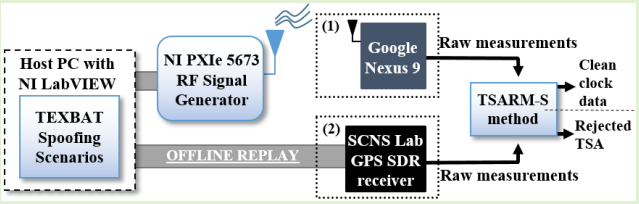
Rejection of Smooth GPS Time Synchronization Attacks via Sparse Techniques

Erick Schmidt, *Member, IEEE*, Junhwan Lee, Nikolaos Gatsis, *Member, IEEE*, and David Akopian, *Senior Member, IEEE*

***Abstract*—This article presents a novel time synchronization attack (TSA) model for the Global Positioning System (GPS) based on clock data behavior changes in a higher-order derivative domain. Further, TSA rejection and mitigation based on sparse domain (TSARM-S) is presented. TSAs affect stationary GPS receivers in applications where precise timing is required, such as cellular communications, financial transactions, and monitoring of the electric power grid. In the present work, higher-order derivatives of the clock bias and clock drift are monitored to reveal TSAs that show up as sparse spike-like events. The smoothness of the attack relates to the derivative order where the sparsity is observed. The proposed method jointly estimates a dynamic solution for GPS timing and rejects clock behavior changes based on such sparse events. An evaluation procedure is presented for two testbeds, namely a commercial receiver and a software-defined radio (SDR). Further, the proposed method is evaluated against real spoofing scenarios available online in the Texas Spoofing Test Battery (TEXBAT). Combined synthetic and real-data results show an average RMS clock bias error of 12.08 m for the SDR platform, and 45.74 m for the commercial device. Furthermore, the technique is evaluated against state-of-the-art mitigation techniques and in a spoofing-plus-multipath scenario for robustness. Finally, TSARM-S can be potentially optimized and implemented in commercial devices via a firmware upgrade.**



***Index Terms*— Global Positioning System (GPS), higher-order derivative, sparsity, spoofing detection, time synchronization attacks (TSAs).**

I. Introduction

THE convergence of radionavigation systems, such as the Global Positioning System (GPS), with diverse domain applications, such as emergency response, air traffic control, financial transactions, and smart power grids, manifests their thriving popularity and availability [1]. However, due to its open accessibility for civilian use, GPS coarse acquisition (C/A) codes are subject to malicious cyber-physical attacks [2].

GPS cyber-physical attacks have been categorized into jamming and spoofing. While jamming completely blocks authentic signals via high powered noise, spoofing exploits smart counterfeit signals to deceive and hijack a target receiver [3]. Once hijacked, the spoofer can inflict an erroneous position, velocity, and time (PVT) solution. Specifically, a Time Synchronization Attack (TSA) is a spoofing attack that alters the target receiver's clock offset. One particular example relates to Smart Grids, where a TSA can disrupt their operation. Smart Grids are electric power networks that provide readings from modern sensors for monitoring, control, and optimization of the network. These sensors are called Phasor Measurement Units (PMUs) and deliver precisely synchronized readings of voltages and currents across the network using GPS time [4]. An imprecise clock offset estimated by a PMU due to a cyber-physical attack could cause stability control failures and power outages [5], [6]. Under a successful TSA, Smart Grids become vulnerable to transmission line faults, voltage instability, and missed event locations [7].

Authors in [2] categorize spoofing attacks based on their complexity, i.e., simplistic, intermediate, and advanced. The simplistic attack relies on retransmission of a delayed GPS signal with augmented power to inflict time delays. Intermediate attack uses a receiver-spoofer device that is placed near the target receiver to retransmit smart GPS-like signals in a more covert fashion. Advanced spoofing uses several spoofer devices orchestrating a more elaborate synchronized attack. The intermediate attack is demonstrated as the most

Manuscript received July 5, 2020; accepted July 26, 2020. Date of publication August 4, 2020; date of current version December 4, 2020. This work was supported by the National Science Foundation under Grant ECCS-1719043. The associate editor coordinating the review of this article and approving it for publication was Prof. Huang Chen Lee. *(Corresponding author: Erick Schmidt.)*

The authors are with the Department of Electrical and Computer Engineering, The University of Texas at San Antonio, San Antonio, TX 78249 USA (e-mail: erickschmidtt@gmail.com; junhwan.lee@utsa.edu; nikolaos.gatsis@utsa.edu; david.akopian@utsa.edu).

Digital Object Identifier 10.1109/JSEN.2020.3014239

cost-effective in terms of implementation and can effortlessly synthesize a TSA. Additionally, cost-accessible software-defined radio (SDR) spoofers have successfully carried out attacks in such receivers as in [8] and [9]. The accessibility of SDR further rises awareness to harden receivers' abilities against spoofing attacks since conventional off-the-shelf receivers typically lack intermediate-to-advanced spoofing mitigation techniques [2].

Monitoring and detection of spoofing attacks is a well-researched topic; see e.g., [10]. However, much work is still to be done on spoofing rejection and mitigation. Existing techniques often offer detection of spoofing or jamming, but lack an actual correction countermeasure. A countermeasure should be able to detect and correct the attack while maintaining normal operation of the receiver with authentic PVT outputs. In particular, mitigation strategies can be organized in four categories [2]: (1) Advanced signal-processing-based techniques for standard single-antenna GNSS receiver that rely on power and automatic gain control (AGC) [11], complex correlation function outputs [12], conventional tracking loop [9], or vector-tracking loops (VTL) [13], [14]; (2) encryption-based defenses relying on encrypted GNSS signal keys that share a unique relationship between civilian open-access and military signals for spoofing detection [15]; (3) drift monitoring techniques that rely on unusual behavior changes in receiver position or clock based on receiver observables [16], [17], positioning filter metrics [18], and sparse techniques [19]–[21]; and (4) signal-geometry-based defenses which rely on multi-antenna systems for angle-of-arrival spoofer detection and mitigation [22], [23]. Further, receiver measurements and observables have been used in machine learning for spoofer detection. The authors in [24] train a support vector machine (SVM) with receiver autocorrelation outputs for spoofer peak classification. Similarly, the authors in [25] use a cross-correlation function of numerous observables as inputs for SVM classification. Additional discussions on spoofing countermeasures can be found in [2], [3], and [10].

This article complements the aforementioned spoofing detection and correction countermeasures. Specifically, the proposed optimization problem determines if an attack has occurred, and solves for the correct timing. Additionally, it introduces a cost-effective technique that can be implemented by means of an inexpensive firmware upgrade to a GPS receiver. The proposed method relies on a dynamic model of the clock bias and clock drift for a stationary receiver. It specifically falls in the drift monitoring mitigation category according to the previously mentioned categorization [2]. Moreover, we focus on a single-antenna single-receiver architecture as opposed to complex multi-receiver architectures [13], [26], [27]. Finally, this work addresses TSA detection and rejection so that reliable timing can be provided to diverse GPS time related applications. For additional discussion on relevant time-dependent applications and how these can be affected by a TSA, the reader is directed to [1], [5], [6], and [7].

A. Related Work

The related work presented herein primarily features sparse-domain detectors. Such formulations rely on optimization problems that include ℓ_1-penalty terms [28]. The premise is that the ℓ_1 penalty provides a sparse vector (that is, a vector with few nonzero entries) indicating the anomalies. However, the related literature differs in the domain in which sparsity is revealed, resulting in different types of interference or attacks that can be identified. The present work leverages sparsity in higher-order derivatives of the attack, which has not been exploited before. The differences with the prior art and the advantages of the proposed approach are explained in the sequel.

Different from previous works that detect and mitigate integrity anomalies in select parallel receiver channels [17], [20], [21], this work mitigates TSAs even in the absence of integrity anomalies, whereby the smart spoofer manipulates all the channels synchronously. The work in [17] relies on advanced receiver autonomous integrity monitoring (RAIM) techniques to detect anomalies per channel, and for every PVT computation. In fact, most RAIM-based techniques rely on anomaly checking per iteration, which entails expensive computations.

In terms of dynamic modeling, the work in [18] monitors the Kalman Filter innovations for potential spoofer attacks, thus relying on simple metrics computed from sequential data averaged over a sliding window. The TSA model in this work is similar to the one in [19] in that both use a two-state model for the clock. However, the model in [19] is not general enough to include the smoothest of the attacks; in [19], only Type I and Type II attacks are defined. The work in [19] jointly computes a dynamic PVT solution and accumulates variation metrics, which are then accrued to gather the correction. It relies on small spoofer alterations accumulated over time thus requiring a correction stage. On the other hand, the proposed method jointly computes the PVT solution while observing higher-order derivatives, where the clock behavior change is detected as a sparse (i.e., spike-like) event. If a sparse event is detected, the proposed method rejects the atypical behavior from the authentic clock data output. The optimization problem in the present work is also different from [19] in that it penalizes the ℓ_1-norm of the second-derivative of the attack on clock drift. As demonstrated in the article, this penalty turns out to be sufficient to capture smooth attacks. In addition, the proposed method includes an additional outlier variable that can also capture inconsistent spoofers. Thus, the method automatically rejects both unexpected behavior changes and anomalies in measurement integrity, as discussed in Section III-A.

Different from the proposed method, sparse methods have also been applied on the pseudorange residuals after PVT computation to detect anomalies in the measurements [20]. Similarly, the work in [21] follows multi-frequency observables for enhanced outlier detection. An important assumption in such sparse estimation is that a small number of the visible satellites are corrupted, which entails sparsity in the measurement residual domain. While [20] uses sparse processing for outlier detection as an indication of integrity failure, the present work exploits sparsity in the overall receiver behavior change for all visible satellites. In other words, the proposed technique relies on sequential data observations,

as opposed to snapshot monitoring, and is applicable when all visible satellites are simultaneously and consistently spoofed.

Finally, many state-of-the-art techniques based on sparse estimation focus on multipath (MP) detection and mitigation [20], [21]. While MP is similar to spoofing attacks, some differences are worth noting: (a) MP effects appear arbitrarily while spoofing is more consistent over time; (b) MP generally affects some satellite and are channel-specific, while smart spoofing attacks affect all channels concurrently and synchronously; and (c) spoofing attacks are two orders of magnitude more hazardous in terms of PVT deviations, e.g., a meaningful TSA may inflict 8000 m, or equivalently, 26.67 μs bias error in the PMU clock [29].

B. Contributions

Previous works have attempted to classify TSAs based on how smoothly (or abruptly) the spoofer attack is induced onto the receiver clock offset [30]; however, such terms necessitate a precise mathematical definition. In this work, we define the smoothness of the attack based on the order of the derivative in which the attack appears to be sparse. The sparsity in the clock bias derivatives of various orders are further leveraged to detect the attack as a sparse spike-like event. Based on the sparse derivative order, we categorize the attacks by their order, e.g., a *third order attack*.

