High-resolution correlator based detection of GPS spoofing attacks using the LASSO

Erick Schmidt
Department of Electrical and Computer Engineering
The University of Texas at San Antonio
San Antonio, TX, USA
erickschmidtt@gmail.com

Nikolaos Gatsis
Department of Electrical and Computer Engineering
The University of Texas at San Antonio
San Antonio, TX, USA
nikolaos.gatsis@utsa.edu

David Akopian
Department of Electrical and Computer Engineering
The University of Texas at San Antonio
San Antonio, TX, USA
david.akopian@utsa.edu

***Abstract*—This work proposes a novel sparsity-based decomposition method for the correlator output signals in GPS receivers capable of detecting spoofing attacks. We model complex correlator outputs of the received signal to form a dictionary of triangle-shaped replicas and employ a sparsity technique that selects potential matching triangle replicas from said dictionary. We formulate an optimization problem at the receiver correlator domain by using the Least Absolute Shrinkage and Selection Operator (LASSO) to find sparse code-phase peaks where such triangle-shaped delays are located. The optimal solution of this optimization technique discriminates two different code-phase values as authentic and spoofed peaks in a sparse vector output. We use a threshold to mitigate false alarms. Additionally, we present an expansion of the model by enhancing the dictionary to a collection of shifted triangles with higher resolution. Our experiments are able to discriminate authentic and spoofer peaks from synthetic GPS-like simulations. We also test our method on a real dataset, namely the Texas Spoofing Test Battery (TEXBAT). Our method achieves less than 1% detection error rate (DER) in nominal signal-to-noise ratio (SNR) conditions.**

***Keywords*—GNSS, GPS, correlators, anti-spoofing, LASSO, high-resolution, dictionary.**

I. Introduction

The U.S. global position system (GPS) is one of the existing global navigation satellite systems (GNSS) that provides position and time information for users in civil, commercial, and military sectors [1]. Because a multitude of applications nowadays rely on GNSS, it is crucial for GNSS receivers to have robustness to intentional or unintentional interference [2].

The GPS coarse acquisition (C/A) codes broadcast unique pseudorandom (PRN) sequences from each satellite which are used for ranging applications and precise timing functions. Such codes are available openly and thus are prone to intentional spoofing and jamming attacks. While jamming attempts to block signal reception by the receiver, spoofing attacks generate GPS-like signals with similar characteristics as the target receiver intending to trick the receiver into faulty position, velocity, and time (PVT) estimations [2].

The development of GPS anti-spoofing techniques is an active topic of research today. In fact, the flexibility introduced by software-defined radio (SDR) solutions make it an ideal option for fast prototyping and testing of new receiver architectures and algorithms [3]. However, SDR can also be used for spoofing techniques development. The work in [4] develops an SDR spoofer-receiver platform that can perpetrate a real-time attack onto a receiver. Spoofing scenarios are available in the Texas Spoofing Test Battery (TEXBAT) [5]. In terms of the attack, the work in [6] categorizes the type of spoofing attack into simplistic, intermediate, and advanced, based on the complexity of the spoofing device.

Various GNSS signal authentication techniques have been developed to detect and mitigate spoofing attacks. There are cryptographic signal authentication methods that are yet to be implemented in civilian GNSS signals [7], cross-correlation methods with other GNSS signals [8], [9] and signal processing based techniques which rely on tracking loops, correlator [3], [10], and/or discriminator level processing [11], [12]. These techniques can be potentially implemented in a commercial receiver via a firmware update or in an SDR receiver via a software upgrade, depending on its complexity. Most countermeasures for intermediate spoofing attacks are based on single antenna [11], [13], [14], and multi-antenna solutions [15], [16], [17]. While multi-antenna solutions discern angle-of-arrival (AOA) between authentic and counterfeit signals, their deployment is cumbersome and adds complexity to the receiver. A related research area develops multipath (MP) mitigation solutions, which can assimilate a spoofing attack [10], [18]. For more elaborated GNSS authentication approaches and countermeasures, the reader is directed to [3], [6], [19].

In this work, we propose an anti-spoofing technique falling under the single-antenna advanced signal processing category. We model and formulate an optimization problem at the GPS correlator domain. Specifically, receiver correlator tap values are modeled as a dictionary of triangle-shaped replicas, or peaks. We then use a sparse signal processing technique that selects potential matching replicas from the dictionary of replicas. In particular, the sparsity is promoted by using the Least Absolute Shrinkage and Selection Operator (LASSO) [20]. The optimal solution of this technique discriminates the presence of a potential spoofing attack by observing two different code-phase peaks (authentic and spoofed) in a sparse vector output. We use a threshold to mitigate false alarms.

978-1-7281-0244-3/20/$31.00 ©2020 IEEE

Also, we present two more variations of the optimization problem by enhancing the dictionary to a *higher-resolution* of shifted triangles without the need to increase number of correlators in the receiver. Finally, we present Monte Carlo (MC) simulations to validate peak detection error rate (DER), which counts the event when a spoofer peak is present along with an authentic peak, but not detected by our method.

