Real-Time Rejection and Mitigation of Time Synchronization Attacks on the Global Positioning System

Ali Khalajmehrabadi, *Student Member, IEEE*, Nikolaos Gatsis, *Member, IEEE*, David Akopian, *Senior Member, IEEE*, and Ahmad F. Taha, *Member, IEEE*

***Abstract*—This paper introduces the time synchronization attack rejection and mitigation (TSARM) technique for time synchronization attacks over the global positioning system (GPS). The technique estimates the clock bias and drift of the GPS receiver along with the possible attack contrary to previous approaches. Having estimated the time instants of the attack, the clock bias and drift of the receiver are corrected. The proposed technique is computationally efficient and can be easily implemented in real time in a fashion complementary to standard algorithms for position, velocity, and time estimation in off-the-shelf receivers. The performance of this technique is evaluated on a set of collected data from a real GPS receiver. Our method renders excellent time recovery consistent with the application requirements. The numerical results demonstrate that the TSARM technique outperforms competing approaches in the literature.**

***Index Terms*—Global positioning system (GPS), spoofing detection, time synchronization attack (TSAs).**

I. Introduction

INFRASTRUCTURES, such as road tolling systems, terrestrial digital video broadcasting, cell phone and air traffic control towers, real-time industrial control systems, and phasor measurement units (PMUs) [1] heavily rely on synchronized precise timing for consistent and accurate network communications to maintain records and ensure their traceability. The global positioning system (GPS) provides a time reference of microsecond precision for these systems [2]–[5].

The GPS-based time-synchronization systems use the civilian GPS channels, which are open to the public [6], [7]. The unencrypted nature of these signals makes them vulnerable to unintentional interference and intentional attacks. Thus, the unauthorized manipulation of GPS signals leads to the disruption of correct readings of GPS-based time references and, thus, is called time synchronization attack (TSA). To address the impact of malicious attacks, for instance, on PMU data, the Electric Power Research Institute published a technical report that recognizes the vulnerability of PMUs to GPS spoofing under its scenario *WAMPAC.12: GPS Time Signal Compromise* [8]. These attacks introduce erroneous time stamps that are eventually equivalent to inducing wrong phase angle in the PMU measurements [9], [10]. The impact of TSAs on generator trip control, transmission line fault detection, voltage stability monitoring, disturbing event locationing, and power system state estimation has been studied and evaluated both experimentally [11] and through simulations [12]–[14].

Intentional unauthorized manipulation of GPS signals is commonly referred to as *GPS spoofing* and can be categorized based on the spoofer mechanism as follows.

1) *Jamming (blocking)*: The spoofer sends high-power signals to jam the normal operation of the receiver by disrupting the normal operation of the victim receiver, often referred to as *loosing lock*. Then, the victim receiver may lock onto the spoofer signal after jamming [9], [15]–[17].
2) *Data-level spoofing*: The spoofer manipulates the navigation data, such as orbital parameters (ephemerides) that are used to compute satellite locations [13], [15], [18].
3) *Signal-level spoofing*: The spoofer synthesizes GPS-like signals that carry the same navigation data as concurrently broadcasted by the satellites [11].
4) *Record-and-replay attack*: The spoofer records the authentic GPS signals and retransmits them with selected delays at higher power [9], [19]. Typically, the spoofer starts from low-power transmission and increases its power to force the receiver to lock onto the spoofed (delayed) signal. The spoofer may change the transmitting signal properties such that the victim receiver miscalculates its estimates.

Common off-the-shelf GPS receivers lack proper mechanisms to detect these attacks. A group of studies have been directed toward evaluating the requirements for successful attacks, theoretically [16] and experimentally [11], [29]–[31]. For instance, in [30], a real spoofer as a software-defined radio that records authentic GPS signals and retransmits fake signals has been designed. It provides the option of manipulating various signal properties for spoofing.

Manuscript received June 23, 2017; revised September 13, 2017 and November 12, 2017; accepted December 6, 2017. Date of publication January 3, 2018; date of current version April 2, 2018. This work was supported in part by the National Science Foundation under Grant ECCS-1719043 and Grant ECCS-1462404. *(Corresponding author: Ali Khalajmehrabadi.)*

The authors are with the Department of Electrical and Computer Engineering, University of Texas at San Antonio, San Antonio, TX 78249 USA (e-mail: ali.khalajmehrabadi@utsa.edu; nikolaos.gatsis@utsa.edu; david.akopian@utsa.edu; ahmad.taha@utsa.edu).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TIE.2017.2787581

TABLE I
GPS SPOOFING DETECTION TECHNIQUES: DETECTION DOMAIN AND IMPLEMENTATION ASPECTS

Method	Attack Detection Domain	Attack	Implementation Aspects	Relevant
EKF	GPS navigation domain	Not estimated	Benchmark for most common GPS receivers	Yes
CUSUM [20]	GPS baseband signal domain	Not estimated	Applies hypothesis testing on packets of received signal	No
Ref. [21]	GPS baseband and power grid domains	Not estimated	Combines the statistics of carrier-to-noise ratio difference between two GPS antennas	No
SPREE [22]	GPS baseband signal domain	Not estimated	Applies auxiliary peak tracking in the correlators of receiver	No
Ref. [23], [24]	GPS baseband signal domain	Not estimated	Applies a position-information-aided vector tracking loop	No
Ref. [25], [26]	GPS navigation domain	Not estimated	Needs collaboration among multiple GPS receivers	No
Ref. [27]	GPS navigation domain	Not estimated	Applies an anti-spoofing particle filter	Yes
Ref. [28]	GPS navigation domain	Not estimated	Applies hypothesis testing on a GPS clock signature	Yes
TSARM	GPS navigation domain	Estimated	Applies a real-time optimization technique	–

A. Spoofing Detection Techniques in the Literature

The first level of countermeasures to reduce the effect of malicious attacks on GPS receivers typically relies on the receiver autonomous integrity monitoring (RAIM) [4]. Off-the-shelf GPS receivers typically apply RAIM consistency checks to detect the anomalies exploiting measurement redundancies. For example, RAIM may evaluate the variance of GPS solution residuals and consequently generate an alarm if it exceeds a predetermined threshold. Similar variance authentication techniques have been proposed in [22] and [32] based on hypothesis testing on the Kalman filter innovations; however, they are vulnerable to smarter attacks that pass RAIM checks or the innovation hypothesis testing.

A plethora of countermeasures have been designed to make the receivers robust against more sophisticated attacks [9], [15], [17]–[19], [21]–[25], [27], [28], [33]–[35]. Vector tracking exploits the signals from all satellites jointly and feeds back the predicted position, velocity, and time (PVT) to the internal lock loops [23], [24], [33]. If an attack occurs, the lock loops become unstable which is an indication of attack. Cooperative GPS receivers can perform authentication checks by analyzing the integrity of measurements through peer-to-peer communications [24], [25], [34], [35]. Also, a quick sanity check for stationary time synchronization devices is to monitor the estimated location. As the true location can be known *a priori*, any large shift that exceeds the maximum allowable position estimation error can be an indication of attack [28]. The receiver carrier-to-noise receiver can be used as an indicator of spoofing attack [17]. In [21], the difference between the carrier-to-noise ratios of two GPS antennas has been proposed as a metric of PMU trustworthiness. In addition, some approaches compare the receiver's clock behavior against its statistics in the normal operation [19], [28], [33].

B. Existing Literature Gaps

As discussed above, prior research studies addressed a breadth of problems related to GPS spoofing. However, there are certain gaps that should still be addressed.

1) Most of the works do not provide analytical models for different types of spoofing attacks. The possible attacking procedure models are crucial for designing the countermeasures against the spoofing attacks.

2) Although some countermeasures might be effective for a certain type of attack, a comprehensive countermeasure development is still lacking for defending the GPS receiver. This is practically needed as the receiver cannot predict the type of attack.

3) The main effort in the literature is in the detection of possible spoofing attacks. However, even with the spoofing detection, the GPS receiver cannot resume its normal operation, especially in PMU applications where the network's normal operation cannot be interrupted. So, the spoofing countermeasures should not only detect the attacks but also mitigate their effects so that the network can resume its normal operation.

4) There is a need for simpler solutions, which can be integrated with current systems.

C. Contributions of This Paper

This paper addresses the previously mentioned gaps for stationary time synchronization systems. To the best of our knowledge, this is the first paper that provides the following major contributions.

1) The new method is not a mere spoofing detector; it also estimates the spoofing attack.

2) The spoofed signatures, i.e., clock bias and drift, are corrected using the estimated attack.

3) The new method detects the smartest attacks that maintain the consistency in the measurement set.

A descriptive comparison between our solution and representative works in the literature is provided in Table I. A review of the spoofing detection domain shows that most of the prior art operates at the baseband signal processing domain, which necessitates the manipulation of the receiver circuitry. Hence, the approach in this paper is compared only to those works whose detection methodology lies in the navigation domain.