The TSAs previously reported in the literature can be detected using the *third order attack* model of this article. In particular, the authors in [19] defined Type I and II attack models, which are subsumed by the more general framework in the present article and can be identified using the proposed technique while achieving better mitigation results. This work develops a mitigation framework for up to *third order attacks*, which is sufficient for most realistic TSAs detailed in the literature, but the proposed framework readily extends to higher orders. Similarly, the proposed technique can detect experimentally demonstrated spoofing attacks reported in [31], as will be seen in Section VI-B. In the following, the technique of this article is referred to as TSA rejection and mitigation based on sparse-domain (TSARM-S).

The contributions of this article are as follows:

1) Novel modeling of TSAs based on behavioral change analysis in clock data derivative domains of various orders is introduced by observing the derivative order in which sparsity shows up. The model allows for the attack to preserve its measurement integrity, which renders it undetected by traditional RAIM techniques.
2) Based on 1), we propose a dynamic model that jointly estimates the clock bias and drift, and rejects a potential TSA by transforming state variables into a higher-order sparse-domain where the TSA is detected and rejected. By transforming into a higher-order derivative, an unmodeled clock behavior appears as a spike-like event, thus leveraging sparse-based detection.
3) The proposed model identifies and rejects the spoofing signatures in the clock data directly without the need of a correction stage, i.e., the output vector is split into the estimated authentic clock data and the spoofer attack. Additionally, the proposed method captures measurement integrity discrepancies from inconsistent spoofers.
4) The method is tested using real data corresponding to raw measurement outputs from two platforms: an in-house SDR at UTSA [32], and a Google Nexus 9 Tablet. Specifically, synthetic attacks are applied to real data recordings, and in addition, two real-data scenarios from The Texas Spoofing Test Battery (TEXBAT) are replayed over-the-air (OTA). Furthermore, a comparison with a spoofing plus MP scenario is evaluated.

The article is organized as follows. Section II introduces the GPS dynamic model. Section III presents the novel TSA modeling. Section IV presents the proposed spoofing mitigation technique, TSARM-S. A testing methodology is described in Section V. Section VI presents simulation results and discussion. Finally, Section VII concludes the article and points to future work.

II. GPS PVT Dynamic Model

In this section, we briefly describe the radionavigation method used in GPS. To resolve the user's position, the GPS receiver uses satellite ranging signals which also contain satellite orbit parameters such as Ephemeris data to estimate the satellites' positions during location estimation [33]. The satellites serve as beacons for trilateration using satellite-to-user ranges measured by the receiver. Without loss of generality, the user (GPS receiver) position can be represented in 3D Earth-centered Earth-fixed (ECEF) coordinates as $\mathbf{p}_u = [x_u, y_u, z_u]^T$ (in m). Similarly, the position of the n-th satellite for $n = 1, 2, \ldots, N$ during each satellite transmit time t_n is represented as $\mathbf{p}_n = [x_n(t_n), y_n(t_n), z_n(t_n)]^T$ (also in m). Further, we denote the signal receive time at the receiver as t_R. The true range between user and the satellite can be defined as $d_n = \|\mathbf{p}_n - \mathbf{p}_u\|_2$, where $\|\cdot\|_2$ denotes the ℓ_2-norm. However, the range is not known and can be expressed as the difference of the transmit and receive time as $d_n = c\left(t_R^{GPS} - t_n^{GPS}\right)$, where t_n^{GPS} and t_R^{GPS} are the accurate transmit and receive times, respectively. By introducing an offset in the measured user time of reception modeling the receiver clock inaccuracy as $t_R = t_R^{GPS} + b_u$, and likewise for the satellite transmit time as $t_n = t_n^{GPS} + b_n$, the receiver computes biased ranges called pseudoranges given by $\rho_n = c(t_R - t_n)$, where c is the speed of light. One can rewrite the pseudorange equation by using the previous two definitions of d_n as:

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

where $\mathbf{p}_n$ is the satellite position at transmit time, $\mathbf{p}_u$ is the user position at receive time, b_u and b_n are the user and satellite clock offsets (in s), respectively, and ϵ_{ρ_n} models combined errors due to atmospheric delays, thermal noise, etc. (in m). The pseudoranges, satellite locations, and satellite clock offsets are known or computed by the receiver, while $(\mathbf{p}_u, b_u)$ are estimated using (1).

Similarly, the receiver can measure the Doppler frequency shift (residual) that is formed on top of the carrier frequency due to the relative difference between the satellite velocity, $\mathbf{v}_n$, and the user velocity, $\mathbf{v}_u$, also expressed in 3D ECEF coordinates. This estimated Doppler residual is related to the rate at

which the pseudorange measurement varies over time, denoted as $\dot{\rho}_n$ (in m/s). The pseudorange rate is then represented as:

$$\dot{\rho}_n = (\mathbf{v}_n - \mathbf{v}_u)^T \frac{\mathbf{p}_n - \mathbf{p}_u}{\|\mathbf{p}_n - \mathbf{p}_u\|} + c\left(\dot{b}_u - \dot{b}_n\right) + \epsilon_{\dot{\rho}_n} \tag{2}$$

where $\mathbf{v}_n$ is the satellite velocity obtained from the navigation message, $\mathbf{v}_u$ is the user velocity, $\dot{b}_u$ and $\dot{b}_n$ are the user and satellite clock drifts (in s/s), and $\epsilon_{\dot{\rho}_n}$ is the modeled noise. Similarly to (1), the unknowns to be estimated from (2) are $\left(\mathbf{v}_u, \dot{b}_u\right)$.

For a conventional low-dynamics receiver, the PVT solution aims to solve for user position, velocity, and the receiver's clock bias and clock drift. This totals 8 unknown variables which are typically computed via Weighted Least Squares (WLS) in a snapshot manner [34], or dynamically by means of an Extended Kalman filter (EKF). The dynamic state equation of an 8-state EKF amounts to a random walk model as follows [35, Ch. 9]:

$$\mathbf{x}_k = \underbrace{\begin{pmatrix} \mathbf{\Phi} & \mathbf{0} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{\Phi} & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{\Phi} & \mathbf{0} \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \mathbf{\Phi} \end{pmatrix}}_{\mathbf{F}_k} \mathbf{x}_{k-1} + \mathbf{w}_k \tag{3}$$

where $\mathbf{x} \equiv \left[\, x_u \;\; \dot{x}_u \;\; y_u \;\; \dot{y}_u \;\; z_u \;\; \dot{z}_u \;\; cb_u \;\; c\dot{b}_u \,\right]^T$ is the state vector, cb_u and $c\dot{b}_u$ are the user clock bias (in m) and clock drift (in m/s), $\mathbf{p}_u = [x_u, y_u, z_u]^T$ is the user location where the components are in meters (m), $\mathbf{v}_u = [\dot{x}_u, \dot{y}_u, \dot{z}_u]^T$ denotes user velocity in m/s, $\mathbf{w}_k$ is the process noise, and $\mathbf{\Phi}$ is a state-transition matrix for the discrete time instant k corresponding to each position-velocity pair as follows:

$$\mathbf{\Phi} = \begin{bmatrix} 1 & \Delta t \\ 0 & 1 \end{bmatrix} \tag{4}$$

where Δt is the discretization time interval for each measurement. The measurements given by equations (1) and (2) for pseudoranges and pseudorange rates are used as inputs to the 8-state EKF based on (3) for the dynamic PVT solution. Note that (1) and (2) model different observables from different circuitry sources measured by the receiver, which are respectively extracted from code-phases and Doppler residuals [33]; however, they are used jointly for the navigation computation.

III. Novel TSA Modeling

In this section, we present a novel model for TSAs that covers a wide range of attacks. The proposed concept interprets smooth attacks as the receiver's clock dynamic behavior change. The change is detected by inspecting higher order derivatives of the estimated clock data sequence. It is demonstrated that the TSA manifests itself as a sparse event such as a combination of few spikes at one of the derivative clock signals. The smoother the attack, the higher the order of the derivative is required to detect the sparse indication of behavior change. Thus, the TSAs are systematized based on such higher-order clock signal derivative domains. We begin by listing some self-consistent spoofer requirements [2].

A. Measurement Integrity Checks

In this subsection, we define two measurement integrity checks associated with the previously defined dynamic model. We assume these integrity checks are incorporated by the spoofer attacks to avoid detection using straightforward techniques.

The attack on pseudoranges and pseudorange rates is modeled as follows:

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

where $\rho_{n,s}$ and $\dot{\rho}_{n,s}$ are the spoofed pseudorange (in m) and pseudorange rate (in m/s) measurements for the n-th satellite, and s_ρ and $s_{\dot{\rho}}$ are the spoofing alterations on pseudoranges and pseudorange rates, respectively. TSAs attempt to steer the user clock bias and clock drift without altering the user position and velocity. To achieve this, the spoofer alterations s_ρ and $s_{\dot{\rho}}$ must be the same in magnitude for all visible satellites. In this case, although the spoofer alterations are the attacks on pseudoranges and pseudorange rates, these attacks will be reflected on the clock bias and drift of the target receiver, respectively [19], [31]. This type of spoofer is categorized as an intermediate attack following [2] and is considered throughout this work. The aforementioned attacks are also not visible to rudimentary schemes that check measurement integrity, such as RAIM [36].

As stated in Section II, the measurement observables, ρ_n and $\dot{\rho}_n$, come from different circuitry parts of the receiver; nonetheless, such measurements should have an integrity due to their physical interpretation. Thus, the first test to determine if measurement integrity is maintained between the pseudoranges and pseudorange rates is defined as follows:

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

Note that the derivative relationship in (6) also holds for the spoofed measurements in (5), namely $\rho_{n,s}$ and $\dot{\rho}_{n,s}$, as well as the spoofer alterations, s_ρ and $s_{\dot{\rho}}$. In fact, this derivative based relationship between the spoofer alterations is assumed as part of a smartly devised attack referenced in this work.

Similarly, because TSAs reflect on the clock bias and clock drift after the PVT computation, the second integrity check is defined as follows:

$$\hat{c\dot{b}}_u[k] \approx \frac{\hat{cb}_u[k] - \hat{cb}_u[k-1]}{\Delta t} \tag{7}$$

where $\hat{b}_u$ and $\hat{\dot{b}}_u$ are the estimated clock bias and drift produced by WLS.

By considering that (6) and (7) are both satisfied for a smart self-consistent TSA, the alterations s_ρ and $s_{\dot{\rho}}$ are directly reflected in the clock bias and clock drift WLS outputs. Thus, without the loss of generality, the spoofer is assumed to perpetrate a TSA with two integrity considerations:

1) The alterations on pseudoranges and pseudorange rates are applied on all visible channels, simultaneously, and each with the same magnitude across all the channels (otherwise it's understood as pseudorange and pseudorange rate having the same magnitude). This inflicts

a deviation on the clock bias and clock drift while avoiding per-channel RAIM detection schemes.

2) The spoofing attack is performed while maintaining measurement integrity checks given by (6) and (7).

To summarize, failure of the attack to satisfy (6) or (7) would be the basis for quick and straightforward detection. The next section focuses on the characteristics of smart attacks that will enable their rejection and mitigation, even when (6) and (7) are satisfied.