Related work on peak detection in correlator outputs has been previously reported in the literature. Authors in [10] analyze correlator outputs using the Fast Fourier Transform (FFT) to detect peaks based on their chip delay. This method requires long non-coherent integration lengths of 40 ms due to noise sensitivity. Similarly, authors in [18] model complex MP scenarios based on certain assumptions to find the delay profile of correlator peaks. This technique uses the maximum likelihood estimator to build such models at the cost of complexity. Also, only MP is studied in both [10] and [18], thus omitting spoofing attacks. There are three main differences between spoofing and MP that are considered in the present work and pertain to a smart spoofer: (1) the spoofed channels show a substantial delay incurred by the attack; (2) the spoofing attack occurs on many, if not all, visible channels concurrently; and (3) such attacks can sustain significantly more damage to the position, velocity, and time (PVT) solution to deviate more substantially when compared to MP. The method in the present paper considers these differences between MP and spoofing while providing higher sensitivity with shorter integration lengths and reasonable complexity.

The paper is organized as follows. Section II presents the authentic signal and spoofer model, Section III presents the problem formulation, and Section IV presents simulations and results for synthetic data and a real dataset. Section V finalizes with concluding remarks and future work.

II. Authentic Signal and Spoofer Model

To be able to estimate a PVT solution, the GPS receiver requires continuous synchronization with satellite signals. This allows to obtain two main elements required for PVT estimation: ranging measurements, and navigation message. Typically, user-to-satellite synchronization initially occurs in an *acquisition* stage, to find satellite signals with their respective residual Doppler components and PRN code offset, and a *tracking* stage, seen as a fine synchronization to lock to the carrier and code phases [21]. For this work, we assume the receiver operates in the tracking stage.

The tracking stage uses closed loops to continuously align the received signal to locally generated replicas with their respective code-phase and carrier-phase values. To estimate the code and carrier phases, a delay locked loop (DLL) for code-phase estimation, and a phase locked loop (PLL) and frequency locked loop (FLL) for carrier-phase estimation, are implemented [21]. Further, a discriminator processes these measurement outputs to provide filtered quantities which adjust current channel tracking parameters for the next iteration (epoch). A set of correlators in the DLL compare shifted code replicas with the incoming signal to adjust the code-phase with sub-chip accuracy [1], [21]. Conventional tracking loops have two main steps: (1) correlation and integration, the so-called *integrate-and-dump* filter [1], and (2) tracking loop discriminators and feedback filters. In this work, we model the received signal after carrier wipe-off and once it enters the integrate-and-dump step. Fig. 1 presents a set of correlators with different delays for the in-phase and quadrature arms.

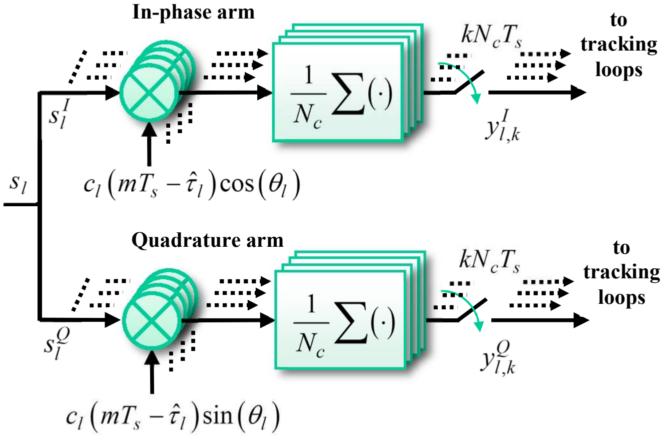
In-phase arm
kN_cT_s
to tracking loops
s_l^I
$\frac{1}{N_c}\sum(\cdot)$
$y_{l,k}^I$
s_l
$c_l(mT_s-\hat{\tau}_l)\cos(\theta_l)$
Quadrature arm
kN_cT_s
to tracking loops
s_l^Q
$\frac{1}{N_c}\sum(\cdot)$
$y_{l,k}^Q$
$c_l(mT_s-\hat{\tau}_l)\sin(\theta_l)$

Fig. 1. A set of correlator for in-phase and quadrature arms for a GPS channel.

A received GPS signal is modeled as an addition of all visible satellite signals (or channels). A single GPS channel l can be modeled as follows:

$$s_l(mT_s)=\sqrt{\rho_l}\,b_l(mT_s-\tau_l)\,c_l(mT_s-\tau_l)\,e^{j\theta_l}+\eta(mT_s) \tag{1}$$

where m is the sample index, T_s is the sampling period, ρ_l is the received power, b_l is the modulated bit, c_l is the C/A code, τ_l and θ_l are the code and carrier phase parameters, respectively, and $\eta(mT_s)$ is the noise. The output of the integrate-and-dump filter for the k-th coherent integration is modeled as (see Fig. 1):

$$x_{l,k}=x_l(kN_cT_s)=\frac{1}{N_c}\sum_{m=kN_c}^{(k+1)N_c-1}s_l(mT_s)\,\ell_l(mT_s,\tau_l)^* \tag{2}$$

where $N_c=f_sT$ is the number of samples of the coherent integration period T, $(\cdot)^*$ is the complex conjugate operator, ℓ_l is the local replica, and the integration time is kN_cT_s, $k\in\{0,1,\ldots\}$.

