

# Tuning-Free, Low Memory Robust Estimator to Mitigate GPS Spoofing Attacks

Junhwan Lee, Ahmad F. Taha<sup>ID</sup>, Nikolaos Gatsis<sup>ID</sup>, and David Akopian<sup>ID</sup>

**Abstract**—The operation of critical infrastructures, such as the electrical power grid, cellphone towers, and financial institutions relies on precise timing provided by stationary global positioning system (GPS) receivers. These GPS devices are vulnerable to a type of spoofing called time synchronization attack (TSA), whose objective is to maliciously alter the timing provided by the GPS receiver. The objective of this letter is to design a tuning-free, low memory robust estimator to mitigate such spoofing attacks. The contribution is that the proposed method dispenses with several limitations found in the existing state-of-the-art methods in the literature that require parameter tuning, availability of the statistical distributions of noise, real-time optimization, or heavy computations. Specifically, we: 1) utilize an observer design for linear systems under unknown inputs; 2) adjust it to include a state-correction algorithm; 3) design a realistic experimental setup with real GPS data and sensible spoofing attacks; and 4) showcase how the proposed tuning-free, low memory robust estimator can combat TSAs. Numerical tests with real GPS data demonstrate that accurate time can be provided to the user under various attack conditions.

**Index Terms**—Robust state estimation, observer design, GPS spoofing, time synchronization attacks, low memory estimation.

## I. INTRODUCTION AND MOTIVATION

THE GLOBAL Positioning System (GPS) is widely utilized in an abundance of applications. The study [1] in particular emphasizes how critical infrastructures such as communications, the power grid, transportation, and even financial services can be disrupted if the integrity of the GPS is compromised.

Since most systems rely on non-encrypted civilian GPS signals [2], the GPS is vulnerable to intentional attacks. There are two types of deliberate attacks on GPS: jamming and spoofing [3]. While jamming completely blocks signal reception by transmitting high power noise, spoofing changes the transmitted signal or data to deceive the GPS receiver.

Manuscript received March 1, 2019; revised May 8, 2019; accepted May 30, 2019. Date of publication June 12, 2019; date of current version June 24, 2019. This work was supported by the National Science Foundation under Grant ECCS-1719043. Recommended by Senior Editor G. Cherubini. (Corresponding author: Ahmad F. Taha.)

The authors are with the Department of Electrical and Computer Engineering, University of Texas at San Antonio, San Antonio, TX 78240 USA (e-mail: junhwan.lee@utsa.edu; ahmad.taha@utsa.edu; nikolaos.gatsis@utsa.edu; david.akopian@utsa.edu).

Digital Object Identifier 10.1109/LCSYS.2019.2922497

Various experiments have shown that different types of spoofing attacks such as data level spoofing, signal level spoofing, delaying, and record-and-reply attacks [4]–[6] could affect off-the-shelf GPS receivers.

A Time Synchronization Attack (TSA) is a particular class of spoofing attacks on *stationary* GPS receivers that provide precise timing in various applications, including phasor measurement units (PMUs), cellphone towers, and financial institutions [7], [8]. The objective of the attack is to mislead the time estimated by the receiver which, in the case of the power grid for example, can disrupt the reliable monitoring of the grid’s cyber-physical status.

Countermeasures against spoofing attacks have been proposed in [9]–[11] and include techniques that rely on multiple GPS receivers [12], [13] or check the magnitude of error in the GPS data [9]; see [5] for a review of anti-spoofing techniques. Another approach to mitigate and detect spoofing TSAs is through robust, dynamic state estimation routines that are designed to deal with outliers and malicious attacks.

The robust state estimation literature is indeed rich with two main classes of methods. The first class is based on robust observers and Lyapunov theory which often does not assume any statistical distribution for unknown inputs or noise [14], [15]. The second class is based on Kalman filter and its derivatives, that often assume statistical distribution of noise [16]–[18]. Relevant to the robust estimation problem under TSAs, a novel anti-spoofing particle filter is devised to find the receiver position even under spoofing interference [10]. In our recent work [11], we develop a real-time optimization method to detect and mitigate TSAs using weighted  $\ell_1$  minimization. The aforementioned methods all require either tuning of some parameters, real-time optimization, or availability of the statistical distribution of noise.

The objective of this letter is to design a robust state estimator that combats TSAs while being endowed with the following properties: (i) It is a tuning-free method that does not require any training; (ii) it has low memory requirement in the sense no heavy computations are needed in real-time; and (iii) the designed tuning-free, low-memory robust estimator can correctly reconstruct the actual physical state of the receiver using a realistic testbed. We note here that our objective is not to develop a generalized theory for robust estimation, but rather to build on the recent theoretical advancement in this field and adapt it to the GPS spoofing problem through a realistic testbed. The robust state estimation method presented in this letter is an adaptation of the method in [19]. The motivation

for using this estimator is provided in great detail in the next sections; this letter's organization is given next.

Section II presents the dynamic modeling of bias and drift in GPS receivers and showcases how TSA attacks can be modeled and designed to mislead standard state estimators. Section III presents a robust state estimator in addition to a state correction and TSA reconstruction routine. Section IV concludes this letter with realistic numerical tests on real GPS data. For reproducibility, the data used in the numerical tests and the results are all provided through a Github link.

## II. DYNAMIC MODELING UNDER GPS SPOOFING

The primary goal of GPS localization is to accurately estimate the position, velocity, clock bias, and clock drift of the receiver in every time step—conventionally referred to as the position, velocity, and time (PVT) solution.