The proposed TSA detection and mitigation approach in this paper consists of two parts. First, a dynamical model is introduced, which analytically models the attacks in the receiver's clock bias and drift. Through a proposed novel TSA rejection and mitigation (TSARM) approach, the clock bias and drift are estimated along with the attack. Second, the estimated clock bias and drift are modified based on the estimated attacks so that the receiver would be able to continue its normal operation with corrected timing for the application. The proposed method

detects and mitigates the effects of the smartest and most consistent reported attacks in which the position of the victim receiver is not altered and the attacks on the pseudoranges are consistent with the attacks on pseudorange rates.

Different from outlier detection approaches presented in [36] and [37], the proposed method detects the anomalous behavior of the spoofer even if the measurement integrity is preserved. The spoofing mitigation scheme has the following desirable attributes.

1) It solves a small quadratic program, which makes it applicable to commonly used devices.

2) It can be easily integrated into existing systems without changing the receiver's circuitry or necessitating mulitple GPS receivers as opposed to [21]–[24], [33], and [34].

3) It can run in parallel with current systems and provide an alert if spoofing has occurred.

4) Without halting the normal operation of the system, corrected timing estimates can be computed.

The proposed antispoofing technique has been evaluated using a commercial GPS receiver with open-source measurements access [38]. These measurements have been perturbed with spoofing attacks specific to PMU operation. Applying the proposed antispoofing technique shows that the clock bias of the receiver can be corrected within the maximum allowable error in the PMU IEEE C37.118 standard [39].

Paper Organization: A brief description of the GPS is described in Section II. Then, we provide the models for possible spoofing attacks in Section III. Section IV elaborates on the proposed solution to detect and modify the effect of these attacks. Our solution is numerically evaluated in Section V followed by the conclusions in Section VI.

II. GPS PVT Estimation

In this section, a brief overview of the GPS PVT estimation is presented.

The main idea of localization and timing through GPS is trilateration, which relies on the known location of satellites as well as distance measurements between satellites and the GPS receiver. In particular, the GPS signal from satellite n contains a set of navigation data, comprising the ephemeris and the almanac (typically updated every 2 h and one week, respectively), together with the signal's time of transmission (t_n). These data are used to compute the satellite's position $\mathbf{p}_n = [x_n(t_n), y_n(t_n), z_n(t_n)]^T$ in Earth Centered Earth Fixed coordinates, through a function known to the GPS receiver. Let t_R denote the time that the signal arrives at the GPS receiver. The distance between the user (GPS receiver) and satellite n can be found by multiplying the signal propagation time $t_R - t_n$ by the speed of light c. This quantity is called *pseudorange*: $\rho_n = c(t_R - t_n),\ n = 1, \ldots, N$, where N is the number of visible satellites. The pseudorange is not the exact distance because the receiver and satellite clocks are both biased with respect to the absolute GPS time. Let the receiver and satellite clock biases be denoted by b_{u} and b_n, respectively. Therefore, the times of reception t_R and t_n are related to their absolute values in GPS time as follows: $t_R = t_R^{\mathrm{GPS}} + b_{\mathrm{u}}; \quad t_n = t_n^{\mathrm{GPS}} + b_n,\ n = 1, \ldots, N$. The b_n's are computed from the received navigation data and are considered known. However, the bias b_{u} must be estimated and should be subtracted from the measured t_R to yield the receiver absolute GPS time t_R^{GPS}, which can be used as a time reference for synchronization. Synchronization systems time stamp their readings based on the Coordinated Universal Time (UTC), which has a known offset with the GPS time as $t_R^{\mathrm{UTC}} = t_R^{\mathrm{GPS}} - \Delta t_{\mathrm{UTC}}$, where Δt_{UTC} is available online.[1]

Let $\mathbf{p}_{\mathrm{u}} = [x_{\mathrm{u}}, y_{\mathrm{u}}, z_{\mathrm{u}}]^T$ be the coordinates of the GPS receiver, and d_n its true range to satellite n. This distance is expressed via the locations $\mathbf{p}_{\mathrm{u}}$, $\mathbf{p}_n$ and the times t_R^{GPS}, t_n^{GPS} as $d_n = \|\mathbf{p}_n - \mathbf{p}_{\mathrm{u}}\|_2 = c(t_R^{\mathrm{GPS}} - t_n^{\mathrm{GPS}})$. Therefore, the measurement equation becomes

$$\rho_n = \|\mathbf{p}_n - \mathbf{p}_{\mathrm{u}}\|_2 + c(b_{\mathrm{u}} - b_n) + \epsilon_{\rho_n} \tag{1}$$

where $n = 1, \ldots, N$, and ϵ_{ρ_n} represents the noise. The unknowns in (1) are $x_{\mathrm{u}}, y_{\mathrm{u}}, z_{\mathrm{u}}$, and b_{u} and, therefore, measurements from at least four satellites are needed to estimate them.

Furthermore, the nominal carrier frequency ($f_c = 1575.42$ MHz) of the transmitted signals from the satellite experiences a Doppler shift at the receiver due to the relative motion between the receiver and the satellite. Hence, in addition to pseudoranges, pseudorange rates are estimated from the Doppler shift and are related to the relative satellite velocity $\mathbf{v}_n$ and the user velocity $\mathbf{v}_{\mathrm{u}}$ via

$$\dot{\rho}_n = (\mathbf{v}_n - \mathbf{v}_{\mathrm{u}})^T \frac{\mathbf{p}_n - \mathbf{p}_{\mathrm{u}}}{\|\mathbf{p}_n - \mathbf{p}_{\mathrm{u}}\|} + \dot{b}_{\mathrm{u}} + \epsilon_{\dot{\rho}_n} \tag{2}$$

where $\dot{b}_u$ is the clock drift.

In most cases, there are more than four visible satellites, resulting in an overdetermined system of equations in (1) and (2). Typical GPS receivers use nonlinear weighted least squares (WLS) to solve (1) and (2) and provide an estimate of the location, velocity, clock bias, and clock drift of the receiver, often referred to as PVT solution. To additionally exploit the consecutive nature of the estimates, a dynamical model is used. The conventional dynamical model for stationary receivers is a random walk model [3, Ch. 9]

$$\begin{pmatrix} x_{\mathrm{u}}[l+1] \\ y_{\mathrm{u}}[l+1] \\ z_{\mathrm{u}}[l+1] \\ b_{\mathrm{u}}[l+1] \\ \dot{b}_{\mathrm{u}}[l+1] \end{pmatrix} = \left(\begin{array}{c:cc} \mathbf{I}_{3\times 3} & \mathbf{0}_{3\times 2} \\ \hdashline \mathbf{0}_{2\times 3} & \begin{matrix} 1 & \Delta t \\ 0 & 1 \end{matrix} \end{array}\right) \begin{pmatrix} x_{\mathrm{u}}[l] \\ y_{\mathrm{u}}[l] \\ z_{\mathrm{u}}[l] \\ b_{\mathrm{u}}[l] \\ \dot{b}_{\mathrm{u}}[l] \end{pmatrix} + \mathbf{w}[l] \tag{3}$$

where l is the time index, Δt is the time resolution (typically 1 s), and $\mathbf{w}$ is the noise. The dynamical system (3) and measurement equations (1) and (2) are the basis for estimating the user PVT using the extended Kalman filter (EKF).

Previous works have shown that simple attacks are able to mislead the solutions of WLS or EKF. Stationary GPS-based time synchronization systems are currently equipped with the position-hold mode option that can potentially detect an attack if the GPS position differs from a known receiver location by

[1][Online]. Available: https://confluence.qps.nl/qinsy/en/utc-to-gps-time-correction-32245263.html (accessed Jan. 16, 2018).

a maximum allowed error [40]. This can be used as the first indication of attack. But, more advanced spoofers, such as the ones developed in [30], have the ability to manipulate the clock bias and drift estimates of the stationary receiver without altering its position and velocity (the latter should be zero). So, even with EKF on the conventional dynamical models, perturbations on the pseudoranges in (1) and pseudorange rates in (2) can be designed so that they directly result in clock bias and drift perturbations without altering the position and velocity of the receiver.

III. Modeling TSAs

This section puts forth a general attack model that encompasses the attack types discussed in the literature. This model is instrumental for designing the antispoofing technique discussed in the next section.

While TSAs have different physical mechanisms, they manifest themselves as attacks on pseudorange and pseudorange rates. These attacks can be modeled as direct perturbations on (1) and (2) as

$$\begin{aligned} \rho_s[l] &= \rho[l] + s_\rho[l] \\ \dot{\rho}_s[l] &= \dot{\rho}[l] + s_{\dot{\rho}}[l] \end{aligned} \tag{4}$$

where s_ρ and $s_{\dot{\rho}}$ are the spoofing perturbations on pseudoranges and pseudorange rates, respectively; and ρ_s and $\dot{\rho}_s$ are, respectively, the spoofed pseudorange and pseudorange rates.

A typical spoofer follows practical considerations to introduce feasible attacks. These considerations can be formulated as follows.