If we consider multiple discrete correlator replicas (or taps) in each channel and for each in-phase and quadrature arms (see Fig. 1), we can define a model based on the autocorrelation function (ACF). If we omit the modulated bit, the model for the l-th channel, the k-th coherent integration, the i-th correlator tap, and the discrete lag τ_i can be written as:

$$y_{l,k}(\tau_i)=\sqrt{\rho_{l,k}}\,R(\Delta\tau_i)\,e^{j\Delta\theta_{l,k}}+\eta_{l,k} \tag{3}$$

where $R(\cdot)$ is the autocorrelation function depicted as a triangle or peak [1], $\Delta\tau_i=\tau_{l,k}-\tau_i$, $\Delta\theta_{l,k}=\theta_{l,k}-\hat{\theta}_{l,k}$, and $\eta_{l,k}$ is the coherent accumulation of residual cross-correlation terms and AWGN. We define the discrete lag as $\tau_i = \hat{\tau}_{l,k} - \delta_i$, where $\hat{\tau}$ is the estimated *code-phase* value, and $\delta_i = (i-1)d - \delta_{E-L}/2$, $i \in \{1,\ldots,n\}$, is a code delay where d is the correlator spacing in chips, δ_{E-L} is the spacing between the earliest and latest correlators, $\delta_{E-L} \geq d$, and $n = \delta_{E-L}/d + 1$ is a fixed number of correlators on each arm for a total of $2n$ correlators. For example, a typical early prompt late (EPL) tracking loop system uses $\delta_{E-L} = 1.0$, $d = 0.5$, and $n = 3$; a narrow correlator uses $\delta_{E-L} = 0.1$, $d = 0.05$, and $n = 3$ [22].

A. *Spoofer model*

A smart spoofing attack consists of synthesizing a GPS-like signal to replicate the target receiver's *carrier-phase* and *code-phase* to very accurate proximity as to avoid detection. Once the spoofer signal is mixed with the authentic signal, the spoofer gradually increases its power so that the receiver locks to the fake correlation peak. Finally, the spoofer drags-off the fake correlation peak to generate an erroneous PVT estimation, while maintaining lock. This event is considered an intermediate spoofing attack and has been successfully implemented in an SDR platform [4]. Additionally, the authentic and spoofer are presumed to have same residual Doppler frequency during the attack. This is called a *frequency locked* attack [5]. We show a snapshot of the intermediate attack as outputs of the correlator taps in Fig. 2. It shows two superimposed triangle shapes (correlation peaks), namely the authentic y_A, and the spoofer y_S. The more correlator taps are used, the higher resolution is seen in the triangle-shaped outputs.

III. Problem Formulation

We begin the problem formulation by modeling a bank of correlators on the in-phase arm initially, but this can be expanded to quadrature. The bank of correlators with n discrete *code-phases* is represented in matrix form as follows (the channel index and coherent integration instance are omitted from the notation for brevity):

$$\mathbf{C} = [\mathbf{c}_1,\ldots,\mathbf{c}_i,\ldots,\mathbf{c}_n]^T \quad (4)$$

where $\mathbf{C} \in \mathbb{R}^{n \times N_c}$, $\mathbf{c}_i = [c(mT_s - \tau_i)], m \in \{1,\ldots,N_c\}$ is a single-period shifted local code replica in column-vector form, and $\tau_i = \hat{\tau} - \delta_i$. Also, we define a *high-resolution* matrix of normalized and noiseless "received" signals with p discrete *code-phases*:

$$\mathbf{S} = [\mathbf{s}_1,\ldots,\mathbf{s}_j,\ldots,\mathbf{s}_p] \quad (5)$$

where $\mathbf{S} \in \mathbb{R}^{N_c \times p}$, and $\mathbf{s}_j = [c(mT_s - \tau_j)], m \in \{1,\ldots,N_c\}$ is also a single-period replica, in column-vector format, and $\tau_j = \hat{\tau} - \gamma_j$. The term *high-resolution* occurs because of more options of potentially occurring *code-phases* in the $\mathbf{S}$ matrix. The delay $\gamma_j = (j - 1 - \lfloor F_p/2 \rfloor) d/F_p - \delta_{E-L}/2, j \in \{1,\ldots,p\}$,

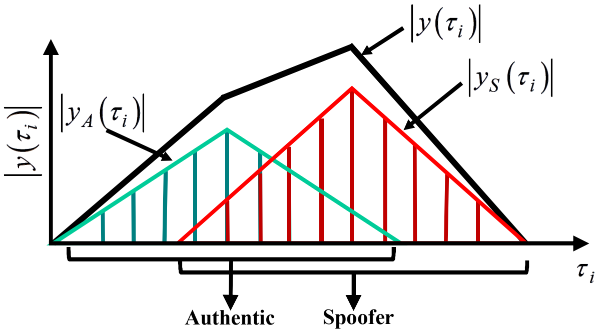

Fig. 2. A superposition of authentic (green) and spoofed (red) correlation triangles.