The position of the GPS receiver (user) in Earth Centered Earth Fixed coordinates is denoted by  $\mathbf{p}_u = [x_u, y_u, z_u]^\top$ . To estimate the receiver's location and velocity, the GPS exploits the known location of satellites and the distance from each satellite to the receiver. Let  $N$  denote the number of fixed satellites visible by the receiver, then  $\mathbf{p}_n = [x_n(t_n), y_n(t_n), z_n(t_n)]^\top$  for  $n = 1, 2, \dots, N$  is the satellite position at the time of transmission  $t_n$ . Also, we consider that  $t_R$  models the arrival time of transmitted signal at the receiver. The approximate distance between each satellite and the receiver can be written as  $\rho_n = c(t_R - t_n)$ , where  $c$  is the speed of light and  $\rho_n$  is commonly known as the pseudorange [20]. The pseudoranges differ from the true distances because  $t_R$  and  $t_n$  are offset by clock biases denoted by  $b_u$  and  $b_n$ . This relationship is established as

$$t_R = t_R^{\text{GPS}} + b_u, \quad t_n = t_n^{\text{GPS}} + b_n \quad (1)$$

where  $t_R^{\text{GPS}}$  defines the reception time in the absolute GPS time, while  $t_n^{\text{GPS}}$  is the signal transmission time in GPS time. Then, if  $d_n$  represents the true distance from the receiver to each satellite, it holds that  $d_n = c(t_R^{\text{GPS}} - t_n^{\text{GPS}})$  using the unbiased transmission and reception times. Alternatively,  $d_n$  can be expressed by taking the 2-norm of position difference between the satellite and the receiver, given by  $d_n = \|\mathbf{p}_n - \mathbf{p}_u\|_2$ . The following pseudorange equation is generated by combining the previous two equations for  $d_n$  [20]

$$\rho_n = \|\mathbf{p}_n - \mathbf{p}_u\|_2 + c(b_u - b_n) + \epsilon_{\rho_n} \quad (2)$$

where  $\epsilon_{\rho_n}$  captures atmospheric effects and receiver noise.

In addition to the pseudoranges, the GPS receiver can also measure the rate at which the pseudoranges vary over time, denoted by  $\dot{\rho}_n$ , and called pseudorange rate. The pseudorange rates are expressed in terms of the satellite velocities  $\mathbf{v}_n$  and the user (GPS receiver) velocity  $\mathbf{v}_u$  as

$$\dot{\rho}_n = (\mathbf{v}_n - \mathbf{v}_u)^\top \frac{\mathbf{p}_n - \mathbf{p}_u}{\|\mathbf{p}_n - \mathbf{p}_u\|} + \dot{b}_u + \epsilon_{\dot{\rho}_n} \quad (3)$$

where  $\dot{b}_u$  represents the GPS receiver clock drift and  $\epsilon_{\dot{\rho}_n}$  is the noise. In (2) and (3), the unknown PVT variables (user position ( $\mathbf{p}_u$ ), user velocity ( $\mathbf{v}_u$ ), clock bias ( $b_u$ ), and clock drift ( $\dot{b}_u$ )) are usually computed using nonlinear weighted least squares.

The random walk model captures the dynamics relating variables in (2) and (3) for stationary applications [20]. The following is the stationary random walk model:

$$\begin{bmatrix} x_u[k+1] \\ y_u[k+1] \\ z_u[k+1] \\ b_u[k+1] \\ \dot{b}_u[k+1] \end{bmatrix} = \begin{bmatrix} \mathbf{I}_{3 \times 3} & \mathbf{0}_{3 \times 2} \\ \mathbf{0}_{2 \times 3} & 1 \quad \Delta t \\ & 0 \quad 1 \end{bmatrix} \begin{bmatrix} x_u[k] \\ y_u[k] \\ z_u[k] \\ b_u[k] \\ \dot{b}_u[k] \end{bmatrix} + \mathbf{w}[k] \quad (4)$$

where  $k$  is the time index;  $\Delta t$  is the time resolution; and  $\mathbf{w}$  is noise in the system. Generally, stand-alone receivers like those present in PMUs, use the Extended Kalman Filter (EKF) to estimate the PVT solution [20].

Since the receiver is stationary, the position ( $\mathbf{p}_u$ ) can be treated as known constant while the receiver velocity ( $\mathbf{v}_u$ ) is known to be zero. Thus, the only variables to be estimated are in fact the clock bias and drift,  $b_u[k]$  and  $\dot{b}_u[k]$ . Based on (2), (3) and the dynamic model in (4), the fundamental plant model is constructed as follows using  $\boldsymbol{\rho}[k] = [\rho_1[k], \dots, \rho_N[k]]^\top$  and  $\dot{\boldsymbol{\rho}}[k] = [\dot{\rho}_1[k], \dots, \dot{\rho}_N[k]]^\top$ :

$$\begin{bmatrix} cb_u[k+1] \\ c\dot{b}_u[k+1] \end{bmatrix} = \mathbf{A} \begin{bmatrix} cb_u[k] \\ c\dot{b}_u[k] \end{bmatrix} + \mathbf{w}[k] \quad (5)$$

$$\begin{bmatrix} \boldsymbol{\rho}[k] \\ \dot{\boldsymbol{\rho}}[k] \end{bmatrix} = \mathbf{C} \begin{bmatrix} cb_u[k] \\ c\dot{b}_u[k] \end{bmatrix} + \mathbf{c}_l[k] + \boldsymbol{\epsilon}[k] \quad (6)$$

where

$$\mathbf{A} = \begin{bmatrix} 1 & \Delta t \\ 0 & 1 \end{bmatrix}, \quad \mathbf{C} = \begin{bmatrix} \mathbf{1}_{N \times 1} & \mathbf{0}_{N \times 1} \\ \mathbf{0}_{N \times 1} & \mathbf{1}_{N \times 1} \end{bmatrix}$$

