the user to satellite geometry [3];
- to use carrier phase measurements in order to detect if all or majority of signals tracked by the receiver arrive from a single direction corresponding to the single spoofing transmitter [4][5];
- to examine positioning solutions obtained when using signals of each antenna individually and detect the spoofing attack when the individual positioning solutions tend to coincide [6].

The detection in spatial domain can be effectively used with various types of spoofing, including so called meaconing. With this type of spoofing the GNSS signals are simply received and re-transmitted in order to force a victim receiver to report the position of the meaconer receiving antenna.

The technique for spoofing detection proposed by the authors in [7] is also based on the signal discrimination in spatial domain. It is assumed that the spatial information is available in form of estimated directions of arrival. Such information can be obtained by using dedicated array signal processing techniques for DOA estimation such as MUSIC or ESPRIT [8] and is often used for constraining an adaptive beamforming process. Also assuming that the attitude of the antenna array is unknown the spoofing detection was treated as a joint problem of the spoofing detection and the estimation of the array attitude.

The performance of the proposed technique has been first evaluated by means of numerical simulations [7] and later by processing the data collected in field trials where a GNSS repeater was used to emulate the meaconing attack [9][10]. The results reported in [9] and [10] demonstrate good spoofing detection performance in static and dynamic user scenarios when using a 2-by-2 uniform rectangular array with a half-wavelength spacing, 0.5λ, of the antenna elements on L1 carrier frequency. In the later work, in order to minimize the antenna footprint a new design of the array has been developed. The element spacing in the new design is reduced to 0.34λ while the side-length of array reduced by factor two from 270 mm to 135 mm. The size reduction of the antenna array generally leads to stronger mutual electromagnetic coupling between array elements and a lower overall antenna gain. In this paper we report the results of the practical field tests of the spoofing detection when using the miniaturized antenna array affected by the mentioned limiting effects

The rest of the paper is organized as follows. The first section describes the design and characteristics of the miniaturized antenna array. The second section briefly summarizes the concept of the antenna-based joint attitude estimation and spoofing detection approach which is described in details in [7]. In the next two sections the results on the spoofing/meaconing detection in realistic scenarios by using both the nominal-size and the miniaturized antenna arrays are presented: the third section focuses on the false alarm performance in an interference-free open-sky scenario, while the fourth section describes the results obtained by post-processing the data collected in a field test where a simple GPS repeater was used to simulate a meaconing attack. The summary of the results and conclusions will be given in the last section.

MINIATURIZED ANTENNA ARRAY

The miniaturized 2-by-2 antenna array was developed in the frame of BaSE (**Ba**varian **SE**curity receiver) project [11], whose goal is a flexible demonstrator platform of a robust user receiver for the Galileo public regulated service (PRS). The array is designed to receive the signals of Galileo PRS with full bandwidth in the E1 and E6 frequency bands allocated for the service. Figure 1 shows the miniaturized array together with the “full-size” E1/E6 antenna array where the typical element spacing of 0.5λ (referred to the E1 carrier frequency) is used. The side-length of the ground plane of the miniaturized array is only 135 mm while the side-length of full-size array is 270 mm. The significantly smaller footprint was achieved by miniaturizing the antenna elements of the array with the help of the material ROGERS RO6010 with a relatively high dielectric constant value of about 10.

The double frequency operation of the array is achieved by exploiting a stacked patch antenna technology as shown in Figure 2. The design of the array elements is based on the use of capacitively-coupled feeding of individual patches and application of relatively thick substrate material (7.5mm in total for the radiation part) that allows reaching the full bandwidth coverage required for the wideband Galileo PRS signals.

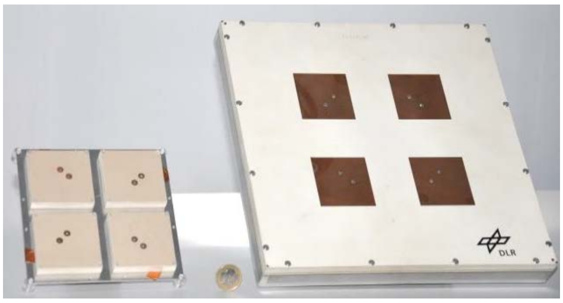


Figure 1: Miniaturized antenna array (left) and full-size array with half-wavelength spacing (right)

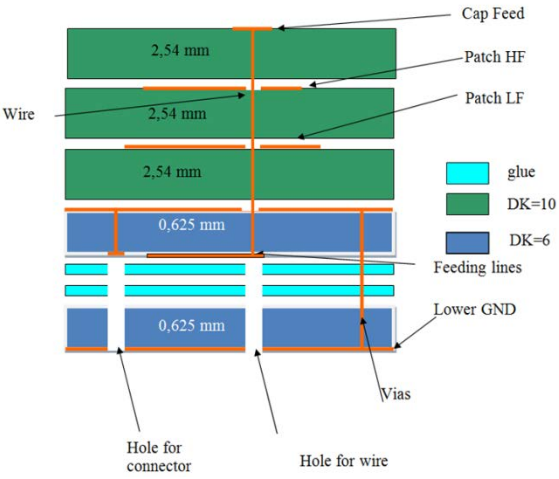


Figure 2: Design of array element

In this work the GPS L1 in air signals were used by a multi-antenna GNSS receiver [12] to collect the correlator output data for post-processing. Therefore only the upper higher-frequency patches and the E1 outputs of the antenna array elements were used. The element spacing of 65 mm (see Figure 3) in the miniaturized array corresponds to 0.34λ at the L1 carrier frequency of 1575.42 MHz. The elements spacing in the full size array is 95 mm which is about 0.5λ at the L1 frequency.