along with a finer correlator spacing $d_p = d/F_p$ define the higher-resolution, where F_p is named the *p-factor* and defines the *high-resolution* integer factor between n correlator taps and p shifted code signals, i.e., $p = nF_p$. As an example, if $\delta_{E-L} = 1.0$, $d = 0.1$, and $F_p = 1$, the correlator resolution grid becomes $\delta = [-0.5, -0.4, \ldots, 0.0, 0.1, \ldots, 0.5]^T$. If we now use $F_p = 5$, this artificially increases the resolution grid from $d = 0.1$ to $d_p = 0.02$. Now, additional peak *code-phases* of $[-0.04, -0.02, 0.0, 0.02, 0.04]$ are available at the correlator tap phase of 0.0, thus increasing the resolution.

We define a *dictionary* of triangle replicas by passing p high-resolution signals with a fixed bank of n correlators as follows:

$$\mathbf{M} = \mathbf{CS} = [\mathbf{m}_1,\ldots,\mathbf{m}_j,\ldots,\mathbf{m}_p] \quad (6)$$

where $\mathbf{M} \in \mathbb{R}^{n \times p}$ is the dictionary of replicas and $\mathbf{m}_j = \mathbf{C}\mathbf{s}_j$ is a triangle-shaped correlation peak of a "received signal" with delay τ_j. The dictionary of replicas can be seen as shifted versions of triangle-shaped correlation peaks. Accordingly, we formulate an optimization problem as follows:

$$\underbrace{\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}}_{\mathbf{y}} = \underbrace{\begin{pmatrix} m_{1,1} & \cdots & m_{1,p} \\ \vdots & \cdots & \vdots \\ m_{n,1} & \cdots & m_{n,p} \end{pmatrix}}_{\mathbf{M}} \underbrace{\begin{pmatrix} \beta_1 \\ \vdots \\ \beta_p \end{pmatrix}}_{\boldsymbol{\beta}} + \eta \quad (7)$$

where $\mathbf{y} \in \mathbb{R}^{n \times 1}$ is the received triangle-shaped ACF model, $y_i = y(\tau_i) = \sqrt{\rho} R(\Delta\tau_i)\cos\Delta\theta + \eta, i \in \{1,\ldots,n\}$ is the i-th correlation tap output; $m_{i,j} \in \mathbb{R}^{n \times p}$ is the i-th correlation tap for the j-th signal shift from the dictionary, $\boldsymbol{\beta} \in \mathbb{R}^{p \times 1}$, and $\beta_j = \beta(\tau_j)$, is a sparse vector. The sparse vector selects one triangle-shaped replica (column) from the dictionary $\mathbf{M}$ that best assimilates the *code-phase* of the received peak, plus noise.

We then propose solving the following $\ell 1$-minimization problem:

$$\hat{\boldsymbol{\beta}} = \underset{\boldsymbol{\beta}}{\operatorname{argmin}} \left\{ \frac{1}{2}\left\| \mathbf{y} - \mathbf{M}\boldsymbol{\beta} \right\|_2^2 + \lambda \left\| \boldsymbol{\beta} \right\|_1 \right\} \tag{8}$$

where λ is a tuning parameter. When there is a spoofer attack, two sparse non-zero values are expected, e.g, $\hat{\beta}_3$ and $\hat{\beta}_7$. Additionally, this model corresponds to only the in-phase arm. To account for the in-phase and quadrature arms (see Fig. 1), we expand the model in (8) to solve for both in-phase and quadrature components as follows:

$$(\hat{\boldsymbol{\beta}}^I, \hat{\boldsymbol{\beta}}^Q) = \underset{\boldsymbol{\beta}^I, \boldsymbol{\beta}^Q}{\operatorname{argmin}} \left\{ \begin{array}{l} \frac{1}{2}\left\| \mathbf{y}^I - \mathbf{M}\boldsymbol{\beta}^I \right\|_2^2 + \lambda \left\| \boldsymbol{\beta}^I \right\|_1 \\ + \frac{1}{2}\left\| \mathbf{y}^Q - \mathbf{M}\boldsymbol{\beta}^Q \right\|_2^2 + \lambda \left\| \boldsymbol{\beta}^Q \right\|_1 \end{array} \right\} \tag{9}$$

where $\mathbf{y} = \mathbf{y}^I + i\mathbf{y}^Q$, and $\boldsymbol{\beta} = \boldsymbol{\beta}^I + i\boldsymbol{\beta}^Q$. Finally, we combine the solutions from both in-phase and quadrature to obtain the following:

$$\left| \hat{\boldsymbol{\beta}} \right| = \left| \hat{\boldsymbol{\beta}}^I + j\hat{\boldsymbol{\beta}}^Q \right|. \tag{10}$$