$$\mathbf{c}_l[k] = \begin{bmatrix} \|\mathbf{p}_1[k] - \mathbf{p}_u[k]\| - cb_1[k] \\ \vdots \\ \|\mathbf{p}_N[k] - \mathbf{p}_u[k]\| - cb_N[k] \\ (\mathbf{v}_1[k] - \mathbf{v}_u[k])^\top \cdot \frac{\mathbf{p}_1[k] - \mathbf{p}_u[k]}{\|\mathbf{p}_1[k] - \mathbf{p}_u[k]\|} - c\dot{b}_1[k] \\ \vdots \\ (\mathbf{v}_N[k] - \mathbf{v}_u[k])^\top \cdot \frac{\mathbf{p}_N[k] - \mathbf{p}_u[k]}{\|\mathbf{p}_N[k] - \mathbf{p}_u[k]\|} - c\dot{b}_N[k] \end{bmatrix}$$

and  $\mathbf{w}[k]$  and  $\boldsymbol{\epsilon}[k]$  represent process/measurement noise; vector  $\mathbf{c}_l[k]$  is based on the known satellite position, velocity and clock characteristics—a time-varying, known quantity. Equations (5) and (6) can be written as

$$\begin{aligned} \mathbf{x}[k+1] &= \mathbf{A}\mathbf{x}[k] + \mathbf{w}[k] \\ \mathbf{y}[k] &= \mathbf{C}\mathbf{x}[k] + \mathbf{c}_l[k] + \boldsymbol{\epsilon}[k]. \end{aligned} \quad (7)$$

The state space model (7), however, does not model potential spoofing attacks. While many different physical spoofing mechanisms are devised to deceive the victim receiver [6], time synchronization attack (TSA) is applied on the stationary GPS receiver. In practical sense, TSA alters the timestamp estimate by inserting the spoofing signal into the authentic pseudorange signals:

$$\boldsymbol{\rho}_s[k] = \boldsymbol{\rho}[k] + \mathbf{s}_\rho[k], \quad \dot{\boldsymbol{\rho}}_s[k] = \dot{\boldsymbol{\rho}}[k] + \mathbf{s}_{\dot{\rho}}[k].$$

where  $\mathbf{s}_\rho[k]$  and  $\mathbf{s}_{\dot{\rho}}[k]$  denote the spoofing attacks, and  $\boldsymbol{\rho}_s[k]$  and  $\dot{\boldsymbol{\rho}}_s[k]$  are the spoofed measurements.

Specifically, there are two different types of TSAs according to the shape of  $\mathbf{s}_\rho$ . While Type I attack injects an abrupt signal, e.g.,  $\mathbf{s}_\rho[k > \alpha] = 8000 \text{ m}$  where  $\alpha$  indicates the initial time of attack, Type II attack modifies the clock bias in gradual

manner manipulated by  $s_\rho[k] = s_\rho[k-1] + s_\rho[k]\Delta t$ ; see [21]. The actual effect of each type of attack on the clock state is thoroughly reviewed in [22].

As an example, in order for the spoofing signal to be considered as intentional attack on a PMU, it has to satisfy certain conditions. According to the IEEE C37.118 Standard, the attack has to result in 1% total variation error, which is equivalent to 26.65  $\mu$ s clock bias error, or 7989 m of distance equivalent bias error in order for the attack to be considered infringing [23]. These types of spoofing attacks—regardless of their physical mechanism—impact the state dynamics as

$$\mathbf{x}[k+1] = \mathbf{A}\mathbf{x}[k] + \mathbf{d}[k]$$

where  $\mathbf{d}[k] = [d_1[k] \ d_2[k]]^\top$  models and lumps TSAs and any process noise. Concrete examples of TSAs are given in Section III. In our previous work [11, Sec. III], we show how specific forms of  $\mathbf{d}[k]$  can mislead the receiver.

### III. ROBUST STATE ESTIMATOR

In this section, we present a state estimation algorithm that is endowed with the following properties: (i) It is a tuning-free method that does not require any knowledge of noise distribution, initial parameters or states, or other coefficients; (ii) it has low memory requirements in the sense no heavy computations are needed which is befitting to devices with limited computational power and limited Internet connectivity; (iii) it is robust to GPS spoofing, time-synchronization attacks.

#### A. GPS Clock Model and Estimator Dynamics

The plant model under the spoofing attack based on the previous can be written as

$$\begin{aligned} \mathbf{x}[k+1] &= \mathbf{A}\mathbf{x}[k] + \mathbf{d}[k] \\ \mathbf{y}[k] &= \mathbf{C}\mathbf{x}[k] + \mathbf{c}_l[k] + \boldsymbol{\epsilon}[k] \end{aligned} \quad (8)$$

where  $\mathbf{x}[k] \in \mathbb{R}^2$  represents the state vector of clock bias and drift at time  $k$ ;  $\mathbf{y}[k] \in \mathbb{R}^{2N}$  represents a single column vector of pseudoranges and pseudorange rates where  $N$  indicates the fixed number of visible satellites at every time index;  $\mathbf{d}[k] \in \mathbb{R}^2$  is the unknown spoofing attack applied to the bias and drift which also includes process noise; state-space matrices  $\mathbf{A}$ ,  $\mathbf{C}$ ,  $\mathbf{c}_l$  are discussed in the previous section.

