Anti-Spoofing Technique Against GPS Time and Position Attacks Based on Sparse Signal Processing

Junhwan Lee, Erick Schmidt, Nikolaos Gatsis, David Akopian

BIOGRAPHY

Junhwan Lee received his B.S. degree in electrical engineering from University of Texas at San Antonio (UTSA) in 2017. He is currently Ph.D. candidate in the Department of Electrical and Computer Engineering, at the University of Texas at San Antonio (UTSA). His research interest includes GNSS interference mitigation technique, state estimation in optimization and control theory.

Erick Schmidt received his B.S. degree in electrical engineering from Monterrey Institute of Technology and Higher Education, Monterrey, Mexico, in 2011 and both his M.S. and Ph.D. degrees in electrical engineering from The University of Texas at San Antonio (UTSA), San Antonio, Texas, United States, in 2015 and 2020 respectively. His research interests include baseband processing in software-defined radio platforms for fast prototyping, WLAN indoor localization systems, and interference mitigation techniques for Global Navigation Satellite System (GNSS). He is a graduate student member of IEEE and ION.

Nikolaos Gatsis received the Diploma degree (Hons.) in electrical and computer engineering from the University of Patras, Patras, Greece, in 2005, and the M.Sc. degree in electrical engineering, in 2010, and the Ph.D. degree in electrical engineering with minor in mathematics, in 2012, from the University of Minnesota, Minneapolis, MN, USA. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, University of Texas at San Antonio, San Antonio, TX, USA. He was a Lutcher Brown Professorship Endowed Fellow for the academic year 2020–2021. His research focuses on optimal and secure operation of smart power grids and other critical infrastructures, including water distribution networks and the Global Positioning System. Dr. Gatsis is a recipient of the NSF CAREER award and the UTSA President's Award for Research Achievement.

David Akopian is a Professor at the University of Texas at San Antonio (UTSA) and Associate Dean of Research for the College of Engineering. Before joining UTSA, he was a Senior Research Engineer and Specialist with Nokia Corporation from 1999 to 2003. From 1993 to 1999, he was a researcher, instructor, and assistant director of a center at the Tampere University of Technology, Finland, where he received his Ph.D. degree in 1997. Dr. Akopian's current research interests include algorithms for communication and navigation receivers, including fast acquisition and massive correlators, spoofing mitigation on different levels of processing chain, and general area of mobile applications. Also, he contributed in positioning algorithms for Assisted-GPS and Labview platform concepts for software-defined radio GPS receivers. Recent efforts include automated human-machine interfaces. He authored and co-authored more than 35 patents and 170 publications. He is a Fellow of the US National Academy of Inventors since 2016. His research has been supported by the National Science Foundation, National Institutes of Health, USAF, US Navy, and Texas foundations.

ABSTRACT

In this paper, we present a cost-effective software-developed Global Positioning System (GPS) anti-spoofing approach against Time Synchronization Attacks (TSAs) and spatial spoofing. We portray two signal-level spoofing characteristics that are predominantly discovered in aforementioned attacks, namely, spoofing profiles and consistency of modifying signals. While the spoofing profiles, which basically describe the inflicting signal shapes affecting the GPS observables, have already been analyzed in our previous research with respect to attacks against timing, this paper still utilizes the idea, yet implements and showcases the applicability of spoofing profiles in position domain. The extension, in fact, brings the idea of joint TSA and spatial spoofing. To jointly consider the time and spatial domains, the pseudorange and range rate equations are linearized with a non-conventional method. An antispoofing technique capable of withstanding TSAs, spatial attacks on single coordinate, and joint attacks is developed for stationary receiver. To validate the proposed approach, we utilize pre-recorded authentic GPS signals in the TEXBAT database for data transmission, which are captured by the Software Defined Radio receiver developed at UTSA. The algorithm is validated in simulations introducing synthetic spoofing and compared against Weighted Least Squares.

 https://doi.org/10.33012/2021.17988

I. INTRODUCTION

Global Navigation Satellite System (GNSS) offers an irreplaceable service on providing Position, Navigation, and Time (PNT) for various applications. The growing reliance on GNSS has generated growing interest on its authentication, validity, and security; which are undeniably challenging due to the external interference. Inherently, the GNSS receiver is susceptible to experiencing a range of disturbances during long-distance satellite-to-receiver communication. The GNSS receiver can thus become a victim of a third-party harmful hacker, a situation that has been shown to be applicable and plausible by the relevant literature [1], [2].

This paper considers one of the deliberate GNSS hacking mechanisms commonly referred to as spoofing. Spoofing occurs when a malicious actor injects disguised counterfeit GNSS signals to a GPS receiver such that the attacked receiver is induced to produce an imprecise user position, velocity, and time (PVT) solution. Smart grid, an infrastructure that has significant reliance on timing synchronization via the GPS, becomes a vulnerable target for malicious spoofing actors. In the work of [3], scenarios where time synchronization attacks (TSAs) lead to failures in power system state estimation are illustrated, which may eventually cause failure to take a corrective action. Another significant application that has attracted prominent research and heavily hinges upon the position and velocity estimations of GNSS receivers is unmanned autonomous vehicle (UAV) navigation. The spatial spoofing research is rich in analyzing attack mechanisms, whose effects are chiefly showcased on UAVs or other vehicles [2],[4].

As much as dangers of spoofing are manifested through research work, a plethora of publications attempt to introduce promising antispoofing countermeasures [5],[6]. Among the presented methodologies, several target the baseband domain and strive to capture unpredictable or abnormal behaviors of any sort. More specifically, the relevant research often times utilizes the observable changes on correlator peaks [7],[8], vector tracking loops [9], or power and automatic gain control [10],[11]. However, such research require supplementary circuitry on top of off-the-shelf receivers, or has to rely on one or more sophisticated receivers.

On the other hand, certain antispoofing techniques focus on the signal-level layer of GPS receiver. Such techniques strive to detect anomalies in observable sequences such as Carrier-to-Noise ratio [12], and navigational drift [13],[14]. The present paper falls in the aforementioned category and exploits common GPS observables, that is, pseudorange and range rate as a pair, to protect the receiver against malicious spoofing. Moreover, the presented algorithm is cost-effective such that it can run on a single rudimentary receiver assisted with software routines such as the freely deployed Android software.