A. The Multi-LASSO technique

To implement the *high-resolution* concept, we define the *multi-LASSO* technique by decimating the $\mathbf{M}$ matrix into F_p individual $n \times n$ matrices. For example, a matrix $\mathbf{M}$ with $\delta_{E-L} = 1.0$, $d = 0.1$, $n = 11$, and $F_p = 5$, has size 11×55. We build five individual 11×11 matrices from $\mathbf{M}$. Each matrix is built by the columns of the original $\mathbf{M}$ matrix as follows:

$$\begin{gathered} \mathbf{M}_K = \mathbf{m}\left(K : F_p : end\right) \\ K \in \left\{1, \ldots, F_p\right\} \end{gathered} \tag{11}$$

We then formulate the following optimization problem for each corresponding $\hat{\boldsymbol{\beta}}_K$ involving each $\mathbf{M}_K$ matrix as follows:

$$(\hat{\boldsymbol{\beta}}^I_{K=1\ldots F_p}, \hat{\boldsymbol{\beta}}^Q_{K=1\ldots F_p}) = \underset{\boldsymbol{\beta}^I_{K=1\ldots F_p}, \boldsymbol{\beta}^Q_{K=1\ldots F_p}}{\operatorname{argmin}} \left\{ \begin{array}{l} \frac{1}{2}\sum_{K=1}^{F_p} \left\| \mathbf{y}^I - \mathbf{M}_K \boldsymbol{\beta}^I_K \right\|_2^2 + \sum_{K=1}^{F_p} \lambda_K \left\| \beta^I_K \right\|_1 \\ + \frac{1}{2}\sum_{K=1}^{F_p} \left\| \mathbf{y}^Q - \mathbf{M}_K \boldsymbol{\beta}^Q_K \right\|_2^2 + \sum_{K=1}^{F_p} \lambda_K \left\| \beta^Q_K \right\|_1 \end{array} \right\} \tag{12}$$

Finally, each in-phase and quadrature outputs are combined to obtain F_p magnitude vectors $\hat{\boldsymbol{\beta}}_K$. We then select the maximum value of each $\hat{\boldsymbol{\beta}}_K$ vector for each correlator tap as follows:

$$\hat{\beta}_{i,\max} = \underset{\hat{\beta}_{K=1\ldots F_p,i}}{\arg\max} \left\{ \hat{\beta}_{1,i}, \ldots, \hat{\beta}_{K,i}, \ldots, \hat{\beta}_{F_p,i} \right\}. \tag{13}$$

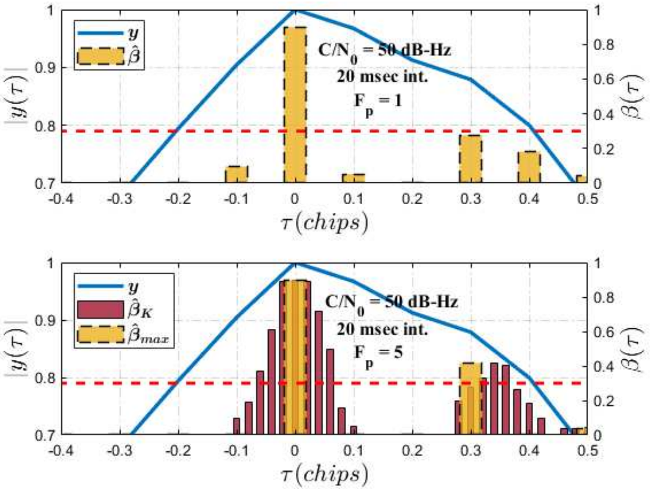

Fig. 3. Normalized received post-correlation vector $\mathbf{y}$ with simulated *code-phase* of 0.34, and CNR of 50 dB-Hz. Proposed non-group method output (top), vs grouped optimal selector outputs with *p-factor* of 5 (bottom).

After finding the maximum peak for $i \in \{1, \ldots, n\}$ taps for all F_p vectors $\hat{\boldsymbol{\beta}}_K$, we obtain $\hat{\boldsymbol{\beta}}_{\max} \in \mathbb{R}^{n \times 1}$. Finally, we use a threshold to distinguish or detect peaks that are meaningful.

IV. Simulations and Results

In this section, we evaluate the optimization technique using a MATLAB interfaced convex-optimization solver, namely, CVX [23], along with synthetic simulations. We present Monte Carlo simulations to assess the sensitivity of the proposed method and we evaluate it against the TEXBAT database.