Consider now a new *modified* state vector  $\mathbf{x}_m[k] \in \mathbb{R}^2$  which represents the state vector without spoofing attack and follows the following dynamics:

$$\mathbf{x}_m[k+1] = \mathbf{x}[k+1] - \mathbf{d}[k] = \mathbf{A}\mathbf{x}[k]. \quad (9)$$

The left-hand side of (9) essentially represents the original state vector considering that the spoofing attack  $\mathbf{d}[k]$  is removed. The modified state vector  $\mathbf{x}_m[k]$  propagates through to  $\mathbf{y}[k]$ . This yields:

$$\begin{aligned} \mathbf{x}_m[k+1] &= \mathbf{A}\mathbf{x}_m[k] + \mathbf{A}\mathbf{d}[k-1] \\ \mathbf{y}[k] &= \mathbf{C}\mathbf{x}_m[k] + \mathbf{c}_l[k] + \mathbf{C}\mathbf{d}[k-1]. \end{aligned} \quad (10)$$

The presented state estimator in this letter is an adaptation of the observer from [19] and follows the difference equation:

#### RobustEstimator

$$\begin{aligned} \hat{\mathbf{x}}_m[k+1] &= \mathbf{A}\hat{\mathbf{x}}_m[k] + \mathbf{A}\hat{\mathbf{d}}[k-1] + \mathbf{L}_1(\mathbf{y}[k] - \hat{\mathbf{y}}[k]) \\ \hat{\mathbf{y}}[k] &= \mathbf{C}\hat{\mathbf{x}}_m[k] + \mathbf{c}_l[k] + \mathbf{C}\hat{\mathbf{d}}[k-1] \end{aligned}$$

$$\begin{aligned} \mathbf{e}[k] &= \mathbf{y}[k] - \hat{\mathbf{y}}[k] \\ \hat{\mathbf{d}}[k] &= \hat{\mathbf{d}}[k-1] + \mathbf{L}_2\mathbf{C}^\top \mathbf{e}[k] \end{aligned} \quad (11)$$

where  $\hat{\mathbf{x}}_m[k] \in \mathbb{R}^2$  is a state estimate of corrected state vector  $\mathbf{x}_m[k]$  at time  $k$ ;  $\hat{\mathbf{y}}[k] \in \mathbb{R}^{2N}$  is the estimate vector of observation  $\mathbf{y}[k]$ ;  $\hat{\mathbf{d}}[k]$  is an estimate of the spoofing attack  $\mathbf{d}[k]$ . We note here that  $\hat{\mathbf{d}}[-1]$ ,  $\hat{\mathbf{x}}_m[0]$ , and  $\hat{\mathbf{y}}[0]$  should be initialized before iteration starts at  $k=0$  with arbitrary initial conditions. Matrices  $\mathbf{L}_1 \in \mathbb{R}^{2 \times 2N}$  and  $\mathbf{L}_2 \in \mathbb{R}^{2 \times 2}$  are optimization variables where  $\mathbf{L}_1$  is akin, in principle, to a Luenberger gain that is designed here to ensure robustness of the state estimation to spoofing attacks.

#### B. Design of Robust Gains $\mathbf{L}_{1,2}$

The design of the robust estimator gains  $\mathbf{L}_{1,2}$  is based on linear matrix inequalities (LMIs). Simply put, the objective of the designed observer is to guarantee asymptotically stable estimation error dynamics. That is, matrices  $\mathbf{L}_1$  and  $\mathbf{L}_2$  are designed to guarantee that  $\lim_{k \rightarrow \infty} \mathbf{e}[k] = 0$  under non-zero spoofing attack  $\mathbf{d}[k]$  and bounded estimation error under spoofing attacks. The **ROBUSTESTIMATOR** variables are designed via solving this low-dimensional feasibility problem with one linear matrix inequality (LMI), given as follows:

#### EstimatorDesign

$$\begin{aligned} \text{find } & \mathbf{G} \in \mathbb{R}^{2 \times 2N}, \mathbf{P} \in \mathbb{R}^{2 \times 2}, \mathbf{Q} \in \mathbb{R}^{2N \times 2N}, \mathbf{M} \in \mathbb{R}^{2 \times 2} \\ \text{s.t. } & \begin{bmatrix} \mathbf{P} & \star & \star & \star \\ \mathbf{0} & \mathbf{Q} & \star & \star \\ \mathbf{G}\mathbf{C} - \mathbf{P}\mathbf{A} & \mathbf{G}\mathbf{C} - \mathbf{P}\mathbf{A} & \mathbf{P} & \star \\ \mathbf{M}\mathbf{C}^\top \mathbf{C} & \mathbf{M}\mathbf{C}^\top \mathbf{C} - \mathbf{Q} & \mathbf{0} & \mathbf{Q} \end{bmatrix} \succ \mathbf{0} \\ & \{\mathbf{P}, \mathbf{Q}, \mathbf{M}\} = \{\mathbf{P}^\top, \mathbf{Q}^\top, \mathbf{M}^\top\} \succ \mathbf{0}, \end{aligned} \quad (12a)$$

$$\{\mathbf{P}, \mathbf{Q}, \mathbf{M}\} = \{\mathbf{P}^\top, \mathbf{Q}^\top, \mathbf{M}^\top\} \succ \mathbf{0}, \quad (12b)$$

where the symbol  $\star$  is used to represent symmetric components in symmetric block matrices. After solving (12) for positive definite matrix variables  $\mathbf{P}$ ,  $\mathbf{Q}$ , and  $\mathbf{M}$ , and real matrix variable  $\mathbf{G}$ , the observer gains are computed as follows

$$\mathbf{L}_1 = \mathbf{P}^{-1}\mathbf{G}, \quad \mathbf{L}_2 = \mathbf{M}\mathbf{Q}^{-1}. \quad (13)$$

As mentioned earlier, the state estimator design is derived from [19]; the reader is referred to that paper for the derivation of the above LMIs. Note that no tuning is required to solve **ESTIMATORDESIGN**, and this LMI can be solved analytically via evaluating the Karush-Kuhn-Tucker conditions for feasibility [24]. Furthermore, any convex optimization toolbox or LMI solver can be used to solve (12). These include MATLAB's LMI solver, CVX [25], and Yalmip [26].