In general, the terminology, antispoofing countermeasure, refers to two fundamental actions practiced while handling applied spoofing attacks. Initially, the algorithm captures abnormal behavior discovered during either baseband or signal-level search; which commonly referred to as *detection*. Several mechanisms halt their mission once spoofing detection is attained. *Mitigation* goes beyond detection in that it rejects the attack signal and produces accurate PVT estimates.

This paper develops an algorithm that is capable of autonomous spoofing detection and mitigation of joint attacks against time and position. Specifically, the present work focuses on stationary receivers and with respect the position attack, it provides an effective method to capture and reject an attack against a single position coordinate. The developed model expands on our previous work [15] that deals with TSAs only. Additionally, unlike our previous work [14], the optimization approach performs countermeasure with single iteration while restraining from estimated attack reconstruction stage.

The paper is organized as follows. Section II explains the studied characteristics uncovered in signal-level spoofing along with summarized linearized measurement equations. Section III presents our improved antispoofing algorithm. Section IV describes the methodology used to simulate the atack and assess the algorithm. Section V provides numerical results illustrating the effectiveness of the algorithm in mitigation of joint attacks.

II. SPOOFING ATTACK MODELING

The pseudorange and range rate equations are presented first. Then, we introduce the updated formulation of such equations whose linearization process is different from the standard one shown in e.g., [16]. Afterwards, two spoofing characteristics that can be applied to TSAs and spatial attacks in conjunction are described.

1. GPS Measurement Pair

Pseudorange refers to a computed satellite-to-receiver distance, which however differs from the true range. Given the visible satellite position $\mathbf{p}_n = [x_n \quad y_n \quad z_n]^\top$ and user position $\mathbf{p}_u = [x_u \quad y_u \quad z_u]^\top$ where $n = 1, 2, ..., N$ represents the total number of visible satellites, the true range is readily computed by using 3-dimensional Euclidean norm. Nonetheless, the discrepancy in the observed ranges originates from the satellite and receiver clock offsets, respectively denoted by b_n and b_u. The pseudorange at every time epoch $k = 1, 2, ..., K$ and for each satellite n is therefore computed via the following:

$$\rho_n[k] = ||\mathbf{p}_n[k] - \mathbf{p}_u[k]||_2 + c(b_u[k] - b_n[k]) + \epsilon_{\rho_n}[k] \tag{1}$$

where c represents the speed of light, $||\cdot||_2$ indicates the l_2 norm, and any Gaussian white noise is captured in ϵ_{ρ_n}. Furthermore, $\mathbf{p}_n[k]$ and $\mathbf{p}_u[k]$ denote the position vector represented in Earth-Centered Earth-Fixed (ECEF) x-y-z coordinates at time epoch k for satellite n and the receiver, respectively. Likewise, $b_n[k]$ and $b_u[k]$ refer to the aforementioned clock biases due to the local clock offset on both satellite and receiver ends.

A complementary component in the measurement pair is considered. Specifically, the Doppler rate, or alternatively referred to as range rate, demonstrates the effect of Doppler shift created between maneuvering satellites and the receiver. The range rate ($\dot{\rho}$) is mathematically defined as

$$\dot{\rho}_n[k] = (\mathbf{v}_n[k] - \mathbf{v}_u[k])^\top \cdot \frac{\mathbf{p}_n[k] - \mathbf{p}_u[k]}{||\mathbf{p}_n[k] - \mathbf{p}_u[k]||_2} + c(\dot{b}_u[k] - \dot{b}_n[k]) + \epsilon_{\dot{\rho}_n}[k] \tag{2}$$

where satellite n's velocity is shown as $\mathbf{v}_n = [\dot{x}_n \quad \dot{y}_n \quad \dot{z}_n]^\top$ and the velocity of receiver as $\mathbf{v}_u = [\dot{x}_u \quad \dot{y}_u \quad \dot{z}_u]^\top$. During satellite-to-receiver data communication, the user readily obtains information in regards to all the visible satellites such as position ($\mathbf{p}_n$), velocity ($\mathbf{v}_n$), and clock offset and bias (b_n and $\dot{b}_n$), which in turn, leaves user PVT variables ($\mathbf{p}_u$, $\mathbf{v}_u$, b_u, and $\dot{b}_u$) as unknown.

With respect to data acquisition, the two aforementioned measurements are obtained from disparate hardware sources in the receiver. Theoretically, however, pseudorange and range rate sequence must satisfy the following equation expressing measurement integrity:

$$\dot{\rho}[k] = \frac{\rho[k+1] - \rho[k]}{\Delta t} \tag{3}$$

where Δt represents the discretized sampling time during the signal reception. Once measurement data is fully captured on the receiver, we performed a sanity check examination via using Eq. (3) to attain the validity of acquired data.

The pair of pseudorange and range rate equations needs to be linearized for two reasons. Specifically, $\mathbf{p}_u$ and $\mathbf{v}_u$ appear in (1), (2) under the l-2 norm, which is nonlinear. Although general-purpose nonlinear programming (NLP) solvers are available, a linearized model can leverage the computational advantages of convex optimization solvers, namely, rapidly calculating PVT solutions without loss of accuracy. The linearization is performed using Taylor series expansion. Since the present work is concerned with stationary receivers, eq. (1) and (2) are linearized with respect to a fixed known user position reference, $\mathbf{p}_{u,ref}$, and zero velocity reference $\mathbf{v}_u = 0$. See [17] for a detailed derivation of the linearization. The resulting model is stated as

$$\begin{cases} z_{\rho_n}[k] & = -\mathbf{1}_{n.ref}^\top[k]\mathbf{p}_u[k] + cb_u[k] + \epsilon_{\rho_n}[k] \\ z_{\dot{\rho}_n}[k] & = \mathbf{v}_n[k]^\top \Phi[k]\mathbf{p}_u[k] - \mathbf{1}_{n.ref}^\top[k]\mathbf{v}_u[k] + c\dot{b}_u[k] + \epsilon_{\dot{\rho}_n}[k] \end{cases} \tag{4}$$

