Multi-period Power System State Estimation with PMUs Under GPS Spoofing Attacks

Paresh Risbud, Nikolaos Gatsis, *Member*, *IEEE*, and Ahmad Taha, *Member*, *IEEE*

***Abstract*—This paper introduces a dynamic network model together with a phasor measurement unit (PMU) measurement model suitable for power system state estimation under spoofing attacks on the global positioning system (GPS) receivers of PMUs. The spoofing attacks may introduce time-varying phase offsets in the affected PMU measurements. An algorithm is developed to jointly estimate the state of the network, which amounts to the nodal voltages in rectangular coordinates, as well as the time-varying attacks. The algorithm features closed-form updates. The effectiveness of the algorithm is verified on the standard IEEE transmission networks. It is numerically shown that the estimation performance is improved when the dynamic network model is accounted for compared with a previously reported static approach.**

***Index Terms*—Dynamic state equation, global positioning system (GPS) spoofing, phasor measurement unit (PMU), state estimation, time synchronization, weighted least squares.**

I. Introduction

THE smart grid is a massive cyber-physical system (CPS) spanning continents. The cyber part consists of a computerized network including two-way digital communication between devices (e.g., voltage and current sensors, power meters) and the network operation center. The physical part is formed by the power grid itself (generation, transmission, and distribution), which can be as large as a continent. Phasor measurement units (PMUs) equipped with global positioning system (GPS) receivers are installed ubiquitously and replace traditional sensors of the supervisory control and data acquisition (SCADA) systems. PMUs use GPS receivers to accurately time stamp and synchronize measurements. The main advantage of PMUs over SCADA is the higher sampling rate, which enables the operator to perform real-time wide area monitoring, protection and control (WAMPAC).

Sensors such as PMUs that measure nodal voltages, among other quantities, cannot be installed on each bus in the network. Thus, state estimation (SE) routines are performed to gain the visibility of the network. According to [1], scenario WAMPAC. 12: GPS Time Signal Compromise highlights the vulnerability of PMUs to GPS spoofing attacks. In particular, GPS spoofing is a class of cyber attacks in which the attacker mimics the GPS signals in order to alter the GPS time estimated by the GPS receiver of the PMU [2]. This attack is also called time synchronization attack (TSA), since it induces erroneous time stamps, thereby inducing wrong phase angle in the PMU measurements.

Various threat scenarios, security gaps, and mitigation strategies in relation to TSAs have been assessed in [3] and [4]. Specific selected works representing effects and mitigation of GPS spoofing attacks in power systems include [5]-[20] and these are reviewed next.

A set of studies has investigated the operation at the GPS receiver level and developed methods to detect GPS spoofing and if possible, to provide accurate timing to the PMU. Specifically, [5] provides a multi-layered approach for reliable GPS-based timing for PMUs against jamming and spoofing. Reference [6] leverages the static nature of PMUs to provide refined signal tracking techniques at the GPS receiver robustifying its operation against jamming and spoofing. Reference [7] develops a multilateration scheme to detect the malicious source of GPS signals by utilizing characteristics of multiple sensors in the grid. Detection techniques against GPS spoofing attacks in power grids based on the visible satellites and the statistics of the receiver clock are implemented in [8]. In an effort to detect attacked PMUs, [9] introduces a trustworthiness measure for PMUs that builds upon antenna- and signal-based techniques at the receiver.

The impacts of GPS spoofing attacks on power grid operation have also been analyzed. In addition to demonstrating the experimental feasibility of spoofing, a false generator trip in a synchrophasor-based automatic control scheme is exhibited in [10]. A simulation-based approach to studing the effect of GPS spoofing on false alarm and missed generation scenarios in the smart grid is the theme of [11]. An optimization problem to demonstrate the feasibility of GPS spoofing attack is formulated in [12], where the objective is to maximize the PMU clock offset before and after the attack. The impact of GPS spoofing on voltage stability monitoring, fault detection, and event location is detailed in [13]. The effect on synchrophasor assisted load shedding are reported in [14].

More recently, power grid operation such as SE have been

Manuscript received: March 1, 2020; accepted: June 4, 2020. Date of Cross-Check: June 4, 2020. Date of online publication: 9 July, 2020.

This work was supported by the U. S. National Science Foundation (No. ECCS-1719043).

P. Risbud, N. Gatsis (corresponding author), and A. Taha are with the Department of Electrical and Computer Engineering, University of Texas at San Antonio, San Antonio, USA (e-mail: Paresh.Risbud@utsa.edu; Nikolaos.Gatsis@utsa.edu; Ahmad.Taha@utsa.edu).

DOI: 10.35833/MPCE.2020.000125

upgraded to account for GPS spoofing attacks on PMUs. Specifically, distributed estimation of power system oscillations under GPS spoofing attacks is developed in [15]. Power system SE resilient to a spoofing attack on a single PMU is furnished in [16], with further computational refinements presented in [17]. In our previous work [18], an alternating minimization (AM) algorithm to jointly perform SE and attack phase angle reconstruction is developed. A sparse error correction for PMU data under GPS spoofing attacks is presented in [19]. A novel GPS spoofing identification and correction algorithm for SE in unbalanced distribution grids is developed in [20]. References [16]-[20] pertain to a static SE setup, whereby a set of measurements from a particular time instant is processed to produce a state estimate corresponding to that time instant. A dynamic SE model under GPS spoofing based on the swing equation is introduced in [21], where the presence of attack is detected using a generalized likelihood ratio test.

The effect of GPS spoofing on PMU measurements bears some resemblance to the problem of imperfect PMU synchronization [22]. The similarity amounts to the fact that imperfect synchronization induces a time offset in the PMU measurement that in effect translates to a phase offset in the measured voltage or current phasor. The chief difference is that the phase offset is typically much smaller in case of imperfect synchronization, as opposed to GPS spoofing. The latter condition enables the use of small angle approximations [23]-[25] which are not generally valid under spoofing attacks. When dynamic state models with imperfect synchronization are considered, it is assumed that the availability of GPS restores the synchronization [26], which is a situation that is not tenable under GPS spoofing.