B. Higher-Order Attacks

We define higher-order *derivatives* of the attack on the pseudorange, $s_\rho[k]$, to categorize the attacks according to the order in which the attack appears as sparse. Table I lists higher order user clock modeling for TSAs. Such categories are derived from a classical physical interpretation of an object displacement over time, where the clock bias corresponds to the position (in m), the clock drift is velocity (in m/s), etc. This should not be confused with GPS dynamic clock modeling such as in [37] and [38]; rather, we use such definitions to facilitate attack detection.

We define the following equations related to $s_\rho[k]$ for velocity, acceleration, and jerk attacks, respectively:

$$\begin{aligned} s_{\dot\rho}[k] &= \frac{s_\rho[k] - s_\rho[k-1]}{\Delta t} \\ s_{\ddot\rho}[k] &= \frac{s_{\dot\rho}[k] - s_{\dot\rho}[k-1]}{\Delta t} \\ s_\rho[k] &= \frac{s_{\ddot\rho}[k] - s_{\ddot\rho}[k-1]}{\Delta t} \end{aligned} \tag{8}$$

Further, the following categories are defined: a) *first order attack*, b) *second order attack*, and c) *third order attack*. A *first order attack* occurs when the sequence $s_{\dot\rho}[k]$ is sparse; a *second order attack* occurs when $s_{\ddot\rho}[k]$ is sparse, but not $s_{\dot\rho}[k]$; a third order attack occurs when $s_\rho[k]$ is sparse, but not $s_{\ddot\rho}[k]$. The attack appears increasingly smooth as the order of the attack is higher, e.g., a *third order attack* is smoother than a *second order attack*. These categories do not define how the spoofer attack is devised, rather they define the order where the sparse event occurs and enable detection and rejection of the attack, as will be developed in Section IV.

Fig. 1 shows examples of *first, second,* and *third order attacks* from top to bottom. The *first order attack* (top) appears as a step function attack on the clock bias with its derivative being a sparse-peak at the clock drift. The *second order attack* appears as a peak on the clock acceleration, a step on the clock drift, and a (smooth) ramp on the clock bias. An even smoother clock bias is seen on the *third order attack,* where the sparse peak appears on the clock jerk. Finally, it can be seen that the highest order attack encompasses lower-order attacks, e.g., the *first order attack* is also sparse on the third order. This can be useful in terms of detection.

Several attacks reported in literature are defined as Type I and II attacks [16], [19]. However, the proposed TSA modeling amounts to a broader framework that incorporates previous definitions. It can be seen in Fig. 1 that Type I attack is in fact a *first order attack*, and Type II attack is a *third order attack*. However, the *second order attack* is not

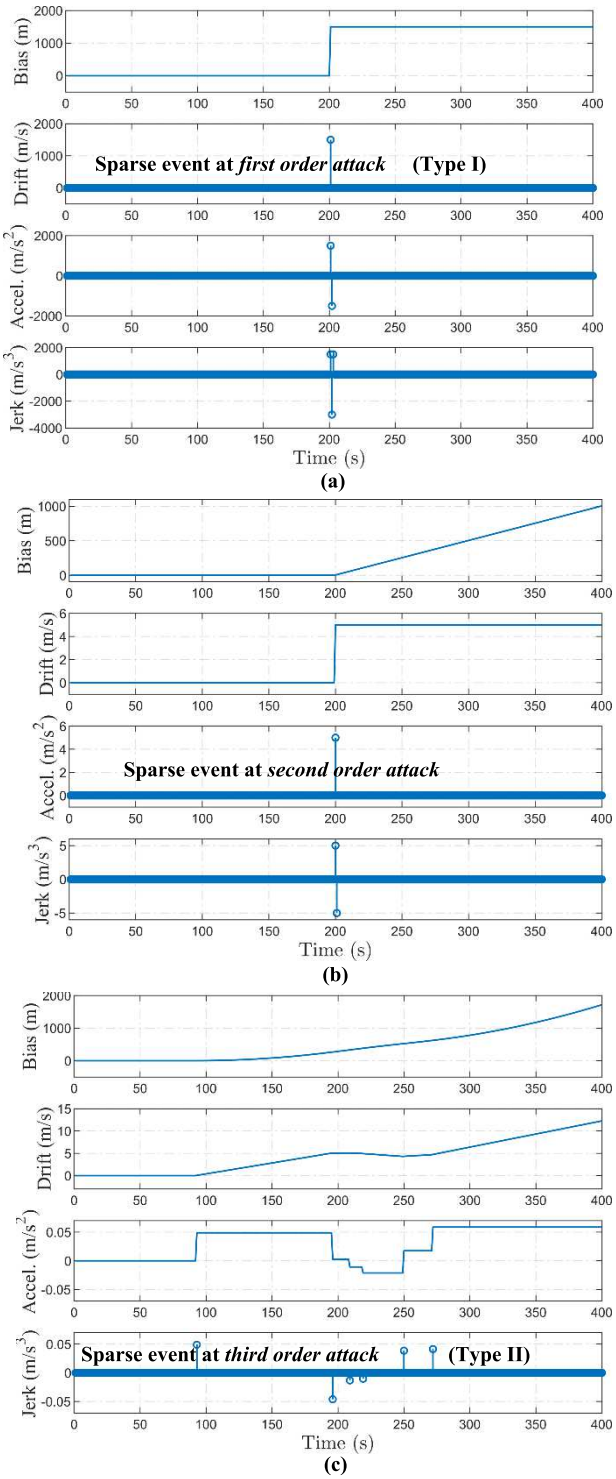


Fig. 1. TSA modeling for higher order derivative for (a) a *first order attack*, (b) a *second order attack*, and (c) a *third order attack*.

previously defined. Table II shows the relationship between these previous definitions and the new TSA models.

In this analysis, the higher the order where the sparse spike-like events appear, the subtler the attack on the clock bias becomes. Hence, while the significance of the attack smoothness has been noted in the literature [30], a systematic definition of *smoothness* is formulated in the present work. It is also mentioned in the literature that the smoothness of

TABLE I
HIGHER ORDER USER CLOCK MODELING FOR TSAs

The TSA exhibits itself as a sparse event on	Attack (derivative) order	Units
Clock bias	0th order	m
Clock drift (velocity)	1st order	m/s
Clock acceleration	2nd order	m/s^2
Clock jerk	3rd order	m/s^3

TABLE II
TSA MODELING COMPARISON WITH PREVIOUS ATTACK TYPES [19]

New attack category	Previously defined attack category	Shape
First order attack	Type I attack	Step
Second order attack	N/A	Ramp
Third order attack	Type II attack	Gradual

the attack on the clock bias is relevant for phase measurement units (PMUs) in smart grids [5], [6]. Finally, the TSA analysis can be readily extended to even higher orders, e.g., clock snap (fourth order) and crackle (fifth order). Based on the existing literature, the third order model (clock jerk) covers enough intermediate spoofing attacks for practical purposes.

IV. TSA REJECTION VIA A SPARSE TECHNIQUE

This section introduces a joint dynamic model and ℓ_1-minimization problem which incorporates TSA models up to a third-order derivative (clock jerk). The dynamic model of Section IV-A introduces the spoofing attack in the measurement equations. Additionally, the optimization formulated in Section IV-B penalizes the outlier based on sparse-domain TSA models previously discussed in Section III-B.

A. Dynamic Model on User Clock

The dynamic model presented here pertains to a stationary receiver and assumes that the user position $\mathbf{p}_u$ is known and the user velocity $\mathbf{v}_u$ is zero [16], [19]. Thus, the model is simplified to estimate only the user clock bias and clock drift as follows:

$$\underbrace{\begin{pmatrix} cb_u[k] \\ c\dot{b}_u[k] \end{pmatrix}}_{\mathbf{x}_k} = \underbrace{\begin{pmatrix} 1 & \Delta t \\ 0 & 1 \end{pmatrix}}_{\mathbf{F}_k} \underbrace{\begin{pmatrix} cb_u[k-1] \\ c\dot{b}_u[k-1] \end{pmatrix}}_{\mathbf{x}_{k-1}} + \underbrace{\begin{pmatrix} cw_b[k] \\ cw_{\dot{b}}[k] \end{pmatrix}}_{\mathbf{w}_k} \quad (9)$$

where $\mathbf{x} \equiv \left[\, cb_u \; c\dot{b}_u \,\right]^T$ is the 2-state vector, $\mathbf{F}_k$ is the state transition matrix, and $\mathbf{w}_k$ is the process noise vector considered as white Gaussian noise with covariance matrix $\mathbf{Q}_k$ related to the crystal oscillator of the user receiver [34].

The spoofer alterations are introduced in the state vector to capture the state estimate along with a potential attack. Specifically, we define $\mathbf{s}_k = \left[cs_b[k], cs_{\dot{b}}[k]\right]^T$ as the spoofer alteration vector, where s_b and $s_{\dot{b}}$ are the attacks on the clock bias and clock drift, respectively. Based on assumptions from Section III-B, it holds that $s_\rho \equiv cs_b$ and $s_{\dot{\rho}} \equiv cs_{\dot{b}}$. Additionally, we define $\boldsymbol{\rho}[k] = \left[\rho_{1,s}[k], \ldots, \rho_{N,s}[k]\right]^T$, and $\dot{\boldsymbol{\rho}}[k] = \left[\dot{\rho}_{1,s}[k], \ldots, \dot{\rho}_{N,s}[k]\right]^T$, as the pseudorange and pseudorange rate measurement vectors, respectively. We then write the measurement equation by combining (1), (2), and (5) as (10), show at the bottom of the next page, where $\mathbf{c}_k$ is a known sequence that relates to the known user position and velocity (which is zero), satellite position, velocity and clock corrections, ϵ_k is the zero mean Gaussian measurement noise with covariance matrix $\mathbf{R}_k = diag\left(\sigma^2_{\rho_1}[k], \ldots, \sigma^2_{\rho_N}[k], \sigma^2_{\dot{\rho}_1}[k], \ldots, \sigma^2_{\dot{\rho}_N}[k]\right)$, and $\sigma^2_{\rho_n}$ and $\sigma^2_{\dot{\rho}_n}$ are the noise variances of respectively the pseudorange and pseudorange rate for the n-th satellite [34]. Equations (9) and (10) can be written as:

$$\begin{aligned} \mathbf{x}_k &= \mathbf{F}_k \mathbf{x}_{k-1} + \mathbf{w}_k \\ \mathbf{z}_k &= \mathbf{H}_k \mathbf{x}_k + \mathbf{H}_k \mathbf{s}_k + \boldsymbol{\epsilon}_k \end{aligned} \quad (11)$$

where $\mathbf{z}_k = \mathbf{y}_k - \mathbf{c}_k$ is called the measurement residual.