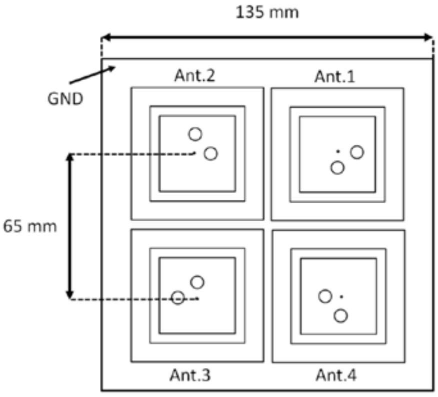
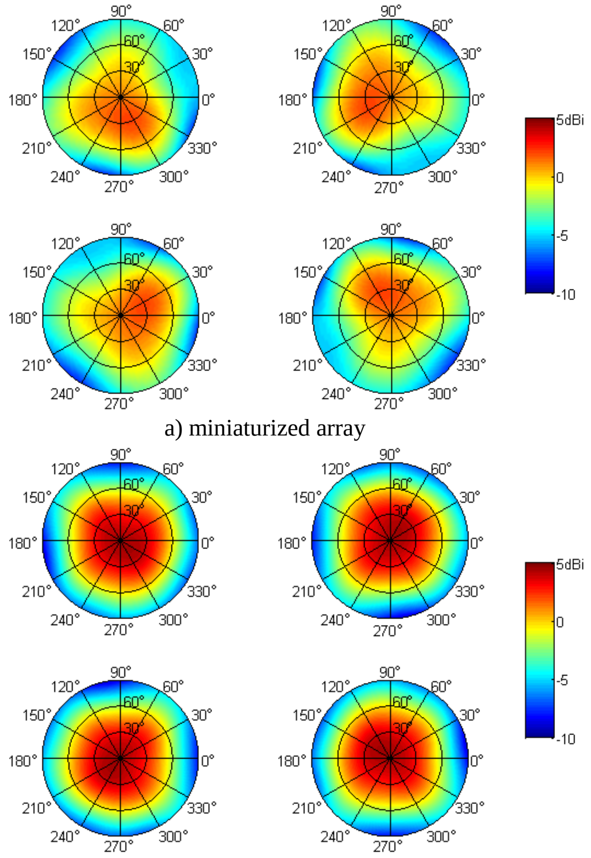


Figure 3: Geometry of miniaturized antenna array

The tighter arrangement of the array elements results in their stronger electromagnetic coupling and larger variations of the gain and phase reception patterns between the elements. This can be observed in Figure 4 and Figure 5 where the gain and phase radiation patterns of the array elements for both miniaturized and full-size arrays are presented for comparison reasons. These patterns were obtained by full-wave electromagnetic simulations performed in HFSS software from Ansys.



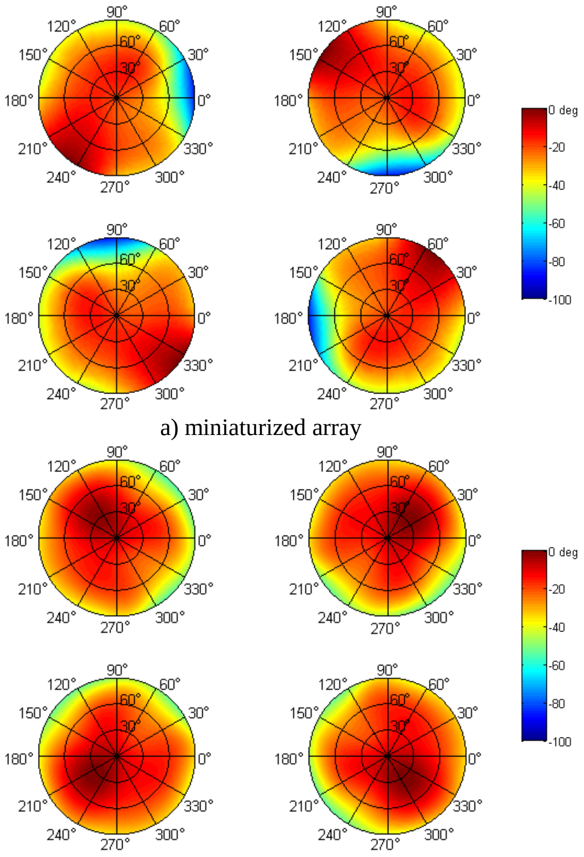
a) miniaturized array

b) full-size array

Figure 4: Gain patterns of array elements

ANTENNA-BASED JOINT ATTITUDE ESTIMATION AND SPOOFING DETECTION

In this section we give a short overview of the technique for joint estimation of the antenna attitude and spoofing detection that was presented by the authors in [7]. This technique is based on the use of estimated directions of arrival (DOAs) for discriminating between the spoofing and authentic GNSS signals. The estimated DOAs which are provided in the local antenna coordinate system are then checked against the directions to the satellites predicted by using the ephemeris data of the GNSS navigation message. These predicted directions are given in the local user's east-north-up (ENU) coordinate frame. Under conditions without spoofing and meaconing, the expected DOAs and the ones estimated in the antenna array processing should be consistent with each other.