Based on a dynamic model for the power system state, this paper develops an SE algorithm that furnishes the phase offsets induced by GPS spoofing across time, in addition to the power system state. There are two approaches to dynamic SE depending on the definition of the state vector [27], and representative references specifically featuring PMU measurements are mentioned next. The first approach features bus voltages as state variables, and the corresponding simplest dynamic model boils down to a random walk [28]-[30]. In the second approach, dynamic models of generators are considered, wherein rotor angles and rotor speeds are the state variables, following the swing equation [21], [31]-[33]. It is worth noting that when the states are the voltages expressed in rectangular coordinates and PMU measurements are used, SE can be performed efficiently by (linear) weighted least squares or the Kalman filter, whose performance is thoroughly analyzed in [28]. Depending on the variability of power injections, it is also possible to partition the network into three areas, i.e., steady, quasi-steady, and fluctuant, and perform a multi-time scale SE [34].

This paper adopts the random walk model for the network voltage states [28]. The first contribution is deriving a state and measurement model that explicitly models the GPS spoofing attack angles. The attack may be time varying and start at an unknown time, but these characteristics are considered in the model. The multi-period SE is formulated as a bi-criterion optimization problem, where the measurement and dynamic state equations are contributing to the overall objective function. The states and attack angles are optimization variables and the resulting problem is nonconvex. The second contribution is developing an AM algorithm to compute the solution of the SE problem. The algorithm features closed-form updates and extends the one in [18] to the dynamic case. The effectiveness of the proposed algorithm is demonstrated on standard IEEE transmission networks. Two types of realistic attacks are applied [35], namely, one that shows up suddenly (step attack), and the other that is ramping. The third contribution is numerically demonstrating that the performance of the multi-period SE is superior to prior work that only considers the static nature of voltages, compared to the presented formulations that consider the voltage dynamics.

The remainder of this paper is organized as follows. Section II details the system and attack models. The SE problem is formulated in Section III. The iterative solver is developed in Section IV. Numerical tests and conclusions are presented in Sections V and VI, respectively.

II. System and Attack Models

This section describes the multi-period state and measurement model with and without TSAs on PMU measurements.

A. Attack-free Dynamic Model

Consider a power network with N_b buses connected via N_l transmission lines. Let $\mathcal{N}_n$ be the set of buses connected to bus n, and define $L_n = |\mathcal{N}_n|$ as the number of lines connected to bus n. The nodal voltage at bus n and discrete time period k is written in complex, rectangular, and polar forms as $V_{n,k} = V_{n,k,r} + \mathrm{j}V_{n,k,i} = |V_{n,k}|\mathrm{e}^{\mathrm{j}\theta_{n,k}}$, where $V_{n,k,r}$ and $V_{n,k,i}$ are the real and imaginary parts of the nodal voltage, respectively; and $\theta_{n,k}$ is the phase of the nodal voltage. The dynamic equation describing the state evolution over discrete time periods indexed by k follows a random walk model:

$$\boldsymbol{v}_k = \boldsymbol{v}_{k-1} + \boldsymbol{w}_k \quad k = 1, 2, \ldots, K \tag{1}$$

where $\boldsymbol{v}_k = [\boldsymbol{v}_{k,r}^{\mathrm{T}}, \boldsymbol{v}_{k,i}^{\mathrm{T}}]^{\mathrm{T}} \in \mathbf{R}^{2N_b \times 1}$ is the system state vector at time k, and vectors $\boldsymbol{v}_{k,r}$ and $\boldsymbol{v}_{k,i}$ collect the real and imaginary parts of nodal voltages $V_{n,k,r}$ and $V_{n,k,i}$ for $n = 1, 2, \ldots, N_b$, respectively; $\boldsymbol{w}_k$ is the state noise, which follows a Gaussian distribution, that is, $\boldsymbol{w}_k \sim \mathcal{N}(\mathbf{0}, \boldsymbol{Q}_k)$, and $\boldsymbol{Q}_k$ is a positive definite covariance matrix at time k; and K is a generic terminal time through which SE is to be performed. The duration of time period k is given by the sampling period T_s. The typical sampling frequency for PMUs ranges between 30 and 120 samples per second, yielding a sampling period T_s of approximately 8-33 ms. The model in (1) is appropriate for the systems where the network dynamics are slow enough compared to the duration of the sampling period [28].

PMUs are installed on the selected buses of the network, and a_n is a binary indicator equal to 1 if a PMU is installed at bus n and 0 otherwise. Vector $\boldsymbol{a}$ collects a_n for $n = 1, 2, \ldots, N_b$. The set of buses where PMUs are installed is denoted by $\mathcal{N}_{\mathrm{PMU}} = \{n \in \{1, 2, \ldots, N_b\} \,|\, a_n = 1\} = \{n_1, n_2, \ldots, n_P\}$, where P is the number of PMUs installed in the network.

A PMU installed at bus n measures, for all time periods k, the complex nodal voltage as well as the complex currents on all lines that bus n is connected to. This collection of measured quantities (in rectangular coordinates) at bus n for time k is concatenated in a vector $\boldsymbol{z}_{n,k} \in \mathbf{R}^{2(1+L_n)}$. To make the notation more compact, define $M_n = 2(1+L_n)$ as the number of distinct real quantities measured by the PMU at bus n for time k.

