Detection and Mitigation of GPS Spoofing Based on Antenna Array Processing

J. Magiera* and R. Katulski

Department of Radio Communications Systems and Networks
Gdansk University of Technology
Gdansk, Poland
*radiokom@eti.pg.gda.pl

ABSTRACT
In this article authors present an application of spatial processing methods for GPS spoofing detection and mitigation. In the first part of this article, a spoofing detection method, based on phase delay measurements, is proposed. Accuracy and precision of phase delay estimation is assessed for various qualities of received signal. Spoofing detection thresholds are determined. Efficiency of this method is evaluated in terms of probability of false alarm and probability of detection when 4 to 8 GPS signals are received. It is shown that the probability of spoofing detection is greater than 99 percent if carrier-to-noise ratio is at least 46 dBHz. The second part of the article presents a GPS spoofing mitigation method which uses spatial filtering (null-steering) for excision of undesired signals. Performance of this method is analyzed in various conditions. Attenuation of undesired signals is estimated to be at least 60 dB when their signal-to-noise ratio is high. Furthermore, statistical analysis of the spatial filtering influence on the availability of true signals is provided. Eventually, a concept of practical anti-spoofing system implementation is proposed.

Keywords: Antenna array, detection, GPS, null-steering, spoofing.

1. Introduction

Global Positioning System receivers are present in many devices, starting from chips installed in simple trackers and smartphones [1], through professional geodetic devices, to high-dynamics receivers used in aviation and space vehicles. Apart from it, GPS is used to provide accurate synchronization to telecommunication networks and power grids. For a large number of these applications integrity of GPS signals and correctness of navigation data is critical, in order to compute accurate position, velocity and time (PVT) information. However, it must be remembered that GPS signals may be easily jammed even by signals of power equal to several Watts, depending on the distance from jammer [2].

GPS spoofing is a more sophisticated technique than jamming, since in this case the interference imitates the true navigation signals arriving from GPS satellites. Without any protective features, a GPS receiver is vulnerable to spoofing. The signals emitted by spoofer (spoofing device) not only jam the true signals but also cause the estimation of incorrect PVT values. Advanced receivers perform the Receiver Autonomous Integrity Monitoring (RAIM) algorithm. However, if the parameters and navigation data of spoofing signals comply with the current orbital parameters, RAIM may not detect the lack of integrity. It is especially probable in scenarios when spoofer initially simulates the true position of receiver and gradually deviates it to the wrong one.

It is clear that additional features are required to detect and mitigate GPS spoofing. Many methods of spoofing detection are proposed [3], such as:

- detecting unusual values or changes of power-related parameters: carrier-to-noise density ratio, absolute received signal power, power variations, L1/L2 band power ratio,

- monitoring time-related parameters: length of interval between phase transitions, delay between signals transmitted on different frequencies,

- analysis of sample values at correlator output,

- spatial processing – detecting multiple signals with the same direction of arrival using a multi-antenna receiver or a mobile single-antenna receiver,

- cryptographic protection,

- using hybrid navigation systems (GNSS+INS) [4], and many others. Nevertheless each of them has some drawbacks, concerning either increased complexity and cost or effectiveness limited to a certain set of spoofing scenarios. For example, one of suggested methods is based on checking whether the received signals are modulated with military P(Y) code, which is usually absent in spoofing signals [5]. Despite being effective, this solution uses two receivers and requires that one of them is protected from spoofing, which is not always possible.

In general, effectiveness of spoofing detection methods depends on the sophistication level of spoofer. For example, carrier-to-noise density detection algorithms may be defeated through adding an artificial white noise and changing the relative instantaneous amplitudes of fake signals.

The most sophisticated spoofers adjust the PRN code phase and carrier phase to match those of true signals arriving to a target receiver [6]. The usage of such device is limited, since it requires the knowledge of precise distance between the spoofer and the attacked receiver. While it may seem to be possible in certain situations, then using multiple scattered antennas to transmit synchronized signals, in order to imitate spatial separation of satellites, is very unlikely. This is the reason why the spoofing detection methods based on spatial processing are highly robust. The relative directions of arrival of signals from different space vehicles (SVs) are likely to be the most reliable factors during distinction between genuine and fake GPS signals. The undisputed advantage of such solutions is the inherent direction of arrival (DoA) estimation, results of which may be used to filter out the spoofing signal through beamforming or null steering.

To restore the correct operation of a spoofed GPS receiver, spoofing mitigation procedures are applied. Various approaches to solve this problem may be found in the literature [3]. Vestigial Signal Detection method, used for spoofing mitigation,

subtracts the local code and carrier replicas from buffered samples of composite received signal and then repeats the acquisition in order to detect and acquire suppressed signals from GPS satellites. When using this method, an assumption is made that the power of false signal is significantly higher than the power of true signal. It may not be fulfilled when the receiver is far from the spoofer. In such case, the true signals may be discarded in favor of the ones used for spoofing. Moreover, if spoofer's signals have considerably higher power than desired signals, the latter may not be detected, due to quantization error.

Another countermeasure, Receiver Autonomous Integrity Monitoring (RAIM), compares pseudorange measurements and discards the outliers resulting from presence of false signals. This approach may fail in scenarios, where spoofer is synchronized with true signals or when all the true signals are jammed, making it impossible to compare the measurements.

The most robust methods of GPS spoofing detection and mitigation seems to be the ones which use spatial processing. The necessity of antenna array usage results in increased complexity of the receiver, but it may be acceptable when robustness is the main criterion.

