A New Architecture for Malicious Interference Mitigation in GPS Signals

Adilson Chinatto[1,2], Cynthia Junqueira[1,3] e João M. T. Romano[1]
[1]University of Campinas, [2]Spectrum Line Ltd., [3]Institute of Aeronautics and Space

***Abstract* — A new architecture for malicious jammer mitigation in GPS signals is proposed. The technique employs a smart antenna array followed by a signal-to-noise ratio (SNR) discriminator. The architecture provides good results in jamming scenarios in which a malicious jammer runs at exact GPS frequency and carries a data stream spread by a valid Gold code. Here, direction of arrival (DOA) estimation is provided by a high resolution eigenstructure and a null steering beamforming beacons a null towards the malicious jammer source. A post-beamforming SNR discriminator, fed by the resultant array output signal, discards ones whose SNR after despread process overcomes a determined theoretical threshold, ensuring additional interference suppression. The results show the efficiency of the proposed methodology in terms of probability of tracking error in function of the DOA displacement between the malicious jammer and the GPS desired signal.**

Keywords- Electronic Warfare, GPS, smart antenna array

I. INTRODUÇÃO

Global Positioning System (GPS) has proven to be very useful in a variety of civil applications as aircraft navigation systems, surveyors, geophysical monitoring and automotive applications among others [1]. Nowadays, with the same purpose, the Global Navigation Satellite System (GNSS) is the system that will encompasses the American GPS [1], the European GALILEO [2] and the Russian GLONASS [3]. It involves the determination of platform position, velocity, and time worldwide.

The main drawback of these systems remains in its high sensibility to interference, multipath and jamming. Recently, several occurrences of malicious jamming in GPS systems of airports, military facilities and civilian navigation have been reported [4]. The interference can reduce the signal-to-noise ratio (SNR) of the navigation signal until it is unable to obtain measurements from the satellite, thus losing its ability to navigate. In order to provide a degree of protection against interference, the GNSS signal is applied to a direct sequence spread-spectrum (DS-SS) [1], but the spreading gain alone is insufficient to yield a fully efficient barrier against interferences.

In spread spectrum communications systems, interference suppression has been an active research topic for many years and different techniques have been developed [1], [2]. Allied to them, smart antennas are considered to be effective tools for GPS anti-jamming [5]. They allow the implementation of spatial nulling and beam steering based on adaptive beamforming and high-resolution direction finding methods.

In a GPS environment, malicious jamming that is carried at the exact GPS frequency and that uses a known spread code can destroy the GPS receiver's tracking ability. Antenna design enhancements as controlled reception pattern antennas (CRPA) [5] can be suitable to mitigate this kind of jamming due to their capability of steering gain nulls towards the jammer sources [6]. Usually, CRPA uses high resolution algorithms, such as MUSIC [7] or ESPIRIT [8], for DOA estimation, although adaptive algorithms are also employed. Literature has been presenting several CRPA architectures with encouraging results [9]. Nevertheless in some cases those architectures might not be sufficient to reduce the interference power to a level sufficiently low to prevent mistaken tracking. One such case is that in which an intentional interference runs at GPS frequency, is BPSK modulated and uses one of the defined spread codes. So, in those cases, some kind of post-beamforming process can be added to the GPS architecture, preventing the reminiscent interference to induce erroneous tracking.

In this paper, an interference suppression technique using a smart antenna is proposed. The technique combines the advantages of null steering beamforming with a post-beamforming SNR-based interference suppressor. This methodology allows GPS interference mitigation through a SNR discriminator connected at the beamformer output, lowering the interference power to levels subjacent to those related to the true GPS signals.

The work is organized as follows: the GPS signal structure and jamming fundamentals are described in Section II; Section III depicts the proposed spatial GPS architecture; in Section IV, results of simulations are presented, confronting conventional GPS receivers and the proposed one; in Section V, conclusions and futures perspectives are presented. Finally, DOA estimation through Matrix Pencil Method (MPM) and the smart antenna array geometry are presented in Appendix A.