It is convenient for subsequent developments to consider the noiseless version of $\boldsymbol{z}_{n,k}$, which is denoted by $\boldsymbol{z}_{n,k}^{\text{true}} \in \mathbf{R}^{M_n}$:

$$\boldsymbol{z}_{n,k}^{\text{true}} = \begin{bmatrix} V_{n,k,r} \\ V_{n,k,i} \\ \{I_{np,k,r}\}_{p\in\mathcal{N}_n} \\ \{I_{np,k,i}\}_{p\in\mathcal{N}_n} \end{bmatrix} = \begin{bmatrix} |V_{n,k}|\cos(\theta_{n,k}) \\ |V_{n,k}|\sin(\theta_{n,k}) \\ \{|I_{np,k}|\cos(\theta_{I_{np,k}})\}_{p\in\mathcal{N}_n} \\ \{|I_{np,k}|\sin(\theta_{I_{np,k}})\}_{p\in\mathcal{N}_n} \end{bmatrix} \tag{2}$$

where $I_{np,k,r}$ and $I_{np,k,i}$ are the real and imaginary parts of the complex current flowing on line (n,p) for time k, respectively; and $|I_{np,k}|$ and $\theta_{I_{np,k}}$ are the corresponding current magnitude and phase, respectively.

To summarize, the noiseless quantities measured at bus $n \in \mathcal{N}_{\text{PMU}}$, for discrete time $k = 1, 2, \ldots, K$, comprise of the real and imaginary parts of the nodal voltage, appended by the real and imaginary parts of the complex currents injected to all lines connected to bus n for time k. Using the bus admittance matrix of the network, $\boldsymbol{z}_{n,k}^{\text{true}}$ can be written as a linear function of the system state $\boldsymbol{v}_k$ as $\boldsymbol{z}_{n,k}^{\text{true}} = \boldsymbol{H}_n \boldsymbol{v}_k$. The corresponding noisy measurement equation evolving over k discrete time periods is given as:

$$\boldsymbol{z}_{n,k} = \boldsymbol{H}_n \boldsymbol{v}_k + \boldsymbol{\varepsilon}_{n,k} \quad n \in \mathcal{N}_{\text{PMU}}, k = 1, 2, \ldots, K \tag{3}$$

where $\boldsymbol{\varepsilon}_{n,k} \sim \mathcal{N}(\mathbf{0}, \boldsymbol{\Sigma}_{n,k})$, and $\boldsymbol{\Sigma}_{n,k}$ is a positive definite measurement noise covariance matrix at time k; and the construction of $\boldsymbol{H}_n \in \mathbf{R}^{M_n \times 2N_b}$ is provided in [36], [37].

B. Attack-aware Dynamic Model

A TSA at node n introduces a generally time-varying delay denoted by $\delta_n(t)$ to all measurements, i.e., voltages and currents, captured by the PMU. To introduce a mathematical model of the attack, let $v_n(t)$ be the instantaneous voltage of bus n, and let $V_n(t)$ be the corresponding phasor at continuous time t. The phasor is time-dependent to allow for description of a system with time-varying state. The sampled phasor at period k is thus $V_{n,k} = V_n(kT_s)$. The attacked instantaneous nodal voltage is written as:

$$v_n(t+\delta_n(t)) = \text{Re}\{\sqrt{2}\, V_n(t+\delta_n(t)) e^{\text{j}2\pi f(t+\delta_n(t))}\} \tag{4}$$

where f is the system operation frequency; and $\text{Re}\{\cdot\}$ is the real part operator. Similar expressions can be written for the line currents. It is worth emphasizing that the same delay $\delta_n(t)$ is introduced across the measurements captured by the PMU at bus n (entries of $\boldsymbol{z}_{n,k}$). The reason is that GPS spoofing affects the time estimated by the GPS receiver of the PMU, which subsequently affects the time stamp of all measurements of the PMU. We also introduce the sampled version of $\delta_n(t)$, denoted by $\delta_{n,k} = \delta_n(kT_s)$, and the corresponding attack angle $\Delta\theta_{n,k} = 2\pi f \delta_{n,k}$.

The objective is to formulate a time-varying measurement model that relates the attacked measurements with the network state and the attack in period k. To this end, it is assumed that $\delta_n(t) \ll T_s$. This assumption is valid as experimentally demonstrated. Other realistic attacks reported in [10], [12], [13] depict attack angles $\Delta\theta_{n,k}$ of 70°, 52° and 60°, respectively. The corresponding delay of the attack is 3.2 ms, 2.4 ms, and 2.8 ms, respectively, which is indeed smaller than T_s. The following theorem characterizes the relationship between the measurement vector, the true state, and the attack at time k.

Theorem 1 The TSA measurement equation at discrete period k is given as:

$$\boldsymbol{z}_{n,k}^{\text{atk}} = \boldsymbol{\Gamma}_{n,k} \boldsymbol{H}_n \boldsymbol{v}_k + \boldsymbol{\varepsilon}_{n,k} \tag{5}$$

where $\boldsymbol{z}_{n,k}^{\text{atk}} \in \mathbf{R}^{M_n}$ is the attacked measurement vector; and $\boldsymbol{\Gamma}_{n,k} \in \mathbf{R}^{M_n \times M_n}$ is a block diagonal matrix consisting of $1+L_n$ blocks where each block is a 2×2 matrix $\begin{bmatrix} \cos(\Delta\theta_{n,k}) & -\sin(\Delta\theta_{n,k}) \\ \sin(\Delta\theta_{n,k}) & \cos(\Delta\theta_{n,k}) \end{bmatrix}$.

Proof The attacked instantaneous voltage at $t = kT_s$ is

$$v_n(kT_s + \delta_n(kT_s)) = \text{Re}\{\sqrt{2}\, V_n(kT_s + \delta_n(kT_s)) e^{\text{j}2\pi f(kT_s + \delta_n(kT_s))}\} \tag{6}$$

Considering that $\delta_n(t) \ll T_s$ and the network dynamics evolve slowly with respect to the sampling period T_s, the voltage phasor at $t + \delta_n(t)$ can be approximated as $V_n(t + \delta_n(t)) \approx V_n(t)$ [21]. Invoking the latter into (6), it follows that

$$\begin{aligned} v_n(kT_s + \delta_n(kT_s)) &\approx \text{Re}\{\sqrt{2}\, V_n(kT_s) e^{\text{j}2\pi f(kT_s + \delta_{n,k})}\} = \\ &\text{Re}\{\sqrt{2}\, V_{n,k} e^{\text{j}2\pi f \delta_{n,k}} e^{\text{j}2\pi f(kT_s)}\} \end{aligned} \tag{7}$$