a) miniaturized array

b) full-size array

Figure 5: Phase patterns of array elements

The relationship between the N_{DOA} DOAs in the estimated and predicted data sets can be mathematically formulated as follows:

$$\mathbf{D}_{loc} = \mathbf{R}(r,p,y)\mathbf{D}_{enu} + \mathbf{N} \qquad (1)$$

where

$\mathbf{D}_{loc}$ is a $[3 \times N_{\mathrm{DOA}}]$ matrix composed of N_{DOA} unit vectors of directional cosines describing the directions of arrival of satellite signals in the local coordinate frame of the antenna array;

$\mathbf{D}_{enu}$ is a $[3 \times N_{\mathrm{DOA}}]$ matrix composed of unit vectors of directional cosines corresponding to the predicted DOAs of the satellite signals in the user ENU coordinate frame;

$\mathbf{R}(r,p,y)$ is a $[3 \times 3]$ unitary rotation matrix (see [13], p.441) describing to the attitude of the antenna array defined by three Eulers angles: roll r, pitch p and yaw y. These angles are referred to the user local ENU coordinate frame;

$\mathbf{N}$ is a $[3 \times N_{\mathrm{DOA}}]$ matrix describing the measurement noise effect. Further for simplicity, we assume that the noise components follow Gaussian distributions with zero means and, in general case, different standard deviations $\sigma_1, \sigma_2, \ldots, \sigma_{N_{DOA}}$.

The solution for the antenna attitude can be obtained by solving (1) for Euler angles (r,p,y) in the least squares sense:

$$(\hat{r},\hat{p},\hat{y}) = \underset{r,p,y}{\arg\min} \|\mathbf{R}(r,p,y)\mathbf{D}_{enu} - \mathbf{D}_{loc}\|^2 \,. \qquad (2)$$

An iterative way of solving the least squares problem (2) is presented in [7].

The quality of the solution for the antenna attitude can be assessed using the sum of squares of errors (SSE) test statistics that is similar to how it is used with receiver autonomous integrity monitoring (RAIM) techniques. The SSE metric is defined as follows

$$\begin{aligned} SSE = \mathrm{trace}\{[\mathbf{R}(r,p,y)\mathbf{D}_{enu} - \mathbf{D}_{loc}]^{\mathrm{T}} \cdot \\ \mathbf{R}_N^{-1}[\mathbf{R}(r,p,y)\mathbf{D}_{enu} - \mathbf{D}_{loc}]\}, \end{aligned} \qquad (3)$$

where the inverse of the covariance matrix of the measurement noise $\mathbf{R}_N^{-1}$ is used for normalizing individual residuals of the least squares solution. Further, we assume that the individual DOA measurement errors are Gaussian and not correlated with each other and the matrix $\mathbf{R}_N$ is a diagonal matrix consisting of the error variances, $\sigma_1^2, \sigma_2^2, \ldots, \sigma_{N_{DOA}}^2$.

As shown in [7], if no systematic offsets observed between the measured and predicted DOAs of the GNSS signals, the SSE metric defined by (3) follows a central chi-squared distribution with $k = (2N_{\mathrm{DOA}} - 3)$ degrees of freedom. In another case, if all or some of the measured DOAs are biased with respects to predicted DOAs, the SSE metric follows a non-central chi-squared distribution with the same number of degrees of freedom as above but with some non-zero non-centrality parameter λ:

$$\begin{aligned} &\mathrm{H}_0(\text{no error}):\ SSE \sim \chi^2(k) \\ &\mathrm{H}_1(\text{error}):\quad SSE \sim \chi'^2(k,\lambda) \\ &k = (2N_{\mathrm{DOA}} - 3) \\ &\lambda = \sum_{n=1}^{N_{\mathrm{DOA}}} \left(\frac{\Delta_n}{\sigma_n}\right)^2 \end{aligned} \qquad (4)$$

where

Δ_n is the bias in the n-th DOA measurement, this bias is expressed as a spatial angle ψ_n between two direction cosines vectors of the measured DOA $\hat{\boldsymbol{d}}_{loc,n}$ and the predicted "almanac" DOA $\hat{\boldsymbol{d}}_{enu,n}$:

$$\Delta_n = \psi_n = \arccos\left(\hat{\boldsymbol{d}}_{loc,n}^{\mathrm{T}} \hat{\boldsymbol{d}}_{enu,n}\right), \qquad (5)$$

σ_n is the standard deviation of the n-th DOA measurement error given in units of the spatial angle ψ_n.

The detection of the systematic biases in DOA measurements can be carried out by using the Neyman-Pearson criterion, i.e. by setting a threshold for the SSE test metric defined by some desired false alarm rate. The presence of systematic biases can then serve as one of the indications for a spoofer / meaconing attack.