II. GPS SIGNAL AND JAMMING

The GPS satellite navigation system transmits two types of signals on two carrier frequencies, L1 (1.575GHz) and L2 (1.227GHz) [1]. The carrier frequency is modulated with a binary phased shift keying (BPSK) scheme. The L1 GPS band comprises a restricted-use precision (P) signal and civilian signal known as the coarse/acquisition (C/A), which is under the focus of this study. Each GPS navigation message is spectrally spread by one of the 32 pseudo random noise (PRN) codes defined in the GPS-ICD-200 [10]. These

Adilson Chinatto, chinatto@espectro-eng.com.br, Tel +55-19-21164433; Cynthia Junqueira, cynthiaccmj@ iae.cta.br, Tel +55-12-39474937, Fax +55-12-39475019; João M. T. Romano, romano@dmo.fee.unicamp.br, Tel. +55-19-35213857.

PRN codes are binary sequences with length of 1023 chips and a transmission rate of 1.023 Mchips/s and are modulo-2 added to the 50 bps navigation message [1].

Due to long path between the satellites and the GPS receiver, the received signal presents a power around –160dBW [1]. The ambient thermal noise spectral density is around –205.2dBW/Hz [1] leading to a GPS C/A code carrier to noise density (C/N_0) of 45.2dB·Hz. So, over the C/A code bandwidth of 1.023MHz, the C/A code power results in a value 14.9dB below the noise power.

The GPS PRN codes are a set of code division multiple access (CDMA) DS-SS that allows suppressing interference. At the GPS receiver, the received signal is modulo-2 added to the same set of PRN codes used in the signal generation [3]. When the right PRN code is applied and is in phase with the PRN code used to create the transmitted spread-spectrum signal, it causes the desired GPS signal to be correlated and the noise and eventual interference to be spectrally spread, resulting in a gain of 30dB in the SNR [1]. In this way, after the dispreading process, the SNR results at most 15.1dB over the noise floor.

Because GPS receivers rely on external radio frequency (RF) signals transmitted from GPS satellites, they are also vulnerable to RF interference, which may cause accuracy degradation or loss of tracking. The RF interference may be friendly or intentional (jammer). Interference can be classified in terms of bandwidth (BW) [11]. The continuous wave (CW) interference occupies less than 1 kHz of bandwidth and in the practical sense can be approximated by one single frequency. The narrowband (NB) interference normally is defined as a signal with 1MHz < BW < 2 MHz. The wideband (WB) interference has a bandwidth typically more than two times greater than the C/A code.

Most of the unintentional interference is efficiently mitigated by a selective (surface acoustic wave) SAW filter at the GPS front-end and by the correlation process. However, the jammer´s objective is to corrupt the navigation service by masking the GPS signal. One of the most efficient intentional jamming technique is the creation of a signal at the same bit rate of GPS navigation data and spectrally spread through one of the PRN codes used in the C/A code. This kind of jammer can lead the receiver to interpret it as a true GPS signal. This situation induces the receiver to produce wrongly estimates. That kind of jamming will be denominated in this paper as malicious and will be considered in the analysis.

III. Proposed Spatial Architecture for Malicious Interference Mitigation in GPS Receiver

One of the most employed techniques for jammer mitigation is the beamforming through adaptive array antennas [12]. Dealing with GPS signals, several works evaluates the CRPA in this task, for instance [5], showing promising results. Generally, the CRPA are designated to mitigate the interference whose power level is higher than the noise floor. Such interference can saturate the GPS receiver front-end, disabling its characteristics of time, position and velocity determination. Usually, beamforming is done through the interference DOA estimation and using this information to handling the array factor to produce a null towards that direction [13]. Several techniques can be used in the DOA estimation. The most common are the subspace methods algorithms like MUSIC [7] and ESPRIT [8], although many others techniques can be employed. Even in the presence of inaccuracies in the DOA estimation due to noise, unbalancing of the antenna array hardware and analog-to-digital conversion, literature shows that CRPA attenuation over interference can exceeds 30dB [5]. This attenuation is generally enough to reduce the interference power to levels below the noise floor.