We note the following. First, the necessary conditions for existence of  $\mathbf{L}_{1,2}$  are standard. These conditions are (a) the detectability of  $(\mathbf{A}, \mathbf{C})$ ; (b) the classical rank matching condition stating that  $\text{rank}(\mathbf{C}\mathbf{B}_d) = \text{rank}(\mathbf{B}_d)$  where  $\mathbf{B}_d = \mathbf{I}_2$  is the matrix coefficient of  $\mathbf{d}[k]$  in (8); and (c) bounded variations of the unknown spoofing signal  $\mathbf{d}[k]$ . Second, this robust estimator not only estimates  $\mathbf{x}[k]$ , but also the spoofing attack  $\mathbf{d}[k]$ . This is instrumental in mitigating and correcting the attack. The next section showcases the design of the gain matrices.

#### C. State Correction Algorithm Under Spoofing

Upon solving the LMIs and running the **ROBUSTESTIMATOR** from any arbitrary initial conditions, the estimator is guaranteed theoretically to produce

**Algorithm 1:** Robust Bias and Drift Estimation

---

```

1 input: Number of satellites  $N$ , matrices  $A$  and  $C$ 
2 initialize:  $\hat{d}[-1]$ ,  $\hat{x}_m[0]$ ,  $\hat{y}[0]$ 
3 Offline Computations
4 Compute  $G, P, Q, M$  given  $A$  and  $C$  by solving (12)
5 Obtain  $L_1$  and  $L_2$  from (13)
6 Online Computations
7 while  $k \geq 0$  do
8   Obtain  $c_l[k]$  from satellite measurements
9   Run (11) and obtain  $\hat{x}_m[k+1]$  and  $\hat{d}[k]$ 
10  Perform spoofing attack correction (15)
11  Perform state and output correction (16)
12   $k \leftarrow k + 1$ 
13 output: Attack-free  $\hat{x}_c[k]$ , TSA estimates  $\hat{d}_c[k]$ 

```

---

bounded estimation error  $e[k]$ , thereby estimating the then-spoofed bias and drift, and reconstructing the spoofing attack  $\hat{d}[k]$ . With that in mind, this does not indicate that the bias and drift are correctly estimated seeing that spoofing attack had already changed the state through the state propagation and difference equation. To that end, this section develops a state correction algorithm to recover the authentic bias and drift values in real-time.

To that end, the dynamics (9) can be written as

$$\begin{aligned} x_m[k+1] &= Ax_m[k] + Ad[k-1] \\ &= A(Ax_m[k-1] + Ad[k-2]) + Ad[k-1]. \end{aligned} \quad (14)$$

This relationship reveals that current spoofing during one time instant comprises the cumulative attacks from the previous time steps. Consequently, the disturbance estimate  $\hat{d}$  is not sufficient enough to correct the attacked states. Rather, a new disturbance estimate vector  $\hat{d}_c$  is formulated to account for the accumulated disturbances. Considering the estimate of spoofing attacks  $\hat{d}[k] = [\hat{d}_1[k] \ \hat{d}_2[k]]^\top$  computed by (11), we propose estimating the new disturbance estimate vector  $\hat{d}_c$  via

$$\hat{d}_c[k] = \begin{bmatrix} \sum_{l=1}^k \hat{d}_1[l] + \sum_{l=1}^{k-1} (k-l)\hat{d}_2[l] \\ \sum_{l=1}^{k-1} \hat{d}_2[l] \end{bmatrix} \quad (15)$$

This equation acknowledges the fact that estimated state  $x_m$  is still contaminated by the attack from the past time step. Therefore, the corrected state  $x_c$  and authentic observation state  $y_c$  could be retrieved by subtracting  $\hat{d}_c$  from  $x_m$  and  $\hat{y}$  as follows:

$$\hat{x}_c[k] = \hat{x}_m[k] - \hat{d}_c[k], \quad \hat{y}_c[k] = \hat{y}[k] - C\hat{d}_c[k] \quad (16)$$

Algorithm 1 showcases the overall problem design, robust state estimation, and the reconstruction of the corrected bias and drift of the GPS receiver. The algorithm takes as inputs: the fixed number of satellites  $N$ ,  $A$  and  $C$ , and satellites data which is encoded through  $c_l[k]$ . The algorithm is divided into two stages—an offline stage and an online one. In the offline stage, the **ROBUSTESTIMATOR** gains  $L_1$  and  $L_2$  are computed via solving (11) and evaluating (13). The online stage includes running the **ROBUSTESTIMATOR** (11) and the cumulative corrections for the states and spoofing attacks. The

**TABLE I**  
VECTOR NOMENCLATURE

Notation	Description
$x_{GT}$	ground truth state vector
$x_{EKF}$	estimated state vector from EKF
$x_{Luen}$	estimated state vector from Luenberger Observer
$\hat{x}_m$	modified state vector estimates
$\hat{x}_c$	corrected state vector via (16)
$d$	attack vector vector applied to $x$
$\hat{d}_c$	corrected spoofing attack vector via (15)

algorithm returns the attack-free, yet still slightly noisy estimates of the bias and drift  $\hat{x}_c[k]$  and an estimate of the actual spoofing attack  $\hat{d}_c[k]$ .