1) An attack is meaningful if it infringes the maximum allowed error defined in the system specification. For instance, in PMU applications, the attack should exceed the maximum allowable error tolerance specified by the IEEE C37.118 Standard, which is 1% total variation error, equivalently expressed as 0.573° phase angle error, 26.65 μs clock bias error, or 7989 m of distance-equivalent bias error [39]. On the other hand, code-division multiple-access (CDMA) cellular networks require timing accuracy of 10 μs.[2]

2) Due to the peculiarities of the GPS receivers, the internal feedback loops may loose lock on the spoofed signal if the spoofer's signal properties change rapidly [11], [29].

3) The designed spoofers have the ability to manipulate the clock drift (by manipulating the Doppler frequency) and clock bias (by manipulating the code delay) [30]. These perturbations can be applied separately; however, the smartest attacks maintain the consistency of the spoofer's transmitted signal. This means that the pertubations on pseudoranges s_ρ are the integration of perturbations over pseudorange rates $s_{\dot{\rho}}$ in (4).

Here, distinguishing between two attack procedures is advantageous as the literature includes very few research reports on the technical intricacies of the spoofer constraints.

1) Type I: The spoofer manipulates the authentic signal so that the bias abruptly changes in a very short time [13], [15], [28]. Fig. 1 illustrates this attack. The attack on the pseudoranges suddenly appears at $t = 30$ s and perturbs the pseudoranges by 8000 m. The equivalent attack on pseudorange rates is a Dirac delta function.

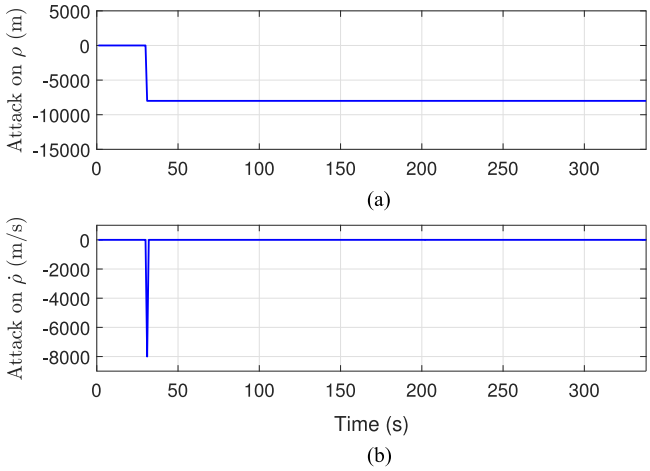


Fig. 1. Type I attack on (a) pseudorange and (b) pseudorange rate versus local observation time.

2) Type II: The spoofer gradually manipulates the authentic signals and changes the clock bias through time [11], [17], [19], [28], [29], [41]. This attack can be modeled by

$$\begin{aligned} s_\rho[l] &= s_\rho[l-1] + s_{\dot{\rho}}[l]\Delta t \\ s_{\dot{\rho}}[l] &= s_{\dot{\rho}}[l-1] + \dot{s}_{\dot{\rho}}[l]\Delta t \end{aligned} \tag{5}$$

where $s_{\dot{\rho}}$ and $\dot{s}_{\dot{\rho}}$ are, respectively, called distance equivalent velocity and distance equivalent acceleration of the attack. To maintain the victim receiver lock on the spoofer's signals, the attack should not exceed a certain distance equivalent velocity. Two such limiting numbers are reported in the literature, namely $|s_{\dot{\rho}}| \leq 400$ m/s in [29] and $|s_{\dot{\rho}}| \leq 1000$ m/s in [11]. The acceleration to reach the maximum spoofing velocity is reported to be $|\dot{s}_{\dot{\rho}}| \leq 5$ m/s^2. The spoofer acceleration $\dot{s}_{\dot{\rho}}$ can be random, which makes Type II attack quite general. The distance equivalent velocity can be converted to the equivalent bias change rate (in s/s) through dividing the velocity by the speed of light. Fig. 2 illustrates this attack. The attack on the pseudoranges starts at $t = 30$ s and perturbs the pseudoranges gradually with distance equivalent velocity not exceeding 400 m/s and maximum distance equivalent random acceleration satisfying $|\dot{s}_{\dot{\rho}}| \leq 5$ m/s^2.

The introduced attack models are quite general and can mathematically capture most attacks on the victim receiver's measurements (pseudoranges and pseudorange rates) discussed in Section I. In another words, Type I and Type II attacks can be the result of data-level spoofing, signal-level spoofing, record-and-replay attack, or a combination of the aforementioned attacks. The main difference between Type I and Type II attacks is the spoofing speed. The speed of the attack depends on the capabilities of the spoofer with respect to manipulating various features of the GPS signals. Indeed, attacks of different speeds have been reported in the literature provided earlier in this section. This

[2][Online]. Available: http://www.endruntechnologies.com/cdma (accessed Sept. 11, 2017).

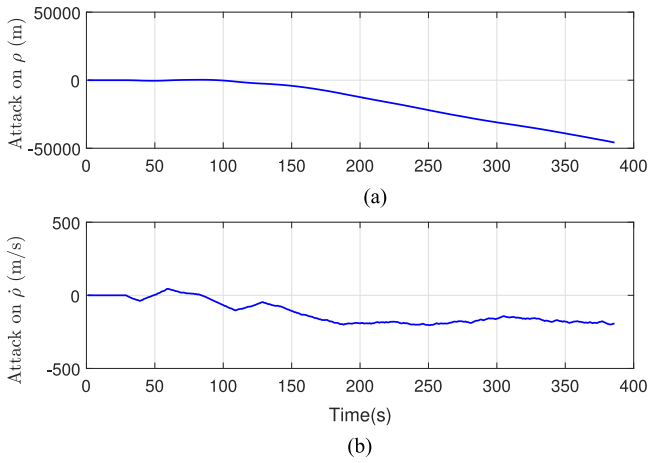


Fig. 2. Type II attack on (a) pseudorange and (b) pseudorange rate versus local observation time.

paper does not deal with jamming, which disrupts the navigation functionality completely, whereas spoofing misleads it.

In the following section, a dynamical model for the clock bias and drift is introduced, which incorporates these attacks. Based on this dynamical model, an optimization problem to estimate these attacks along with the clock bias and drift is proposed.

IV. TSA-Aware Dynamical Model and TSARM

This section introduces a dynamical model to accommodate the spoofing attack and a method to estimate the attack. Afterward, a procedure for approximately nullifying the effects of the attack on the clock bias and drift is introduced.

A. Novel TSA-Aware Dynamical Model

Modeling of the attack on pseudoranges and pseudorange rates is motivated by the attack types discussed in the previous section. These attacks do not alter the position or velocity, but only the clock bias and clock drift. Our model does not follow the conventional dynamical model for stationary receivers that allows the position of the receiver to follow a random walk model (3). Instead, the *known* position and velocity of the victim receiver are exploited jointly. The state vector contains the clock bias and clock drift, and the attacks are explicitly modeled on these components, leading to the following dynamical model

$$\underbrace{\begin{pmatrix} cb_{\mathrm{u}}[l+1] \\ c\dot{b}_{\mathrm{u}}[l+1] \end{pmatrix}}_{\mathbf{x}_{l+1}} = \underbrace{\begin{pmatrix} 1 & \Delta t \\ 0 & 1 \end{pmatrix}}_{\mathbf{F}} \underbrace{\begin{pmatrix} cb_{\mathrm{u}}[l] \\ c\dot{b}_{\mathrm{u}}[l] \end{pmatrix}}_{\mathbf{x}_l} + \underbrace{\begin{pmatrix} cs_b[l] \\ cs_{\dot{b}}[l] \end{pmatrix}}_{\mathbf{s}_l} + \underbrace{\begin{pmatrix} cw_b[l] \\ cw_{\dot{b}}[l] \end{pmatrix}}_{\mathbf{w}_l} \tag{6}$$

where s_b and $s_{\dot{b}}$ are the attacks on clock bias and clock drift, respectively, and w_b and $w_{\dot{b}}$ are colored Gaussian noise samples with covariance function defined in [3, Ch. 9]. Here, both sides are multiplied with c, which is a typically adopted convention. The state noise covariance matrix $\mathbf{Q}_l$ is particular to the crystal oscillator of the device.