Most of the low power interference signals is totally obliterated by the extremely selective band-pass SAW filter and correlation process at the GPS receiver. The combination of beamforming techniques implemented in CRPA and the signal processing at the GPS receiver are sufficient to efficiently mitigate most of types of jammers as CW and WB. On the other hand, malicious jamming schemes can induce false tracking at the GPS receiver [10]. This kind of jammer can be not mitigated by the CRPA if its power level lies below the noise floor, or the CRPA capability mitigation can be not enough to reduce its power to a level lower than the desired GPS signal.

Using CRPA, a set of situations in which a malicious jammer can destructively affect the positioning system can be established. Be σ_S^2 the desired GPS signal power, σ_J^2 the jammer power and σ_N^2 the noise floor considering a band pass filter of 2MHz. Three hypotheses can be considered:

a) $\sigma_J^2 > \sigma_N^2$. In this case, CRPA beamforming reduces the malicious jammer power to $\sigma_{Jb}^2 < \sigma_J^2$, leading to two different situations:

a.1) $\sigma_{Jb}^2 < \sigma_S^2$, in which the GPS receiver correctly tracks, ignoring the malicious jammer;

a.2) $\sigma_{Jb}^2 > \sigma_S^2$, in which the GPS receiver wrongly tracks, identifying the malicious jammer as a desired satellite signal.

b) $\sigma_N^2 > \sigma_J^2 > \sigma_S^2$. In this case, CRPA provides a flat beamforming as the malicious jammer power lies below the noise floor. This leads the GPS receiver to wrongly tracks because jammer power is higher than desired satellite signal.

c) $\sigma_N^2 > \sigma_S^2 > \sigma_J^2$. In this case, CRPA provides a flat beamforming as the malicious jammer power lies below the noise floor. In addition, the malicious jammer power is lower than the desired satellite signal one. So, GPS receiver correctly tracks the desired satellite signal.

Thus, CRPA beamforming for interference mitigation is successful in hypotheses (a.1) and (c). Conversely, in hypotheses (a.2) and (b), CRPA is inefficient against malicious jammers.

The spatial GPS receiver architecture for malicious interference mitigation proposed in this paper combines the null steering capability of a CRPA allied to a hard decision circuit at the antenna array output, leading to malicious jammer detection and elimination. The block diagram of proposed architecture is depicted in Fig. 1. Firstly, signals provided by the set of receive antennas are processed by a DOA estimation algorithm. Signal sources whose power lies in hypothesis (a) are mitigated by the CRPA through a deterministic null steering beamforming (NSB) algorithm.

The resultant signal feeds a set of parallel correlator (CORR) blocks, each one running under a pre-defined satellite PRN code.

The correlators blocks perform spectral despreading of the received signals, producing 30dB elevation in the SNR of the signals spread by the same PRN. The despread signals are sent to a set of SNR estimators (SNR ESTIM) whose objective is to determine the power level of the despread signal related to the noise floor. As the maximum SNR of a despread signal lies around +15.1dB, it is possible to establish a threshold above which a signal may be classified as a malicious jammer. The SNR estimations are performed simultaneously by each SNR ESTIM block through Algorithm I, showed in Table I. Case the post-despreading SNR overlays the threshold, the SNR ESTIM block feedbacks the respective CORR block. At this point, the CORR block restarts the search for the next correlation maximum, resulting in a new acquisition. This process is repeated until the SNR estimated by the SNR ESTIM block presents value below the threshold. Once this condition is reached, the despread signal is forwarded to the navigation processing block.

TABLE I ALGORITHM I

Step	SNR Estimation
i. Estimate the total power:	$P_t = \frac{1}{1023}\sum_{i=1}^{1023} a_i^* a_i$
ii. Estimate the signal mean:	$\mu_a = \frac{1}{1023}\sum_{i=1}^{1023} a_i$
iii. Estimate the signal power:	$P_s = \mu_a \mu_a^*$
iv. Estimate the noise power:	$P_n = P_t - P_s$
v. Estimate the SNR	$SNR = 10\log\frac{P_s}{P_n}$

Considering:
$a_n, 1 \le n \le 1023$: the received signal after despreading;
$(^*)$: complex conjugate.