B. TSARM-S Problem Formulation

TSARM-S focuses on sparse-like behavior changes occurring on a higher-order derivative. To achieve this, we introduce an outlier detection scheme in the measurement model and define an ℓ_1-minimization problem based on (11) [28]. By leveraging the defined TSA model in Section III-B, specifically up to the clock jerk smoothness level of detection, we define the minimization problem as follows. Let $\mathbf{x} = [\mathbf{x}_1, \ldots, \mathbf{x}_K]^T$ and $\mathbf{s} = [\mathbf{s}_1, \ldots, \mathbf{s}_K]^T$ be the optimization variables by respectively collecting the vectors $\mathbf{x}_k$ and $\mathbf{s}_k$ for time instants $k = 1, \ldots, K$. Thus, we present the problem in compact form as follows:

$$\begin{aligned} \left(\hat{\mathbf{x}}, \hat{\mathbf{s}}\right) = \underset{\mathbf{x},\mathbf{s}}{\operatorname{argmin}} \Bigg\{ & \frac{1}{2} \sum_{k=1}^{K} \|\mathbf{z}_k - \mathbf{H}_k \mathbf{x}_k - \mathbf{H}_k \mathbf{s}_k\|^2_{\mathbf{R}_k^{-1}} \\ & + \frac{1}{2} \sum_{k=1}^{K} \|\mathbf{x}_k - \mathbf{F}_k \mathbf{x}_{k-1}\|^2_{\mathbf{Q}_k^{-1}} + \lambda \left\|\mathbf{D}_2 \mathbf{s}'\right\|_1 \Bigg\} \end{aligned} \quad (12)$$

where $\|\mathbf{x}\|^2_{\mathbf{M}} = \mathbf{x}^T \mathbf{M} \mathbf{x}$, $\hat{\mathbf{x}} = \left[\hat{\mathbf{x}}_0, \ldots, \hat{\mathbf{x}}_K\right]^T$ are the estimated states, $\hat{\mathbf{s}} = \left[\hat{\mathbf{s}}_1, \ldots, \hat{\mathbf{s}}_K\right]^T$ are the estimated spoofer alterations, $\mathbf{s}' = \left[cs_{\dot{b}}[1], \ldots, cs_{\dot{b}}[k]\right]^T$ is a sub-vector of $\mathbf{s}$ which only contains the alterations on the clock drift, λ is a tuning parameter, and $\mathbf{D}_2$ is a $K \times K$ second order total variation matrix applied to K spoofer alterations of the clock drift $cs_{\dot{b}}$ in $\mathbf{s}'$ and is defined as follows [39]:

$$\mathbf{D}_2 = \begin{pmatrix} -2 & 1 & 0 & \ldots & 0 \\ 1 & -2 & 1 & \ldots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \ldots & 1 & -2 & 1 \end{pmatrix} \quad (13)$$

The first term in (12) comes from the measurement equation which contains the state and attack estimates. At the same time, the second term defines the EKF random walk model, and finally the third term promotes sparsity on the jerk of the attack by applying a second order total variation matrix on the attack velocity. If an attack is present, that is, if sparse peaks are found on the third-order derivative (or clock jerk), the minimization rejects the clock alterations from the state vector $\hat{\mathbf{x}}$, and places them in vector $\hat{\mathbf{s}}$ instead. In other words, there is no need for a correction stage, as rejection occurs

automatically, given the proper tuning of λ to promote sparsity. The sparsity is promoted by penalizing the ℓ_1-norm of the clock jerk of the attack when adjusting λ. In other words, the higher the λ, the more sparse the $\left\|\mathbf{D}_2\mathbf{s}'\right\|_1$ term will appear, thus increasing the sensitivity in detection and rejection of non-modeled behavior changes in the sparse-domain. This is achieved altogether while estimating the user clock dynamic model. Finally, the value of λ must be tuned for each receiver, as it indirectly depends on the hardware that produces the measurements and related covariances.

Additionally, the first and second term jointly constrain the measurement integrity in the user clock bias and clock drift, corresponding to equations (6) and (7). If the measurement integrity does not hold for the dynamical model in (12), i.e. the second term, the outlier (alteration) variables in the first term, s_b and $s_{\dot{b}}$, absorb such erratic behaviors. This means that the proposed model is able to capture the attack as either a measurement integrity failure, or as a sparse event regardless of the TSA. Therefore, the functionality of the proposed method is three-fold:

1) A dynamic model of the user clock data based on the first and second term of (12);
2) An attack detection and automatic capturing based on the first and third term of (12), and based on the third order TSA modeling from Section III-B, and the promoted sparsity; and
3) A measurement integrity detection that is absorbed by the alteration variables s_b and $s_{\dot{b}}$.

Finally, the optimization problem in (12) is a quadratic program which can be solved with off-the-shelf solvers such as CVX [40]. Additionally, numerical optimization methods for such quadratic programs can run on the receiver's CPU and memory [41]. The next section presents the testing methodology and numerical results achieved from (12).

V. Testing Methodology on TSAs

This section presents a testing methodology to evaluate the rejection and mitigation of TSAs with the TSARM-S technique. The Android Location Team from Google recently made available GNSS raw measurements to study high accuracy positioning techniques relevant to mass market applications [42]. They provide an Android application *GNSS Logger* along with MATLAB post-processing scripts to obtain pseudoranges and pseudorange rates from select Android devices. This provides an opportunity for commercial device testing on well-known spoofing testbeds such as TEXBAT [31]. Also, increasing in popularity are real-time SDR solutions [32], which provide access to the receiver chain from baseband to the navigation domain.

A. Testbed Setup

In this work, we present a study on the effects of previously discussed TSAs (see Section III-B) on an integrated testbed at the University of Texas at San Antonio's (UTSA) Software Communication & Navigation Systems (SCNS) Lab.

This study includes two main platforms for spoofing research along with real spoofing TEXBAT scenarios: (a) a commercial-grade Android-based Google Nexus 9 tablet with an embedded GPS chipset, providing raw measurements and MATLAB post-processing scripts from [42]; and (b) an in-house real-time LabVIEW-based single-frequency GPS L1 SDR receiver previously reported in [32], which provides raw measurements in a similar fashion. The integrated testbed for both receivers (a) and (b) can be seen in Fig. 2. Three TEXBAT static scenarios are explored, namely spoofing scenarios 2 and 3, and a clean static scenario for comparison purposes [31]. TEXBAT scenario 2 implements an overpowered time push attack that deals a 600 m offset on the clock bias. Similarly, scenario 3 deals a 600 m attack but in a power-matched manner. For this work, both attacks are considered TSAs. For further descriptions of these scenarios, the reader is directed to [31].

We assess the testbed in two steps: first, we inject synthetic *first, second* and *third order TSAs* on pseudoranges and pseudorange rates for the TEXBAT clean static scenario; and second, we process TEXBAT scenarios 2 and 3 as real spoofing attacks. The synthetic simulations provide worst-case scenarios where the attacks occur with negligible losses in carrier and code alignment, i.e., a perfect spoofing attack. Inversely, the real spoofing attacks from TEXBAT scenarios 2 and 3 provide a more realistic setup.

$$\underbrace{\begin{pmatrix}\rho\,[k]\\ \dot{\rho}\,[k]\end{pmatrix}}_{\mathbf{y}_k}=\underbrace{\begin{pmatrix}\mathbf{1}_{N\times 1} & \mathbf{0}_{N\times 1}\\ \mathbf{0}_{N\times 1} & \mathbf{1}_{N\times 1}\end{pmatrix}}_{\mathbf{H}_k}\underbrace{\begin{pmatrix}cb_u\,[k]\\ c\dot{b}_u\,[k]\end{pmatrix}}_{\mathbf{x}_k}+\underbrace{\begin{pmatrix}\mathbf{1}_{N\times 1} & \mathbf{0}_{N\times 1}\\ \mathbf{0}_{N\times 1} & \mathbf{1}_{N\times 1}\end{pmatrix}}_{\mathbf{H}_k}\underbrace{\begin{pmatrix}cs_b\,[k]\\ cs_{\dot{b}}\,[k]\end{pmatrix}}_{\mathbf{s}_k}$$
$$+\underbrace{\begin{pmatrix}\|\mathbf{p}_1\,[k]-\mathbf{p}_u\,[k]\|_2-cb_1\,[k]\\ \vdots\\ \|\mathbf{p}_N\,[k]-\mathbf{p}_u\,[k]\|_2-cb_N\,[k]\\ (\mathbf{v}_1\,[k]-\mathbf{v}_u\,[k])^T\cdot\dfrac{\mathbf{p}_1\,[k]-\mathbf{p}_u\,[k]}{\|\mathbf{p}_1\,[k]-\mathbf{p}_u\,[k]\|_2}-c\dot{b}_1\,[k]\\ \vdots\\ (\mathbf{v}_N\,[k]-\mathbf{v}_u\,[k])^T\cdot\dfrac{\mathbf{p}_N\,[k]-\mathbf{p}_u\,[k]}{\|\mathbf{p}_N\,[k]-\mathbf{p}_u\,[k]\|_2}-c\dot{b}_N\,[k]\end{pmatrix}}_{\mathbf{c}_k}+\underbrace{\begin{pmatrix}\epsilon_{\rho_1}\\ \vdots\\ \epsilon_{\rho_N}\\ \epsilon_{\dot{\rho}_1}\\ \vdots\\ \epsilon_{\dot{\rho}_N}\end{pmatrix}}_{\boldsymbol{\epsilon}_k} \tag{10}$$

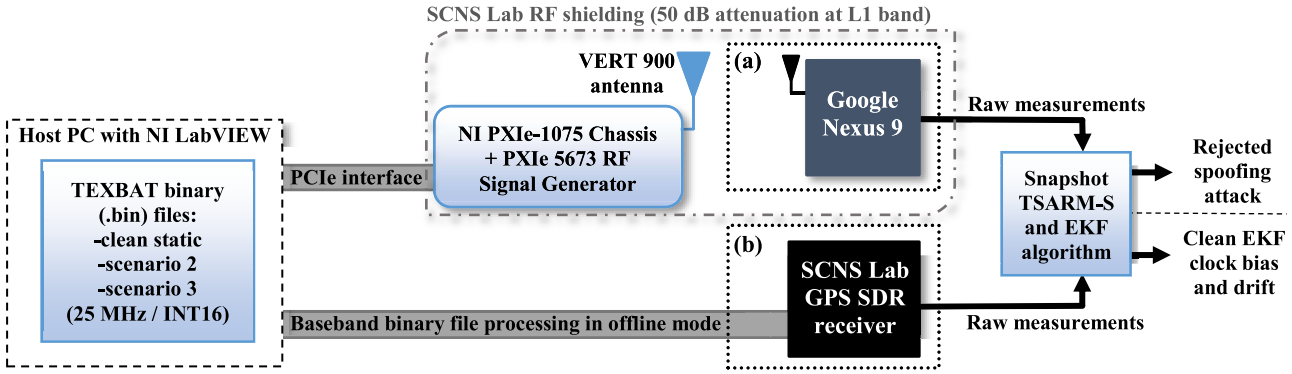


Fig. 2. Testbed for TEXBAT testing on TSARM-S with (a) record-and-replay on Google Nexus 9, and (b) baseband offline processing on a GPS SDR receiver.