Another metric for spoofing/meaconing detection we use later in this work is based on the observation of the correlations between the single estimated DOAs [10]. Strong correlation between the majority of the directions of arrival gives the indication that the corresponding signals are likely to originate from a single source but not from the GNSS satellites in orbit.

In the next two sections, both SSE and DOA-correlation test metrics will be applied to the recorded data of field tests without and with a simulated meaconing attack.

PERFORMANCE IN INTERFERENCE-FREE SCENARIO

Preliminary tests under interference-free signal conditions have been performed at DLR Oberpfaffenhofen location. The miniaturized and full-size antenna array, one at a time, were installed on the roof of the DLR Institute of communications and navigation (see Figure 6) and connected to the experimental multi-antenna receiver GALANT [12]. The experimental receiver was used to collect the data blocks of post-correlation samples. Each block of 4x50 samples corresponds to 50 ms observation time. Two such blocks per second were collected for each GPS L1 satellite being tracked by the receiver. The collected data blocks were then post-processed with unitary ESPRIT for the direction of arrival estimation.

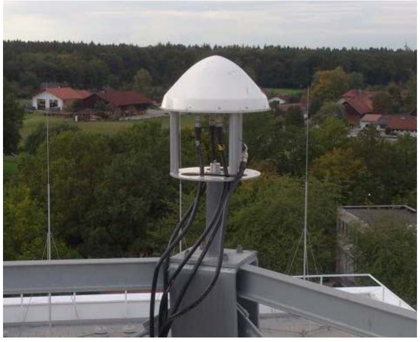
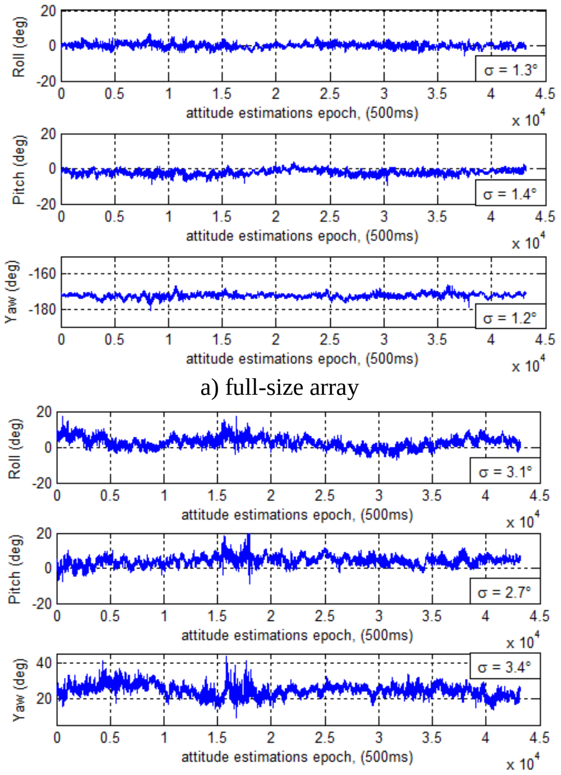


Figure 6: Roof installation of antenna array

The obtained DOAs of satellite signals were used for performing the estimation of the attitude of the antenna array. The rate of the attitude estimation was kept the same as the rate of the DOA estimation, i.e. 2 Hz. For the assessment of the DOA estimation error, mean antenna attitude angles (i.e. pitch, roll and yaw) have been obtained by averaging the single-epoch estimations over 6 hours data block. The time evolution of the single-epoch estimations of the Euler angles are presented in Figure 7. It can be observed that the standard deviations of the estimated Euler angles grow significantly when we moved from the full-size array (Figure 7, a) to the miniaturized one (Figure 7, b).

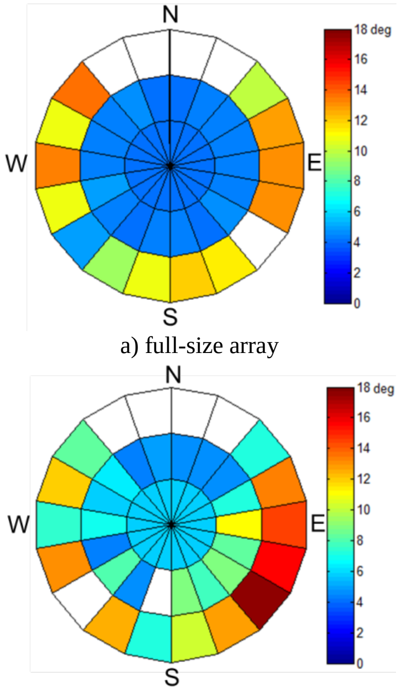


a) full-size array

b) miniaturized array

Figure 7: Estimated Euler angles of antenna array attitude

The mean errors of DOA estimation given in terms of a spatial angle between two unit vectors describing the estimated and reference directions are shown in Figure 8.