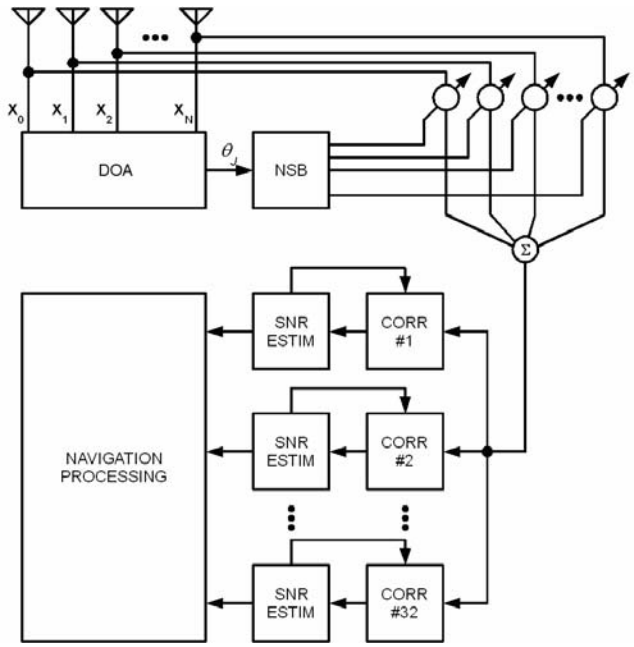

Fig. 1. Proposed GPS receiver architecture.

IV. SIMULATION AND RESULTS

To investigate the tracking capability of the proposed GPS receiver architecture, a set of simulations was performed dealing with a GPS receiver impinged by a malicious jammer. In this paper it was considered an uniform linear antenna (ULA) array, as defined in Appendix A. Targeting a future hardware implementation, the subspace method known as Matrix Pencil Method (MPM) was considered as the DOA estimation algorithm. The MPM for ULA is also defined in Appendix A and was chosen due to its ability to perform estimation by handling only a single array output snapshot. This characteristic leads to a simplification in the hardware.

Three case studies were considered:

1) a GPS L1 receiver without any auxiliary malicious jammer mitigation technique was employed;

2) a GPS L1 receiver with SNR ESTIM block was used;

3) a GPS L1 receiver preceded by a NSB and with SNR ESTIM block, was utilized.

The same scenario was considered for the three cases, in which the device was impinged by GPS signals and malicious jammer. Two GPS signals were considered in the simulations. They were taken from the constellation of the seven visible satellites in Campinas, Brazil (–47°05'W; –22°54'S; 709m) on February, 4th 2012, 14h00 BRT. For the sake of clarity, these satellites were called satellite #1 and #2, being BPSK modulated at L1 frequency and DS-SS with PRN codes 27 and 15, respectively. The SNR of both GPS signals was also randomly generated, assuming values between –17.9dB and –14.9dB.

The malicious jammer was considered to have a fixed jamming to noise ratio (JNR) of +30dB and was generated as a signal with BPSK modulation at L1 frequency. Moreover, the malicious jammer was DS-SS with the PRN code 27, which corresponds to the PRN code used by one of the GPS satellite signal, asynchronously related to the true GPS signal.

In the simulations in which the MPM was used, it was considered an ULA with $N + 1$ element, formed by hemispherical receiver antennas, where N ranges from 3 to 8. Conversely, in the case studies *#1* and *#2*, $N = 0$. As in practical applications the receiver GPS antennas present a 3dB beam width of 120° [1], the angle displacement between the GPS signals DOA and interferer DOA was chosen from 0° and 120°

In the three cases, the efficiency of the GPS receiver was analyzed in terms of probability of C/A tracking error as a function of the angular displacement ($\Delta\phi$) between the GPS signal DOA and the jammer DOA, whose resolution was defined as 1°. Finally, for each $\Delta\phi$ a set of 1000 iterations was performed and averaged.

The first set of results, depicted in Fig. 2, is related to the case studies #1 and #2 and shows the performances of the GPS receivers in terms of tracking error probability. In case study #1 the tracking is accomplished without any auxiliary method. It is observed a complete tracking fail (100% of tracking error probability) due to the presence of the malicious jammer. In case study #2 the tracking process is

aided by the SNR ESTIM block as the key parameter for mitigate the malicious jammer. The results are around 85% of fail, not regarding the displacement between GPS signal DOA and malicious jammer DOA.