The initial simulation compares $F_p = 1$ with $F_p = 5$, and we use $\delta_{E-L} = 1.0$, $d = 0.1$, and $n = 11$. We use a sampling rate of 25 MHz and a carrier-to-noise ratio (CNR) of 50 dB-Hz. Fig. 3 shows an example of a received signal with two peaks: the authentic peak at correlator tap 0.0, and the spoofer peak at correlator tap 0.34. The authentic peak power is normalized, and the spoofer peak has -3 dB power relative to the authentic peak. The distorted triangle shape is the received post-correlator signal with two peaks and noise. The left y-axis represents normalized signal power, and the right y-axis represents $\hat{\boldsymbol{\beta}}$ magnitudes. The dotted red line shows a threshold level of 30%, which we consider a realistic value, since it corresponds to -10.5 dB attenuation. The top graph of Fig. 3, which corresponds to $F_p = 1$, shows a peak split between taps 0.3 and 0.4, due to its coarse grid. The bottom graph shows the higher-resolution multi-LASSO technique where the outputs of $\hat{\boldsymbol{\beta}}_K$ have red bars, along with the maximized output $\hat{\boldsymbol{\beta}}_{\max}$ in yellow. The spoofer code-phase at 0.34 is detected above the threshold level.

A. Monte Carlo simulations

For the Monte Carlo simulations, we generate an authentic peak at tap 0.0 and a spoofer peak at variable taps $[0.1, \ldots, 1.0]$, with 1000 realizations per delay, at a fixed CNR of 50 dB-Hz.

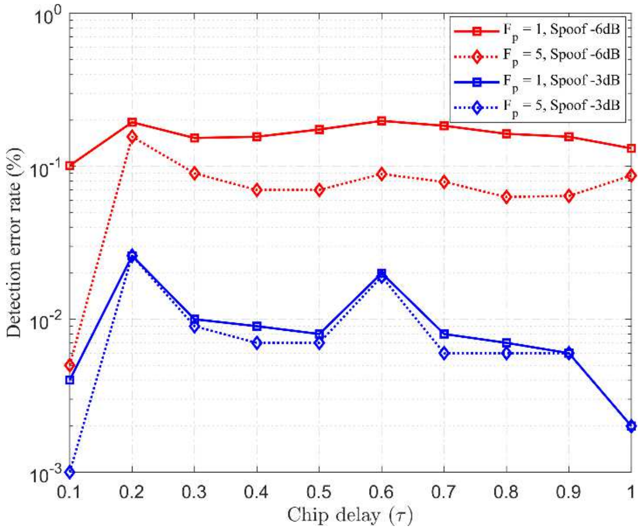

Fig. 4. Simulation results DER vs different spoofer *code-phases* $\Delta\tau_S$ from 0.1 to 1.0 chips with CNR of 50 dB-Hz and 1 msec integration length.

We compare $F_p = 1$ and $F_p = 5$. Further, we define a detection error rate (DER) metric. If the spoofer peak is not detected at the simulated delay, it is considered a detection miss. In terms of detection, we choose the two peaks with the maximum value. Similar to the previous experiment, we use the same correlator configuration and spacing, with 11 in-phase correlators and same sampling rate. We use an integration length of 1 msec to highlight the gains between $F_p = 1$ and $F_p = 5$. Finally, the spoofer peak is simulated at -3 dB and -6 dB for each delay scenario, that is, half-power and quarter-power with respect to the authentic peak, respectively.

Fig. 4 shows the DER curve vs *code-phase* for the previously mentioned scenarios. For the spoofer power of -6 dB, the *multi-LASSO* technique with $F_p = 5$ is a clear improvement over the $F_p = 1$ technique. Table 1 shows the average DER values per scenario. The multi-LASSO technique is clearly superior to the single LASSO technique by more than twice the DER value. simulation is 5.7% and 2.9%, for $F_p = 1$ and $F_p = 5$, respectively.

B. *TEXBAT evaluation*

TABLE I. COMPARISON OF AVERAGE DER VS. SPOOFER CHIP-DELAYS

Average DER	*Spoofer -6 dB*	*Spoofer -3 dB*
P-factor 1	16.10%	1.0%
P-factor 5 (multi-LASSO)	7.73%	0.89%