Spatial processing methods which use multiple antennas for reception of GNSS signals have already been proposed in various approaches in the last few years [7], [8]. Their applications are mostly related to jamming and interference mitigation. However, the performance of these spatial algorithms in various conditions is usually insufficiently investigated. In subsequent chapters of this article authors present an example solution which applies the antenna array processing for GPS spoofing detection and mitigation. Effectiveness of this method is also assessed.

2. Spatial processing

There are various ways of obtaining the direction of arrival or angle of arrival estimate. They include: mechanically or electronically controlledreception pattern antennas, phase interferometry, subspace-based methods such as MUSIC or ESPRIT and others. Most of these possibilities require additional signal processing blocks. In GNSS receivers available on the market, signal processing blocks

are usually integrated into one chip without any external access to samples of received signals. That is why the best way to assess the performance of DoA estimation is to use a software receiver with an analog front-end. Off-the-shelf chip-scale GPS front ends are available, yet they usually provide only one or two bit output sample resolution, which is sufficient for GPS signal reception, but it may be too low for DoA application. It is better to use a separate preamplifier and an analog down converter followed by a high-resolution multi-channel digitizer.

Subspace-based methods of DoA estimation are computationally efficient and accurate, however they require relatively high Signal-to-Noise Ratio, which is not the case of GPS signals hidden almost 20dB below noise floor. Nevertheless, they may be applied to the post-correlation signals [9]. The other approach, selected by authors of this article, is to measure the received signals' phase shifts which may be used to estimate theDoA through phase interferometry.

Direction of arrival corresponds to the phase delay differences of signals at the outputs of receiving antenna array elements. The level of ambiguity in resolving DoA is highly dependent on array geometry and characteristics of array elements (sensors).

Since spoofing signals are practically always radiated from a single source, they arrive to the receiver from the same direction, no matter if it is a line-of-sight or a reflected signal. On the other hand, genuine signals from GPS satellites arrive from different directions within the whole hemisphere, assuming the clear view of the sky. Basing on this assumption, GPS spoofing is detected when multiple received signals have the same or very similar DoAs.

Azimuth and elevation, which represent two-dimensional DOAs, are non-linear functions of phase delays. That is why a relation between the phase delay estimation error and the DoA estimation error depends on relative orientation between source of signal and receiving antenna. Thus for GPS spoofing detection it is more reliable to compare the phase delays than to compare the actual DoAs.

3. Simulation model

In this paragraph the model of received GPS signals as well as the model of the antenna array are described. They are necessary assumptions to assess the performance of proposed counter-spoofing methods.

3.1 Signal model

In order to determine the effectiveness of proposed spoofing detection method, a simulation model was developed. This model assumes that transmitted signals are only subject to the additive white Gaussian noise (AWGN) and their delays are proportional to the distances between the source of signal and particular elements of the antenna array.

Signals received by multiple antenna elements may be described as follows:

$$s_i(t) = \sqrt{2P_i} \cdot c(t - \tau_i) \cdot d(t - \tau_i) \cdot \cos(2\pi f_c t - \tau_i) + n_i(t) \quad (1)$$

where $i = 1, ..., M$ is the array element number, P_i is the received power of i-th signal, τ_i is the total delay of transmission from the signal source to the i-th element, c is the pseudorandom C/A code sequence, d is the navigation message data sequence, f_c is carrier frequency and n_i is the additive noise at i-th element.

One of the antenna array elements is selected to be the reference. Only the signals received through this element pass the full signal processing path of GPS receiver, that is acquisition and tracking phase, including C/A code phase and carrier phase estimation. Acquisition procedure, as well as code and carrier tracking loops are implemented in software, according to algorithms presented in [10]. The remaining blocks of GPS receiver, i.e. pseudorange estimation, navigation message decoding etc. are not involved in spoofing detection procedure.

Signals from the rest of the outputs of antenna array are correlated with the same local replica which is used for correlation with the reference signal. Since the relative delays between signals are less than one L1 carrier period, which is over

1500 times shorter than duration of one C/A code chip, the code phases of corresponding signals at all antenna elements are practically the same.

Multiplying the received signal with a C/A code replica provides the carrier modulated with navigation data. The next operation is correlation with complex carrier which provides the information about the phase shift:

$$\varphi_i = \arctan\left(\frac{\mathrm{Im}\{Z_i\}}{\mathrm{Re}\{Z_i\}}\right) \tag{2}$$

where Z_i is the complex sample at correlator output. Phase of carrier replica is adjusted to match the phase of the reference signal from the first sensor. Thus, the rest of computed phase shifts are the DoA-related phase delays between the first and the other array elements.

3.2 Antenna array model

While selecting an antenna array configuration for DoA estimation, many factors have to be taken into consideration. First, the number of sensors. Two sensors may be used for phase delay discrimination [7] and for limited estimation of the angle of arrival. However, when using such an array, the same phase shifts are possible for baseline-symmetrical azimuths. Adding the third non-in-line element to the array eliminates the ambiguity of the azimuth. Even more elements are necessary for unambiguous two-dimensional DoA estimation. On the other hand the number of sensors must not be too high. There are limitations on the size of the antenna array. When the distance between sensors is larger than half of the wavelength, phase ambiguity occurs. A large number of closely-spaced sensors increases mutual coupling. Also more signal processing paths are required in this case, which increases hardware and computational complexity.

Besides the number of elements, their arrangement is important. The most popular are planar arrangements: uniform linear/rectangular array (ULA,URA) [11], as well as circular array or circular array with additional central sensor. Non-

planar arrays may be beneficial for 2D DoA estimation [12].