The results of case study #3 are displayed in Fig. 3 and 4. Here, the array is composed by a number of antennas varying from 4 to 9. In Fig. 3 the GPS signal and malicious jammer have the same PRN code, which is the most critical jamming situation. It is observable that for DOA displacement bigger than 20° the tracking error probability is around 18% and this result is independent of the number of antennas. The inset shows the dependence of the tracking error probability with the number of antennas for a displacement DOA up to 20°.

In the Fig. 4, the case study #3 is depicted when the GPS signal and malicious jammer have different PRN codes. This situation shows fewer difficulties to tracking the satellite signal, even considering the jamming. Independent of the number of antennas, for displacement angles bigger than 10°, the probability of error is zero, except for 4 elements in the array, when the error probability is around 14% for a displacement of 26°.

The comparison of the tracking error probability among the three case studies show a relevant gain in the performance of the GPS signal tracking when the proposed architecture for malicious jammer interference mitigation is employed.

V. CONCLUSIONS

In this paper, a new architecture for malicious interference mitigation in GPS signals that allies beamforming and SNR discrimination is proposed. The architecture uses the Matrix Pencil Method to estimate the DOA of a malicious jammer impinging an antenna array. The DOA information is used by a deterministic beamformer that beacons a null towards the interference origin. In addition, the resultant signal at the antenna array output feeds a SNR discriminator that selects the signal whose SNR is immediate lower than a determined threshold. This procedure provides additional interference suppression, improving the robustness of GPS receiver to a superior level when compared with traditional CRPAs.

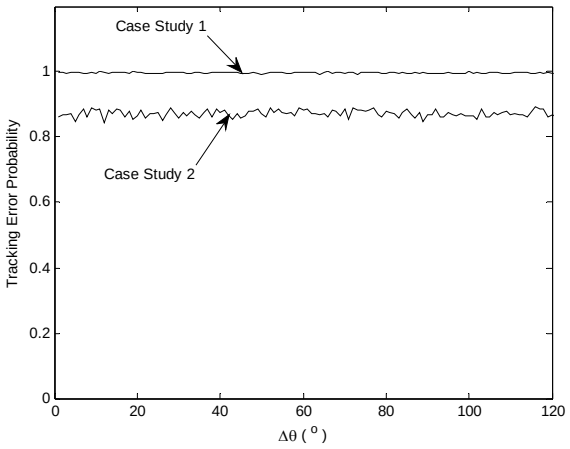

Fig. 2. Tracking error probability –case studies #1 and #2.

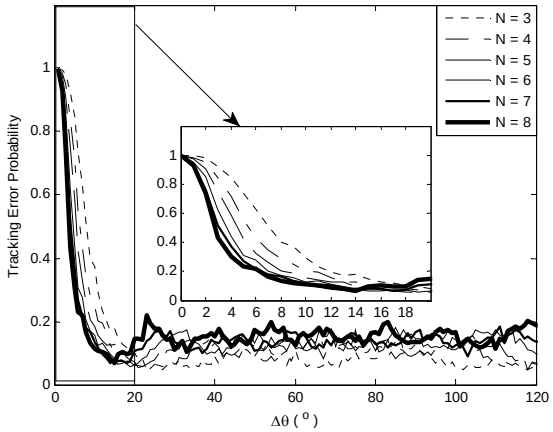

Fig. 3. Tracking error probability – case study #3 (GPS signal and malicious jammer signal with same PRN code).

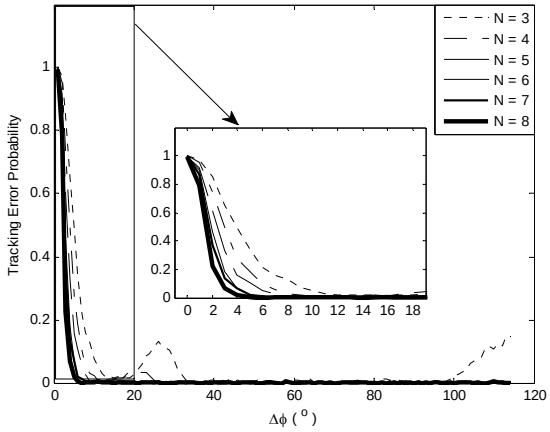

Fig. 4. Tracking error probability – case study #3 (GPS signal and malicious jammer signal with different PRN code).