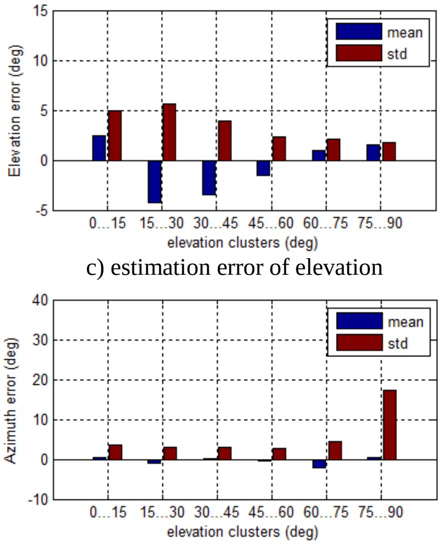


a) full-size array

a) miniaturized array

Figure 8: Mean angular error of DOA estimation

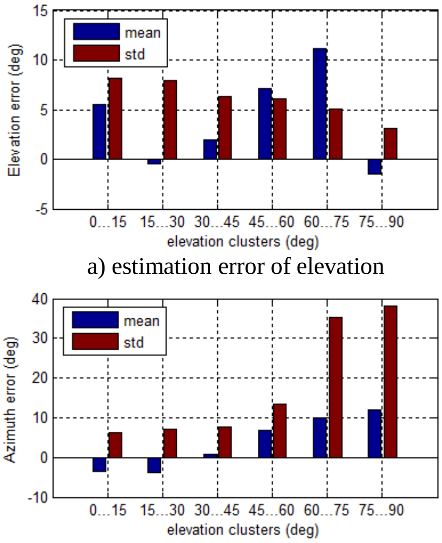
The computed mean and standard deviation of the DOA estimation error in terms of azimuth and elevations angles are presented in Figure 9 for the full-size antenna array and in Figure 10 for the miniaturized array. For convenience, the error values in these figures are grouped by several elevation clusters.



c) estimation error of elevation

d) estimation error of azimuth

Figure 9: DOA estimation error in terms of azimuth and elevation angles, full-size array



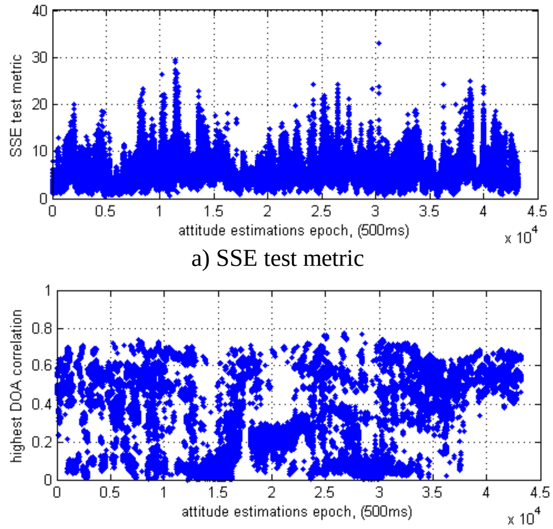
a) estimation error of elevation

b) estimation error of azimuth

Figure 10: DOA estimation error in terms of azimuth and elevation angles, miniaturized array

As can be seen from Figure 8, Figure 9 and Figure 10 the miniaturized antenna array delivers larger errors of the DOA estimation. To a big part this is because of the reduction of the aperture size. Another reasons for this effect is also a stronger model mismatch in the ESPRIT algorithm, which assumes rotation invariance in the reception patterns of the array elements.

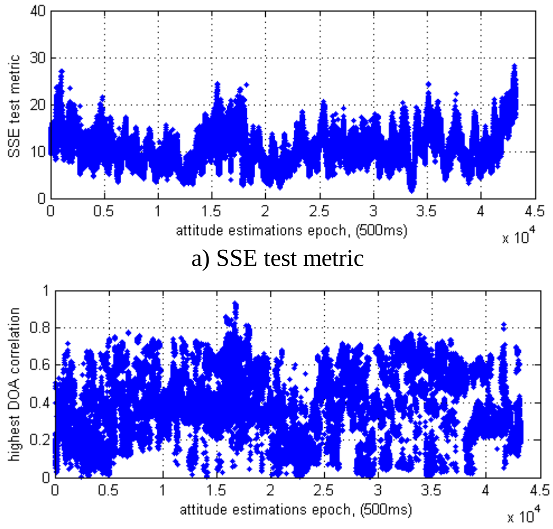
The results for spoofing detection metrics obtained both with the full-size and miniaturized arrays are presented in Figure 11 and Figure 12, correspondingly. It can be observed, that the values of the detection metrics are comparable between the two array options. The relative growth of the DOA estimation error in case of the miniaturized antenna array was accounted in the weighted least squares solution used by the detection algorithm (see Eq. (3)).