where

$$\mathbf{1}_{n.ref}[k] = \frac{\mathbf{p}_n[k] - \mathbf{p}_{u.ref}[k]}{||\mathbf{p}_n[k] - \mathbf{p}_{u.ref}[k]||_2} = \begin{bmatrix} x_{n.ref}[k] \\ y_{n.ref}[k] \\ z_{n.ref}[k] \end{bmatrix} \in \mathbb{R}_{3\times 1}$$

$$\mathbf{\Phi}_n[k] = \frac{(\mathbf{p}_n[k] - \mathbf{p}_{u.ref}[k])(\mathbf{p}_n[k] - \mathbf{p}_{u.ref}[k])^\top}{||\mathbf{p}_n[k] - \mathbf{p}_{u.ref}[k]||_2^3} - \frac{\mathbf{I}}{||\mathbf{p}_n[k] - \mathbf{p}_{u.ref}[k]||_2} \in \mathbb{R}_{3\times 3}$$

The system considers $\mathbf{1}_{n.ref}$ and $\mathbf{\Phi}_n$ as known vectors since $\mathbf{p}_n$ is readily provided by satellite and updated on every time epoch k. Regarding the user position reference, $\mathbf{p}_{u.ref}$, we manually fix it to the initial estimated user position vector as $\mathbf{p}_u[1]$. The linearized system still satisfies the measurement integrity, eq. (3).

In the presence of spoofing, modifying signals are modeled as additive to the measurement pair. The following equations manifest the conventional representation of spoofed psuedorange and range rate:

$$\begin{aligned} z_{n,s}[k] &= z_{\rho_n}[k] + s_{\rho_n}[k] \\ \dot{z}_{n,s}[k] &= z_{\dot{\rho}_n}[k] + s_{\dot{\rho}_n}[k] \end{aligned} \tag{5}$$

where s_{ρ_n} and $s_{\dot{\rho}_n}$ represent spoofing signals injected on pseudorange and range rate, respectively. The attacked pseudoranges and pseudorange rates are conventionally provided as inputs to traditional algorithms such as Weighted Least Squares (WLS) or extended Kalman Filter (EKF), which output the PVT solutions to the end user. Thus, the the abnormal behavior captured in pseudoranges is transferred on the PVT solutions. In this work, to facilitate spoofing mitigation, we present certain characteristics of the spoofing signals in the next subsections, namely, spoofing attack order and consistency check.

2. Spoofing Attack Order

In this subsection, we revisit spoofing profiles that are mainly determined on the basis of the shape of spoofing signal. Specifically, in our previous work [15], we specifically consider TSAs and examine whether higher-order discrete-time derivatives of the spoofing signal are sparse, that is, exhibit spike-like behavior. The present paper extends the premise to attacks against a single position coordinate, and we specifically focus on z domain. Following [15], we analyze the smallest order derivative where the attack exhibits evident spikes, and define the attack accordingly. For instance, a so-called Type I attack in [13] can be re-identified as *first order* attack for the sparsity occurs in velocity domain, or equivalently in the first derivative of position. Considering the position domain, we define *second order* and *third order* attacks with examples depicted in Figure 1. The second order attack with increasing trend is shown in Figure 1a, whose second derivative (the acceleration) features two spikes at 100 and 300 seconds. Figure 1b depicts subtle gradual changes akin to third order attack where the sparsity is achieved on the third derivative (jerk domain).

The chief advantage in defining spoofing profiles for benefiting the development of antispoofing models is the fact that sparsity appears on the jerk domain for the majority of the attacks reported in the literature. It is worth mentioning that the aforementioned shapes of first, second, and third order attacks are popularly utilized in spoofing research [18],[19].