Although any DOA estimation algorithm could be used in the proposed architecture, in this work DOA estimation was performed by Matrix Pencil Method. This method was chosen due to its low computational complexity when compared with the others subspace methods and the next step in the work plan is the implementation of the architecture in a real-time programmable logic device as FPGA, using smart antenna array hardware.

APPENDIX A

THE MATRIX PENCIL METHOD FOR DOA ESTIMATION AND ANTENNA ARRAY

The Matrix Pencil Method (MPM) is described in the literature which is more robust to noise in the sampled data when compared for instance, with a polynomial-type method and also computationally more efficient. This matrix technique is also a tool to estimate the coefficients of a sum of complex exponentials [14], [15].

The MPM can be employed in the problem of DOA estimation in antenna array, [12], [16]. To better clarify this statement, the definition of an uniform linear array (ULA) of ominidirectional isotropic antennas and the Matrix Pencil method it will be described below.

Considering a set of plane waves defined as $s_p = A_p e^{(j\gamma_p)}$, $0 \le p \le P$, where A_p is the amplitude and γ_p

is the phase of each of $P+1$ incident plane waves arriving at a d spaced $N+1$element uniform linear antenna array (ULA), the signal at the output of the n-th antenna can be expressed by

$$x_n = \sum_{p=0}^{P} s_p e^{\left(j\frac{2\pi d}{\lambda} n \sin\phi_p\right)}, \quad 0 \le n \le N \tag{1}$$

where ϕ_p is the DOA of each of $P+1$ incident plane waves. Giving a known jamming DOA ϕ_J it is possible to combine the $N+1$ antenna outputs in order to determining the null steering in the ϕ_J direction by evaluating

$$y = x_0 - \frac{1}{N}\sum_{n=1}^{N} x_i e^{-jn\theta_J} \tag{2}$$

where $\theta_J = \frac{2\pi d}{\lambda}\sin\phi_J$.

For ULA, using (1), s_p and defining the general element $a_p = \exp(j2\pi d(\sin\phi_p)/\lambda)$ one can define each antenna output as $\mathbf{x} = \mathbf{A}\mathbf{s}$, where $\mathbf{x} = [x_0\ x_1 \cdots x_N]^T$, $\mathbf{s} = [s_0\ s_1 \cdots s_P]^T$ and

$$\mathbf{A} = \begin{bmatrix} a_0^0 & a_1^0 & \cdots & a_P^0 \\ a_0^1 & a_1^1 & \cdots & a_P^1 \\ \vdots & \vdots & \ddots & \vdots \\ a_0^N & a_1^N & \cdots & a_P^N \end{bmatrix}, \tag{4}$$

and construct a $L\times(N-L+2)$ Henkel matrix of a snapshot of $\mathbf{x}$

$$\mathbf{X} = \begin{bmatrix} x_0 & x_1 & \cdots & x_{N-L+1} \\ x_1 & x_2 & \cdots & x_{N-L+2} \\ \vdots & \vdots & \ddots & \vdots \\ x_{L-1} & x_L & \cdots & x_N \end{bmatrix} \tag{5}$$

where L, called the *pencil parameter*, must satisfy $P+2 \le L \le N-P+1$. Performing the singular value decomposition (SVD), $\mathbf{X}$ can be expressed as

$$\mathbf{X} = \mathbf{U}\mathbf{\Sigma}\mathbf{V}^H \tag{6}$$

where $\mathbf{U}$ is the $L\times L$ unitary matrix whose columns are the eigenvectors of $\mathbf{X}\mathbf{X}^H$, $\mathbf{\Sigma}$ is the $L\times(N-L+2)$ diagonal matrix formed by the singular values of $\mathbf{X}$ in descending order and $\mathbf{V}$ is the $(N-L+2)\times(N-L+2)$ unitary matrix whose columns are the eigenvectors of $\mathbf{X}^H\mathbf{X}$. At this point, define two matrices $\mathbf{U}_1$ and $\mathbf{U}_2$ such that $\mathbf{U}_1$ corresponds to the matrix $\mathbf{U}$ with the last row deleted and $\mathbf{U}_2$ corresponds to the matrix $\mathbf{U}$ with the first row deleted, and form