a) SSE test metric

b) DOA correlation test metric

Figure 11: Spoofing detection metrics, full-size array used



a) SSE test metric

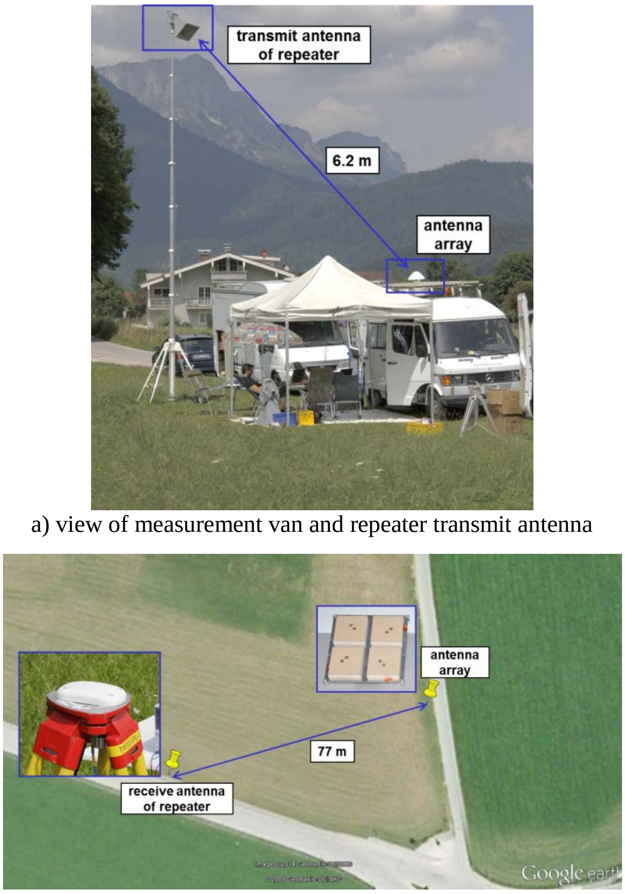
b) DOA correlation test metric

Figure 12: Spoofing detection metrics, miniaturized array used

PERFORMANCE UNDER SIMULATED MEACONING ATTACK

The field tests with a simple GPS L1 repeater simulating a meaconing attack were carried out in the area of the

Galileo test environment (GATE) in Berchtesgaden, Germany. The measurement set-up of the field tests is shown in Figure 13. The data used for post-processing and analysis were collected in the same way as during the preliminary tests in DLR Oberpfaffenhofen. The all-in-view active receive antenna of the GPS repeater was placed at a distance of 77 m from the measurements vehicle where the GALANT receiver was installed. The transmit antenna of the repeater was mounted on a mast of 8.6 m height. The slant distance between the miniaturized antenna array installed on the roof of the measurement vehicle and the repeater transmit antenna, a calibrated horn antenna, was 6.2 m. An additional low-noise amplifier was used to compensate for cabling losses. The power of the re-transmitted GPS L1 signals could be reduced in 1 dB steps by up to 20 dB using a variable attenuation.

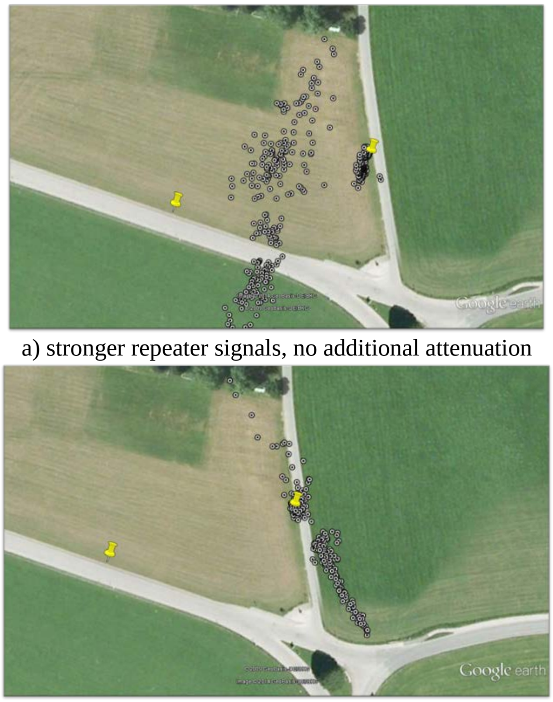


a) view of measurement van and repeater transmit antenna

b) geometry of repeater set-up

Figure 13: Measurement set-up

The effect of the re-transmitted signals of the GPS repeater on the positioning solution in the receiver is shown in Figure 14 for two different values of attenuation values: 0 dB (Figure 14a) and 10 dB (Figure 14b).

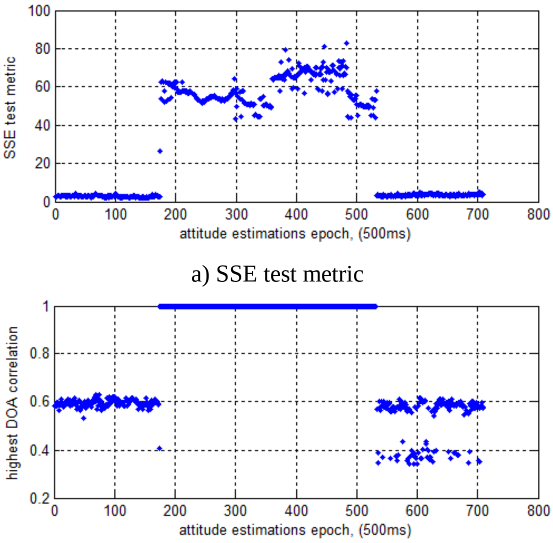


a) stronger repeater signals, no additional attenuation

b) weaker repeater signals, attenuation of 10 dB

Figure 14: Effect of repeater on position solution of experimental multi-antenna receiver, no spoofing mitigation activated