Similarly, define $\boldsymbol{\rho}[l] = [\rho_1[l], \ldots, \rho_N[l]]^T$ and $\dot{\boldsymbol{\rho}}[l] = [\dot{\rho}_1[l], \ldots, \dot{\rho}_N[l]]^T$. The measurement equation can be given as

$$\underbrace{\begin{pmatrix} \boldsymbol{\rho}[l] \\ \dot{\boldsymbol{\rho}}[l] \end{pmatrix}}_{\mathbf{y}_l} = \underbrace{\begin{pmatrix} \mathbf{1}_{N\times 1} & \mathbf{0}_{N\times 1} \\ \mathbf{0}_{N\times 1} & \mathbf{1}_{N\times 1} \end{pmatrix}}_{\mathbf{H}} \underbrace{\begin{pmatrix} cb_{\mathrm{u}}[l] \\ c\dot{b}_{\mathrm{u}}[l] \end{pmatrix}}_{\mathbf{x}_l} + \underbrace{\begin{pmatrix} \|\mathbf{p}_1[l] - \mathbf{p}_{\mathrm{u}}[l]\| \\ \vdots \\ \|\mathbf{p}_N[l] - \mathbf{p}_{\mathrm{u}}[l]\| \\ (\mathbf{v}_1[l] - \mathbf{v}_{\mathrm{u}}[l])^T \cdot \frac{\mathbf{p}_1[l]-\mathbf{p}_{\mathrm{u}}[l]}{\|\mathbf{p}_1[l]-\mathbf{p}_{\mathrm{u}}[l]\|} \\ \vdots \\ (\mathbf{v}_N[l] - \mathbf{v}_{\mathrm{u}}[l])^T \cdot \frac{\mathbf{p}_N[l]-\mathbf{p}_{\mathrm{u}}[l]}{\|\mathbf{p}_N[l]-\mathbf{p}_{\mathrm{u}}[l]\|} \end{pmatrix}}_{\mathbf{c}_l} - \begin{pmatrix} cb_1[l] \\ \vdots \\ cb_N[l] \\ c\dot{b}_1[l] \\ \vdots \\ c\dot{b}_N[l] \end{pmatrix} + \underbrace{\begin{pmatrix} \epsilon_{\boldsymbol{\rho}_1}[l] \\ \vdots \\ \epsilon_{\boldsymbol{\rho}_N}[l] \\ \epsilon_{\dot{\boldsymbol{\rho}}_1}[l] \\ \vdots \\ \epsilon_{\dot{\boldsymbol{\rho}}_N}[l] \end{pmatrix}}_{\boldsymbol{\epsilon}_l}. \tag{7}$$

Explicit modeling of $\mathbf{p}_{\mathrm{u}}$ and $\mathbf{v}_{\mathrm{u}}$ in $\mathbf{c}_l$ indicates that the dynamical model benefits from using the stationary victim receiver's known position and velocity (the latter is zero). The measurement noise covariance matrix $\mathbf{R}_l$ is obtained through the measurements in the receiver. A detailed explanation of how to obtain the state and measurement covariance matrices $\mathbf{Q}_l$ and $\mathbf{R}_l$ is provided in Section V. It should be noted that the state covariance $\mathbf{Q}_l$ only depends on the victim receiver's clock behavior and does not change under spoofing. However, the measurement covariance matrix $\mathbf{R}_l$ experiences contraction. The reason is that to ensure that the victim receiver maintains lock to the fake signals, the spoofer typically applies a power advantage over the real incoming GPS signals at the victim receiver's front end [17].

Comparing (5)–(7), TSAs that do not alter the position and velocity transfer the attack on pseudoranges and pseudorange rates directly to clock bias and clock drift. Thus, it holds that $s_{\dot{\rho}} = cs_b$ and $\dot{s}_{\dot{\rho}} = cs_{\dot{b}}$.

B. Attack Detection

Let $l = k, \ldots, k+L-1$ define the time index within the observation window of length L, where k is the running time index. The solution to the dynamical model of (6) and (7) is obtained through stacking L measurements and forming the following optimization problem

$$(\hat{\mathbf{x}}, \hat{\mathbf{s}}) = \underset{\mathbf{x},\mathbf{s}}{\operatorname{argmin}} \left\{ \frac{1}{2} \sum_{l=k}^{k+L-1} \|\mathbf{y}_l - \mathbf{H}\mathbf{x}_l - \mathbf{c}_l\|^2_{\mathbf{R}_l^{-1}} + \frac{1}{2} \sum_{l=k}^{k+L-1} \|\mathbf{x}_{l+1} - \mathbf{F}\mathbf{x}_l - \mathbf{s}_l\|^2_{\mathbf{Q}_l^{-1}} + \sum_{l=k}^{k+L-1} \lambda \|\mathbf{D}\mathbf{s}_l\|_1 \right\} \tag{8}$$

where $\|\mathbf{x}\|^2_{\mathbf{M}} = \mathbf{x}^T\mathbf{M}\mathbf{x}$ and $\hat{\mathbf{x}} = [\hat{\mathbf{x}}_1, \ldots, \hat{\mathbf{x}}_L]^T$ are the estimated states, $\hat{\mathbf{s}} = [\hat{\mathbf{s}}_1, \ldots, \hat{\mathbf{s}}_L]^T$ are the estimated attacks, λ is a regularization coefficient, and $\mathbf{D}$ is an $L \times 2L$ total variation

matrix that forms the variation of the signal over time as [42]

$$\mathbf{D} = \begin{pmatrix} -1 & 0 & 1 & 0 & \dots & 0 \\ 0 & -1 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \dots & 0 & -1 & 0 & 1 \end{pmatrix}. \tag{9}$$

The first term is the weighted residuals in the measurement equation, and the second term is the weighted residuals of the state equation. The last regularization term promotes sparsity over the total variation of the estimated attack.

In (8), the clock bias and clock drift are estimated jointly with the attack. Here, the model of the two introduced attacks should be considered. In a Type I attack, a step attack is applied over the pseudoranges. The solution to the clock bias equivalently experiences a step at the attack time. The term $\|\mathbf{D}\mathbf{s}_l\|_1 = \sum_{l=k+1}^{k+L-1} \left[|s_b[l] - s_b[l-1]| + |s_{\dot{b}}[l] - s_{\dot{b}}[l-1]|\right]$ indicates a rise as it tracks the significant differences between two subsequent time instants. If the magnitude of the estimated attack in two adjacent times does not change significantly, the total variation of the attack is close to zero. Otherwise, in the presence of an attack, the total variation of the attack includes a spike at the attack time.

In a Type II attack, the total variation of the attack does not show significant changes as the attack magnitude is small at the beginning and the sparsity is not evident initially. Although we explained why it is meaningful to expect only few nonzero entries in the total variation of the attacks, in general, this is not a necessary condition for capturing the attacks during initial small total variation magnitudes. This means that explicit modeling of the attacks in (6) and estimation through (8) does not require the attacks to exhibit sparsity over the total variation. Furthermore, when the bias and bias drift are corrected using the estimated attack (we will provide one mechanism in Section IV-C), sparsity over the total variation appears for subsequent time instants. In these time instants, the attack appears to be more prominent, and in effect, the low dynamic behavior of the attack is magnified, a fact that facilitates the attack detection and will also be verified numerically. This effect is a direct consequence of (8) and the correction scheme discussed in the next section.

The optimization problem of (8) boils down to solving a simple quadratic program. Specifically, the epigraph trick in convex optimization can be used to transform the ℓ_1-norm into linear constraints [43]. The observation window L slides for a lag time $T_{\text{lag}} < L$, which can be set to $T_{\text{lag}} = 1$ for a real-time operation. The next section details the sliding window operation of the algorithm and elaborates on how to use the solution of (8) in order to provide corrected bias and drift.

C. State Correction

In observation window of length L, the estimated attack $\hat{\mathbf{s}}$ is used to compensate the impact of the attack on the clock bias, clock drift, and measurements.

Revisiting the attack model in (6), the bias at time $l+1$ depends on the clock bias and clock drift at time l. This dependence successively traces back to the initial time. Therefore, any attack on the bias that occurred in the past is accumulated through time. A similar observation is valid for the clock drift. The clock bias at time l is, therefore, contaminated by the cumulative effect of the attack on both the clock bias and clock drift in the previous times. The correction method takes into account the previously mentioned effect and modifies the bias and drift by subtracting the cumulative outcome of the clock bias and drift attacks as follows:

$$\begin{pmatrix} c\tilde{b}_{\text{u}}[l] \\ \tilde{\boldsymbol{\rho}}[l] \end{pmatrix} = \begin{pmatrix} c\hat{b}_{\text{u}}[l] \\ \boldsymbol{\rho}[l] \end{pmatrix} - \left(\sum_{l'=k}^{l} \hat{s}_b[l'] - \sum_{l'=k}^{l-1} \hat{s}_{\dot{b}}[l'] \Delta t \right) \mathbf{1} \tag{10}$$

$$\begin{pmatrix} c\tilde{\dot{b}}_{\text{u}}[l] \\ \tilde{\dot{\boldsymbol{\rho}}}[l] \end{pmatrix} = \begin{pmatrix} c\hat{\dot{b}}_{\text{u}}[l] \\ \dot{\boldsymbol{\rho}}[l] \end{pmatrix} - \left(\sum_{l'=k}^{l} \hat{s}_{\dot{b}}[l'] \right) \mathbf{1}$$

where $\tilde{b}_{\text{u}}$ and $\tilde{\dot{b}}_{\text{u}}$ are, respectively, the corrected clock bias and clock drift, $\tilde{\boldsymbol{\rho}}$ and $\tilde{\dot{\boldsymbol{\rho}}}$ are, respectively, the corrected pseudorange and pseudorange rates, and $\mathbf{1}$ is an all one vector of length $N+1$. In (10), $l = 1, \dots, L$ for the first observation window ($k = 1$) and $k + L - T_{\text{lag}} \leq l \leq k + L - 1$ for the observation windows afterward. This ensures that the measurements and states are not doubly corrected. The corrected measurements are used for solving (8) for the next observation window.