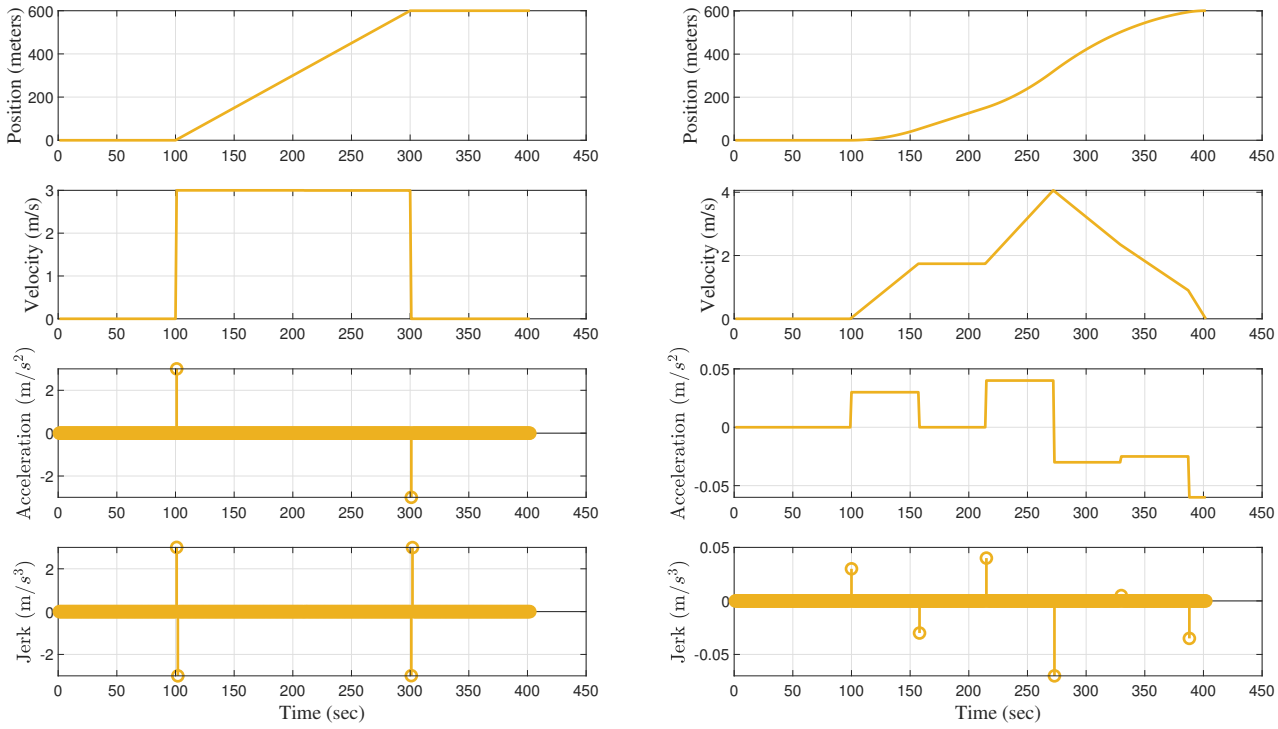


Figure 1: Figure (a) indicates an example of second order attack. The initial sparse spikes appear on the second derivative of position vector, which is the acceleration domain. Sparsity still is achieved in the jerk domain, where more spikes appear. Figure (b) depicts a subtle gradual changes, which is an example of third order attack with spike showing up in the jerk domain.

3. Spoofing Consistency

Attack consistency is inspired by the measurement integrity equation (3); and applying the rationale to the spoofing signal, a *consistent* attacks is required to satisfy the following condition:

$$s_{\dot{\rho}}[k] \approx \frac{s_{\rho}[k] - s_{\rho}[k-1]}{\Delta t} \tag{6}$$

If the attacks fail to satisfy (6), it can referred to as *non-consistent* attack.

An example of *consistent* attack is TSA [13]. While fulfilling measurement integrity, deviating signals on psuedorange and range rate are explicitly manifested on clock bias and drift.Particular applications vulnerable to TSAs are electric power grid operations that are driven by Phasor Measurement Unit (PMU) readings. PMUs are equipped with (stationary) GPS receivers, whose timing errors translate into voltage and current phase angle deviations. These can subsequently lead to erroneous state estimation for the power grid [20]. The authentic spoofing database TEXBAT, corroborates the aforementioned TSA characteristics, which can also be incited with baseband spikes.

In case of spatial spoofing, attack may be defined as *consistent* or *non-consistent* depends on the targeted domain. If the spoofer aims to solely vary a position estimate and leaves the velocity domain intact, that would be an example of a *non-consistent* attack. *Consistent* spatial attack result in modification on position and velocity domains.

This paper considers attacks against two domains: TSA (clock bias b) and single-coordinate position (coordinate z), whereby time and spatial solutions are simultaneously affected. This condition is called a joint attack. In practical applications, such complicated spoofing can be achieved by having the receiver hacked by different data sources [21]. For joint attack simulation, we only examine *consistent* attack since TSA must be applied with the spoofing integrity.

The ensuing section describes the antispoofing optimization function that can reject any of the aforementioned attacks.

III. ANTI-SPOOFING TECHNIQUE

In this section, we present the suggested anti-spoofing technique to detect and mitigate the aforementioned attack types. To adequately express the technique, we present a proper GPS dynamic equation along with the linearized measurement equations.

1. GPS Dynamic Equations

The GPS receiver is described by a dynamical system that follows the random walk model [16]:

$$\underbrace{\begin{pmatrix}\mathbf{p}_u[k]\\ cb_u[k]\\ \mathbf{v}_u[k]\\ c\dot{b}_u[k]\end{pmatrix}}_{\mathbf{x}_k}=\underbrace{\begin{pmatrix}\mathbf{I}_{4\times4} & \Delta t\mathbf{I}_{4\times4}\\ \mathbf{0}_{4\times4} & \mathbf{I}_{4\times4}\end{pmatrix}}_{\mathbf{F}_k}\underbrace{\begin{pmatrix}\mathbf{p}_u[k-1]\\ cb_u[k-1]\\ \mathbf{v}_u[k-1]\\ c\dot{b}_u[k-1]\end{pmatrix}}_{\mathbf{x}_{k-1}}+\mathbf{w}_k \tag{7}$$

where $\mathbf{F}_k$ is the state transition matrix and $\mathbf{w}_k$ refers to the state transition noise. Although in a stationary environment, the position does not vary and the velocities in x, y, z remain zero, eq. (7) is adopted in the present work because $\mathbf{x}_k$ may contain deviating signals, and specifically, attacks that modify the solution in the b or z domains. Including the unknwon $\mathbf{x}_k$ as an optimization variable may be beneficial towards recovering the authentic PVT solution.

Further, as mentioned earlier, the spoofing signal variables are appended to Eq. (4) for the system to delineate authentic PVT solutions with inflicting signals, with linearized measurement vectors $\mathbf{z}_\rho = [z_{\rho_1} \quad z_{\rho_2} \quad \cdots \quad z_{\rho_N}]^\top$, $\mathbf{z}_{\dot\rho} = [z_{\dot\rho_1} \quad z_{\dot\rho_2} \quad \cdots \quad z_{\dot\rho_N}]^\top$, which can be expressed as following:

$$\begin{aligned}\underbrace{\begin{pmatrix}\mathbf{z}_\rho[k]\\ \mathbf{z}_{\dot\rho}[k]\end{pmatrix}}_{\mathbf{z}_k}&=\underbrace{\begin{pmatrix}\mathbf{E}_{N\times3} & \mathbf{1}_{N\times1} & \mathbf{0}_{N\times3} & \mathbf{0}_{N\times1}\\ \boldsymbol{\Psi}_{N\times3} & \mathbf{0}_{N\times1} & \mathbf{E}_{N\times3} & \mathbf{1}_{N\times1}\end{pmatrix}}_{\mathbf{H}_k}\underbrace{\begin{pmatrix}\mathbf{p}_u[k]\\ b_u[k]\\ \mathbf{v}_u[k]\\ \dot b_u[k]\end{pmatrix}}_{\mathbf{x}_k}\\ &+\underbrace{\begin{pmatrix}-\mathbf{z}_{n.ref} & \mathbf{1}_{N\times1} & \mathbf{0}_{N\times1} & \mathbf{0}_{N\times1}\\ \boldsymbol{\psi}_{\mathbf{z}} & \mathbf{0}_{N\times1} & -\mathbf{z}_{n.ref} & \mathbf{1}_{N\times1}\end{pmatrix}}_{\mathbf{G}_k}\underbrace{\begin{pmatrix}s_z[k]\\ s_b[k]\\ s_{\dot z}[k]\\ s_{\dot b}[k]\end{pmatrix}}_{\mathbf{s}_k}+\underbrace{\begin{pmatrix}\boldsymbol{\epsilon}_{\rho_n}\\ \boldsymbol{\epsilon}_{\dot\rho_n}\end{pmatrix}}_{\epsilon_k}\end{aligned} \tag{8}$$