Four-sensor uniform circular array was selected for purpose of described simulation research. Configuration of elements is presented in Fig. 1. Spacing d between neighboring elements is equal to 0.45 wavelength. It is less than half wavelength in order to decrease the level of phase ambiguity when the noisy signal impinges on the array from direction parallel to any of the array's baselines.
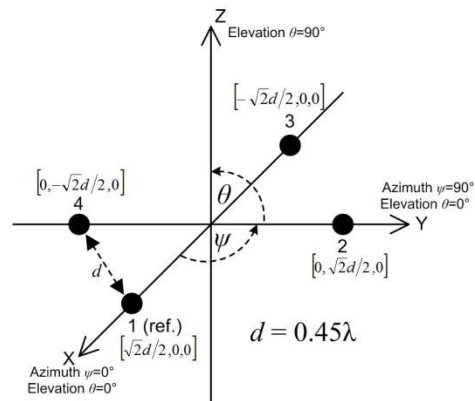

Figure 1. Proposed configuration of the antenna array elements.

As all of the elements are located on a plane which is parallel to the ground, there exists an uncertainty whether the elevation is positive or negative. However, in case of GPS antennas, signals are received only from directions with positive elevations, so estimated elevation angles may be mapped to range from 0 to 90 degrees.

Coupling between sensors, which depends on specific types of antenna elements, is not taken into consideration in this model. It may have a significant influence on amplitude and phase of received signals, thus should be investigated in practical implementations.

4. Simulation results

Preliminary performance assessment of the described spoofing detection and mitigation methods was made basing on the results of the following simulations.

4.1 Mean and RMS value of phase delay estimation error

A series of simulations were conducted in order to assess the accuracy and precision of phase delay estimation with various signal-to-noise ratios. In each scenario two parameters were measured for phase delays: mean value offset and root-mean-square error (RMSE).

Since the power spectral density of GPS signals is below the noise floor and all the signals share the same frequency band, it is difficult to estimate the wideband SNR value. In this case, carrier to noise density ratio (C/N_0) is used to assess the received signal quality. It is calculated after correlation, when the pseudorandom C/A code and the navigation data are removed from carrier. The relation between signal-to-noise ratio and C/N_0 in civilian GPS is:

$$\frac{C}{N_0}[dBHz] = \frac{S}{N}[dB] + 10\log(B[Hz]) =$$
$$= \frac{S}{N}[dB] + 63.1[dBHz] \tag{3}$$

where B is the GPS C/A signal bandwidth equal to 2.046 MHz. Simulations were performed for C/N_0 from 35dBHz to 60dBHz, as it is a range of values mostly occurring during reception of real GPS signals. Four uncorrelated realizations of AWGN were added to relatively delayed GPS waveforms to obtain desired SNR. To check whether it is the only source of signal distortion, C/N_0 was estimated using three different procedures described in [13],[14]: Variance Summing method, Beaulieu's method and Moments method. For each method, the difference between theoretical and measured value in range from 40 dBHz to 60 dBHz was less than 0.5 dB. Measured C/N_0 error values are presented in Fig. 2.

Phase delay measurements are calculated after correlation with 1ms integration time. They are contained in-π to π range by default. If the nominal phase delays are close to the borders of this range, phase wrapping may cause the increase in RMS error and mean value offset. That is why the computed phase delays are additionally mapped into -2π to 0 and 0 to 2π ranges. For each pair of array elements the

range with the lowest variance within last 100ms is selected to provide the samples used to assess accuracy and precision.
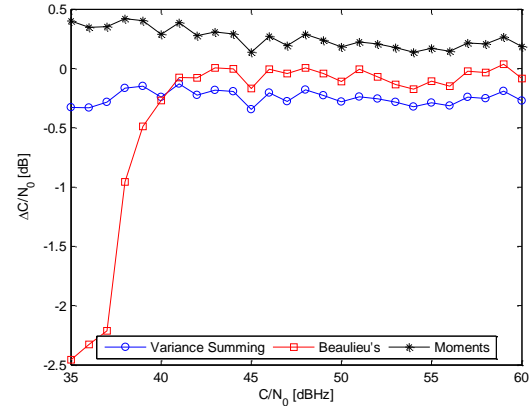

Figure 2. Carrier-to-noise ratio estimation error.

The charts presenting mean value offset and RMS error as a function of C/N_0 are shown in Figs. 3 and 4respectively. For each C/N_0 value, 10 iterations were executed and the average value was taken. In each iteration 5 seconds of signal were analyzed. Simulations were conducted for various directions of arrival and each time the results were very similar, which means that phase delay error is independentfrom nominal phase delay.

As may be seen, the offset of mean value oscillates around zero value in entire C/N0 range. It proves that AWGN does not decrease the accuracy of phase estimation.
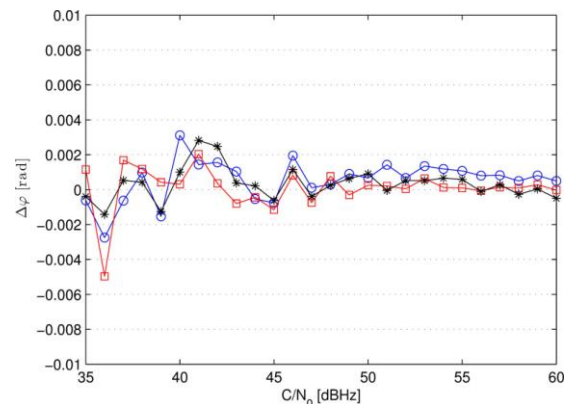

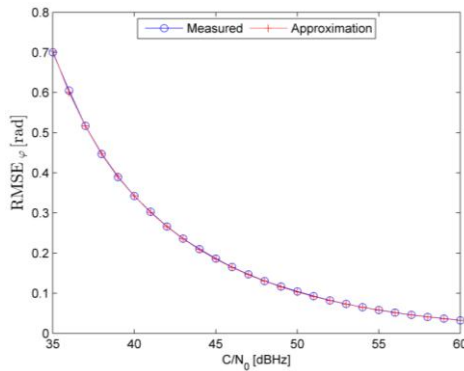Figure 3. Mean phase delay offset from nominal value.