TABLE III
TEXBAT SCENARIOS AND SYNTHETIC ATTACKS PARAMETERS

	Parameter	Value
TEXBAT scenarios 2 and 3	Recording length (s)	241
	GPS week[a]	1705
	GPS sec[a]	477986 to 478226
	SVs for baseband processing	3, 6, 10, 13, 16, 19, 23, 30
First order attack	Attack start time (s)	100
	Bias max magnitude (m)	1500
	Drift max magnitude (m/s)	1500
Second order attack	Attack start time (s)	50
	Bias max magnitude (m)	955
	Drift max magnitude (m/s)	5
Third order attack	Attack start time (s)	10
	Bias max magnitude (m)	750
	Drift max magnitude (m/s)	5

[a]The TEXBAT recording UTC Time is September 14, 2012 at 12:50:10.41 PM

TEXBAT binary files are available at UT Austin Radionavigation Laboratory website [43]. For testbed (a), since the Nexus is a commercial receiver, we replay the TEXBAT recordings over-the-air (OTA) by using the following NI equipment: A host PC with a LabVIEW-based record-and-replay software, an NI PXIe-1075 Chassis with a PXIe 5673 RF Signal Generator via PCIe interface, and a VERT 900 antenna. For OTA transmissions, the SCNS Lab is equipped with a custom-made RF shielding area explicitly designed for GPS research. It uses 50 dB attenuation curtains at the L1 band to follow FCC regulations. The specifications of the TEXBAT recordings are set to 25-MHz sampling rate with INT16 in-phase and quadrature interleaved baseband samples, adequate for the NI equipment. The Nexus is properly shielded as to receive OTA replayed recordings. For (b), the binary files from TEXBAT are replayed in offline mode directly into the SDR receiver, thus avoiding OTA transmission effects.

B. Synthetic Simulations

The synthetic attack simulations are implemented on the clean static scenario. Table III shows the recording length and specific GPS time used, along with synthetic attack parameters. The GPS time is used to synchronize between different TEXBAT scenarios. Also, all final attack bias magnitudes sufficiently surpass the distance of 600 m or 2 μs in time, for a complete channel capture [30]. Fig. 3 shows the synthetic *third order attack* injected to the pseudoranges and pseudorange rates of the clean static scenario adhering to the measurement integrity checks described in Section III-A. This shape is chosen to assimilate TEXBAT scenario 2, as will be seen in Section VI-B [31]. As for the synthetic *first* and *second order attacks*, see Fig. 1 shapes along with start and stop times listed in Table III.

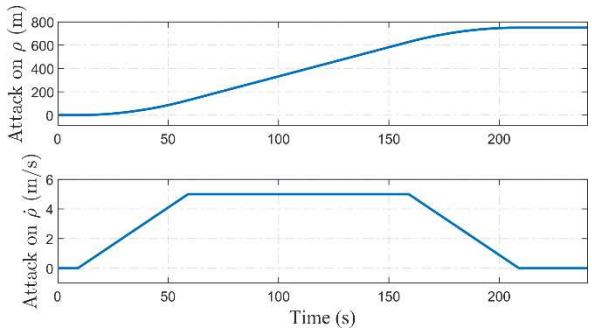


Fig. 3. An injected synthetic *third order attack* on pseudoranges and pseudorange rates.

C. Offline MATLAB Evaluations

For evaluation, we implement TSARM-S in MATLAB environment in offline mode, i.e., in a snapshot manner, after obtaining a window of K raw measurements from testbeds (a) and (b) (see Fig. 2). Both the Nexus and the SDR provide the raw measurements for the recordings that are used, as per Fig. 2. To solve the quadratic program in (12), the MATLAB-based convex optimization solver CVX [40] is used. Specifically, we implement the optimization problem in a non-recursive manner, i.e., using all K measurements. We implement the EKF in a similar mode for comparison purposes. In regards to the variances in matrix $\mathbf{R}_k$, the Nexus post-processing scripts provide such values [42], and the SDR has its own implementation based on receiver characteristics [34], [35, Ch. 9]. To model the clock state covariance matrix $\mathbf{Q}_k$, the Allan variance coefficients for a temperature-controlled crystal oscillator (TCXO) are used [35, Ch. 9]. The output of the conventional EKF is used to obtain the *ground*

TABLE IV
SUMMARY OF EVALUATED SCENARIOS

	TEXBAT clean static synthetic attacks			TEXBAT real scenarios	
	1st order	2nd order	3rd order	Scenario 2	Scenario 3
Nexus 9	✓	✓	✓	✓	×
SDR	✓	✓	✓	✓	✓

truth from the TEXBAT clean static scenario for comparison against synthetic attacks and TEXBAT scenarios 2 and 3. Regarding the λ parameter, Nexus simulations used values between 0.05 and 0.2, and the SDR utilized values between 250 and 1000. The tuning of this parameter can be achieved via cross-validation [40]. Overall, one attempts to find the best λ value that minimizes the multi-objective function in (12), while maintaining a good sensitivity in the detection.

D. Performance Metric

As for the performance metric, our numerical test clock data outputs are compared against the ground truth values via the root mean square error (RMSE) for all scenarios. Let K denote the total length of observation time. The RMSE is defined as

$$RMSE = \sqrt{\frac{1}{K}\sum_{k=0}^{K-1}\left(c\hat{b}_u\,[k] - cb_{u,GT}\,[k]\right)^2} \qquad (14)$$

where $cb_{u,GT}$ is the *ground truth* clock bias, and $c\hat{b}_u$ is the estimated clock bias for each method.

E. Scenarios

A total of nine scenarios are evaluated, as seen in Table IV. In the ensuing Section VI, only illustrative scenarios are shown to demonstrate the TSARM-S method on a commercial receiver, while the SDR testbed is used to further validate the results. The Nexus did not post-process scenario 3 properly, because this attack requires additional tuning and RAIM bypass, which was only possible on the SDR, as will be discussed in Section VI-C. Additionally, a comparison of TSARM-S against state-of-the-art techniques for the clean static scenario corrupted by a first order attack and MP is discussed in Sections VI-D and VI-E.

VI. SIMULATION RESULTS

A. Synthetic Simulation Results

This subsection presents results for synthetic attacks on the Nexus testbed. The Nexus results are shown initially to demonstrate the TSARM-S capabilities on commercial receivers, and both Nexus and SDR results are shown in the next subsection for validation.

1) Synthetic First Order Attack on Nexus 9: Fig. 4 shows the results for the TEXBAT clean static scenario with the *first order synthetic attack*. Fig. 4(a) shows the clock bias and clock drift for the clean, attacked, and corrected outputs of the EKF and TSARM-S, respectively. The clock bias is corrected to a 20.17 m RMSE while the drift error is maintained at less than 1 m/s. Fig. 4(b) shows the estimated spoofer alteration values,

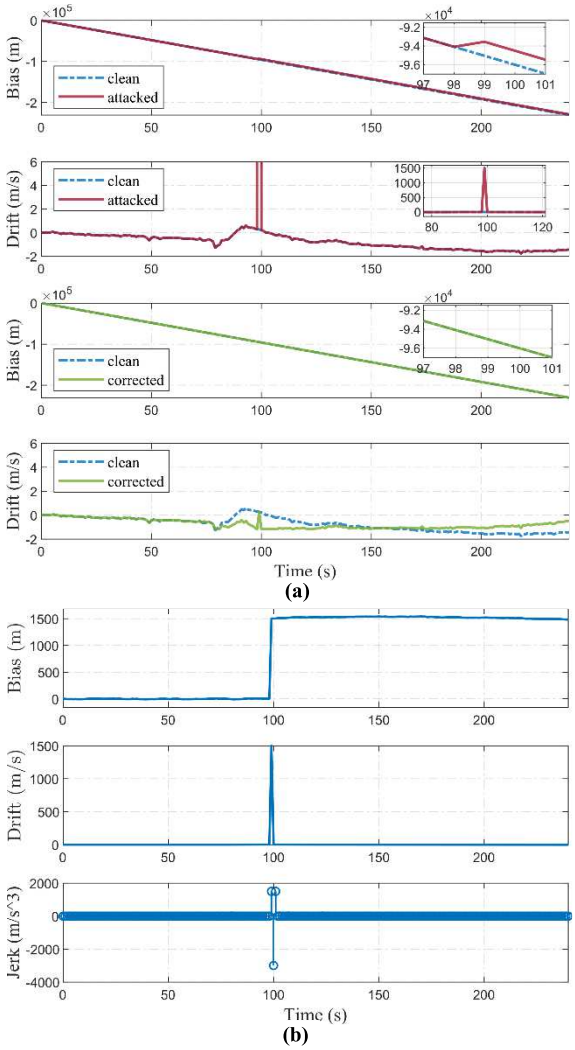


Fig. 4. Synthetic *first order attack* evaluation on Nexus 9. Clean, attacked, and corrected clock bias and clock drift plots on (a), and estimated spoofer alteration plots on (b).

s_ρ and $s_{\dot{\rho}}$, obtained directly from the simulations. The attack is properly captured in the outlier vector and the sparse peaks are seen in the clock jerk.

2) Synthetic Second Order Attack on Nexus 9: Fig. 5 shows the results for the *second order attack* on the Nexus device. The characteristic ramp attack on the clean vs. attacked clock bias is smoother than the step attack, nonetheless, a total bias attack of almost 1000 m is seen in second 229 (see Fig 5(a) zoom-in plot). The corrected bias shows an offset of 99 m bias at the same second. And the corrected clock drift is within 1 m/s. Further λ tuning and proper clock modeling could improve this output, however the RMSE is quite an acceptable 42.47 m bias error from the ground truth. Also, the estimated spoofer alterations in Fig. 5(b) show clear ramp and step shapes detected for the clock bias and drift, respectively, and the clock jerk shows evident detection spikes.