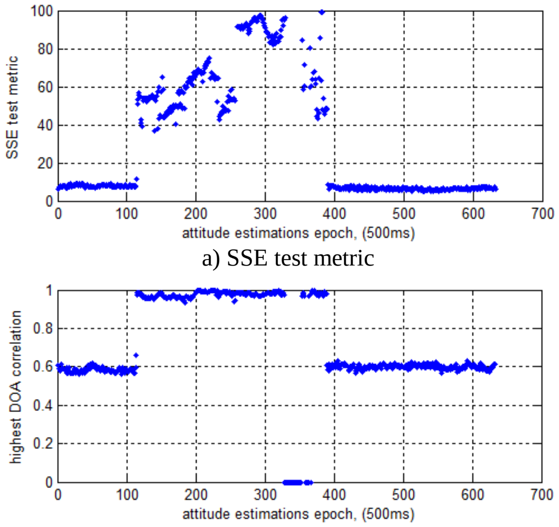
The results for spoofing detection metrics in case of the stronger and weaker repeater signals and the miniaturized antenna array used by the multi-antenna receiver are presented in Figure 15 and Figure 16, respectively. The corresponding detection flags issued by the detection algorithm are shown in Figure 17.



a) SSE test metric

b) DOA correlation

Figure 15: Spoofing detection metrics, stronger repeater signals

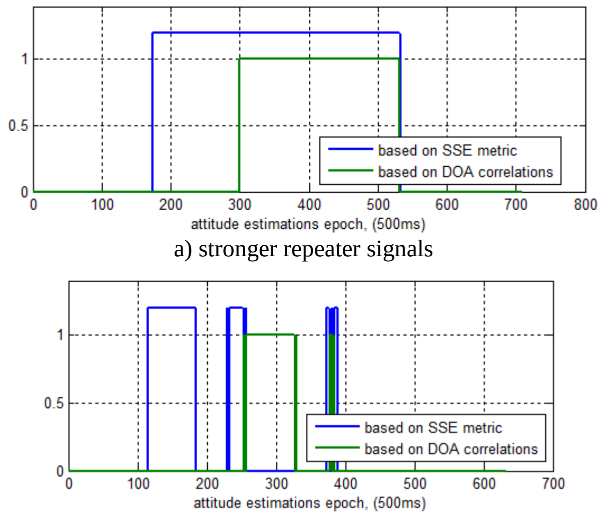


a) SSE test metric

b) DOA correlation

Figure 16: Spoofing detection metrics, weaker repeater signals

It can be observed in Figure 17 that the stronger repeater signals can be easily detected all the time they are radiated. The weaker repeater signals can be detected most of time with the help of at least one of the utilized test metrics. Some portion of time, however, the detection is not possible because of disturbed signal tracking and unavailability of the DOA measurements (see Figure 18).



a) stronger repeater signals

b) weaker repeater signals

Figure 17: Spoofing detection flags

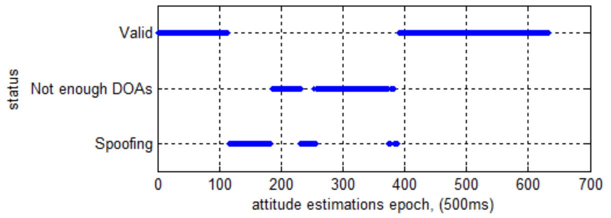
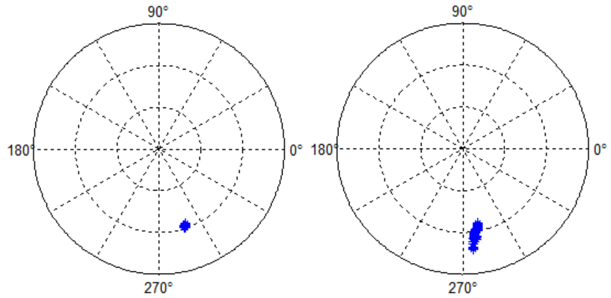


Figure 18: Status of spoofing detection in case of weak signals of GPS repeater

The estimated direction to the source of spoofing signals, i.e. in the case of GPS repeater – the direction to the repeater transmit antenna, is shown in Figure 19. This direction is estimated by using the average of the remarkably strong correlated DOAs which are identified in the spoofing detection process. As it can be seen in Figure 19b, the weak interfering signals result in the larger uncertainty of the estimated direction to their source.



a) stronger repeater signals b) weaker repeater signals

Figure 19: Estimated direction to spoofing source

SUMMARY AND CONCLUSIONS

In this paper the performance of the spoofing detection technique [7] while using a miniaturized antenna array has been studied. The performance analysis was based on the post-processing of data-blocks with the PRN-correlator outputs collected by using a multi-antenna GPS receiver in field tests under realistic signal conditions. The obtained results demonstrate that the DOA estimation performance degrades as the aperture of the antenna array becomes smaller. Consequently, the larger errors in the DOA estimation affect correspondingly the array attitude estimation. The field tests with the simulated meaconing attacks demonstrate that the spoofing detection with the miniaturized antenna array performed well and not much different than with the full-size antenna array. This is due to the fact that the detection is based on the identification of really strong signal anomalies in the spatial domain, which is still possible even with a degraded DOA estimation performance.