Equation (7) reveals that the measured phasor is

$$V_{n,k} e^{\text{j}2\pi f \delta_{n,k}} = |V_{n,k}| e^{\text{j}\theta_{n,k}} e^{\text{j}\Delta\theta_{n,k}} = |V_{n,k}| e^{\text{j}(\theta_{n,k} + \Delta\theta_{n,k})} \tag{8}$$

Extracting the real and imaginary parts of the latter, and repeating for the current measurements, the noisy attacked PMU measurement at bus n for time period k is given by (cf. (2)):

$$\boldsymbol{z}_{n,k}^{\text{atk}} = \begin{bmatrix} |V_{n,k}|\cos(\theta_{n,k} + \Delta\theta_{n,k}) \\ |V_{n,k}|\sin(\theta_{n,k} + \Delta\theta_{n,k}) \\ \{|I_{np,k}|\cos(\theta_{I_{np,k}} + \Delta\theta_{n,k})\}_{p\in\mathcal{N}_n} \\ \{|I_{np,k}|\sin(\theta_{I_{np,k}} + \Delta\theta_{n,k})\}_{p\in\mathcal{N}_n} \end{bmatrix} + \boldsymbol{\varepsilon}_{n,k} \tag{9}$$

Upon introducing the trigonometric identities $\cos(a+b) = \cos(a)\cos(b) - \sin(a)\sin(b)$ and $\sin(a+b) = \sin(a)\cos(b) + \cos(a)\sin(b)$ into (9) and combining with (2) and $\boldsymbol{z}_{n,k}^{\text{true}} = \boldsymbol{H}_n \boldsymbol{v}_k$, the measurement model in (5) is obtained.

The assumed relationship between $\delta_n(t)$ and T_s enables the approximation $V_n(t + \delta_n(t)) \approx V_n(t)$. Thus, when $\delta_n(t)$ is smaller, but not significantly smaller, than T_s, the validity of the assumption and the resulting approximation are eventually determined by the extent in which the network dynamics are slow compared to the duration of the sampling period.

The model in (5) expresses the attacked PMU measurement $\boldsymbol{z}_{n,k}^{\text{atk}}$ in terms of the spoofing attack $\boldsymbol{\Gamma}_{n,k}$, the system $\boldsymbol{H}_n$, and the state $\boldsymbol{v}_k$ at time k. This model is leveraged in the next section to formulate the SE problem with spoofed PMU measurements.

III. Multi-period SE

This section presents the joint SE and attack angle reconstruction formulation. Both measurement and state equations are considered in a multi-objective optimization. Let $\boldsymbol{v} \in \mathbf{R}^{2N_b K}$ collect $\boldsymbol{v}_k$ for $k = 1, 2, \ldots, K$. Likewise, vector $\Delta\boldsymbol{\theta}$ collects $\Delta\theta_{n,k}$ for $n \in \mathcal{N}_{\text{PMU}}$ and $k = 1, 2, \ldots, K$. The optimization is formulated as follows:

$$(\hat{\boldsymbol{v}}, \Delta\hat{\boldsymbol{\theta}}) = \underset{\boldsymbol{v}, \Delta\boldsymbol{\theta}}{\arg\min}\ (J_1(\boldsymbol{v}, \Delta\boldsymbol{\theta}) + J_2(\boldsymbol{v})) \tag{10}$$

where J_1 represents the nonlinear weighted least squares problem of estimating $\boldsymbol{v}$ and $\Delta\boldsymbol{\theta}$ based on the measurement equation (5), as given in (11); and J_2 represents the weighted least squares problem of estimating $\boldsymbol{v}$ from the state equation (1), as given in (12).

$$J_1 = \frac{1}{2}\sum_{n=1}^{N_b}\sum_{k=1}^{K} a_n \|\boldsymbol{z}_{n,k}^{\text{atk}} - \boldsymbol{\Gamma}_{n,k}(\Delta\theta_{n,k})\boldsymbol{H}_n\boldsymbol{v}_k\|^2_{\boldsymbol{\Sigma}_{n,k}^{-1}} \tag{11}$$

$$J_2 = \frac{1}{2}\sum_{k=1}^{K} \|\boldsymbol{v}_k - \boldsymbol{v}_{k-1}\|^2_{\boldsymbol{Q}_k^{-1}} \tag{12}$$

where the norm notation $\|\boldsymbol{x}\|_{\boldsymbol{P}}^2 = \boldsymbol{x}^{\mathrm{T}}\boldsymbol{P}\boldsymbol{x}$ is used. The initial state vector $\boldsymbol{v}_0 \in \mathbf{R}^{2N_b}$ is considered known, which is an assumption akin to typical multi-period estimation setups that rely on, for example, the Kalman filter.

Problem (10) is nonconvex due to the bilinear term $\boldsymbol{\Gamma}_{n,k}(\Delta\theta_{n,k})\boldsymbol{H}_n\boldsymbol{v}_k$ and the sinusoidal dependence of $\boldsymbol{\Gamma}_{n,k}$ on $\Delta\boldsymbol{\theta}$ in J_1. Following [18], a reformulation of (10) that can lead to an efficient solution algorithm is pursued in the sequel. Specifically, a change of variable is introduced as follows:

$$\boldsymbol{\gamma}_{n,k} = [\gamma_{n,k,1} \quad \gamma_{n,k,2}]^{\mathrm{T}} = [\cos(\Delta\theta_{n,k}) \quad \sin(\Delta\theta_{n,k})]^{\mathrm{T}} \tag{13}$$

where $\boldsymbol{\gamma}_{n,k} \in \mathbf{R}^{2\times 1}$; $n \in \mathcal{N}_{\text{PMU}}$; and $k = 1, 2, \ldots, K$. The variable $\Delta\theta_{n,k}$ is eliminated, and the matrix $\boldsymbol{\Gamma}_{n,k}$ has blocks of the form $\begin{bmatrix} \gamma_{n,k,1} & -\gamma_{n,k,2} \\ \gamma_{n,k,2} & \gamma_{n,k,1} \end{bmatrix}$. The variables $\boldsymbol{\Gamma}_{n,k}$ and $\boldsymbol{\gamma}_{n,k}$ are thus used interchangeably.