It is noteworthy to mention the following. First, the offline component of the algorithm—albeit offline—can be solved analytically seeing that the problem dimension is very small, when considering that only few satellite measurements are needed. Second, the algorithm and the LMI feasibility problem both only require a fixed *number* of satellites, rather than a fixed satellite combination. This is important considering that different satellites are visible each time. In short, the proposed algorithm in this letter only assumes a minimum fixed number of satellites  $N$ , where these  $N$  satellites can be changing in real time without impacting the algorithm or the design of the robust estimator.

Third, Algorithm 1 works for any reasonable initial conditions, that is, the estimation should converge regardless of the initial conditions choice. Fourth, this method is truly tuning-free: no prior knowledge of the statistical distribution of noise, or prior knowledge or tuning of any parameters is needed. The algorithm is also low-memory, as the only computation needed to be performed online is running the **ROBUSTESTIMATOR** and the correction models—both require a small number of matrix-vector multiplications. This implies that the proposed algorithm can be implemented in low-memory devices without the need for any intensive computational effort or Internet connectivity. Finally, we note that the proposed algorithm has no stopping criterion seeing that it runs in real time.

#### IV. CASE STUDIES: A REALISTIC TESTBED

This section discusses the detection and mitigation of TSAs via various approaches. First, the experimental procedure is discussed. Then, we compare the performance of the extended Kalman filter (EKF)—which has long been used in the literature [20] as a *ground truth* for estimating the bias and drift—and the classical Luenberger observer under spoofing attacks. Then, the performance of the proposed robust estimator under TSAs is showcased, followed by thorough comparison of the performance of the approaches. The following link includes all codes and data used to generate the results, including the acquired GPS data: [github.com/junhwanlee95/Robust-Estimator](https://github.com/junhwanlee95/Robust-Estimator). Table I summarizes the important vector nomenclature.

##### A. Setup: Model Simulation & Obtaining Raw GPS Data

A Google Nexus 9 tablet, which has an embedded GPS chipset, is used to collect real GPS signals, which are recorded on November 4, 2018 at the University of Texas at San Antonio main campus. The data are available for the reader through the aforementioned Github link. While



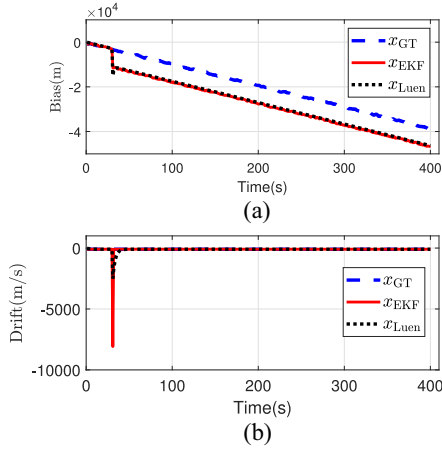


Fig. 1. Comparison of ground truth, EKF and Luenberger observer estimates under Type I attack: (a) clock bias; (b) clock drift.

the receiver acquires the signal, the device remained still to simulate the stationary scenario. Raw GPS data is post-processed to obtain pseudorange and pseudorange rate data by *GNSS Logger*, the Android application released by the Google Android location team [27]. Then, Type I and II attacks are injected into the pseudorange and pseudorange rate data to simulate spoofing as discussed in Section II and shown in [11, Sec. III]. The initial conditions for the robust estimator are chosen to be different than the actual, ground truth conditions.

### B. EKF and Luenberger Performances Under Attacks

Here, we are interested in testing whether the EKF and the classical Luenberger observer [28] can withstand TSAs of Type I and II. After Type I and II attacks are applied from  $t = 30$  s to  $t = 400$  s, the performance of the EKF and Luenberger observer—which does not assume any statistical distribution about the noise—are shown in Fig. 1 and 2.

While the ground truth clock bias and drift,  $x_{GT}$ , are acquired through EKF by processing the authentic pseudorange data, the  $x_{EKF}$  bias and drift are generated by applying the EKF to the spoofed pseudoranges. Another comparison to  $x_{GT}$  is offered by the Luenberger observer estimate  $x_{Luen}$  produced after designing the observer gain  $L_1$  such that the closed loop system eigenvalues are at 0.5 and 0.7. The performances of EKF and Luenberger observer are shown respectively in Fig. 1 and Fig. 2. It is evident that both approaches fail to estimate the correct states in the presence of the attack.

### C. Robust Estimator Performance Under Type I/II TSAs

In this section, we test the proposed robust estimator and run Algorithm 1 which contains an offline stage and an online one. First, we set  $N = 4$ , i.e., we choose to sample data from only four satellites. We solve the LMIs (12) for the estimator gains. Using these estimator gains, the online portion of Algorithm 1 is run. Pertaining to Type I attack, Fig. 3 shows the performance of **ROBUSTESTIMATOR**. Due to the attack at  $t = 30$  s, the  $\hat{x}_c$  clock estimates are initially not correct, but the clock bias and drift approach the respective ground truth values within approximately 3 and 11 seconds (see Fig. 3(a) and 3(b) respectively).