3) Synthetic Third Order Attack on Nexus 9: The synthetic *third order attack* results on Nexus is seen in Fig 6. Out of all three, this is the subtlest and hardest to detect. In fact, it

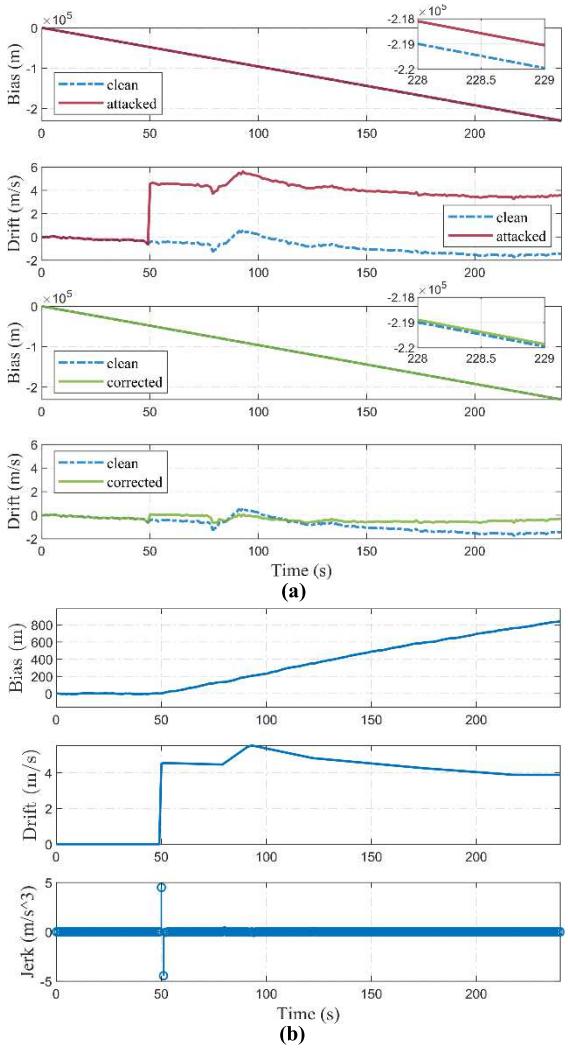


Fig. 5. Synthetic *second order attack* evaluation on Nexus 9. Clean, attacked, and corrected clock bias and clock drift plots on (a), and estimated spoofer alteration plots on (b).

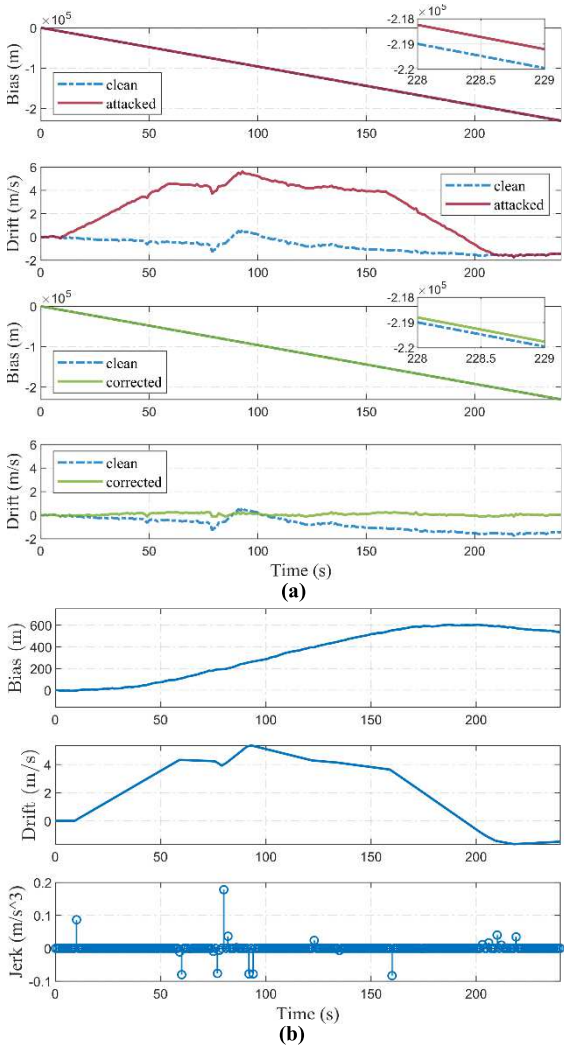


Fig. 6. Synthetic *third order attack* evaluation on Nexus 9. Clean, attacked, and corrected clock bias and clock drift plots on (a), and estimated spoofer alteration plots on (b).

assimilates TEXBAT scenario 2 [31]. Nonetheless, Fig. 6(b) displays the clock jerk spikes that are reflected on the estimated spoofer bias and drift alterations. The RMSE of the corrected bias is 93.38 m, and the corrected clock drift is within 1 m/s of the ground truth as opposed to the injected 5 m/s attack.

B. Real Scenario Results

This subsection presents results for TEXBAT scenario 2 on both Nexus and SDR testbeds, and for scenario 3 on the SDR.

1) TEXBAT Scenario 2 on Nexus 9: Fig. 7 shows the results for the real TEXBAT scenario 2 attack and mitigation with TSARM-S on the Nexus. An impressive 26.72 m RMSE is achieved even with OTA replay effects. The spikes depicted in the jerk plot in Fig. 7(b) distinctly correspond to the trapezoidal shape of the attacked clock drift. This is clearly a *third order attack*. The estimated clock drift is very similar to the one seen on the attacked clock drift plot in Fig. 7(a), and the 600 m clock bias attack reported in [31] is accurately estimated. The corrected clock bias and drift are maintained very closely to the clean version.

2) TEXBAT Scenario 2 on SDR: The SDR evaluation results for the real TEXBAT scenario 2 are seen in Fig. 8. The performance is similar to the one of Nexus with a slightly higher RMSE of 31.83 m. The spikes are quite visible nonetheless, as seen in Fig. 8(b). A small deviation on the corrected clock bias of around 50 m is seen at the end of Fig. 8(a). Further λ tuning might improve such errors, as discussed in Section IV-B. The trapezoidal shape on the attacked clock drift is also seen in Fig. 8(a) as well as in the estimated spoofer clock drift in Fig 8(b).

3) TEXBAT Scenario 3 on SDR: Fig. 9 shows evaluation results for TEXBAT scenario 3 from the SDR. The attack on the clock bias of 600 m is clearly detected in the estimated spoofer alterations plot of Fig. 9(b). However, no significant spikes are seen in the clock jerk output. Nonetheless, the TSA was successfully detected and rejected based on a lack of measurement integrity for an all-channel simultaneous attack (it turns out that the scenario 3 attacks do not satisfy (6) and (7) for all channels). The proposed method achieved an RMSE of 15.92 m as a small ramp residual of 30 m on the corrected clock bias is seen in Fig. 9(a).

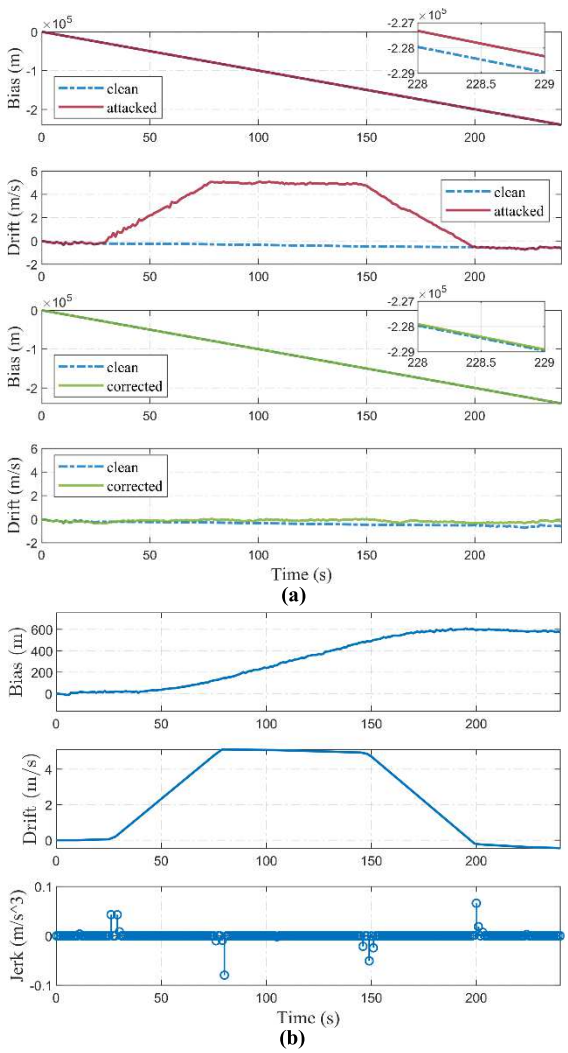


Fig. 7. TEXBAT scenario 2 attack evaluation on Nexus 9. Clean, attacked, and corrected clock bias and clock drift plots on (a), and estimated spoofer alteration plots on (b).

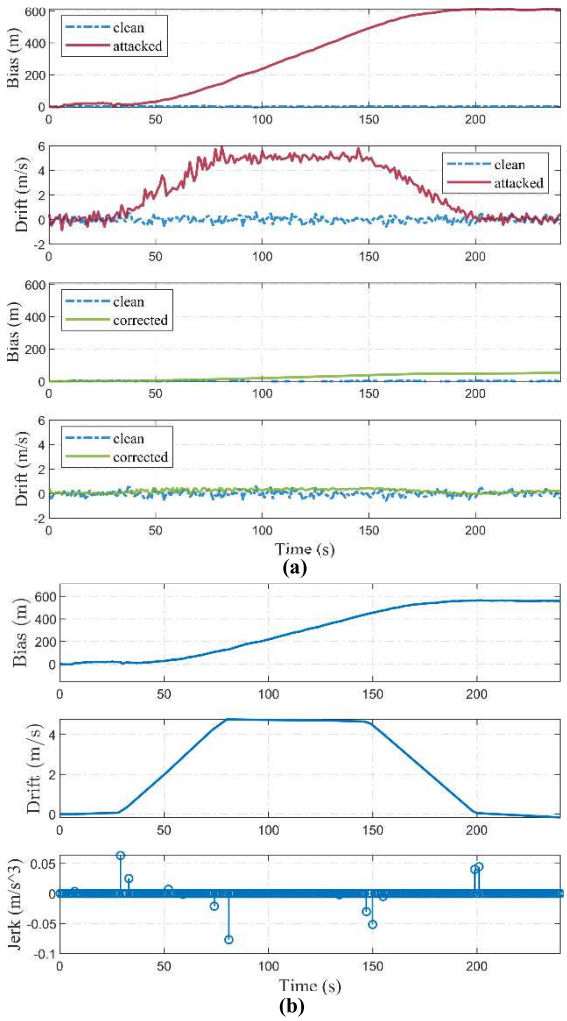


Fig. 8. TEXBAT scenario 2 attack evaluation on SDR. Clean, attacked, and corrected clock bias and clock drift plots on (a), and estimated spoofer alteration plots on (b).

TABLE V
RMS ERROR RESULTS FOR SYNTHETIC AND REAL SCENARIOS (IN m)

	Nexus 9		SDR	
Scenario	EKF	TSARM-S	EKF	TSARM-S
1st order	1151.40	20.17	1151.40	5.06
2nd order	492.78	42.70	492.78	3.16
3rd order	496.71	93.38	496.71	4.45
Scenario 2	425.39	26.72	403.91	31.83
Scenario 3	N/A	N/A	397.71	15.92

C. Analysis and Discussion

Table V shows the RMSE comparison summary between EKF and TSARM-S for all 9 scenarios. Overall, the SDR achieved an average 12.08 m clock bias RMSE, or roughly 40 ns time offset, outperforming the Nexus 9 featuring an average of 45.74 m RMSE, or 152 ns, for all tested scenarios. The SDR shows improved detection due to its stable clock bias and drift outputs and high configurability. The clock model for the SDR matches its true Allan parameters better than the model adopted for the Nexus. Additionally, the Nexus OTA transmission adds further wireless channel effects. Proper clock modeling (availability of Allan parameters) improves detection by handling the expected oscillator noise output, thus allowing more accurate behavior change detection in the clock jerk, as seen in the TSARM-S spoofer alteration outputs.