In order to uniquely map the vector $\boldsymbol{\gamma}_{n,k}$ back to an angle $\Delta\theta_{n,k}$, it is necessary and sufficient to impose the constraint $\boldsymbol{\gamma}_{n,k}^{\mathrm{T}}\boldsymbol{\gamma}_{n,k} = 1$. Define $\boldsymbol{\gamma}$ as the vector including $\boldsymbol{\gamma}_{n,k}$ for all $n \in \mathcal{N}_{\text{PMU}}$, $k = 1, 2, \ldots, K$. Then, problem (10) becomes equivalent to the following:

$$(\hat{\boldsymbol{v}}, \hat{\boldsymbol{\gamma}}) = \underset{\boldsymbol{v}, \boldsymbol{\gamma}}{\arg\min}\ (J_1(\boldsymbol{v}, \boldsymbol{\gamma}) + J_2(\boldsymbol{v})) \tag{14}$$

s.t.

$$\boldsymbol{\gamma}_{n,k}^{\mathrm{T}}\boldsymbol{\gamma}_{n,k} = 1 \quad n \in \mathcal{N}_{\text{PMU}}, k = 1, 2, \ldots, K \tag{15}$$

In order to facilitate the development of an algorithm for the solution of (3), it is supposed that the following condition holds for the measurement model in (3).

Assumption 1 The matrix $[\boldsymbol{H}_{n_1}^{\mathrm{T}}, \boldsymbol{H}_{n_2}^{\mathrm{T}}, \ldots, \boldsymbol{H}_{n_p}^{\mathrm{T}}]^{\mathrm{T}}$ is full column-rank.

This assumption pertains to the observation matrix corresponding to all PMU measurements. It ensures that under normal operation (i. e., no spoofing), the power network is observable and the SE problem has a unique solution [38]. This condition is readily satisfied with proper placement of PMUs, a topic that has been well researched in the literature.

The transformation of the original unconstrained nonlinear problem (10) into the nonconvex quadratically constrained quadratic program (3) enables the development of an iterative solver with closed-form updates. This is the theme of the next section.

IV. Estimation Algorithm

This section develops an AM algorithm, to jointly solve (15) for $\boldsymbol{v}$ and $\boldsymbol{\gamma}$. The algorithm minimizes two sets of variables one after the other. In the first step, the objective is minimized with respect to one set of variables while treating the second set as constant. In the second step, the minimization occurs with respect to the second set of variables upon substituting the updated values of the first set of variables. In this instance, the vectors $\boldsymbol{v}$ and $\boldsymbol{\gamma}$ constitute the two sets of variables.

The procedure is repeated until convergence. The initialization step includes $\boldsymbol{\gamma}_{n,k} = [1, 0]^{\mathrm{T}}$ for all n and k. The two minimizations can be performed in closed form, and the related updates are described in the sequel.

A. Minimization with Respect to State

In order to derive the update for $\boldsymbol{v}$, the objectives J_1 and J_2 are re-written as explicit functions of the vector $\boldsymbol{v}$ instead of $\boldsymbol{v}_k$. Specifically, J_1 is written as:

$$J_1(\boldsymbol{v}, \boldsymbol{\gamma}) = \frac{1}{2}\sum_{n=1}^{N_b}\sum_{k=1}^{K} a_n \|\boldsymbol{z}_{n,k}^{\text{atk}} - \boldsymbol{\Gamma}_{n,k}\boldsymbol{H}_n\boldsymbol{B}_k\boldsymbol{v}\|^2_{\boldsymbol{\Sigma}_{n,k}^{-1}} \tag{16}$$

where $\boldsymbol{B}_k \in \mathbf{R}^{2N_b \times 2N_b K}$ is a matrix such that $\boldsymbol{v}_k = \boldsymbol{B}_k\boldsymbol{v}$. In particular, $\boldsymbol{B}_k$ is constructed as a block diagonal matrix with the $2N_b \times 2N_b$ identity matrix in the k^{th} block.

Similarly, J_2 can be written as:

$$J_2(\boldsymbol{v}) = \frac{1}{2}\left(\|\boldsymbol{E}\boldsymbol{v} - \boldsymbol{v}_0\|^2_{\boldsymbol{Q}_1^{-1}} + \sum_{k=2}^{K}\|\boldsymbol{A}_k\boldsymbol{v}\|^2_{\boldsymbol{Q}_k^{-1}}\right) \tag{17}$$

where $\boldsymbol{E} \in \mathbf{R}^{2N_b \times 2N_b K}$ and $\boldsymbol{A}_k \in \mathbf{R}^{2N_b \times 2N_b K}$ $(k = 2, 3, \ldots, K)$ are matrices such that $\boldsymbol{v}_1 = \boldsymbol{E}\boldsymbol{v}$ and $\boldsymbol{v}_k - \boldsymbol{v}_{k-1} = \boldsymbol{A}_k\boldsymbol{v}$. Specifically, matrix $\boldsymbol{E}$ includes the identity matrix in the top $2N_b \times 2N_b$ diagonal block and is zero otherwise. Matrix $\boldsymbol{A}_k$ is constructed as a fat matrix with negative identity matrix at the $(k-1)^{\text{th}}$ block and identity matrix at the k^{th} block.