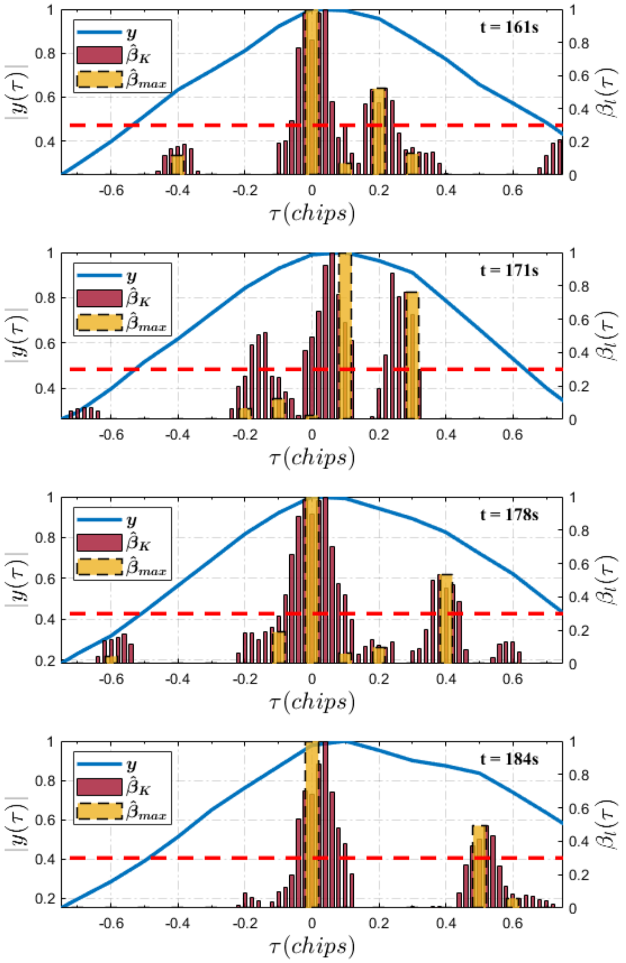

Fig. 5. *Multi-LASSO* with *p-factor* of 5 on real dataset from TEXBAT *DS2* scenario for *code-phase* spoofer at 0.2, 0.3, 0.4, and 0.5 chips, respectively.

In this section, we test our method against a scenario from the TEXBAT database using an in-house SDR GPS receiver from the Software Communications and Navigation Systems (SCNS) Laboratory at the University of Texas at San Antonio (UTSA) [24]. We specifically evaluate scenario 2 which represents a static example with an intermediate spoofing attack as described in [5]. The attack begins at $t \cong 100$ s and as it drags-off, it gradually overpowers the authentic signal by 10 dB. The total *code-phase* drag-off is around 2.1 chips, which corresponds to around 600 m offset. We run the proposed method at snapshots of the attack time to find the spoofer peak at 0.2, 0.3, 0.4, and 0.5 *code-phases,* corresponding to discrete snapshot locations $t = 161s$, $t = 171s$, $t = 178s$, and $t = 184s$. TEXBAT signals were recorded with high fidelity equipment from National Instruments at 25 MHz sampling rate, and 16-bit sample resolution in interleaved in-phase and quadrature format. The SDR receiver post-processes the binary file in offline mode to extract the correlator outputs. We configure the correlators as follows: $\delta_{E-L} = 1.6$, $d = 0.1$, and $n = 17$, and evaluate the *multi-LASSO* technique with $F_p = 5$.

Fig. 5 shows the snapshot evaluations where the *multi-LASSO* technique is able to discriminate between two peaks at said delays. In our real dataset tests we assume our proposed method works for frequency locked scenarios. Working with real data introduces interesting phenomena seen near the vicinity of the center peak or DLL discriminator *residuals*, as the main peak typically shows visible side-lobes (see Fig. 5 at $t = 171s$). Based on these phenomena, the selector might find several peaks near the center as MP. Finally, our proposed technique is tuned for spoofer detection but can potentially be used for MP.

V. Conclusion

In this work, a spoofing detection algorithm based on LASSO is proposed to discern correlation peaks from dictionary of triangle replicas. We further extend this technique to use a high-resolution grid for detection based on several delayed triangle replicas. Additionally, MC simulations for DER vs chip delay are performed. The detector is able to maintain overall 1.0% DER for several chip delays with a spoofer peak at -3 dB. An in-house SDR receiver from UTSA is used to collect correlation points from signals in the real dataset TEXBAT. The proposed algorithm was able to detect the spoofer peak at correlator taps 0.2, 0.3, 0.4, and 0.5, respectively. For future work, several computationally efficient algorithms for solving the LASSO, such as least angle regression (LARS) [25], are to be explored for a possible real-time implementation.

VI. Acknowledgement

This work was supported by the National Science Foundation under Grant ECCS-1719043.

References

[1] P. Misra and P. Enge, *Global Positioning System: Signals, Measurements, and Performance*, Lincoln, Massachusetts: Ganga-Jamuna Press. 2012.

[2] M. G. Amin, P. Closas, A. Broumandan and J. L. Volakis, "Vulnerabilities, Threats, and Authentication in Satellite-Based Navigation Systems [scanning the issue]," *Proc. IEEE*, vol. 104. no. 6, pp. 1169–1173, 2016.

[3] E. Schmidt, Z. Ruble, D. Akopian and D. J. Pack, "Software-Defined Radio GNSS Instrumentation for Spoofing Mitigation: A Review and a Case Study," *IEEE Trans. Instrum. Meas.*, pp. 1-17, 2018. [Online].

[4] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, Jr., "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proc. 21st Int. Tech. Meeting Satell. Div. Inst. Navig. (ION GNSS)*, Savannah, GA, USA, Sep. 2008, pp. 2314–2325.

[5] T.E. Humphreys, J.A. Bhatti, D.P. Shepard, and K.D. Wesson, "The Texas Spoofing Test Battery: Toward a Standard for Evaluating GPS Signal Authentication Techniques," in *Proc. 25th Int. Tech. Meeting Satell. Div. Inst. Navig. (ION GNSS)*, Nashville, TN, Sep. 2012, pp. 3569-3583.

[6] M. L. Psiaki and T. E. Humphreys, "GNSS Spoofing and Detection," *Proc. IEEE*, vol. 104, no. 6, pp. 1258-1270, 2016.