In the reported work, we used the unitary ESPRIT algorithm for DOA estimation. The signal model utilized by this technique is based on the assumption of array elements with identical characteristics. Since the mutual coupling between the array elements results in significantly different reception patterns, the performance of the DOA estimation degrades due to the model mismatch. This problem can be avoided by using other DOA estimation methods, such as MUSIC and maximum likelihood estimators, which allow accounting for the radiation patterns of the array elements.

ACKNOWLEDGMENTS

The study which results are reported in this paper was performed in the frame of BaSE-II (Bavarian security receiver) project co-funded by the Bavarian Ministry of Economic Affairs. This support is greatly acknowledged.

REFERENCES

[1] T. E. Humphreys, B. Ledvina, and M. Psiaki, “Assessing the spoofing threat: Development of a portable GPS civilian spoofer,” in *Proceedings of ION GNSS 2008*, 2008, p. 12.

[2] K. Wesson, D. Shepard, and T. Humphreys, “Straight Talk on Anti-Spoofing Securing the Future of PNT,” *GPS World*, no. January, 2012.

[3] P. Montgomery and T. E. Humphreys, “A Multi-Antenna Defense: Receiver-Autonomous GPS Spoofing Detection,” *Insid. GNSS*, no. March/April, pp. 40–46, 2009.

[4] M. L. Psiaki, T. C. Thomas, S. P. Powell, and B. W. O’Hanlon, “GNSS Spoofing Detection Using Antenna Differential Carrier Phase,” in *ION GNSS 2014*, 2014.

[5] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandon, and G. Lachapelle, “A low-complexity GPS anti-spoofing method using a multi-antenna array,” in *Proc. ION GNSS 2012*, 2012, pp. 1233–1243.

[6] P. Swaszek and R. Hartnett, “A Multiple COTS Receiver GNSS Spoof Detector--Extensions,” in *Proc. ION ITM 2014*, pp. 316–326.

[7] M. Meurer, A. Konovaltsev, M. Cuntz, and C. Hättich, “Robust Joint Multi-Antenna Spoofing Detection and Attitude Estimation using Direction Assisted Multiple Hypotheses RAIM,” in *Proc. ION GNSS 2012*, 2012.

[8] H. L. Van Trees, *Optimum Array Processing (Detection, Estimation, and Modulation Theory, Part IV)*. Wiley-Interscience, 2002, p. 1456.

[9] A. Konovaltsev, M. Cuntz, C. Hättich, and M. Meurer, “Performance Analysis of Joint Multi-Antenna Spoofing Detection and Attitude Estimation,” in *Proc. of ION International Technical Meeting 2013 (ION ITM 2013)*, 2013.

[10] A. Konovaltsev, M. Cuntz, C. Haettich, and M. Meurer, “Autonomous Spoofing Detection and Mitigation in a GNSS Receiver with an Adaptive Antenna Array,” in *Proc. ION GNSS+ 2013*, 2013, p. 12.

[11] A. Ruegamer, P. Neumaier, P. Sommer, F. Garzia, G. Rohmer, A. Konovaltsev, M. Sgammini, M. Meurer, J. Wendel, F. Schubert, and S. Baumann, “BaSE-II: A Robust and Experimental PRS Receiver Development Platform,” in *Presented on ION GNSS+ 2014*, 2014.

[12] M. V. T. Heckler, M. Cuntz, A. Konovaltsev, L. A. Greda, A. Dreher, and M. Meurer, “Development of Robust Safety-of-Life Navigation Receivers,” *IEEE Trans. Microw. Theory Tech.*, vol. 59, no. 4, pp. 998–1005, Apr. 2011.

[13] B. Hofmann-Wellenhof, H. Lichtenegger, and E. Wasle, *GNSS - Global Navigation Satellite Systems: GPS, GLONASS, Galileo, and more*. Wien: Springer-Verlag, 2007, p. 548.

[14] M. Wax and T. Kailath, “Detection of signals by information theoretic criteria,” *IEEE Trans. Acoust.*, vol. 33, no. 2, pp. 387–392, Apr. 1985.

[15] M. Haardt, “Efficient One-, Two-, and Multidimensional High-Resolution Array Signal Processing,” Ph.D. dissertation, Technical University of Munich, 1997.

[16] H. Krim and M. Viberg, “Two decades of array signal processing research: the parametric approach,” *IEEE Signal Process. Mag.*, vol. 13, no. 4, pp. 67–94, Jul. 1996.

[17] R. D. DeGroat, E. M. Dowling, and D. A. Linebarger, “The constrained MUSIC problem,” *IEEE Trans. Signal Process.*, vol. 41, no. 3, pp. 1445–1449, Mar. 1993.

[18] M. Sgammini, F. Antreich, L. Kurz, M. Meurer, and T. G. Noll, “Blind Adaptive Beamformer Based on Orthogonal Projections for GNSS,” in *25th International Technical Meeting of The Satellite Division of the Institute of Navigation - ION GNSS*, 2011, no. 1.