The minimization with respect to $\boldsymbol{v}$ is an unconstrained minimization with a convex quadratic objective function. The solution is obtained by solving the first-order optimality condition $\nabla_{\boldsymbol{v}} J(\boldsymbol{v}) = 0$ and is given as:

$$\hat{\boldsymbol{v}}_{\text{AM}} = \boldsymbol{M}^{-1}\left[\sum_{n=1}^{N_b}\sum_{k=1}^{K} a_n(\boldsymbol{\Gamma}_{n,k}\boldsymbol{H}_n\boldsymbol{B}_k)^{\mathrm{T}}\boldsymbol{\Sigma}_{n,k}^{-1}\boldsymbol{z}_{n,k}^{\text{atk}} + \boldsymbol{E}^{\mathrm{T}}\boldsymbol{Q}_1^{-1}\boldsymbol{v}_0\right] \tag{18}$$

$$\boldsymbol{M} = \boldsymbol{E}^{\mathrm{T}}\boldsymbol{Q}_1^{-1}\boldsymbol{E} + \sum_{k=2}^{K}\boldsymbol{A}_k^{\mathrm{T}}\boldsymbol{Q}_k^{-1}\boldsymbol{A}_k + \sum_{n=1}^{N_b}\sum_{k=1}^{K} a_n(\boldsymbol{\Gamma}_{n,k}\boldsymbol{H}_n\boldsymbol{B}_k)^{\mathrm{T}}\boldsymbol{\Sigma}_{n,k}^{-1}\boldsymbol{\Gamma}_{n,k}\boldsymbol{H}_n\boldsymbol{B}_k \tag{19}$$

The following result asserts that matrix $\boldsymbol{M}$ is indeed invertible.

Theorem 2 Given that Assumption 1 holds and the entries in $\boldsymbol{\gamma}$ satisfy (15), then matrix $\boldsymbol{M}$ is invertible.

Proof It follows by the structure of $\boldsymbol{M}$ and the positive definiteness of $\boldsymbol{Q}_k$ and $\boldsymbol{\Sigma}_{n,k}$ that $\boldsymbol{M}$ is positive semidefinite. We will show that the third term comprising $\boldsymbol{M}$ is full-rank,

and therefore, $\boldsymbol{M}$ is invertible. The third term in $\boldsymbol{M}$ can be written as shown in (20).

$$\sum_{k=1}^{K}\boldsymbol{B}_k^{\mathrm{T}}\begin{bmatrix}\boldsymbol{H}_{n_1}\\ \boldsymbol{H}_{n_2}\\ \vdots\\ \boldsymbol{H}_{n_P}\end{bmatrix}^{\mathrm{T}}\begin{bmatrix}\boldsymbol{\Gamma}_{n_1,k} & 0 & \cdots & 0\\ 0 & \boldsymbol{\Gamma}_{n_2,k} & \cdots & 0\\ \vdots & \vdots & & \vdots\\ 0 & 0 & \cdots & \boldsymbol{\Gamma}_{n_P,k}\end{bmatrix}^{\mathrm{T}}\begin{bmatrix}\boldsymbol{\Sigma}_{n_1,k}^{-1} & 0 & \cdots & 0\\ 0 & \boldsymbol{\Sigma}_{n_2,k}^{-1} & \cdots & 0\\ \vdots & \vdots & & \vdots\\ 0 & 0 & \cdots & \boldsymbol{\Sigma}_{n_P,k}^{-1}\end{bmatrix}\begin{bmatrix}\boldsymbol{\Gamma}_{n_1,k} & 0 & \cdots & 0\\ 0 & \boldsymbol{\Gamma}_{n_2,k} & \cdots & 0\\ \vdots & \vdots & & \vdots\\ 0 & 0 & \cdots & \boldsymbol{\Gamma}_{n_P,k}\end{bmatrix}\begin{bmatrix}\boldsymbol{H}_{n_1}\\ \boldsymbol{H}_{n_2}\\ \vdots\\ \boldsymbol{H}_{n_P}\end{bmatrix}\boldsymbol{B}_k \tag{20}$$

The central matrix in (20) is full-rank because the convariance matrices $\boldsymbol{\Sigma}_{n,k}$ are positive definite. The matrices $\boldsymbol{\Gamma}_{n,k}$ are full-rank as long as the entries in $\boldsymbol{\gamma}$ satisfy (15). Finally, the matrix consisting of the $\boldsymbol{H}_{n_i}$ is full-rank due to Assumption 1. By successive application of the Sylvester inequality [39], it follows that the matrix enclosed between $\boldsymbol{B}_k^{\mathrm{T}}$ and $\boldsymbol{B}_k$, which has size $2N_b \times 2N_b$, has full rank for $k = 1, 2, \ldots, K$.

By the construction of $\boldsymbol{B}_k$, the pre- and post-multiplication by $\boldsymbol{B}_k^{\mathrm{T}}$ and $\boldsymbol{B}_k$, respectively, generates a $2N_bK \times 2N_bK$ block diagonal matrix. The k^{th} block in this larger matrix is full-rank, according to the previous explanation. Therefore, the matrix in (19) is full-rank.

The invertibility of $\boldsymbol{M}$ relies upon the $\boldsymbol{\gamma}_{n,k}$ values substituted in (2) satisfying (15). This condition is ensured by the next step.

B. Minimization with Respect to Attack Angles

In order to perform the minimization with respect to $\boldsymbol{\gamma}$, only the first of the two objectives in (14) is relevant. Due to the separability of the objective $J_1(\boldsymbol{v}, \boldsymbol{\gamma})$ (cf. (16)) and constraints per n and k, this minimization can be performed in parallel with respect to the variables pertaining to different PMUs and time periods. The resulting problem is stated for $n \in \mathcal{N}_{\text{PMU}}$ and $k = 1, 2, \ldots, K$ as follows:

$$\begin{cases}\min\limits_{\boldsymbol{\gamma}_{n,k}} \left[(\boldsymbol{z}_{n,k}^{\text{atk}} - \boldsymbol{\Gamma}_{n,k}\boldsymbol{H}_n\boldsymbol{v}_k)^{\mathrm{T}}\boldsymbol{\Sigma}_{n,k}^{-1}(\boldsymbol{z}_{n,k}^{\text{atk}} - \boldsymbol{\Gamma}_{n,k}\boldsymbol{H}_n\boldsymbol{v}_k)\right]\\ \text{s.t. } \boldsymbol{\gamma}_{n,k}^{\mathrm{T}}\boldsymbol{\gamma}_{n,k} = 1\end{cases} \tag{21}$$