where

$$\boldsymbol{\Psi}=\begin{bmatrix}\mathbf{v}_1^\top\boldsymbol{\Phi}_1\\ \mathbf{v}_2^\top\boldsymbol{\Phi}_2\\ \vdots\\ \mathbf{v}_N^\top\boldsymbol{\Phi}_N\end{bmatrix}=[\boldsymbol{\psi}_{\mathbf{x}} \quad \boldsymbol{\psi}_{\mathbf{y}} \quad \boldsymbol{\psi}_{\mathbf{z}}]\in\mathbb{R}_{N\times3}$$

$$\mathbf{E} = \begin{bmatrix} -x_{1.ref} & -y_{1.ref} & -z_{1.ref} \\ -x_{2.ref} & -y_{2.ref} & -z_{2.ref} \\ \vdots & \vdots & \vdots \\ -x_{N.ref} & -y_{N.ref} & -z_{N.ref} \end{bmatrix} \in \mathbb{R}_{N\times 3}$$

in which $\mathbf{s}_k$ place-holds captured deviating signals introduced on z-position (s_z), velocity, ($s_{\dot{z}}$), clock bias (s_b), and drift ($s_{\dot{b}}$). Such formulation aims to capture the attack introduced onto the clock timing and z-domain. Lastly, $\boldsymbol{\epsilon}_k$ represents the zero mean Gaussian measurement noise with covariance matrix $\mathbf{R}_k = \mathrm{diag}(\sigma^2_{\rho_1}, ..., \sigma^2_{\rho_N}, \sigma^2_{\dot{\rho}_1}, ..., \sigma^2_{\dot{\rho}_N})$ that can determine uncertainties of observed measurements.

2. Proposed Anti-Spoofing Technique

The proposed anti-spoofing technique utilizes the minimization function that aims to become robust against the spoofing attacks described in Section II. The following minimization is performed as solver estimates $\hat{\mathbf{x}} = [\hat{\mathbf{x}}_1, ..., \hat{\mathbf{x}}_K]^\top$ and $\hat{\mathbf{s}} = [\hat{\mathbf{s}}_1, ..., \hat{\mathbf{s}}_K]^\top$:

$$(\hat{\mathbf{x}}, \hat{\mathbf{s}}) = \underset{\mathbf{x},\mathbf{s}}{\operatorname{argmin}} \left\{ \frac{1}{2}\sum_{k=1}^{N} ||\mathbf{z}_k - \mathbf{H}_k\mathbf{x}_k - \mathbf{G}_k\mathbf{s}_k||^2_{\mathbf{R}_k^{-1}} + \frac{1}{2}\sum_{k=1}^{N} ||\mathbf{x}_{k+1} - \mathbf{F}_k\mathbf{x}_k||^2_{\mathbf{Q}_\mathbf{k}^{-1}} + \lambda_z||\mathbf{D}s_z||_1 + \lambda_b||\mathbf{D}\mathbf{s}_b||_1 \right\} \quad (9)$$

where $||\mathbf{x}||^2_\mathbf{M}$ defines a quadratic norm which is equivalently expressed as $\mathbf{x}^\top\mathbf{M}\mathbf{x}$. Note that $s_z = [s_z[1], ..., s_z[K]]$ and $\mathbf{s}_b = [s_b[1], ..., s_b[K]]$ are sub-vectors of $\mathbf{s}_k$.

Eq. (9) consists of four objectives that serve the anti-spoofing scheme. First summation term is derived from measurement equation (8). The second term examines the PVT behaviors in relation to the random walk model. The third and fourth terms, nominally referred to as penalization functions, each represent the higher-order domain where sparse spikes are likely to be displayed in position and clock aspects, respectively. The first and second terms jointly encourage PVT solutions that satisfy measurement integrity. With the help of penalization terms, the technique is capable of filtering accurate PVT estimations against attacks. The matrix $\mathbf{D}$ constructs the third-order derivative of the respective sequences and is defined as follows:

$$\mathbf{D}_z = \mathbf{D}_b = \begin{bmatrix} -1 & 3 & -3 & 1 & ... & 0 \\ 0 & -1 & 3 & -3 & ... & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots & \vdots \\ 0 & 0 & ... & 3 & -3 & 1 \end{bmatrix}$$

The selection hinges upon the observation that realistic spoofing typically exhibits sparsity in the third-order derivative domain (jerk).

The performance of the technique depends on the selection of the factors λ_z and λ_b. These must be selected for each receiver. The proper values of λ_z and λ_b can tune the level of sparsity that emerges as solution from (9), as well as the relative emphasis that is placed between the two penalization functions and as well as the among the four objectives in 9. Proper tuning based on realistic attacks and in representative environments is therefore recommended. Another parameter that affects the quality of solution is the state noise covariance matrix. This must be set up with appropriate values corresponding to the static receiver.