Figure 4. Root mean square error of phase delay.

The RMS error is the same for all three pairs of array elements. Eq. 4 describes the least squares approximation of $RMSE_\varphi$ as a function of C/N_0.

$$RMSE_\varphi[rad] = \sqrt{10^{\left(3.037-\frac{C/N_0}{10.083}\right)} + 10^{\left(7.093-\frac{C/N_0}{4.508}\right)}} \quad (4)$$

4.2 Phase delay error distribution

Distribution of phase delay difference error must be known in order to evaluate the probability of spoofing detection, as well as the probability of false alarm. Statistical analysis was conducted on the samples of phase delay error to decide whether it follows a normal distribution. A sample histogram of phase delay estimation error is presented in Fig. 5. As may be seen, it resembles the Gaussian bell curve. However, to make sure that it is in fact normal, another two tests were carried out.
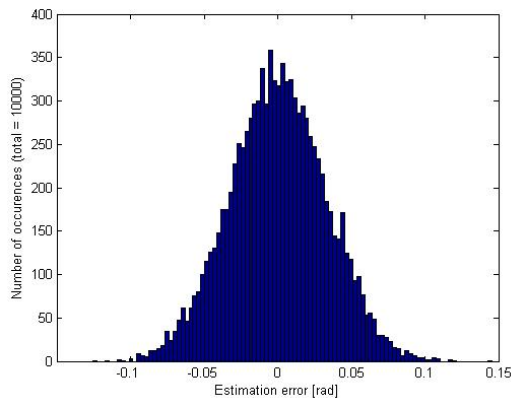

Figure 5. Sample histogram of phase delay estimation error (C/N0 = 60 dBHz).

First, the obtained phase delay estimation error values were plotted on a normal test plot. The distribution is assumed to be normal, if the samples coincide with the diagonal line. As may be seen in Fig. 6, the coincidence is very good.
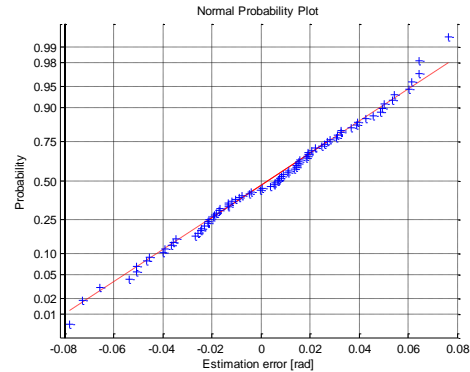

Figure 6. Normal test plot of phase delay error.

Another test was the calculation of the Anderson-Darling statistic in order to numerically assess the goodness of fit. For significance level α=0.05, it is said that the distribution is normal if the statistic value is less than 0.752. Calculations were done for integer values of C/N_0 in range from 40 dBHz to 60 dBHz. The results are shown in Fig. 7. All of the values do not exceed the threshold, so it may be assumed that the phase delay error is distributed normally.
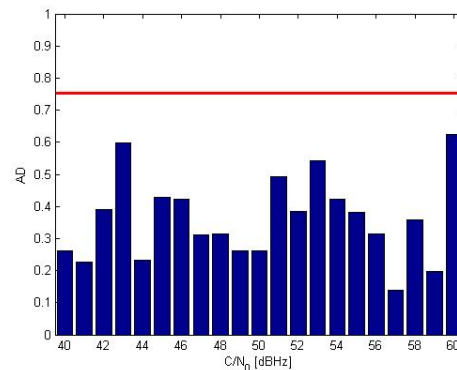

Figure 7. Anderson-Darling statistic of phase delay error.

4.3 Probability of spoofing detection

In ideal conditions, all spoofing signals would cause the same phase delays. In the noisy

channel they are not exactly the same. Presence of spoofing might be detected by checking whether the phase delay differences of multiple GPS signals are below the specific threshold. Knowledge about possible phase delay error is important for selection of such threshold levels which would maximize the probability of detection.

Incorrect GPS spoofing detection, called false alarm, may occur in situations when multiple true satellite signals are received from similar directions and all phase delay differences are below predefined threshold. In order to determine how large these differences may be, the positions of all GPS satellites within 24 hours period were computed with 1 minute interval. For each time interval, a number (from four to eight) of visible satellites, with most similar directions of arrival, were selected and nominal values of phase delay differences were calculated. Assuming that probability of false alarm P_{fa} is not greater than 10^{-4}, threshold level Φ_{th} may be evaluated from:

$$P_{fa} = \prod_{i=2}^{M} \prod_{j=1}^{N} P\left(\left|\Phi_{ij}\right| \le \Phi_{th}\right) \quad (5)$$

where Φ_{ij} is the j-th difference of phase delays between first and i-th element of antenna array, $N=(K\text{-}1)\cdot K/2$ and K is the considered number of spoofing signals (fake satellites).

If phase delays are normal random variables with variance $\sigma^2 \approx RMSE_\varphi^{\,2}$, then:

$$P_{fa} = \prod_{i=2}^{M} \prod_{j=1}^{N} 0.5\left[1 + erf\left(\frac{\Phi_{th} - \left|\Phi_{ij0}\right|}{\sqrt{2}\sigma}\right)\right] \quad (6)$$

where Φ_{ij0} are the true differences of phase delays, i.e. without error caused by noise.