$$\mathbf{U}_2 - \lambda\mathbf{U}_1 = 0 \tag{7}$$

Performing some algebraic manipulations, it can be shown that

$$\mathbf{U}_1^+\mathbf{U}_2\mathbf{X} = \lambda\mathbf{X} \tag{8}$$

where $\mathbf{U}_1^+$ is the Moore-Penrose pseudo-inverse of $\mathbf{U}_1$. It can be shown that the eigenvalues of $\mathbf{U}_1^+\mathbf{U}_2$ provide values for the exponents a_p and the DOA ϕ_p are obtained from

$$\phi_p = \arcsin\left[\frac{\ln(a_p)}{j2\pi\frac{d}{\lambda}}\right] \tag{9}$$

REFERENCES

[1] B. W. Parkinson and J. J. Spilker, Eds, *Global Positioning System: Theory and Applications*, vol 1, AIA,Wahington, DC: 1996.

[2] European Space Agency. *Galileo: The European Programme for Global Navigation Services*, v. 186, ESA BR, ESA publications Division, 2002.

[3] B. H. Wellenhof, H. Lichtenegger and E. Wasle, *GNSS: global navigation satellite systems*. Springer Wien New York, 2008.

[4] S. Pullen and G. X. Gao, "GNSS Jamming in the Name of Privacy: Potential Threat to GPS Aviation", Inside GNSS, vol. 7, no. 2, Mar./Apr. 2012.

[5] H. W. Tseng, R. Kurtz, A. Brown, D. Nathans, F. Pahr, "Test Results of a Dual Frequency (L1/L2) Small Controlled Reception Pattern Antenna." In *ION National Technical Meeting 2002*, San Diego, CA, Jan. 2002.

[6] L. Scott, "RFI and Jamming Concerns for GNSS and GPS IIIa." In *ION GPS 200* ,Tutorial 700C, Salt Lake City, USA, September 19-22, 2000.

[7] R. O. Schmidt "Multiple emitter location and signal parameter estimation." *IEEE Trans. on Antennas and Propagation*, New York, AP-34, n3, pp. 276-280 1996

[8] R. Roy, T. Kailath, "Espirit-estimation of signal parameters via rotational invariance techniques." *IEEE Trans. on accustics, Speech, and Signal Processing*, v. 37, pp. 984-995, Jul. 1986.

[9] R. Silva, R. Worrell, A. Brown, "Reprogramable, Digital Beam Steering GPS receiver Technology for Enhanced Space Vehicle Operations." In *Proc. of 2002 Core Technologies for space Systems Conference*, Colorado Springs, USA, Nov. 2002.

[10] ICD-GPS-200, "NAVSTAR GPS Space Segment/Navigation User Interfaces", Oct. 1997.

[11] H. Hu, N. Wei, "A study of GPS jamming and anti-jamming," in *Proc. PEITS 2009*, Shenzhen, China, Dec. 19-20. 2009, pp. 388-391.

[12] T. K. Sarkar, M. C. Wicks, M. Salazar-Palma, R. J. Bonneau, *Smart Antennas*. John Willey and Sons, 2003.

[13] R. Mozingo and T. Miller, *Introduction to Adaptive Arrays*. Fullerton: John Willey, 1980.

[14] T. K. Sarkar and O. Pereira, " Using the Matrix Pencil Method to Estimate the Parameters of a Sum of Complex Exponentials," *IEEE Antennas and Propagation Magazine*, v. 37, n. 1, Feb. 1995.

[15] Y. Hua and T. K. Sarkar, " Matrix Pencil Method for Estimating Parameters of Exponentially Damped/Undamped Sinnusoids in Noise." *IEEE Trans. on Accustics, Speech, and Signal Processing*, v. 35, n.5, May 1990.

[16] Y. Hua "Estimating Two-Dimensional Frequencies by Matrix Enhancement and Matrix Pencil," *IEEE Trans. on signal Processing*, v. 40, n. 9, 1992.