Overall, the optimization problem in (9) is a convex quadratic program that can be solved with relatively small computational effort.

$$\mathbf{Q}_k = \begin{bmatrix} \mathbf{Q_p} & \mathbf{0} & \mathbf{Q_{pv}} & \mathbf{0} \\ \star & Q_b & \mathbf{0} & Q_{bf} \\ \star & \star & \mathbf{Q_v} & \mathbf{0} \\ \star & \star & \star & Q_f \end{bmatrix} \quad (10)$$

IV. SIMULATION METHODOLOGY

Previous sections described the importance of emerging dangers in artificially designed spoofing on the GPS receiver. To simulate and visualize the malignant effect of various spoofing types, we prepared a GPS receiver test bed which incorporate the wired and wireless signal transmission and reception simulations. Since two integrated receivers are capable of capturing real-time transmitted signals on run, we chose to insert a pre-recorded GPS signal into the signal generator, namely *Clean Static* scenario from TEXBAT database [1]. Interfaced with LabView developed software as well as attached PCIe, the GPS signal transmitter utilizes NI PXIe-1075 Chassis with a PXIe 5673 RF Signal Generator broadcasting via Vert 900 antenna. Once

transmitter setup is completed, user has two choices as per the simulation. The unprocessed data is to be directly fed into the wired lab-produced Software Defined Radio (SDR) [22], which rapidly process the raw data into precise and comprehensible GPS information for the user. On the other hand, user can opt to deliver the signal over-the-air (OTA) via the connected antenna, in which Huawei receiver, approximately located about 5-6 meters away from transmitter, captures and processes signal with *GNSSLogger* application [23]. The wireless route inherently contains more noise and consequently has higher uncertainties than the wired method. Thus, wired SDR empowers the PVT processing algorithm *i.e.* WLS and EKF to deliver more accurate position and time estimation; and this is manifested in Section V.

In the present paper, we exploit synthetically fabricated spoofing attacks while targeting a single position and time domain, namely z-domain in ECEF coordinate and clock bias estimation. We initially confirm that our algorithm attains robustness against TSA in various spoofing profiles as our previous works do [15], then simulation manifests that algorithm also can detect and mitigate the disturbance which aims to inflict 1) sole z-domain and 2) z-domain and clock bias simultaneously. Each spoofing scenarios is comprised of *first*, *second*, and *third order* types of attack while maintaining minimum of 600 meters of deviation. The routines processing raw measurements, that are reported from two receiver test beds, as well as PVT acquisition algorithms, namely, WLS, EKF, and our algorithm are all written in MATLAB language. The MATLAB-friendly covex optimization modeling software, cvx, is used to solve the quadratic program in the novel algorithm, and is employed in the effort to estimate the correct PVT solution and the spoofing attack.

V. NUMERICAL RESULTS

This section reports and examines the output of synthetic attack simulations. Both the SDR and the Huawei commercial receiver accumulate the TEXBAT *clean static* data, and we added the tailored spoofing scenarios onto the processed pseudorange pair. Multiple figures depict the outstanding performance of our suggested algorithm, yet numerically compared by using Root-Mean-Sqaure-Error (RMSE) values against the estimation produced by EKF. The following equation defines the RMSE:

$$RMSE = \sqrt{\frac{1}{K}\sum_{k=1}^{K}(\hat{\mathbf{x}}_{\text{estimated},i}[k] - \hat{\mathbf{x}}_{\text{ground truth},i}[k])^2} \tag{11}$$

where i selects the state vector entry corresponding to z, $\dot{z}$ The scenarios are comprised with 1) TSA third order *consistent* attack, 2) spatial z-domain second order *non-consistent* attack, and 3) joint third order *consistent* attack. For the sake of simplicity, all scenarios depict the result of SDR recording, while only second scenario explores the spoofing condition in the Huawei wireless receiver.

1. Scenario 1: TSA

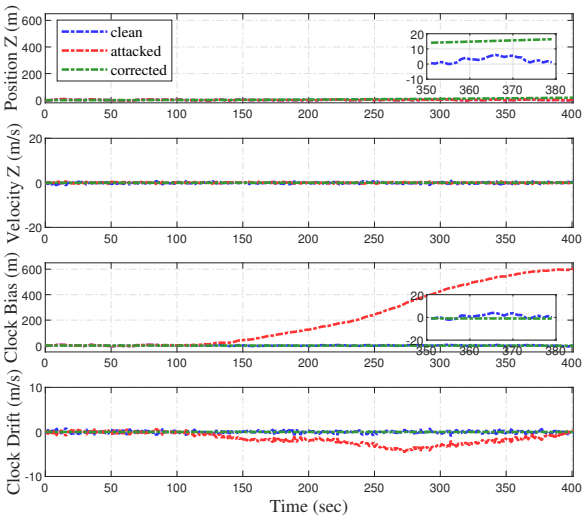
Figure 2 shows the result of sole TSA spoofing on the SDR receiver. A total of 600 meter magnitude deviation is applied to the clock bias; and the drift changes accordingly. The third order spoofing profile has the smoothest shape that can have numerous sparse spikes on the jerk domain. Based on the consistency characteristic of TSA, the deviating shape and magnitude applied on clock bias are exactly identical to modifying signals on psuedoranges. Though the spoofing setting is identical to the experience executed in the work of [15], the algorithm based on the minimization of (9), differs from the approach shown in aforementioned paper.

The primary task of third component in (9) is to filter the estimated attack from the correct PVT solution, $\mathbf{x}_k$. We select $\lambda_b = 10$. The optimization problem acknowledges the abnormal behavior on the bias domain, also by expecting subtle sparse peaks on jerk. Figure 2a shows the clean (WLS output), attacked (EKF output), and corrected (optimization output) of z position, velocity, clock bias, and drift estimations. As figure suggests, the corrected solutions all maintained to be less than absolute 20 meters. Further, the RMSE error on z coordinate is reduced from 389.22 meters to 2.25 meters. Figure 2b depicts the estimated attack, which turns out to be similar to the applied attack.

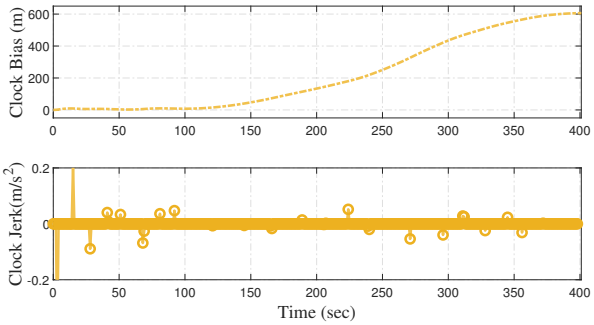
2. Scenario 2: Spatial Spoofing

Second scenario explores the second order spatial spoofing where only position estimate gets affected by the pseudorange deviation. The deviating magnitude gradually increases from 100 to 300 seconds with ultimate amplitude of 600 meters. The second order spoofing profile expects to show peaks in acceleration and jerk domains. The major improvement made with respect to our previous approach [15] is attaining robustness against spatial spoofing. Due to measurement linearization, our algorithm has capability to search more than clock domain.