Under the same condition and procedure, Algorithm 1 is applied on Type II attack to detect and correct the spoofed

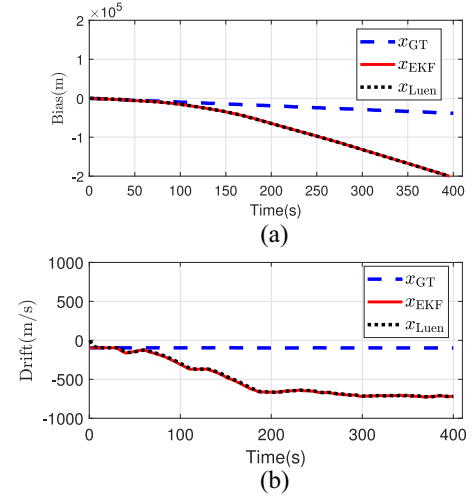


Fig. 2. Comparison of ground truth, EKF and Luenberger observer estimates under Type II attack: (a) clock bias; (b) clock drift.

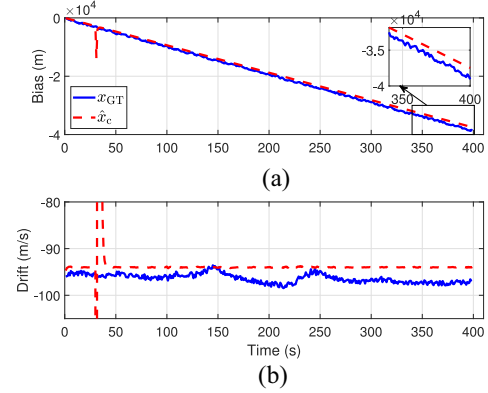


Fig. 3. Comparison of ground truth and corrected state through the correction (16) under Type I attack: (a) clock bias; (b) clock drift.

states. The results of obtaining the corrected state  $\hat{x}_c$  are shown in Fig. 4. In order to accurately depict the performance of **ROBUSTESTIMATOR**, the relative estimation error is calculated as  $\frac{\|\hat{x}_c - x_{GT}\|}{\|x_{GT}\|}$  for each of the two states in  $x$  over time. The resulting graphs are shown in Fig. 5. Comparison between  $\hat{x}_c$  and the  $x_{GT}$  reveals that the maximum error between the two biases is 952.09 m or  $3.17 \mu s$ . It is thus demonstrated that the Robust Estimator of Algorithm 1 successfully detects and corrects the Type II attack.

In the interest of gauging the performance of each approach, the root mean square error (RMSE) of the estimated clock bias is calculated under both attack types. Let  $K$  denote the total length of observation time ( $K = 400$  in this experiment). The RMSE is defined as  $RMSE = \sqrt{\frac{1}{K} \sum_{k=0}^{K-1} (c\hat{b}_u[k] - c\check{b}_u[k])^2}$  where  $c\check{b}_u[k]$  is the ground truth clock bias under normal conditions, and  $c\hat{b}_u[k]$  equals to the estimated clock bias value from each approach. Under Type II attack, the RMSE for EKF and the Luenberger observer are  $RMSE_{EKF} = 74344$  m and  $RMSE_{Luenberger} = 74433$  m respectively, while that of the robust estimator is  $RMSE_{RobustEstimator} = 354.9$  m. As for Type I attack, the RMSEs are as follows:  $RMSE_{EKF} = 8477.3$  m,  $RMSE_{Luenberger} = 8104.9$  m, and  $RMSE_{RobustEstimator} = 1029$  m. This illustrates the performance of this tuning-free, low-memory robust estimator

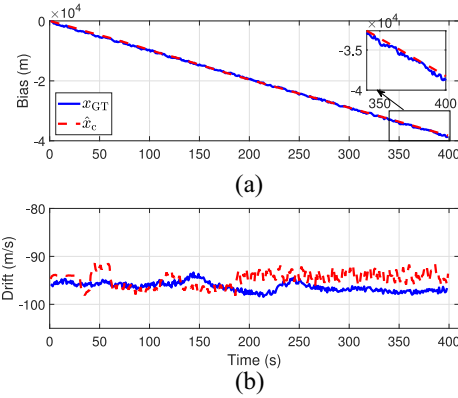


Fig. 4. Comparison of ground truth and corrected state through the correction (16) under Type II attack: (a) clock bias; (b) clock drift.

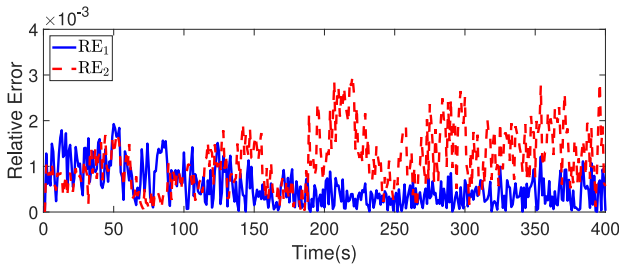


Fig. 5. Relative estimation error for clock bias and drift defined as:  $RE_1 = \frac{|\hat{x}_c(1) - x_{GT}(1)|}{x_{GT}(1)}$ ,  $RE_2 = \frac{|\hat{x}_c(2) - x_{GT}(2)|}{x_{GT}(2)}$ .

in detecting spoofing attacks, while correctly reconstructing the bias and drift states of the GPS receiver.

## V. PAPER SUMMARY AND FUTURE WORK

In this letter, the design and realistic application of a low-memory, real-time **ROBUSTESTIMATOR** is studied. Utilizing the GPS receiver on a Google Nexus 9, real GPS data are collected and post-processed by injecting time-synchronization attacks to spoof the clock bias and drift of the device. Two types of attacks are introduced, and tested by the designed estimator. The estimator successfully detects and estimates the spoofing attacks on each state, and mitigates the spoofing on both types of attack by furnishing the corrected clock states to the user. Future work will focus on developing robust estimators under spoofing attacks for non-stationary GPS receivers, which involve nonlinearities in the GPS measurement model.

## ACKNOWLEDGMENT

The authors acknowledge suggestions made by the Editor and reviewers.