[7] K. D. Wesson, J. N. Gross, T. E. Humphreys and B. L. Evans, "GNSS Signal Authentication Via Power and Distortion Monitoring," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 54, no. 2, pp. 739-754, 2018.

[8] K. D. Wesson, D. P. Shepard, J. A. Bhatti and T. E. Humphreys, "An Evaluation of the Vestigial Signal Defense for Civil GPS Anti-Spoofing," in *Proc. 24st Int. Tech. Meeting Satell. Div. Inst. Navig. (ION GNSS)*, Portland, OR, USA, Sep. 2011, pp. 2646-2656.

[9] M. L. Psiaki, B. W. O'Hanlon, J. A. Bhatti, D. P. Shepard and T. E. Humphreys, "GPS Spoofing Detection via Dual-Receiver Correlation of Military Signals," I*EEE Trans. Aerosp. Electron. Syst.*, vol. 49, no. 4, pp. 2250-2267, 2013.

[10] C. Sun, H. Zhao, W. Feng and S. Du, "A Frequency-Domain Multipath Parameter Estimation and Mitigation Method for BOC-Modulated GNSS Signals," *Sensors (Basel)*, vol. 18(3), no. 721, pp. 1-24, 2018.

[11] W. Wang, N. Li, R. Wu and P. Closas "Detection of Induced GNSS Spoofing Using S-Curve-Bias," *Sensors (Basel)*, vol. 19(4), no. 922, pp. 1-17, 2019.

[12] A. Pirsiavash, A. Broumandan and G. Lachapelle, "Characterization of Signal Quality Monitoring Techniques for Multipath Detection in GNSS Applications," *Sensors (Basel)*, vol. 17(7), no. 1579, pp. 1-17, 2017.

[13] E. McMilin, D. S. De Lorenzo, T. Walter, T. H. Lee, and P. Enge Single antenna GPS spoof detection that is simple, static, instantaneous and backwards compatible for aerial applications In *Proc. 27th Int. Tech. Meeting Satell. Div. Inst. Navig. (ION GNSS)*, Tampa, FL, USA, 2014, pp. 2233–2242.

[14] F. Wang, H. Li and M. Lu, "GNSS Spoofing Countermeasure With a Single Rotating Antenna," *IEEE Access*, vol. 5, pp. 8039-8047, 2017.

[15] P. Y. Montgomergy, T. E. Humphreys, and B. M. Ledvina "Receiver-autonomous spoofing detection: Experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer," In *Proc. ION Int. Tech. Meeting (ION GNSS)*, Anaheim, CA, USA, Jan. 2009, pp. 124–130.

[16] S. Daneshmand, A. Jafarnia-Jahromi, A. Broumandon and G. Lachapelle "A Low-Complexity GPS Anti-Spoofing Method Using a Multi-Antenna Array," in *Proc. 25st Int. Tech. Meeting Satell. Div. Inst. Navig. (ION GNSS)*, Nashville, TN, USA, Sep. 2012, pp. 1233-1243.

[17] R. L. Fante and J. J. Vaccaro, "Wideband Cancellation of Interference in a GPS Receive Array," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 36, no. 2, pp. 549-564, 2000.

[18] C. Enneking and F. Antreich, "Exploiting WSSUS Multipath for GNSS Ranging," *IEEE Trans. Veh. Technol.*, vol. 66, no. 9, pp. 7663-7676, Sep. 2017.

[19] C. Gunther, "A Survey of Spoofing and Countermeasures," *NAVIGATION, Journal of The Institute of Navigation*, vol. 61, no. 3, pp. 159-177, 2014.

[20] R. Tibshirani, "Regression shrinkage and selection via the lasso," *J. Roy. Statist. Soc. B, Methodol.*, vol. 58, no. 1, pp. 267–288, 1996.

[21] B.W. Parkinson, J. J. Spilker, P. Axelrad, and P. Enge*, Global Positioning System: Theory and Applications, vol. I.* Washington, DC, USA: Amer. Inst. Aeronaut. Astronaut., 1996.

[22] A. J. Van Dierendonck, P. Fenton and T. Ford, "Theory and Performance of Narrow Correlator Spacing in a GPS Receiver," *NAVIGATION, Journal of The Institute of Navigation*, vol. 39, no. 3, Fall 1992, pp. 265-284.

[23] CVX Research, Inc., "CVX: Matlab software for disciplined convex programming, version 2.1," Dec. 2018. [Online]. Available: http://cvxr.com/cvx

[24] E. Schmidt, D. Akopian, and D. J. Pack, "Development of a realtime software-defined GPS receiver in a labVIEW-based instrumentation environment," *IEEE Trans. Instrum. Meas.*, vol. 67, no. 9, pp. 2082–2096, Sep. 2018.

[25] B. Efron, T. Hastie, I. Johnstone and R. Tibshirani, "Least Angle Regression," *The Annals of Statistic*s, vol. 32, no. 2, pp. 407-499, 2004.