The overall attack detection and modification procedure is illustrated in Algorithm 1. After the receiver collects L measurements, problem (8) is solved. Based on the estimated attack, the clock bias and clock drift are cleaned using (10). This process is repeated for a sliding window and only the clock bias and drift of the time instants that have not been cleaned previously are corrected. In another words, there is no duplication of modification over the states.

The proposed technique boils down to solving a simple quadratic program with only few variables and can, thus, be

Algorithm 1: TSA Rejection and Mitigation (TSARM).

1: Set $k = 1$
2: **while** True **do**
3: Batch $\mathbf{y}_l \ \forall l = k, \dots, k + L - 1$
4: Construct $\mathbf{H}, \mathbf{c}_l, \mathbf{F} \ \forall l = k, \dots, k + L - 1$
5: Compute $\mathbf{Q}_l$ and $\mathbf{R}_l$ (details provided in Section V)
6: Estimate $\hat{\mathbf{x}}, \hat{\mathbf{s}}$ via (8)
7: Assign $c\hat{b}_{\text{u}}[l] = \hat{\mathbf{x}}[m], m = 2l - 1$ and $c\hat{\dot{b}}_{\text{u}}[l] = \hat{\mathbf{x}}[m], m = 2l \ \ \forall l = k, \dots, k + L - 1$
8: Assign $\hat{s}_b[l] = \hat{\mathbf{s}}[m], m = 2l - 1$ and $\hat{s}_{\dot{b}}[l] = \hat{\mathbf{s}}[m], m = 2l \ \ \forall l = k, \dots, k + L - 1$
9: Modify $\hat{b}_{\text{u}}[l]$, $\hat{\dot{b}}_{\text{u}}[l]$, $\boldsymbol{\rho}[l]$ and $\dot{\boldsymbol{\rho}}[l]$ via (10) $\forall l = 1, \dots, L$ for the first window and $k + L - T_{\text{lag}} \leq l \leq k + L - 1$ for the windows afterwards
10: Set $\mathbf{y}_l = \begin{pmatrix} \tilde{\boldsymbol{\rho}}[l] \\ \tilde{\dot{\boldsymbol{\rho}}}[l] \end{pmatrix} \forall l = k, \dots, k + L - 1$
11: Output $t_R^{\text{UTC}}[l] = t_R[l] - \tilde{b}_{\text{u}}[l] - \Delta t_{UTC} \ \forall l = k, \dots, k + L - 1$ to the user for time stamping
12: Slide the observation window by setting $k = k + T_{\text{lag}}$
13: **end while**

performed in real time. For example, efficient implementations of quadratic programming solvers are readily available in low-level programming languages. The implementation of this technique in GPS receivers and electronic devices is thus straightforward and does not necessitate creating new libraries.

V. Numerical Results

We first describe the data collection device and then assess three representative detection schemes in the literature that fail to detect the TSA attacks. These attacks mislead the clock bias and clock drift, while maintaining correct location and velocity estimates. The performance of our detection and modification technique over these attacks is illustrated afterward.

A. GPS Data Collection Device

A set of real GPS signals has been recorded with a Google Nexus 9 Tablet at the University of Texas at San Antonio on June, 1, 2017.[3] The ground truth of the position is obtained through taking the median of the WLS position estimates for a stationary device. This device has been recently equipped with a GPS chipset that provides raw GPS measurements. An android application, called `GNSS Logger`, has been released along with the postprocessing MATLAB codes by the Google Android location team [38].

Of interest here are the two classes of the `Android.location` package. The `GnssClock`[4] provides the GPS receiver clock properties and the `GnssMeasurement`[5] provides the measurements from the GPS signals both with subnanosecond accuracies. To obtain the pseudorange measurements, the transmission time is subtracted from the time of reception. The function `getReceivedSvTimeNanos()` provides the transmission time of the signal which is with respect to the current GPS week (Saturday–Sunday midnight). The signal reception time is available using the function `getTimeNanos()`. To translate the receiver's time to the GPS time (and GPS time of week), the package provides the difference between the device clock time and GPS time through the function `getFullBiasNanos()`.

The receiver clock's covariance matrix $\mathbf{Q}_l$ is dependent on the statistics of the device clock oscillator. The following model is typically adopted:

$$\mathbf{Q}_l = \begin{pmatrix} c^2\sigma_b^2\Delta t + c^2\sigma_{\dot{b}}^2\frac{\Delta t^3}{3} & c^2\sigma_{\dot{b}}^2\frac{\Delta t^2}{2} \\ c^2\sigma_{\dot{b}}^2\frac{\Delta t^2}{2} & c^2\sigma_{\dot{b}}^2\Delta t \end{pmatrix} \tag{11}$$

where $\sigma_b^2 = \frac{h_0}{2}$ and $\sigma_{\dot{b}}^2 = 2\pi^2 h_{-2}$; and we select $h_0 = 8 \times 10^{-19}$ and $h_{-2} = 2 \times 10^{-20}$ [44, Ch. 9]. For calculating the measurement covariance matrix $\mathbf{R}_l$, the uncertainty of the pseudorange and pseudorange rates are used. These uncertainties are available from the device together with the respective measurements.[5] In the experiments, we set $\lambda = 5 \times 10^{-10}$, because the distance magnitudes are in tens of thousands of meters. The estimated clock bias and drift through EKF in a normal operation is considered as the ground truth for the subsequent analysis. In what follows, reported times are local.

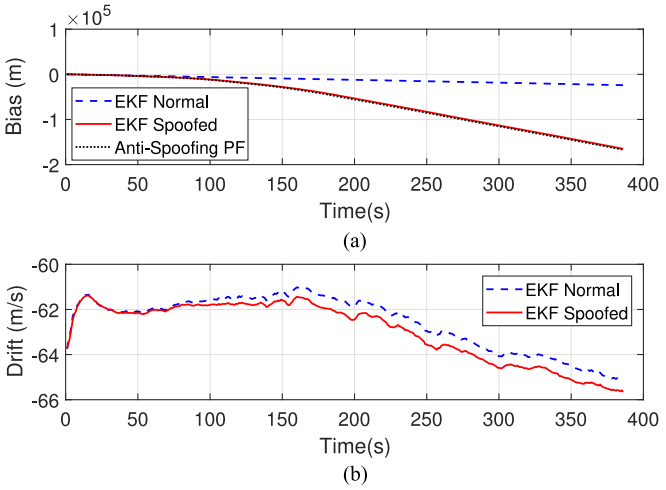


Fig. 3. Effect of Type II attack on the EKF and the antispoofing particle filter [27] on (a) clock bias and (b) clock drift. The attack started at $t = 30$ s. Panel (b) does not include the drift.

B. Failure of Prior Work in Detecting Consistent Attacks

This section demonstrates that three relevant approaches from Table I may fail to detect consistent attacks, that is, attacks where s_ρ is the integral of $s_{\dot{\rho}}$ in (4).

The performance of the EKF and the antispoofing particle filter of [27] subject to a Type II attack is reported first. The perturbations over GPS measurements are the same as in Fig. 2 and are used as an input to the EKF and the particle filter. The attack starts at $t = 30$ s. Fig. 3 depicts the effect of attack on the clock bias and drift. The EKF on the dynamical model in (6) and (7) blindly follows the attack after a short settling time. The antispoofing particle filter only estimates the clock bias and assumes the clock drift is known from WLS. Similarly to the EKF, the particle filter is not able to detect the consistent spoofing attack. The maximum difference between the receiver estimated position obtained from the EKF on (3) under Type II attack and under normal operation is $x_{\text{diff}} = 67$ m, $y_{\text{diff}} = 112$ m, and $z_{\text{diff}} = 71$ m. The position estimate has thus not been considerably altered by the attack.

The third approach to be evaluated has been proposed in [28] and monitors the statistics of the receiver clock, as a typical spoofing detection technique [33]. Considering that off-the-shelf GPS receivers compute the bias at regular Δt intervals, a particular approach is to estimate the GPS time after k time epochs and confirm that the time elapsed is indeed $k\Delta t$ [28]. To this end, the following statistic can be formulated: $\mathcal{D}(k) = [t_R^{\text{GPS}}(k) - t_R^{\text{GPS}}(1) - (k-1)\Delta t - \sum_{k'=1}^{k} \hat{\dot{b}}[k']\Delta t]c$. The test statistic $\mathcal{D}$ is normally distributed with mean zero when there is no attack and may have nonzero mean depending on the attack, as will be demonstrated shortly. Its variance needs to be estimated from a

[3][Online]. Available: https://github.com/Alikhalaj2006/UTSA_GPS_DATA.git

[4][Online]. Available: https://developer.android.com/reference/android/location/GnssClock.html (accessed Feb. 20, 2017).