## REFERENCES

- [1] "GPS disruptions: Efforts to assess risks to critical infrastructure and coordinate agency actions should be enhanced," U.S. Govt. Accountability Office, Washington, DC, USA, Rep. GAO-14-15, Nov. 2014. [Online]. Available: <https://www.gao.gov/products/GAO-14-15>
- [2] 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.
- [3] D. Schmidt, K. Radke, S. Camtepe, E. Foo, and M. Ren, "A survey and analysis of the GNSS spoofing threat and countermeasures," *ACM Comput. Surveys*, vol. 48, no. 4, pp. 1–31, May 2016.
- [4] T. Nighswander, B. Ledvina, J. Diamond, R. Brumley, and D. Brumley, "GPS software attacks," in *Proc. ACM Conf. Comput. Commun. Security*, Raleigh, NC, USA, Oct. 2012, pp. 450–461.
- [5] M. L. Psiaki and T. E. Humphreys, "GNSS spoofing and detection," *Proc. IEEE*, vol. 104, no. 6, pp. 1258–1270, Jun. 2016.
- [6] L. Heng *et al.*, "Reliable GPS-based timing for power systems: A multi-layered multi-receiver architecture," in *Proc. Power Energy Conf. Illinois (PECI)*, Champaign, IL, USA, Feb./Mar. 2014, pp. 1–7.
- [7] T. E. Humphreys, B. M. Ledvina, M. Psiaki, B. W. O'Hanlon, and J. P. M. Kintner, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proc. 21st Int. Tech. Meeting Satellite Division Inst. Navig. (ION GNSS)*, Savannah, GA, USA, Sep. 2008, pp. 2314–2325.
- [8] 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, 3rd Quart., 2016.
- [9] F. Zhu, A. Youssef, and W. Hamouda, "Detection techniques for data-level spoofing in GPS-based phasor measurement units," in *Proc. Int. Conf. Sel. Topics Mobile Wireless Netw. (MoWNeT)*, Cairo, Egypt, Apr. 2016, pp. 1–8.
- [10] 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. (ICC)*, Sydney, NSW, Australia, Jun. 2014, pp. 5413–5418.
- [11] 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.
- [12] 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.*, Oxford, U.K., Jul. 2014, pp. 99–104.
- [13] 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.*, Los Angeles, CA, USA, Dec. 2016, pp. 237–250.
- [14] S. Bhattacharyya, "Observer design for linear systems with unknown inputs," *IEEE Trans. Autom. Control*, vol. AC-23, no. 3, pp. 483–484, Jun. 1978.
- [15] W. Kang, A. J. Krener, M. Xiao, and L. Xu, "A survey of observers for nonlinear dynamical systems," in *Data Assimilation for Atmospheric, Oceanic and Hydrologic Applications*, vol. 2, S. K. Park and L. Xu, Eds. Berlin, Germany: Springer, 2013, pp. 1–25. [Online]. Available: [https://doi.org/10.1007/978-3-642-35088-7\\_1](https://doi.org/10.1007/978-3-642-35088-7_1)
- [16] C. Masreliez and R. Martin, "Robust Bayesian estimation for the linear model and robustifying the Kalman filter," *IEEE Trans. Autom. Control*, vol. 22, no. 3, pp. 361–371, Jun. 1977.
- [17] A. H. Jazwinski, *Stochastic Processes and Filtering Theory*. Mineola, NY, USA: Dover, 2007.
- [18] G. A. Einicke and L. B. White, "Robust extended Kalman filtering," *IEEE Trans. Signal Process.*, vol. 47, no. 9, pp. 2596–2599, Sep. 1999.
- [19] B. A. Charandabi and H. J. Marquez, "Observer design for discrete-time linear systems with unknown disturbances," in *Proc. IEEE 51st IEEE Conf. Decis. Control (CDC)*, Dec. 2012, pp. 2563–2568.
- [20] P. Axelrad and R. G. Brown, "GPS navigation algorithms," in *Global Positioning System: Theory and Applications*, vol. 1, B. W. Parkinson, J. J. Spilker, P. Axelrad, and P. Enge, Eds. Washington, DC, USA: Amer. Inst. Aeronaut. Astronaut., 1996, ch. 9.
- [21] 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, nos. 3–4, pp. 146–153, 2012.
- [22] T. Humphreys, J. Bhatti, D. Shepard, and K. Wesson, "The Texas spoofing test battery: Toward a standard for evaluating GPS signal authentication techniques," in *Proc. 25th Int. Tech. Meeting Satellite Division Inst. Navig. (ION GNSS)*, Nashville, TN, USA, Sep. 2012, pp. 3569–3583.
- [23] *IEEE Standard for Synchrophasor Measurements for Power Systems*, IEEE Standard C37.118.1-2011, 2011.
- [24] S. Boyd and L. Vandenberghe, *Convex Optimization*. Cambridge, U.K.: Cambridge Univ. Press, 2004.
- [25] M. Grant and S. Boyd. (2014). *CVX: MATLAB Software for Disciplined Convex Programming, Version 2.1*. [Online]. Available: <http://cvxr.com/cvx>
- [26] J. Löfberg, "YALMIP: A toolbox for modeling and optimization in MATLAB," in *Proc. CACSD Conf.*, vol. 3. Taipei, Taiwan, 2004, pp. 284–289.
- [27] *Android GNSS*. Accessed: Feb. 20, 2017. [Online]. Available: <https://developer.android.com/guide/topics/sensors/gnss.html>
- [28] D. Luenberger, "Observers for multivariable systems," *IEEE Trans. Autom. Control*, vol. 11, no. 2, pp. 190–197, Apr. 1966.