Considering that $\boldsymbol{v}_k$ is not a variable in (21), the objective in (21) can be rearranged as follows:

$$\begin{cases}\min\limits_{\boldsymbol{\gamma}_{n,k}} \left[(\boldsymbol{z}_{n,k}^{\text{atk}} - \tilde{\boldsymbol{A}}_{n,k}\boldsymbol{\gamma}_{n,k})^{\mathrm{T}}\boldsymbol{\Sigma}_{n,k}^{-1}(\boldsymbol{z}_{n,k}^{\text{atk}} - \tilde{\boldsymbol{A}}_{n,k}\boldsymbol{\gamma}_{n,k})\right]\\ \text{s.t. } \boldsymbol{\gamma}_{n,k}^{\mathrm{T}}\boldsymbol{\gamma}_{n,k} = 1\end{cases} \tag{22}$$

where $\tilde{\boldsymbol{A}}_{n,k}$ is given by

$$\tilde{\boldsymbol{A}}_{n,k} = \begin{bmatrix}\boldsymbol{h}_{n,1}^{\mathrm{T}}\boldsymbol{v}_k & -\boldsymbol{h}_{n,2}^{\mathrm{T}}\boldsymbol{v}_k\\ \boldsymbol{h}_{n,2}^{\mathrm{T}}\boldsymbol{v}_k & \boldsymbol{h}_{n,1}^{\mathrm{T}}\boldsymbol{v}_k\\ \vdots & \vdots\\ \boldsymbol{h}_{n,M_n-1}^{\mathrm{T}}\boldsymbol{v}_k & -\boldsymbol{h}_{n,M_n}^{\mathrm{T}}\boldsymbol{v}_k\\ \boldsymbol{h}_{n,M_n}^{\mathrm{T}}\boldsymbol{v}_k & \boldsymbol{h}_{n,M_n-1}^{\mathrm{T}}\boldsymbol{v}_k\end{bmatrix} \tag{23}$$

where $\boldsymbol{h}_{n,i}^{\mathrm{T}}$ is the i^{th} row of $\boldsymbol{H}_n$ $(i = 1, 2, \ldots, M_n)$.

Problem (21) is nonconvex due to the quadratic equality constraints. A problem of this form has been thoroughly analyzed in [18], where a procedure to obtain a closed form solution based on Lagrangian duality is detailed. Furthermore, when the covariance matrices $\boldsymbol{\Sigma}_{n,k}$ have special structure, the solution of (21) is particularly easy to be obtained. As this is a practically relevant case, this result is stated next.

Theorem 3 Suppose that $\boldsymbol{\Sigma}_{n,k}$ is a diagonal matrix with equal variances for the real and imaginary parts corresponding to each measurement, that is, the diagonal entries of $\boldsymbol{\Sigma}_{n,k}$ satisfy the following for all n and k:

$$\begin{cases}\sigma_{n,k,1}^2 = \sigma_{n,k,2}^2\\ \sigma_{n,k,3}^2 = \sigma_{n,k,4}^2\\ \vdots\\ \sigma_{n,k,M_n-1}^2 = \sigma_{n,k,M_n}^2\end{cases} \tag{24}$$

Then, the solution of (21) is given as follows:

$$\hat{\boldsymbol{\gamma}}_{n,k} = \frac{\tilde{\boldsymbol{A}}_{n,k}^{\mathrm{T}}\boldsymbol{\Sigma}_{n,k}^{-1}\boldsymbol{z}_{n,k}^{\text{atk}}}{\|\tilde{\boldsymbol{A}}_{n,k}^{\mathrm{T}}\boldsymbol{\Sigma}_{n,k}^{-1}\boldsymbol{z}_{n,k}^{\text{atk}}\|_2} \tag{25}$$

Note that the measurement covariance matrix is routinely assumed diagonal, and the particular structure mentioned in Theorem 3 can be found in [23], [36], [40].

Algorithm 1 describes the AM steps for SE and attack reconstruction, incorporating the results of the present section. The convergence criterion checks whether at least one of two conditions hold: $\|O_{curr} - O_{prev}\|_2 \le \epsilon$ or $|O_{curr} - O_{prev}|/|O_{curr}| \le \epsilon$, where O_{prev} and O_{curr} are the values of the objective function (14) before and after the update, respectively; and ϵ is a predefined tolerance.

Algorithm 1: SE and attack reconstruction

Result: state estimate $\hat{\boldsymbol{v}}_{\text{AM}}$ and attack angle $\Delta\theta_{n,k}$, $n \in \mathcal{N}_{\text{PMU}}$, $k = 1, 2, \ldots, K$
Input: $\boldsymbol{z}_{n,k}^{\text{atk}}$
Initialization: solve (18) for $\hat{\boldsymbol{v}}_{\text{AM}}$ by setting $\boldsymbol{\gamma}_{n,k} = [1, 0]^{\mathrm{T}}$
repeat
  for $k = 1, 2, \ldots, K$ **do**
    for $n \in \mathcal{N}_{\text{PMU}}$ **do**
      Find the corresponding $\hat{\boldsymbol{\gamma}}_{n,k}$ via (25)
    end
  end
  Update $\hat{\boldsymbol{v}}_{\text{AM}}$ using (18)
until convergence or maximum iterations

Algorithm 1 minimizes the objective function after each update of the state and the attack angles. Because the objective function is lower bounded, the sequence of produced objective function values converges to a limit. This point may not be the global minimum, as the problem is nonconvex. Nevertheless, the numerical tests of Section V indicate very favorable SE performance.

C. Rolling Window Implementation

Algorithm 1 can be implemented in a rolling window fashion. Specifically, suppose that the state estimates for periods $\{1, 2, \ldots, K\}$ are available, and measurements for periods $\{K, K+1, \ldots, L\}$ are obtained, where $K \le L \le 2K$. Then, Algo-

rithm 1 can be applied to provide state estimates for $\{L-K+1, L-K+2, \ldots, L\}$, where the value $\boldsymbol{v}_{L-K}$ available from the previous window plays the role of the known $\boldsymbol{v}_0$ for the current window. Thus, the windows may be overlapping, and the process continues.