[5][Online]. Available: https://developer.android.com/reference/android/location/GnssMeasurement.html (accessed Feb. 20, 2017).

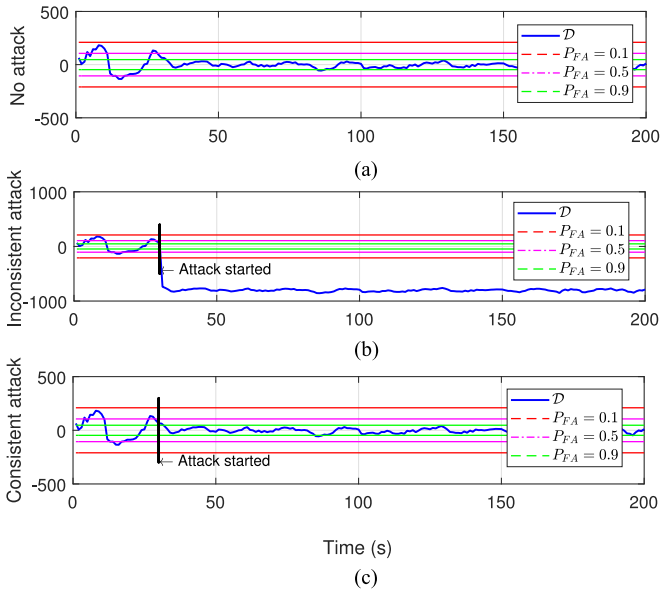


Fig. 4. Performance of hypothesis testing based on statistic (see Section V-B) [28] under Type I attack for different false alarm probabilities: (a) no attack, (b) inconsistent attack, and (c) consistent attack.

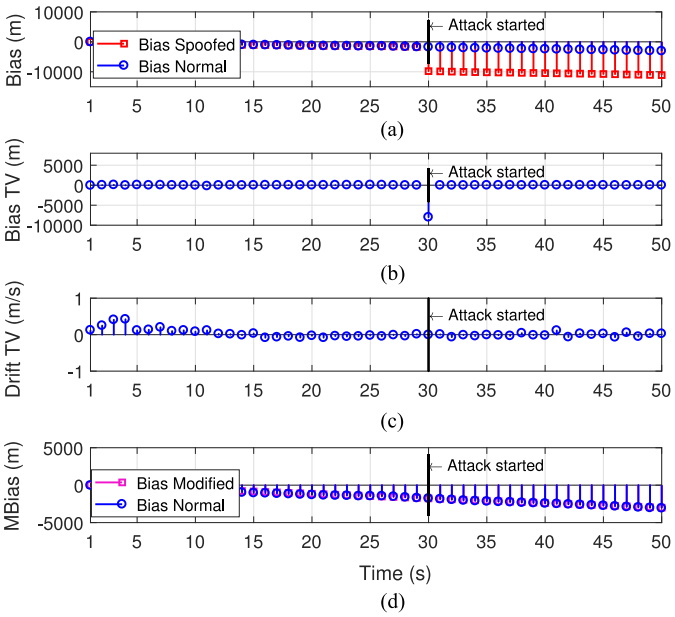


Fig. 5. Result of attack detection and modification over a Type I attack that started at $t = 30$ s. From top to bottom: (a) normal clock bias (blue) and spoofed bias (red), (b) total variation of the estimated bias attack $\hat{s}_b$, (c) total variation of the estimated drift attack $\hat{s}_{\dot{b}}$, and (d) true bias (blue) and modified bias (magenta).

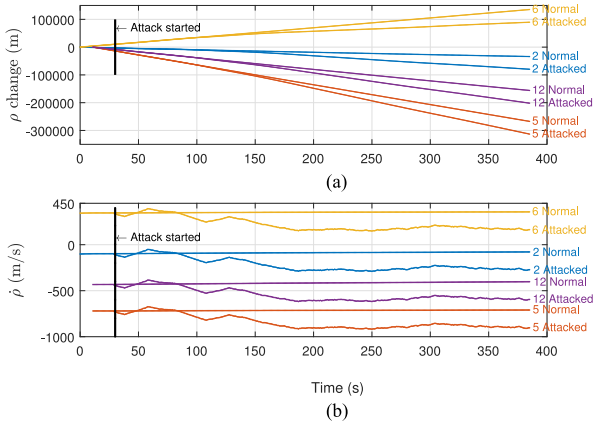


Fig. 6. Comparison of (a) normal pseudorange change ($\rho(k) - \rho(1)$) and spoofed pseudoranges change ($\rho_s(k) - \rho_s(1)$), and (b) normal pseudorange rates ($\dot{\rho}$) and spoofed pseudorange rates ($\dot{\rho}_s$) under Type II attack for some of the visible satellites. The attack started at $t = 30$ s.

few samples under normal operation. The detection procedure relies on statistical hypothesis testing. For this, a false alarm probability P_{FA} is defined. Each P_{FA} corresponds to a threshold γ to which $\mathcal{D}(k)$ is compared against [45, Ch. 6]. If $|\mathcal{D}(k)| \geq \gamma$, the receiver is considered to be under attack.

The result of this method is shown in Fig. 4 for different false alarm probabilities. Fig. 4(a) depicts $\mathcal{D}(k)$ when the system is not under attack. The time signature lies between the thresholds only for low false alarm probabilities. The system can detect the attack in case of an inconsistent Type I attack, in which s_ρ is not the integration of perturbations over pseudorange rates $s_{\dot{\rho}}$, and only pseudoranges are attacked. Fig. 4(b) shows that the attack is detected right away. However, for smart attacks, where the spoofer maintains the consistency between the pseudorange and pseudorange rates, Fig. 4(c) illustrates that the signature $\mathcal{D}(k)$ fails to detect the attack. This example shows that the statistical behavior of the clock can remain untouched under smart spoofing attacks. In addition, even if an attack is detected, the previous methods cannot provide an estimate of the attack.

C. Spoofing Detection on Type I Attack

Fig. 5 shows the result of solving (8) using the GPS measurements perturbed by the Type I attack of Fig. 1. The spoofer has the capability to attack the signal in a very short time so that the clock bias experiences a jump at $t = 30$ s. The estimated total variation of bias attack renders a spike right at the attack time. The modification procedure of (10) corrects the clock bias using the estimated attack.

D. Spoofing Detection on Type II Attack

The impact of the Type II attack on the pseudoranges and pseudorange rates is shown in Fig. 6. Specifically, Fig. 6(a) illustrates the normal and spoofed pseudorange changes with respect to their initial value at $t = 0$ s for some of the visible satellites in the receiver's view. Fig. 6(b) depicts the corresponding pseudorange rates. The tag at the end of each line indicates the satellite ID and whether the pseudorange (or pseudorange rate) corresponds to the normal operation or operation under attack. The spoofed pseudoranges diverge quadratically starting at $t = 30$ s following the Type II attack.

For the Type II attack, Algorithm 1 is implemented for an sliding window with $L = 50$ s with $T_{\text{lag}} = 10$ s. Fig. 7 shows the attacked clock bias starting at $t = 30$ s. Since the attack magnitude is small at initial times of the spoofing, neither the estimated attack $\hat{s}_b$ nor the total variation does not show

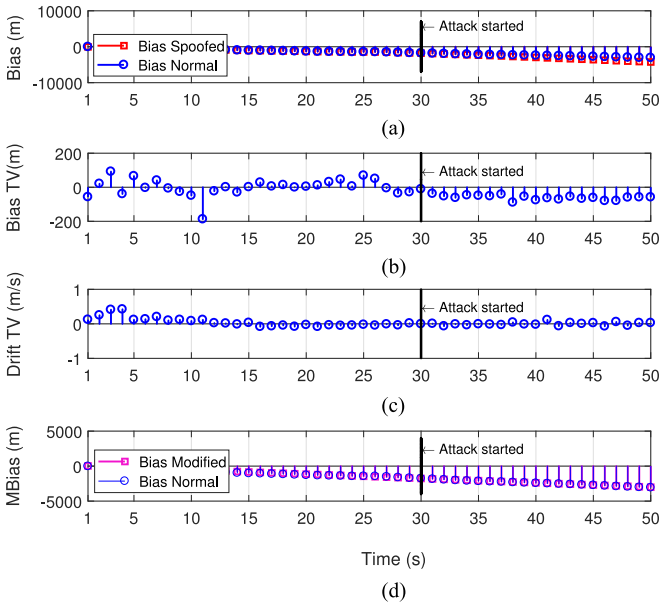


Fig. 7. Result of attack detection and modification over Type II attack for $t = 1$ s through $t = 50$ s. The attack started at $t = 30$ s. From top to bottom: (a) normal clock bias (blue) and spoofed bias (red), (b) estimated bias attack $\hat{s}_b$, (c) total variation of the estimated bias attack, and (d) true bias (blue) and modified bias (magenta).