1) TEXBAT Scenario 3 Measurement Integrity: As seen in Fig. 9, TEXBAT scenario 3 lacks measurement integrity (see Section III-A). The clock drift does not follow the derivative of the clock bias. This can be seen as the attack on the clock bias reaches 600 m, while the drift remains unaltered in Fig. 9(a). Because the spoofer alterations are unconstrained in (12), the outlier variable captures these integrity discrepancies and successfully mitigates the attack on the clock bias. Thus, scenario 3 attack was successfully rejected due to a lack of measurement integrity and not because of a sparse event.

Also, the OTA experiments for this scenario with the Nexus testbed were unsuccessful: the device dropped channels during OTA replay and failed to attain a PVT solution after the attack had started around second 100. We hypothesize that the Nexus has simple self-integrity checks such as RAIM. In light of this evidence, the SDR was tuned to post-process scenario 3 in

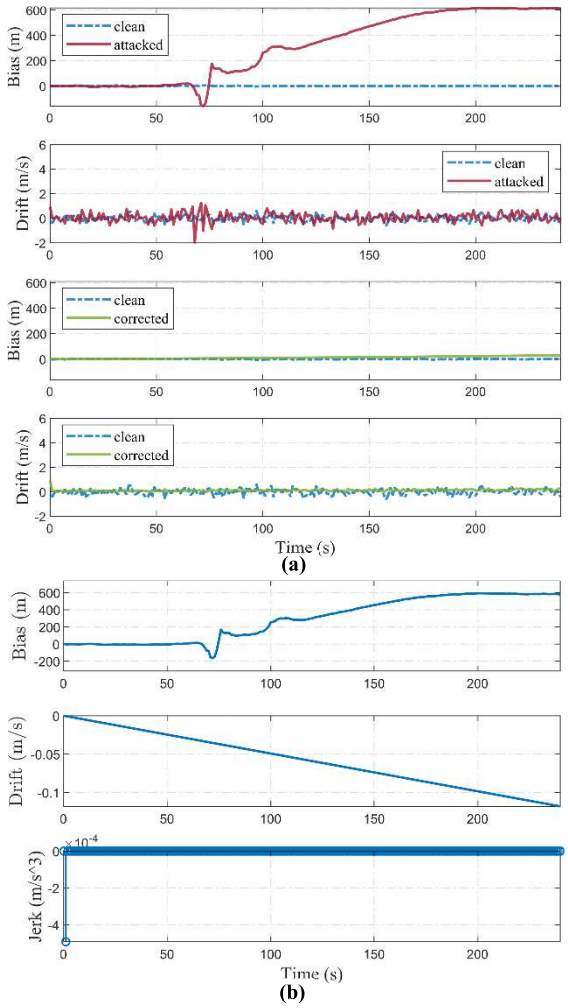


Fig. 9. TEXBAT scenario 3 attack evaluation on SDR. Clean, attacked, and corrected clock bias and clock drift plots on (a), and estimated spoofer alteration plots on (b).

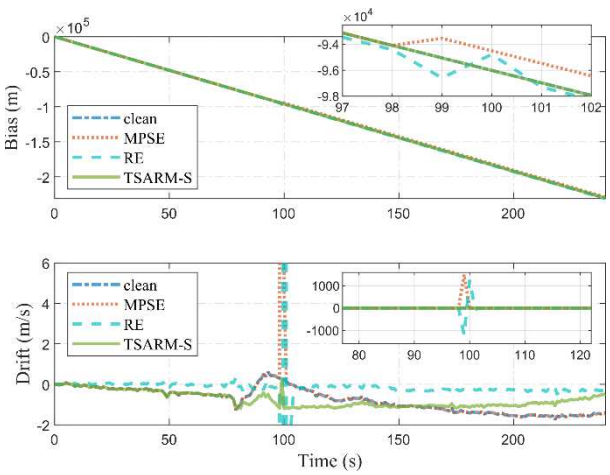


Fig. 10. Synthetic *first order attack* evaluation on Nexus 9 and comparison with state-of-the-art techniques. Top and bottom plots show clean and corrected clock bias and clock drift, respectively.

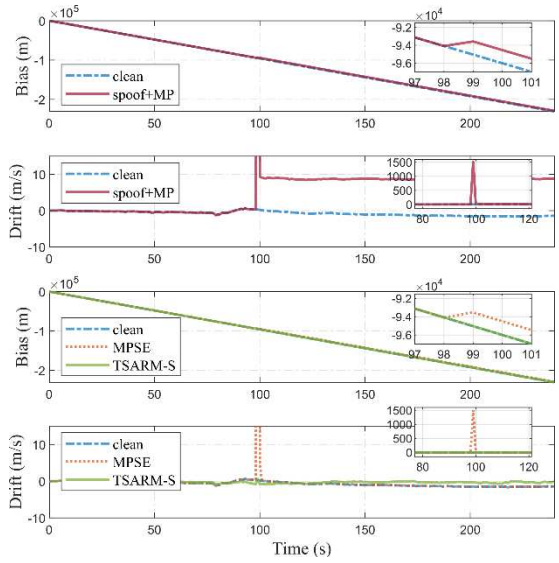


Fig. 11. Synthetic *first order attack* plus multipath evaluation on Nexus 9 and comparison against state-of-the-art MPSE technique. Top and bottom plots show clean and corrected clock bias and clock drift, respectively.

offline mode with deactivated features such as RAIM and other channel dropping mechanisms. Therefore, we conclude that a smart spoofer attack must maintain measurement integrity to successfully bypass rudimentary commercial device tests.

D. Comparison With State-of-the-Art Techniques

In the following, TSARM-S is compared against a state-of-the-art TSA rejection technique, namely, a Robust Estimator (RE) [16]. Similarly, a multipath sparse estimation (MPSE) technique is evaluated due to its similarity in terms of sparse detection [20]. The Nexus testbed along with a synthetic *first order attack* is evaluated (see Table III and Fig. 1). In this experiment, the RE and MPSE techniques are evaluated similar to TSARM-S, i.e., in a snapshot, non-recursive, post-processing manner along with a static scenario where the user position and velocities are known and not estimated. Thus, we focus on TSA detection and correction. The real-time implementation aspects of TSARM-S are left for future work, as mentioned in Section VII.

Fig. 10 shows the corrected clock bias (top) and drift (bottom) outputs from MPSE, RE, and TSARM-S against their clean versions. The MPSE assumes an MP setting, i.e., that only a few pseudorange and pseudorange rate measurements are affected. Since the TSA affects all measurements alike, the method is not effective in detecting the simulated *first order attack*. The RMSE for the MPSE is 1149.92 m. The RE achieves clock bias RMSE of 407.62 m. It is worth noting the RE's primary application is to reject TSAs that affect PMUs and therefore induce a clock bias error of 8000 m; thus a 1500 m attack is considered small.

E. Application to a Spoofing Plus Multipath Scenario

To further validate that TSARM-S provides an accurate clock bias and drift under diverse settings, a scenario with both a TSA and MP is explored. Also, we compare with MPSE [20]. The TSA and MP scenario is evaluated on the Nexus testbed as a *first order attack* along with synthetic MP alterations as in [20]. Specifically, the MP is simulated

similarly to a step attack with pseudorange alterations of 80 m and pseudorange rates of -24 m/s on two satellites. This MP is injected at similar times as the *first order attack*. Fig. 11 shows the clean and attacked clock bias and drift outputs of the EKF. The MP is barely noticeable in the bias since the TSA inflicts a 1500 m alteration, however the drift shows a step of around 9 m/s. Also, note that the MP model from [20] does not follow measurement integrity as given in Section III-A. In reference to the bottom two plots of Fig. 11, TSARM-S achieves an RMSE of 45.39 m, while MPSE achieves 1151.23 m RMSE. The bias seems unaffected by the MPSE as expected from TSA characteristics, however the drift appears to be corrected. Nonetheless, TSARM-S corrects the TSA within an acceptable error. It is worth emphasizing that TSARM-S is not intended for multipath mitigation, however this simulation numerically demonstrates that a reasonably accurate clock bias estimate can be produced, even if some multipath outliers are present.

VII. Conclusion and Future Work

This work presented a novel modeling of GPS TSAs based on higher-order sparse-domains where the attack appears as a spike while a behavior change can be detected on the user clock. Further, it proposed a TSA rejection and mitigation technique based on a joint dynamic model and a higher order total variation operator. A test methodology was applied to first order, second order, and third order spoofing attacks as described in the TSA modeling. Also, real-data TEXBAT scenarios were evaluated. These attacks were successfully corrected in a commercial receiver and a GPS SDR receiver [32]. In both testbeds, TSARM-S rejected smart spoofing attacks and achieved an average RMSE of 12.08 m for the SDR testbed, and 45.74 m for the Nexus. Both results translate to an RMSE of roughly 40 ns and 153 ns, respectively. TSARM-S was also evaluated against state-of-the-art spoofing mitigation techniques and MP techniques. Numerical simulations demonstrated that TSARM-S achieves reasonably accurate clock bias estimates under TSA and MP scenarios.

The proposed method is computationally feasible and can be implemented as an inexpensive firmware upgrade for commercial receivers. TSARM-S proved that a proper dynamic clock bias and drift model can achieve TSA rejection tasks by sensing behavior changes in higher-order sparse domains as well as measurement integrity gaps. Finally, due to the proposed systematic TSA modeling, simple adjustments to the dynamic model in (12) can potentially detect more complex (and smoother) attacks at domains of even higher order.

As future work, further improvement of the clock model (via the Allan coefficients) on the target device such as the Nexus 9 is planned to improve the sensitivity with respect to the attack detection and mitigation. Also, further tuning of the λ parameter for different scenarios is expected. Other aspects include investigation of the impact of noise, where certain limitations to the proposed algorithm can be expected, as the studied scenarios were evaluated in representative nominal conditions. Finally, because the proposed method uses a window of K measurements in a snapshot manner, a real-time implementation, i.e. by means of a sliding window, is anticipated.

References

[1] M. Goldstein and J. Kirschbaum "GPS disruptins: Efforts to assess risks to critical infrastructure and coordinate agency actions should be enhanced," U.S. Govt. Accountability Office, Washington, DC, USA, Tech. Rep. GAO-14-15, Nov. 2014. [Online]. Available: https://www.gao.gov/products/GAO-14-15

[2] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proc. IEEE*, vol. 104, no. 6, pp. 1258–1270, Jun. 2016.

[3] C. Gänther, "A survey of spoofing and counter-measures: A survey of spoofing and counter-measures," *Navigation*, vol. 61, no. 3, pp. 159–177, Sep. 2014.

[4] Y. Wang and J. P. Hespanha, "Distributed estimation of power system oscillation modes under attacks on GPS clocks," *IEEE Trans. Instrum. Meas.*, vol. 67, no. 7, pp. 1626–1637, Jul. 2018.