The plots in Figure 3 express the result of sole spatial spoofing in z-domain, namely, the result of the optimization after applying the synthetic attack to the replayed *CS* scenario over the SDR and the Huawei receiver. Even though the Huawei recordings

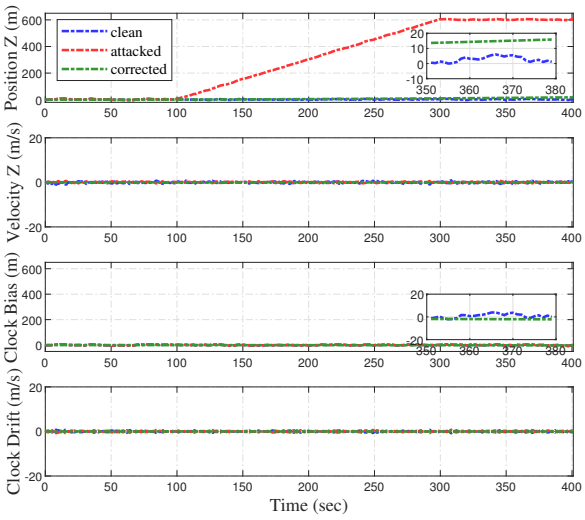


(a)

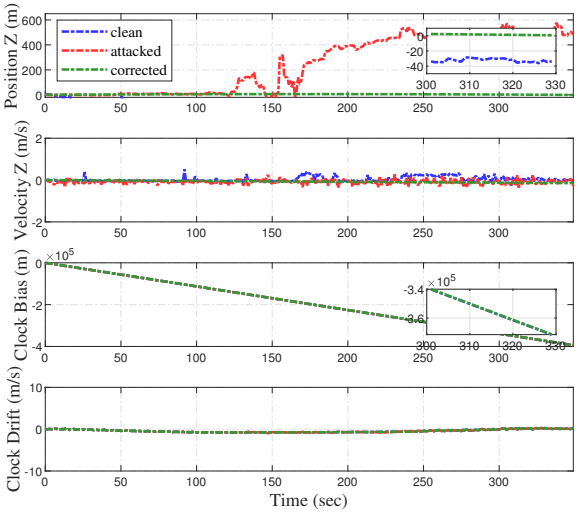


(b)

Figure 2: These figures depict the result of the optimization under third order TSA spoofing. In Figure 2a, red line shows the EKF estimation of modified data, blue shows the ground truth obtained by WLS, and green line shows the corrected estimates. Figure 2b indicates the captured attack on clock bias, whose sparsity is manifested on clock jerk domain.



(a)



(b)

Figure 3: These figures depict the result of the optimization under z-domain non-consistent spatial spoofing. The synthetic attack is applied on the TEXBAT *CS* scenario, after it is replayed over the SDR [fig. (a)] or the Huawei receiver [fig. (b)]. Due to the evident second order attack in Figure 3a, sparsity in jerk domain is guaranteed and captured by the optimization problem.

in Figure 3b have more noise than the SDR recordings shown in Figure 3a, both cases successfully captured and mitigated the attack using a tuning parameter of $\lambda_z = 10$. Further, the RMSE value for the z domain in the SDR case reduced from 389.22 meters to 6.03 meters; and the corresponding one for the Huawei receiver decreased from 357.37 meters to 32.77 meters. Other variables produced by the optimization such as z-velocity, clock bias, and drift, are estimated very closely to the ground truth.

3. Scenario 3: Joint Attack

The third spoofing scenario for stationary receiver is the joint TSA and spatial attack. Since TSA is supposed to be a *consistent* attack, we simulate an overall consistent joint attack with 600 meters maximum magnitude and third-order profile. The joint spoofing was only able to be rejected upon tuning of the peanalization terms. Figure 4 indicates that the algorithm successfully mitigates the attack on any domains of search. The RMSE value has also been reduced similarly to Scenario 1 and 2. This manifests that the developed algorithm can deny any types of spoofing attack whether that targets singular or multiple domains.

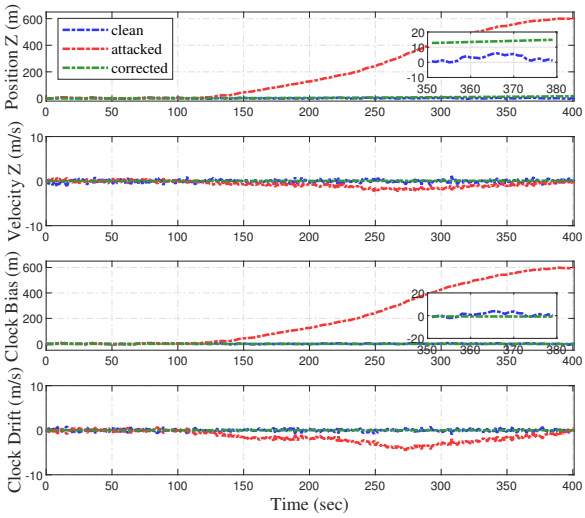


Figure 4: This figure shows the result of third order *consistent* joint attack against z-domain and clock timings.

VI. CONCLUSION AND SUMMARY

This paper develops a technique to mitigate joint spoofing against time and single position coordinate in stationary GPS receivers. To this end, a suitable linearization of the GPS measurement equations is presented and sparsity characteristics of attacks are reviewed. The technique relies on minimization of a multi-criterion objective that include penalization giving rise to sparse solutions. Three synthetic spoofing scenarios are successfully mitigated. The resulting RMSE values in each scenario is reduced significantly versus the EKF estimations, meanwhile the absolute error is small as well.