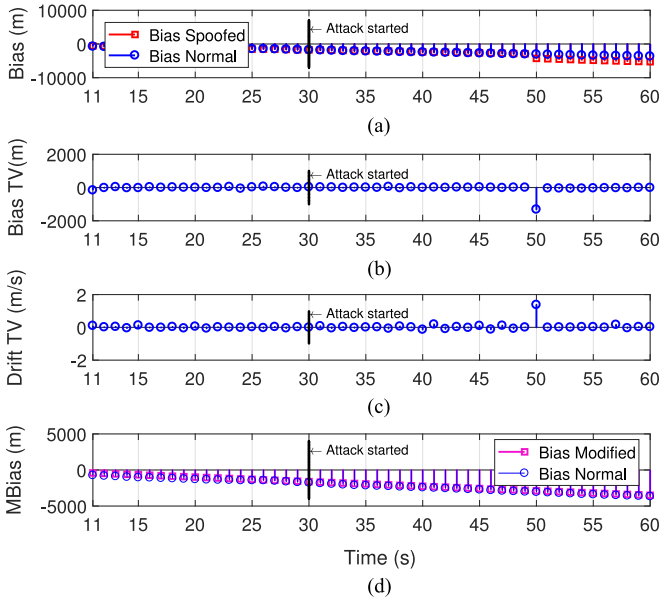


Fig. 8. Result of attack detection and modification over Type II attack for $t = 11$ s through $t = 60$ s. From top to bottom: (a) normal clock bias (blue) and spoofed bias (red), (b) estimated bias attack $\hat{s}_b$, (c) total variation of the estimated bias attack, and (d) true bias (blue) and modified bias (magenta).

significant values. The procedure of the sliding window is to correct the current clock bias and clock drift for all the times that have not been modified previously. Hence, at the first run the estimates of the whole window are modified. Fig. 8 shows the estimated attack and its corresponding total variation after one T_{lag}. As is obvious from the figure, the modification of the previous clock biases transforms the low dynamic behavior of

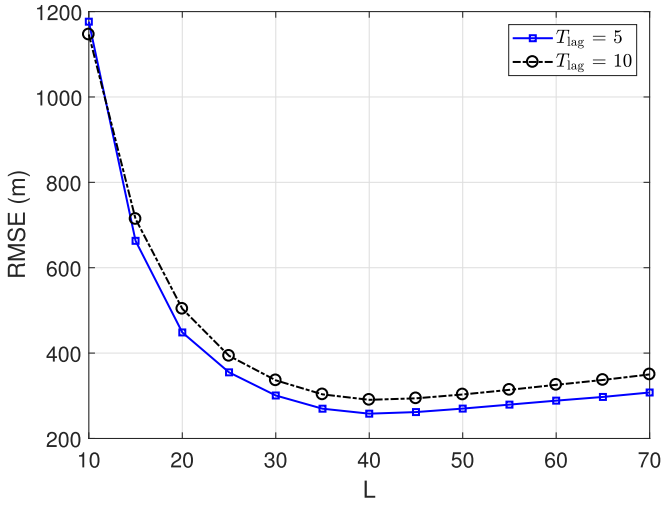


Fig. 9. RMSE of TSARM for various values of L and T_{lag}.

the spoofer to a large jump at $t = 50$ s, which facilitates the detection of attack through the total variation component in (8). The clock bias and drift have been modified for the previous time instants and need to be cleaned only for $t = 50$ s $- 60$ s.

E. Analysis of the Results

Let K be the total length of the observation time (in this experiment, $K = 386$). The root mean square error (RMSE) is introduced: $\text{RMSE} = \frac{c}{K}\sqrt{\sum_{k=0}^{K-1}(\tilde{b}_u[k] - \check{b}_u[k])^2}$, which shows the average error between the clock bias that is the output from the spoofing detection technique, $\tilde{b}_u$, and the estimated clock bias from EKF under the normal operation, $\check{b}_u$, which is considered as the ground truth. Comparing the results of the estimated spoofed bias from the EKF and the normal bias shows that $\text{RMSE}_{\text{EKF}} = 3882$ m. This error for the antispoofing particle filter is $\text{RMSE}_{\text{PF}} = 3785$ m. Having applied TSARM, the clock bias has been modified with a maximum error of $\text{RMSE}_{\text{TSARM}} = 258$ m. Fig. 9 illustrates the RMSE of TSARM for a range of values for the window size L and the lag time T_{lag}. When the observation window is smaller, fewer measurements are used for state estimation. On the other hand, when L exceeds 40 s, the number of states to be estimated grows although more measurements are employed for estimation. The numerical results illustrate that (6) models the clock bias and drift attacks effectively, which are subsequently estimated using (8) and corrected through (10).

VI. Concluding Remarks and Future Work

This paper discussed the research issue of TSAs on devices that rely on GPS for time tagging their measurements. Two principal types of attacks are discussed, and a dynamical model that specifically models these attacks is introduced. The attack detection technique solves an optimization problem to estimate the attacks on the clock bias and clock drift. The spoofer manipulated clock bias and drift are corrected using the estimated attacks. The proposed method detects the behavior of spoofer even if the measurements integrity is preserved. The numeri-

cal results demonstrate that the attack can be largely rejected, and the bias can be estimated within 0.86 μs of its true value, which lies within the standardized accuracy in PMU and CDMA applications. The proposed method can be implemented for a real-time operation.

In this paper, the set of GPS signals are obtained from an actual GPS receiver in a real environment, but the attacks are simulated based on the characteristics of real spoofers reported in the literature. Experimentation on the behavior of the proposed detection and mitigation approach under real spoofing scenarios is the subject of future research.

REFERENCES

[1] Energy.gov, Office of Electricity Delivery & Energy Reliability. Online. Available: http://energy.gov/oe/services/technology-development/smart-grid. Accessed: Aug. 8, 2016.

[2] Gps.gov, Official U.S. government information about the global positioning system (GPS) and related topics." [Online]. Available: http://www.gps.gov/applications/timing/

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

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

[5] P. Misra and P. Enge, *Global Positioning System: Signals, Measurements, and Performance*, 2nd ed. Lincoln, MA, USA: Ganga-Jamuna Press, 2006.

[6] I. Yaesh and U. Shaked, "Neuro-adaptive H_∞ estimation and its application to improved tracking in GPS receivers," *IEEE Trans. Ind. Electron.*, vol. 56, no. 3, pp. 642–647, Mar. 2009.

[7] X. Li and Q. Xu, "A reliable fusion positioning strategy for land vehicles in GPS-denied environments based on low-cost sensors," *IEEE Trans. Ind. Electron.*, vol. 64, no. 4, pp. 3205–3215, Apr. 2017.

[8] "Electric sector failure scenarios and impact analyses—Version 3.0," Elect. Power Res. Inst., Rep. Tech. Working Group 1, Version 1.0, Dec. 2015.

[9] D. Schmidt, K. Radke, S. Camtepe, E. Foo, and M. Ren, "A survey and analysis of the GNSS spoofing threat and countermeasures," *ACM Comput. Survey*, vol. 48, no. 4, pp. 64:1–64:31, May 2016.

[10] B. Moussa, M. Debbabi, and C. Assi, "Security assessment of time synchronization mechanisms for the smart grid," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 1952–1973, Third Quarter 2016.

[11] 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. Protect.*, vol. 5, pp. 146–153, Dec. 2012.

[12] 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.

[13] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela, and A. D. Dominguez-García, "Spoofing GPS receiver clock offset of phasor measurement units," *IEEE Trans. Power Syst.*, vol. 28, no. 3, pp. 3253–3262, Aug. 2013.

[14] P. Risbud, N. Gatsis, and A. Taha, "Vulnerability analysis of smart grids to GPS spoofing," *IEEE Trans. Smart Grid*, to be published.

[15] T. Nighswander, B. Ledvina, J. Diamond, R. Brumley, and D. Brumley, "GPS software attacks," in *Proc. ACM Conf. Comput. Commun. Security*, Oct. 2012, pp. 450–461.

[16] N. O. Tippenhauer, C. Pöpper, K. B. Rasmussen, and S. Čapkun, "On the requirements for successful GPS spoofing attacks," in *Proc. 18th ACM Conf. Comput. Commun. Security*, Oct. 2011, pp. 75–86.

[17] 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. PP, no. 99, pp. 1–1, doi: 10.1109/TAES.2017.2765258.

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

[19] P. Papadimitratos and A. Jovanovic, "GNSS-based positioning: Attacks and countermeasures," in *Proc. Military Commun. Conf.*, San Diego, CA, USA, Nov. 2008, pp. 1–7.

[20] Q. Zeng, H. Li, and L. Qian, "GPS spoofing attack on time synchronization in wireless networks and detection scheme design," in *IEEE Military Commun. Conf.*, Oct. 2012, pp. 1–5.