Threshold levels were calculated for C/N_0 range from 35dBHz to 60dBHz. Receiving antenna positions were set to 0, 15, 30, 45, 60, 75, 90 degrees north and 0 degrees of longitude, according to WGS84 coordinates. Final threshold level was selected for each case as the minimum from values obtained for different positions of the receiver. Results, for various

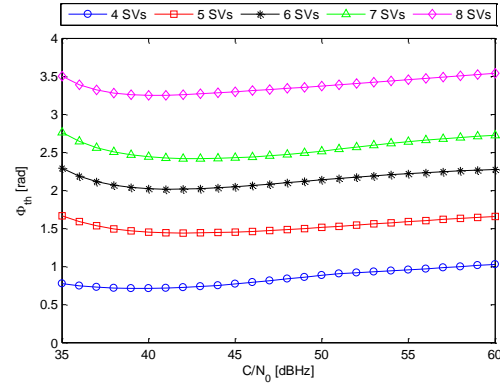numbers of satellites involved in spoofing, are shown in Fig. 8.

Figure 8. Threshold levels for phase delay difference.

After determination of the detection thresholds, probability of spoofing detection P_d was estimated using expression similar to Eq. 6:

$$P_d = \prod_{i=2}^{M} \prod_{j=1}^{N} 0.5\left[1 + erf\left(\frac{\Phi_{th}}{\sqrt{2}\sigma}\right)\right] \quad (7)$$

Probabilities of detection, as functions of C/N_0 and number of satellites, are presented in Fig. 9. For C/N_0 greater than 47 dBHz practically every presence of spoofing will be detected, irrespective to the number of fake satellites. To provide at least 99% probability of detection with 4 to 8 satellites, carrier-to-noise ratio must not be less than 46, 41 and 39, 38 and 36 dBHz respectively.
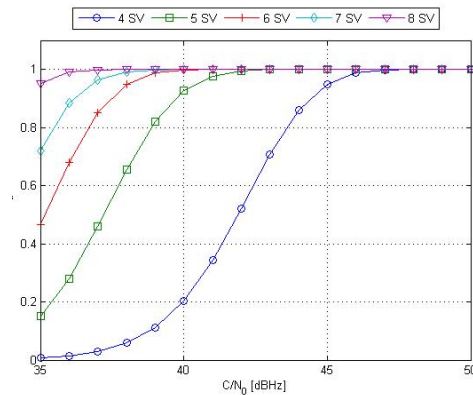

Figure 9. Probability of spoofing detection.

4.4 Performance of null-steering for spoofing mitigation

After information about relative phase delays of spoofing signal is obtained, null-steering is applied to suppress all the signals arriving from particular direction. The optimum complex weight vector **w** for null-steering using *M*-element antenna array is:

$$\mathbf{w} = \left[1, \quad -\frac{1}{M-1}\exp(-i \cdot \Delta\varphi_{1,2}), \quad \ldots \quad -\frac{1}{M-1}\exp(-i \cdot \Delta\varphi_{1,M}) \right]^{T}$$

(8)

where $\Delta\varphi_{1,m}$ is the unwanted signal phase delay between the first (reference) and *m*-th element of array [16]. Filtering process is performed according to the following expression:

$$s_{filt}(t) = \text{Re}\left\{ \left[s_1(t) \quad \ldots \quad s_M(t) \right] \cdot \mathbf{w} \right\}$$

(9)

where $s_{filt}(t)$ is the antenna array output signal and $s_m(t)$ is the signal received through *m*-th sensor of array.

Complex signal *y(t)* at the output of proposed antenna array may evaluated using Eq, 10, assuming unitary power of arriving signal:

$$y\left(\psi, \theta, \vec{w}, t\right) = \sqrt{2}\exp(-i \cdot \varphi_c(t)) + \sqrt{2}\sum_{m=2}^{4} w_m \cdot \exp\left(-i \cdot \alpha_m\right)$$

(10)

$$\alpha_m = \left[\varphi_c(t) + \frac{2\pi d_{1,m}}{\lambda}\cos\left(\psi + (3-m)\frac{\pi}{4}\right)\cos(\theta) \right]$$

(11)

where ψ is the DoA azimuth angle, θ is the DoA elevation angle, $\varphi_c(t)$ is carrier phase at reference sensor, w_m is the *m*-th element of weight vector, $d_{1,m}$ is distance between first and *m*-th array element and λ is wavelength. Elements of array are assumed to be isotropic. Array gain is calculated in the following way:

$$G\left(\psi, \theta, \vec{w}\right) = \frac{1}{T}\int_0^T \left[\text{Re}\left\{ y\left(\psi, \theta, \vec{w}, t\right) \right\} \right]^2 dt$$

(12)

where *T* is equal to one carrier period.

Pattern described by Eq. 12 refers to the signal component located exactly at L1 frequency. Since the dimensions of antenna array are related to a particular wavelength, the attenuation varies for different frequency components of received signals. In addition, this variation is a function of DoA. For example, if elevation angle is equal to 90°, all relative phase delays are zero and high attenuation is constant in whole frequency range. Largest differences of attenuation occur for low elevation angles and azimuth angles close to 0° and 180°. Fig. 10.shows the example frequency characteristics of the selected array in 2.046 MHz band around L1 frequency, at 0° DoA azimuth. As may be seen, center frequency component is completely eliminated from output signal. Attenuation on the borders of analyzed frequency range is much lower. Assuming that spectrum of noisy spoofer's signal is flat, total attenuation G_{GPS} in 2.046 MHz band, at 0° elevation of arrival and 0° or 180° azimuth of arrival, is equal to about –60 dB.
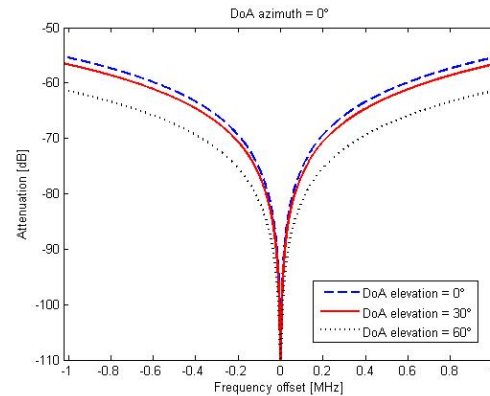

Figure 10. Frequency characteristics of proposed antenna array.