[5] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," *Int. J. Crit. Infrastruct. Protection*, vol. 5, nos. 3–4, pp. 146–153, Dec. 2012.

[6] P. Risbud, N. Gatsis, and A. Taha, "Vulnerability analysis of smart grids to GPS spoofing," *IEEE Trans. Smart Grid*, vol. 10, no. 4, pp. 3535–3548, Jul. 2019.

[7] Z. Zhang, S. Gong, A. D. Dimitrovski, and H. Li, "Time synchronization attack in smart grid: Impact and analysis," *IEEE Trans. Smart Grid*, vol. 4, no. 1, pp. 87–98, Mar. 2013.

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

[9] 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.*, vol. 68, no. 8, pp. 2768–2784, Aug. 2019, doi: 10.1109/TIM.2018.2869261.

[10] R. T. Ioannides, T. Pany, and G. Gibbons, "Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques," *Proc. IEEE*, vol. 104, no. 6, pp. 1174–1194, Jun. 2016.

[11] 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, Apr. 2018.

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

[13] S. Bhamidipati, T. Y. Mina, and G. X. Gao, "GPS time authentication against spoofing via a network of receivers for power systems," in *Proc. IEEE/ION Position, Location Navigat. Symp. (PLANS)*, Monterey, CA, USA, Apr. 2018, pp. 1485–1491.

[14] B. Xu, Q. Jia, and L.-T. Hsu, "Vector tracking loop-based GNSS NLOS detection and correction: Algorithm design and performance analysis," *IEEE Trans. Instrum. Meas.*, vol. 69, no. 7, pp. 4604–4619, Jul. 2020.

[15] 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," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 49, no. 4, pp. 2250–2267, Oct. 2014.

[16] J. Lee, A. F. Taha, N. Gatsis, and D. Akopian, "Tuning-free, low memory robust estimator to mitigate GPS spoofing attacks," *IEEE Control. Syst. Lett.*, vol. 4, no. 1, pp. 145–149, Jan. 2020.

[17] L.-T. Hsu, H. Tokura, N. Kubo, Y. Gu, and S. Kamijo, "Multiple faulty GNSS measurement exclusion based on consistency check in urban canyons," *IEEE Sensors J.*, vol. 17, no. 6, pp. 1909–1917, Mar. 2017.

[18] Y. Liu, S. Li, Q. Fu, Z. Liu, and Q. Zhou, "Analysis of Kalman filter innovation-based GNSS spoofing detection method for INS/GNSS integrated navigation system," *IEEE Sensors J.*, vol. 19, no. 13, pp. 5167–5178, Jul. 2019.

[19] 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. Ind. Electron.*, vol. 65, no. 8, pp. 6425–6435, Aug. 2018.

[20] J. Lesouple, T. Robert, M. Sahmoudi, J.-Y. Tourneret, and W. Vigneau, "Multipath mitigation for GNSS positioning in an urban environment using sparse estimation," *IEEE Trans. Intell. Transp. Syst.*, vol. 20, no. 4, pp. 1316–1328, Apr. 2019.

[21] P. Zhang, D. Li, J. Zhao, and J. Cheng, "Multipath mitigation in GNSS positioning by the dual-path compression estimation," *IEEE Sensors J.*, vol. 20, no. 6, pp. 3087–3100, Mar. 2020.

[22] Y. Hu, S. Bian, B. Li, and L. Zhou, "A novel array-based spoofing and jamming suppression method for GNSS receiver," *IEEE Sensors J.*, vol. 18, no. 7, pp. 2952–2958, Apr. 2018.

[23] F. Wang, H. Li, and M. Lu, "GNSS spoofing countermeasure with a single rotating antenna," *IEEE Access*, vol. 5, pp. 8039–8047, 2017, doi: 10.1109/ACCESS.2017.2698070.
[24] F. Gallardo and A. P. Yuste, "SCER spoofing attacks on the galileo open service and machine learning techniques for end-user protection," *IEEE Access*, vol. 8, pp. 85515–85532, 2020, doi: 10.1109/ACCESS.2020.2992119.
[25] S. Semanjski, A. Muls, I. Semanjski, and W. De Wilde, "Use and validation of supervised machine learning approach for detection of GNSS signal spoofing," in *Proc. Int. Conf. Localization GNSS (ICL-GNSS)*, Nuremberg, Germany, Jun. 2019, pp. 1–6, doi: 10.1109/ICL-GNSS.2019.8752775.
[26] S. Bhamidipati and G. X. Gao, "GPS multireceiver joint direct time estimation and spoofer localization," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 55, no. 4, pp. 1907–1919, Aug. 2019.
[27] Y. Zhang, J. Wang, and J. Liu, "Attack identification and correction for PMU GPS spoofing in unbalanced distribution systems," *IEEE Trans. Smart Grid*, vol. 11, no. 1, pp. 762–773, Jan. 2020.
[28] R. Tibshirani, "Regression shrinkage and selection via the lasso," *J. Roy. Stat. Soc., Ser. B Methodol.*, vol. 58, no. 1, pp. 267–288, Jan. 1996.
[29] *IEEE Standard for Synchrophasor Measurements for Power Systems*, Standard C37.118.1-2011, Dec. 2011, pp. 1–61.
[30] D. P. Shepard and T. E. Humphreys, "Characterization of receiver response to spoofing attacks," in *Proc. 24th Int. Tech. Meeting Satell. Div. Inst. Navig.*, Portland, OR, USA, Sep. 2011, pp. 2608–2618.
[31] 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, USA, Sep. 2012, pp. 3569–3583.
[32] 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. Instrum. Meas.*, vol. 67, no. 9, pp. 2082–2096, Sep. 2018.
[33] P. Misra and P. Enge, *Global Positioning System: Signals, Measurements, and Performance*, 2nd ed. Lincoln, MA, USA: Ganga-Jamuna Press, 2006.
[34] P. Axelrad and R. G. Brown, "GPS navigation algorithms," in *Global Positioning System: Theory Application*, vol. 1, B. W. Parkinson, J. J. Spilker, P. Axelrad, and P. Enge, Eds. Washington, DC, USA: American Institute of Aeronautics and Astronautics, 1996, ch. 9.
[35] R. G. Brown and P. Y. C. Huang, "Kalman filter applications to the GPS and other navigation systems," in *Introduction to Random Signals Applicaation Kalman Filtering With MATLAB Exercises*, 4th ed, R. G. Brown and P. Y. C. Huang Eds. Hoboken, NJ, USA: Wiley, 2012, ch. 9.
[36] B. W. Parkinson, J. J. Spilker, P. Axelrad, and P. Enge, *Global Positioning System: Theory and Applications*, vol. 2, Washington, DC, USA: American Institute of Aeronautics and Astronautics, 1996.
[37] F.-c. Chan, M. Joerger, and B. Pervan, "Stochastic modeling of atomic receiver clock for high integrity gps navigation," *IEEE Trans. Aerosp. Electron. Syst.*, vol. 50, no. 3, pp. 1749–1764, Jul. 2014.
[38] S. Martikainen, R. Piche, and S. Ali-Loytty, "Outlier-robust estimation of GPS satellite clock offsets," in *Proc. Int. Conf. Localization GNSS*, Starnberg, Germany, Jun. 2012, pp. 1–5, doi: 10.1109/ICL-GNSS.2012.6253107.
[39] B. Hao, J. Wang, and J. Zhu, "A fast linearized alternating minimization algorithm for constrained high-order total variation regularized compressive sensing," *IEEE Access*, vol. 7, pp. 143081–143089, 2019.
[40] C. Research. (Dec. 2018). *CVX: MATLAB Software for Disciplined Convex Programming, Version 2.1*. [Online]. Available: http://cvxr.com/cvx
[41] J. Nocedal and S. J. Wright, *Numerical Optimization*. New York, NY, USA: Springer. 2006.
[42] *Android GNSS*. Accessed: Mar. 10, 2019. [Online]. Available: https://developer.android.com/guide/topics/sensors/gnss
[43] *Index of/Datastore/Texbat*. Accessed: Apr. 5, 2019. [Online]. Available: http://radionavlab.ae.utexas.edu/datastore/texbat/

Erick Schmidt (Member, IEEE) received the B.S. (Hons.) degree in electronics and computer engineering from the Monterrey Institute of Technology and Higher Education, Monterrey, Mexico, in 2011, and the M.S. and Ph.D. degrees in electrical engineering from The University of Texas at San Antonio, San Antonio, TX, USA, in 2015 and 2020, respectively.

From 2011 to 2013, he was a Systems Engineer with Qualcomm Incorporated, San Diego, CA, USA. His current research interests include software-defined radio, indoor navigation, global navigation satellite system, spoofing mitigation algorithms, and fast-prototyping methods and accelerators for baseband communication systems.

Dr. Schmidt is a Student Member of the Institute of Navigation.

Junhwan Lee was born in Siheung, South Korea, in 1995. He received the B.S. degree in electrical engineering from The University of Texas at San Antonio (UTSA) in 2018, where he is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering. His current research interest includes spoofing mitigation in global positioning system (GPS) through optimization algorithm.

Nikolaos Gatsis (Member, IEEE) received the Diploma (Hons.) degree in electrical and computer engineering from the University of Patras, Greece, in 2005, and the M.Sc. degree in electrical engineering and the Ph.D. degree in electrical engineering with minor in mathematics from the University of Minnesota in 2010 and 2012, respectively.

He is currently an Associate Professor with the Department of Electrical and Computer Engineering, The University of Texas at San Antonio. His research focuses on optimal and secure operation of smart power grids and other critical infrastructures, including water distribution networks and the global positioning systems.

Dr. Gatsis was a recipient of the NSF CAREER Award. He co-organized symposia in the area of smart grids in the IEEE GlobalSIP 2015 and 2016. He has served as a Co-Guest Editor for a Special Issue of the IEEE JOURNAL ON SELECTED TOPICS IN SIGNAL PROCESSING on Critical Infrastructures. He was also selected to present to the 2020 NSF Engineering CAREER Proposal Writing Workshop.

David Akopian (Senior Member, IEEE) received the Ph.D. degree from the Tampere University of Technology, Finland, in 1997.

From 1993 to 1999, he was a Researcher, an Instructor, and an Assistant Centre Director of the Tampere University of Technology. He was a Senior Research Engineer and Specialist with Nokia Corporation from 1999 to 2003. He is a Professor with The University of Texas at San Antonio (UTSA). He has authored and coauthored more than 35 patents and 160 publications. His current research interests include algorithms for communication and navigation receivers, positioning, dedicated hardware architectures and platforms for software-defined radio, and communication technologies for healthcare applications. He has been a Fellow of the U.S. National Academy of Inventors since 2016. He has served in organizing and program committees for many IEEE conferences and co-chaired an annual conference on Multimedia and Mobile Devices. His research has been supported by the National Science Foundation, National Institutes of Health, USAF, U.S. Navy, and Texas foundations.