[21] Y. Fan, Z. Zhang, M. Trinkle, A. D. Dimitrovski, J. B. Song, and H. Li, "A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart grids," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 2659–2668, Nov. 2015.

[22] A. Ranganathan, H. Ólafsdóttir, and S. Capkun, "SPREE: A spoofing resistant GPS receiver," in *Proc. 22nd Annu. Int. Conf. Mobile Comput. Netw.*, 2016, pp. 348–360.

[23] D. Chou, L. Heng, and G. X. Gao, "Robust GPS-based timing for phasor measurement units: A position-information-aided approach," in *Proc. 27th Int. Tech. Meeting Satellite Division Inst. Navig.*, Sep. 2014, pp. 1261–1269.

[24] Y. Ng and G. X. Gao, "Advanced multi-receiver position-information-aided vector tracking for robust GPS time transfer to PMUs," in *Proc. 28th Int. Tech. Meeting Satellite Division Inst. Navig.*, Sep. 2015, pp. 3443–3448.

[25] D.-Y. Yu, A. Ranganathan, T. Locher, S. Čapkun, and D. Basin, "Short paper: Detection of GPS spoofing attacks in power grids," in *Proc. ACM Conf. Security Privacy Wireless Mobile Netw.*, 2014, pp. 99–104.

[26] K. Jansen, N. O. Tippenhauer, and C. Pöpper, "Multi-receiver GPS spoofing detection: Error models and realization," in *Proc. 32nd Annu. Conf. Comput. Security Appl.*, 2016, pp. 237–250.

[27] S. Han, D. Luo, W. Meng, and C. Li, "A novel anti-spoofing method based on particle filter for GNSS," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2014, pp. 5413–5418.

[28] F. Zhu, A. Youssef, and W. Hamouda, "Detection techniques for data-level spoofing in GPS-based phasor measurement units," in *Proc. 2016 Int. Conf. Sel. Topics Mobile Wireless Netw.*, Apr. 2016, pp. 1–8.

[29] D. P. Shepard and T. E. Humphreys, "Characterization of receiver response to a spoofing attacks," in *Proc. 24th Int. Tech. Meeting Satellite Division Inst. Navig.*, Portland, OR, USA, Sep. 2011, pp. 2608–2618. [Online]. Available: https://www.ion.org/publications/abstract.cfm?articleID=9814

[30] 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 Satellite Division Inst. Navig.*, Savannah, GA, USA, Sep. 2008, pp. 2314–2325.

[31] B. Motella *et al.*, "Performance assessment of low cost GPS receivers under civilian spoofing attacks," in *Proc. 5th ESA Workshop Satellite Navig. Technol. Eur. Workshop GNSS Signals Signal Process.*, Dec. 2010, pp. 1–8.

[32] P. Teunissen, "Quality control in integrated navigation systems," *IEEE Aerosp. Electron. Syst. Mag.*, vol. 5, no. 7, pp. 35–41, Jul. 1990.

[33] L. Heng, J. J. Makela, A. D. Dominguez-García, R. B. Bobba, W. H. Sanders, and G. X. Gao, "Reliable GPS-based timing for power systems: A multi-layered multi-receiver architecture," in *Proc. Power Energy Conf. Illinois*, Feb. 2014, pp. 1–7.

[34] L. Heng, D. B. Work, and G. X. Gao, "GPS signal authentication from cooperative peers," *IEEE Trans. Intell. Transp. Syst.*, vol. 16, no. 4, pp. 1794–1805, Aug. 2015.

[35] D. Radin, P. F. Swaszek, K. C. Seals, and R. J. Hartnett, "GNSS spoof detection based on pseudoranges from multiple receivers," in *Proc. 2015 Int. Tech. Meeting Inst. Navig.*, Jan. 2015, pp. 657–671.

[36] C. Masreliez and R. Martin, "Robust Bayesian estimation for the linear model and robustifying the Kalman filter," *IEEE Trans. Autom. Control*, vol. AC-22, no. 3, pp. 361–371, Jun. 1977.

[37] S. Farahmand, G. B. Giannakis, and D. Angelosante, "Doubly robust smoothing of dynamical processes via outlier sparsity constraints," *IEEE Trans. Signal Process.*, vol. 59, no. 10, pp. 4529–4543, Oct. 2011.

[38] "Android GNSS." [Online]. Available: https://developer.android.com/guide/topics/sensors/gnss.html. Accessed on: Feb. 20, 2017.

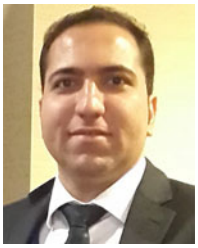
[39] *IEEE Standard for Synchrophasor Measurements for Power Systems*, IEEE Std C37.118.1-2011 (Revision of IEEE Std C37.118-2005), Dec. 2011, pp. 1–61.

[40] "Model 1088b GPS satellite clock (40 ns)." [Online]. Available: http://www.arbiter.com/catalog/product/model-1088b-gps-satellite-precis ion-time-clock-40ns.php. Accessed on: Feb. 20, 2017.

[41] 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.

[42] F. I. Karahanoglu, Bayram, and D. V. D. Ville, "A signal processing approach to generalized 1-D total variation," *IEEE Trans. Signal Process.*, vol. 59, no. 11, pp. 5265–5274, Nov. 2011.

[43] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge UK: Cambridge Univ. Press, 2004.
[44] R. G. Brown and P. Y. C. Hwang, *Introduction to Random Signals and Applied Kalman Filtering: With MATLAB Exercises and Solutions,* 3rd ed. New York, NY, USA: Wiley, 1997.
[45] S. M. Kay, *Fundamentals of Statistical Signal Processing, Volume II: Detection Theory*. Englewood Cliffs, NJ, USA: Prentice-Hall, 1993.



Ali Khalajmehrabadi (S'16) received the B.Sc. degree in electrical and computer engineering from the Babol Noshirvani University of Technology, Babol, Iran, in 2010, and the M.Sc. degree in electrical-electronics and telecommunications from the University Technology Malaysia, Johor Bahru, Malaysia, in 2012. He is currently working toward the Ph.D. degree in electrical engineering with the Department of Electrical and Computer Engineering, University of Texas at San Antonio, San Antonio, TX, USA.

His research interests include indoor localization and navigation systems, collaborative localization, and global navigation satellite systems.

Mr. Khalajmehrabad was the recipient of the Best Graduate Student Award. He is a Student Member of the Institute of Navigation.

Nikolaos Gatsis (S'04–M'05) received the Diploma (with Hons.) degree in electrical and computer engineering from the University of Patras, Patras, Greece, in 2005, and the M.Sc. degree in electrical engineering and the Ph.D. degree in electrical engineering with minor in mathematics, both from the University of Minnesota, Minneapolis, MN, USA, in 2010 and 2012, respectively.

He is currently an Assistant Professor with the Department of Electrical and Computer Engineering, University of Texas at San Antonio, San Antonio, TX, USA. He has coorganized symposia in the area of smart grids in IEEE GlobalSIP 2015 and IEEE GlobalSIP 2016. His research interests include the areas of smart power grids, communication networks, and cyberphysical systems, with an emphasis on optimal resource management and statistical signal processing.

Dr. Gatsis has served as a Co-Guest Editor for a special issue of the IEEE JOURNAL ON SELECTED TOPICS IN SIGNAL PROCESSING on critical infrastructures.

David Akopian (M'02–SM'04) received the Ph.D. degree in electrical engineering from Tampere University of Technology, Finland, in 1997.

He is currently a Professor with the University of Texas at San Antonio, San Antonio, TX, USA. He was a Senior Research Engineer and a Specialist with Nokia Corporation from 1999 to 2003. From 1993 to 1999, he was a Researcher and an Instructor with the Tampere University of Technology, Finland. He has authored and coauthored 140 publications and holds more than 30 patents. He served in organizing and program committees of many IEEE conferences and cochairs annual SPIE Multimedia on Mobile Devices conferences. His current research interests include digital signal processing algorithms for communication and navigation receivers, positioning, dedicated hardware architectures, and platforms for software-defined radio and communication technologies for healthcare applications. His research has been supported by the National Science Foundation, National Institutes of Health, USAF, U.S. Navy, and Texas foundations.

Ahmad F. Taha (S'07–M'15) received the B.E. degree from the American University of Beirut, Beirut, Lebanon, in 2011, and the Ph.D. degree from Purdue University, West Lafayette, IN, USA, in 2015, both in electrical and computer engineering.

In Summer 2010, Summer 2014, and Spring 2015, he was a Visiting Scholar with MIT, University of Toronto, and Argonne National Laboratory. He is currently an Assistant Professor with the Department of Electrical and Computer Engineering, The University of Texas, San Antonio, San Antonio, TX, USA. He is interested in understanding how complex cyber-physical systems operate, behave, and *misbehave*. His research interests includes optimization and control of power systems, observer design and dynamic state estimation, and cyber security.