Our current work [17] focuses on expanding the model to receivers with slow dynamics, successful mitigation of joint attacks an all PVT domains (x, y, z, b, $\dot{x}$, $\dot{y}$, $\dot{z}$, and $\dot{b}$), analyzing the effects of different attack orders and degrees of consistency, and validation with authentic spoofed signals from the TEXBAT database, as opposed to synthetic attacks only.

VII. ACKNOWLEDGMENT

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

REFERENCES

[1] 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," *Proc. of the 25th Int. Tech. Meeting of the Sat. Div. of The Inst. of Nav. (ION GNSS 2012)*, p. 3569–3583, Nashville,TN, September 17–21 2012.

[2] D. P. Shepard, J. A. Bhatti, T. E. Humphreys, and A. A. Fansler, "Evaluation of Smart Grid and Civilian UAV Vulnerability to GPS Spoofing Attacks," in *Proc. 25th Int. Tech. Meeting of the Sat. Div. of The Inst. of Nav. (ION GNSS)*, Nashville, TN, Sept. 2012, pp. 3591–3605.

[3] P. Risbud, N. Gatsis, and A. Taha, "Vulnerability Analysis of Smart Grids to GPS Spoofing," *IEEE Transactions on Smart Grid*, vol. 10, no. 4, pp. 3535–3548, 2019.

[4] C. Ma, J. Yang, J. Chen, Z. Qu, and C. Zhou, "Effects of a Navigation Spoofing Signal on a Receiver Loop and a UAV

Spoofing Approach," *GPS Solutions*, vol. 24, 05 2020.

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

[6] A. Broumandan, A. Jafarnia-Jahromi, S. Daneshmand, and G. Lachapelle, "Overview of Spatial Processing Approaches for GNSS Structural Interference Detection and Mitigation," *Proceedings of the IEEE*, vol. 104, no. 6, pp. 1246–1257, 2016.

[7] E. Schmidt, N. Gatsis, and D. Akopian, "A GPS Spoofing Detection and Classification Correlator-Based Technique Using the LASSO," *IEEE Trans. on Aero. and Elect. Systems*, vol. 56, no. 6, pp. 4224–4237, 2020.

[8] F. Wang, H. Li, and M. Lu, "GNSS Spoofing Detection and Mitigation Based on Maximum Likelihood Estimation," *Sensors*, vol. 17, June 2017.

[9] B. Xu, Q. Jia, and L.-T. Hsu, "Vector Tracking Loop-Based GNSS NLOS Detection and Correction: Algorithm Design and Performance Analysis," *IEEE Trans. on Instrum. and Meas.*, vol. 69, no. 7, pp. 4604–4619, 2020.

[10] K. D. Wesson, J. N. Gross, T. E. Humphreys, and B. L. Evans, "GNSS Signal Authentication Via Power and Distortion Monitoring," *IEEE Trans. on Aero. and Elect. Systems*, vol. 54, no. 2, pp. 739–754, 2018.

[11] A. Broumandan, A. Jafarnia-Jahromi, and G. Lachapelle, "Spoofing Detection, Classification and Cancelation (SDCC) Receiver Architecture for a Moving GNSS Receiver," *GPS Solutions*, vol. 19, pp. 475–487, 2014.

[12] V. D. J. Nielsen and G. Lachapelle., "Effectiveness of GNSS Spoofing Countermeasure Based on Receiver CNR Measurements," *Int. Journ. of Nav. and Obs.*, vol. 2012, 2012.

[13] A. Khalajmehrabadi, N. Gatsis, D. Akopian, and A. F. Taha, "Real-Time Rejection and Mitigation of Time Synchronization Attacks on the Global Positioning System," *IEEE Trans. on Industrial Electronics*, vol. 65, no. 8, pp. 6425–6435, 2018.

[14] J. Lee, A. F. Taha, N. Gatsis, and D. Akopian, "Tuning-Free, Low Memory Robust Estimator to Mitigate GPS Spoofing Attacks," *IEEE Control Systems Letters*, vol. 4, no. 1, pp. 145–150, 2020.

[15] E. Schmidt, J. Lee, N. Gatsis, and D. Akopian, "Rejection of Smooth GPS Time Synchronization Attacks via Sparse Techniques," *IEEE Sensors Journal*, vol. 21, no. 1, pp. 776–789, 2021.

[16] P. Axelrad and R. G. Brown, "GPS Navigation Algorithms," in *Global Positioning System: Theory and Applications*, B. W. Parkinson, J. J. Spilker, P. Axelrad, and P. Enge, Eds., 1996, vol. I, ch. 9.

[17] J. Lee, E. Schmidt, N. Gatsis, and D. Akopian, "Detection and Mitigation of Spoofing Attacks Against Time Synchronization and Positioning," *submitted for publication*, 2021.

[18] F. Zhu, A. Youssef, and W. Hamouda, "Detection techniques for data-level spoofing in gps-based phasor measurement units," in *2016 International Conference on Selected Topics in Mobile Wireless Networking (MoWNeT)*, 2016, pp. 1–8.

[19] D. P. Shepard and T. E. Humphreys, "Characterization of Receiver Response to a Spoofing Attacks," in *Proceedings of the 24th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2011)*, Portland,OR, September 2011 2011, pp. 2608–2618.

[20] Z. Zhang, S. Gong, A. D. Dimitrovski, and H. Li, "Time Synchronization Attack in Smart Grid: Impact and Analysis," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 87–98, 2013.

[21] D. Miralles, N. Levigne, D. Akos, J. Blanch, and S. Lo, "Android Raw GNSS Measurements as the New Anti-Spoofing and Anti-Jamming Solution," in *Proc. of the 31st Int. Tech. Meeting of the Sat. Div. of The Inst. of Nav. (ION GNSS+ 2018)*, Miami, Floridar, September 2018 2018, pp. 334–344.

[22] E. Schmidt, D. Akopian, and D. J. Pack, "Development of a Real-Time Software-Defined GPS Receiver in a LabVIEW-Based Instrumentation Environment," *IEEE Trans. on Inst. and Meas.*, vol. 67, no. 9, pp. 2082–2096, 2018.

[23] "Raw GNSS Measurements; Android Developers." [Online]. Available: https://developer.android.com/guide/topics/sensors/gnss