Phase estimation error causes changes in shape of antenna array reception pattern. Erroneous phase delays are not connected with specific DoA, so the pattern does not have a distinct null. In other words, presence of noise and interference decreases the attenuation of all signals arriving from the direction of spoofing source. To constrain a null in direction close to DoA of spoofing signal, the best-fit DoA is calculated for inaccurate phase delays. Error function is selected to be the mean-square difference of phase delays:

$$E(\psi, \theta) = \frac{1}{M-1}\sum_{m=2}^{M}\left[\Delta\varphi_{1,m}(\psi, \theta) - \Delta\varphi_{1,m}^*\right]^2$$

(13)

where $\Delta\varphi(\psi,\theta)$ is a phase delay connected with specific DoA while $\Delta\varphi^*$ is the phase delay estimated in presence of noise. Gradient optimization is used to evaluate the best-fit DoA. It involves an iterative procedure which may be described in the following way:

$$\begin{bmatrix} \psi_{k+1} \\ \theta_{k+1} \end{bmatrix} = \begin{bmatrix} \psi_k \\ \theta_k \end{bmatrix} + \beta \cdot \begin{bmatrix} \dfrac{\partial E}{\partial \psi}(\psi_k, \theta_k) \\ \dfrac{\partial E}{\partial \theta}(\psi_k, \theta_k) \end{bmatrix} \qquad (14)$$

where k is iteration index and β is a real constant coefficient which affects the convergence of the procedure and the number of iterations required to achieve acceptable error value. Initial null direction is set to $\{\psi_0, \theta_0\} = [0°, 45°]$. Eventually, new set of phase delays is calculated, based on resulting DoA. These phase delays, instead of those primarily estimated, are used to form the array weight vector as in Eq. 8. Average attenuation of spoofing signals, arriving from 0 azimuth and 0 elevation, before and after optimization of weight vectors, is presented in Fig. 11. Results, for each C/N_0 value, were obtained by averaging 1000 attenuation values calculated for normally distributed random phase delays. It may be seen that the optimization significantly increases the attenuation of undesired signals. As C/N_0 increases, attenuation approaches the –60 dB value, which is the limit for signals impinging on array of proposed configuration from mentioned DoA. On the other hand, if no optimization is performed, the attenuation of spoofing signals is not satisfactory, especially for low C/N_0.
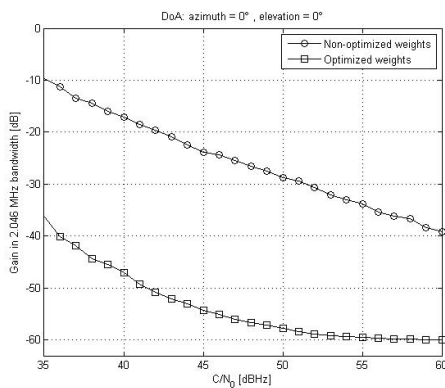

Figure 11. Mean attenuation of spoofer's signals in presence of noise.

4.5 Influence of null-steering on reception of true GPS signals

Null-steering towards source of spoofing signal results not only in excision of this unwanted signal, but may also have negative influence on quality of desired, true signals, arriving from GPS satellites. A ttenuation of satellite signals may be estimated from Eq. 10, considering wide bandwidth. Relative noise power between input and output of the array must be also taken into account to calculate changes in signal-to-noise ratio caused by spatial filtering. Since the ambient noise does not have a one specific source in space, its attenuation G_n depends only on the weights vector and is expressed in the following way:

$$G_n = \left\| \mathbf{w} \right\|^2 = \sum_{m=1}^{M} \left| w_m \right|^2 \qquad (15)$$

Simulation research was conducted to estimate the probability that SNR decrease exceeds acceptable level for given number of visible satellites. This level depends on expected SNR in receiver's location without spoofing activity. Positions of all operating satellites were computed, basing on GPS almanac, within 24-hour period with 1 minute interval. GPS receiver's positions were set to 0°, 15°, 30°, 45°, 60°, 75° and 90° North, 0° of longitude with 0 m height, according to WGS-84 coordinates. DoAs and corresponding changes of SNR were computed for all of satellites' and receiver's positions. DoAs of spoofer's signals, represented by pairs of azimuth and elevation angles, were selected respectively in ranges from 0° to 360° and from 0° to 90°, with 5° step. For each of analyzed acceptable SNR decrease levels, a cumulative distribution function (CDF) was calculated as the minimum of CDFs estimated for all receiver's positions. Resultant probability distribution was evaluated through differentiation of this CDF. Statistical representation of obtained results is shown in Fig. 12. If 12 dB SNR decreaseis acceptable, full satellite visibility is most likely. On the other hand, when quality of true signals is poor and only 3 dB SNR decrease is tolerated, number of excised signals is larger, with 2 being the most probable value. From practical point of view, information about the number of signals possible to receive is more important than about the absolute number of excised signals, since the total number of

visible satellites varies with time and receiver's position. Thus, another investigation was performed in order to evaluate the probabilities that certain number of satellite signals are possible to be received when null-steering is enabled. Results of this analysis are presented in Fig. 13. Probability that at least 4 satellites are visible is over 95 %, if acceptable SNR decrease is less than –1 dB. To provide over 95 % probability of at least 5, 6 and 7 visible satellites ΔSNR thresholds must be set to –2 dB, –4 dB and –7 dB, respectively.
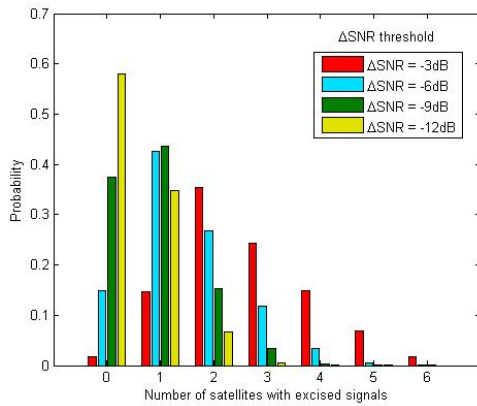

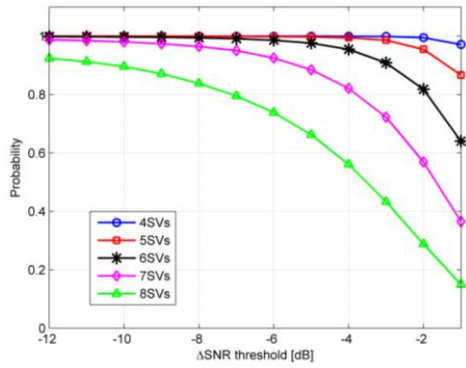Figure 12. Probability of true signals' excision due to null steering.

Figure 13. Probability that not less than given number of satellites are visible.

5. Concept of the anti-spoofing system

In order to verify the results obtained from simulations, a proof-of-concept of the proposed anti-spoofing system is going to be implemented. The general concept is presented in Fig. 14.

Signals from the outputs of a four-element antenna array are amplified and downconverted from RF to IF in an analogue front-end which also performs automatic gain control. IF signals at 2.5 MHz are sampled in the data acquisition board installed in a high-end PC. The following stages of signal processing are performed in dedicated software. Amplified and bandpass filtered RF signals are transmitted form the front end to a null-steering board which consists of four signal paths, eachincluding a wideband phase shifter and a voltage controlled attenuator. Values of attenuation and phase shift are set according to spoofing signals phase delays estimated in software. Next, the signal which is a sum of four phase shifted component signals is provided to a commercial GPS receiver, so that the result of spoofing mitigation may be assessed.
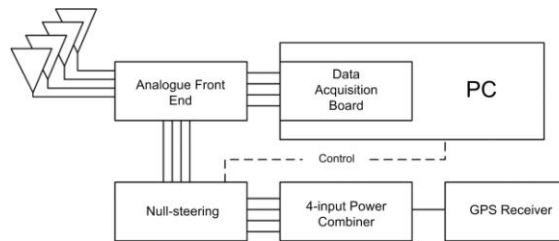

Figure 14. Block scheme of the anti-spoofing system.

The functions which are realized in software are depicted in form of a block diagram in Fig. 15. First, four signals which are sampled in DAQ board with 8.192MHz sampling frequency are written to a long buffer in random access memory. This buffer can contain 60 seconds of signal and after that period the oldest data are replaced with currently acquired samples. The samples from buffer may be written to a file as a reference signal for post-processing. Next, GPS signals acquisition procedure is realized based on samples acquired in the first signal path. Acquisition function returns the number of received signals, satellite identification numbers, coarse carrier Doppler shifts and C/A code phase shifts. These parameters, along with signal samples, are passed to GPS signal tracking loop, which follows the changes of Doppler frequency and phase of C/A code. Carrier phase is also estimated so the coherent carrier replica may be generated locally.
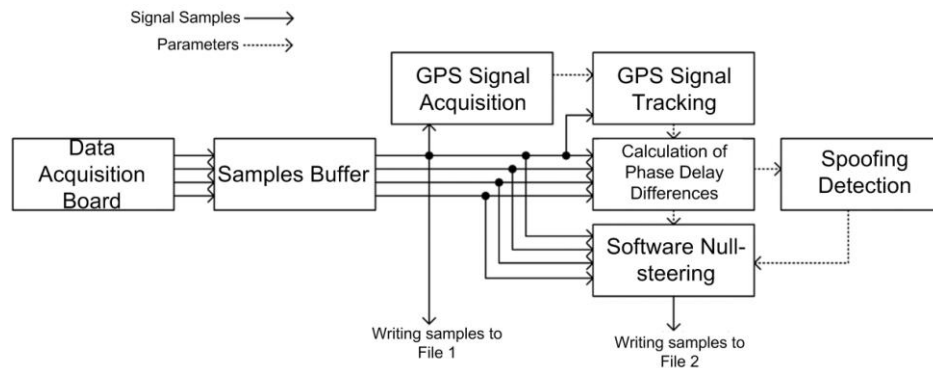
Figure 15. Block scheme of the software part of the system.

Carrier phase shifts in the second, third and fourth signal paths are estimated through multiplication of samples with this replica and C/A code. Next step is the calculation of phase delays between the signals from the first and the other signal paths. After that, differences of respective phase delays are calculated for all of the visible satellites. Spoofing detection procedure is executed basing on these data. If all of the phase delay differences are below the threshold, it is decided that multiple signals arrive from the same direction, which means that spoofing is present.

In case of spoofing detection, estimated phase delays are passed to the null-steering board which filters out the unwanted signals. In addition, software null steering may be performed using the same phase delays. The samples of filtered signals are stored in a file for post-processing. Samples of signals before and after null-steering may be fed to a software GPS receiver in order to verify the effectiveness of spoofing mitigation.

The presented block diagrams describe a new concept which is currently being practically implemented.

6. Conclusion

GPS spoofing is a serious threat and, in fact, it is not very difficult to realize such an attack. It is clear that robust countermeasures, composed of detection and mitigation algorithms, are required.

Spatial signal processing, which takes advantage of multi-antenna reception is one of the most effective ways of distinguishing between true and fake GPS signals.

Results of simulations presented in this article show that comparison of phase delays may be used for GPS spoofing detection. It provides low probability of false alarm and high probability of detection, unless only four signals with low signal-to-noise ratios are received.

Additive white Gaussian noise was assumed in simulation as the only interference with received GPS signals. Other types of disturbance, such as narrowband signals or selective fading are spread during correlation and result in raised noise spectral density. Probability of detection in presence of interference of any type may be estimated if C/N_0 is known.

There is a possibility to extend the presented method of spoofing detection to create a combined detection and mitigation solution. Estimated phase delays of spoofing signals may be used to calculate complex weight vector. This vector shapes the antenna array pattern in a way that a null is pointed towards source of spoofing signal, without rejecting true signals from satellites.

This article proves that spatial filtering may be used as a robust way of GPS spoofing mitigation. Proposed optimization of array weights provides high attenuation of undesired signals. Furthermore, large probability of at least four useful satellite visibility is sustained, unless their nominal signal-to-noise ratio is low in receiver's location. Spatial processing is also beneficial, as it may be

successfully used in combined spoofing detection and mitigation solution. It is also worth mentioning that proposed approach does not require any additional information about the antenna's attitude, since the reference frame is array-fixed.

During this research authors assumed that false signals arrive only from one direction at a time. Some additional investigations should be done to evaluate the performance of proposed methods in a multipath environment, where replicas of undesired signals may arrive from different directions.

References

[1] L. C. Chen, Y. C. Lai, Y. H. Yeh, J. W. Lin, C. N. Lai, H. C. Weng, "Enhanced Mechanisms for Navigation and Tracking Services in Smart Phones", Journal of Applied Research and Technology, vol. 11, no. 2, pp. 272-283, April 2013.

[2] R. Katulski, J. Magiera, J. Stefanski, A. Studanska, "Research Study on Reception of GNSS Signals in Presence of Intentional Interference", Proc. of the 34th Int. Conf. on Telecommunications and Signal Processing, 2011, pp. 452-456.

[3] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, G. Lachapelle, "GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques," International Journal of Navigation and Observation, vol. 2012, 16 pages, 2012.

[4] D. J. Jwo, F. C. Chung, K. L. Yu, "GPS/INS Integration Accuracy Enhancement Using the Interacting Multiple Model Nonlinear Filters", Journal of Applied Research and Technology, vol. 11, no. 4, pp. 496-509, August 2013.

[5] M. Psiaki, B. O'Hanlon, J. Bhatti, D. Shepard, T. Humphreys, "Civilian GPS Spoofing Detection based on Dual-Receiver Correlation of Military Signals", Proc. of ION GNSS, Portland, Oregon, 2011.

[6] B. Ledvina, W. Bencze, B. Galusha, I. Miller, "An In-Line Anti-Spoofing Device for Legacy Civil GPS Receivers," Proceedings of the 2010 Int. Technical Meeting of The Institute of Navigation, San Diego, CA, January 2010, pp. 698-712.

[7] B. Ledvina, P. Montgomery, T. Humphreys, "A Multi-Antenna Defense: Receiver Autonomous GPS Spoofing Detection", Inside GNSS, vol. March/April 2009, pp. 40-46, 2009.

[8] M. Meurer, A. Konovaltsev, M. Cuntz, C. Hättich, "Robust Joint Multi-Antenna Spoofing Detection and Attitude Estimation using Direction Assisted Multiple Hypotheses RAIM," Proc. of the 25th Int. Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS 2012), Nashville, TN, September 2012.

[9] G. Kappen, C. Haettich, M. Meurer, "Towards a robust multi-antenna mass market GNSS receiver," Proc. of Position Location and Navigation Symposium (PLANS), 2012 IEEE/ION , vol., no., pp.291-300, 23-26 April 2012.

[10] J. Bao-Yen Tsui, Fundamentals of Global Positioning Receivers: A Software Approach, Wiley & Sons, 2000, pp. 133-192.

[11] Z. Chen, G. Gokeda, Y. Yu, Introduction to Direction-of-Arrival Estimation, Artech House, 2010, pp. 33-37, 41-45.

[12] A. Brown, B. Mathews, "GPS Multipath Mitigation Using a Three Dimensional Phased Array", Proc. of the Int. Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS '05), Long Beach, CA, 2005, pp. 659-666.

[13] M. Sharawi, D. Akos, D. Aloi, "GPS C/N0 Estimation in the presence of Interference and Limited Quantization Levels", IEEE Trans. Aerospace and Electronic Systems, vol. 43, No. 1/2007, pp. 227-238.

[14] E. Faletti, M. Pini, L. Lo Presti, "Low Complexity Carrier-to-Noise Ratio Estimators for GNSS Digital Receivers", IEEE Trans. Aerospace and Electronic Systems, vol. 47, No. 1/2011, pp. 420-437.

[15] Vulnerability assessment of the transportation infrastructure relying on the Global Positioning System," JohnA.Volpe National Trasportation Systems Center, 2001.

[16] M. Li, A. G. Dempster, A.T. Balaei, C. Rizos and F. Wang, "Switchable beam steering/null steering algorithm for CW interference mitigation in GPS C/A code receivers.", Aerospace and Electronic Systems, IEEE Transactions on , vol.47, no.3, pp.1564-1579, July 2011.