V. Numerical Tests

This section presents the state and attack angle estimation tests using the AM algorithm. The numerical tests are performed on the standard IEEE 14- and 118-bus systems. All network parameters are provided in case files case14.m and case118.m of MATPOWER [41], from which $\boldsymbol{H}_n$ is computed. The PMU placement vector $\boldsymbol{a}$ for all test cases is obtained using the criterion in [36] based exclusively on the availability of PMU measurements. Table I lists the buses with installed PMUs for each network. Similar to [28], the state noise covariance $\boldsymbol{Q}_k$ is diagonal, and its diagonal entries result from standard deviation of 0.001 p.u.. The measurement noise covariance $\boldsymbol{\Sigma}_{n,k}$ is also diagonal resulting from standard deviation of 0.001 p.u. for bus voltage and line current measurements. The measurement noise standard deviation is chosen such that PMU measurements do not violate the IEEE C37.118 standard [42]. In fact, with this choice of standard deviation, the majority of measurements incur a 0.1%-0.2% total variation error [28]. For simplicity, the state and measurement noise covariance matrices are assumed constant across all time periods k.

TABLE I
Optimal PMU Location for IEEE Test Networks

Test case	$\lvert\mathcal{N}_{\text{PMU}}\rvert$	Bus number
IEEE 14-bus	6	2, 4, 6, 7, 10, 14
IEEE 118-bus	94	1-5, 7-19, 21-25, 27-36, 40, 43, 44, 46, 47, 48, 50, 51, 52, 53, 55-60, 64, 65, 66, 67, 68, 70, 71, 73, 75, 76, 77, 80-83, 85-90, 92, 94-104, 106-111, 113-118

The PMU sampling rate is set to 30 samples per second. The simulation considers a time horizon of 35 s. Two realistic attacks, namely, Type I (step) and Type II (ramp) are performed [35]. The AM algorithm is first tested with attacks on the PMUs located at buses 14 and 7 of the IEEE 14- and 118-bus networks, respectively.

The Type I attack occurs suddenly at a particular time instant and remains constant thereafter. In this test, a Type I attack of 0.5787° appears at 30 s [12]. It is customary in the GPS community to also express the attack in meters by multiplying the time offset of the attack by the speed of light $c = 3\times10^8$ m/s; the particular attack is thus 8000 m. The value of the attack is chosen so that the measurement exceeds the total variation error of 1% specified by the IEEE C37.118 standard [42]. The Type II attack changes gradually through time. For the attack to be successful, it cannot exceed the distance-equivalent velocity of 400 m/s [10]. Adhering to this value, the attack in this test starts at 10 s from value 0 m and gradually increases to 1000 m at 35 s.

To demonstrate the effectiveness of the algorithm, representative results pertaining to individual buses and the entire network are presented. The true and estimated voltage magnitudes and phase angles at bus 2 of the IEEE 14- and 118-bus networks across the time horizon are given in Fig. 1 and Fig. 2, respectively (bus 2 is not attacked). It is observed that estimated values closely follow the corresponding true values. Figures 3 and 4 depict the true and estimated attack angles at buses 14 and 7, respectively, for the Type I and II attacks in the IEEE 14- and 118-bus networks. It is observed that the estimated attack angles closely follow their true values.

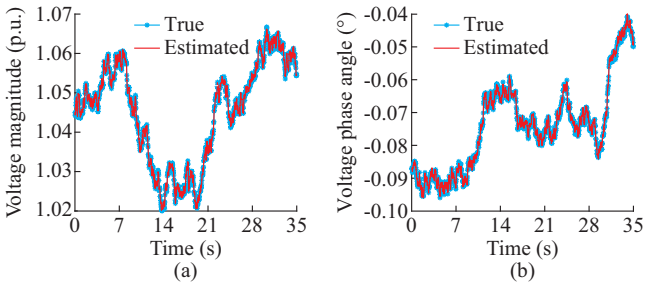

Fig. 1. True and estimated voltage magnitudes and phase angles at bus 2 of IEEE 14-bus network across time horizon. (a) Voltage magnitude. (b) Voltage phase angle.

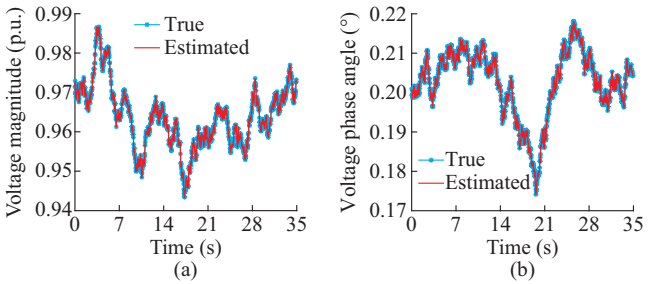

Fig. 2. True and estimated voltage magnitudes and phase angles at bus 2 of IEEE 118-bus network across time horizon. (a) Voltage magnitude. (b) Voltage phase angle.

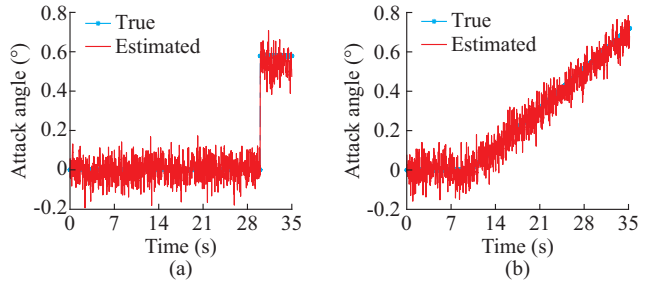

Fig. 3. True and estimated Type I and Type II attack angles at bus 14 in IEEE 14-bus network across time horizon. (a) Type I. (b) Type II.

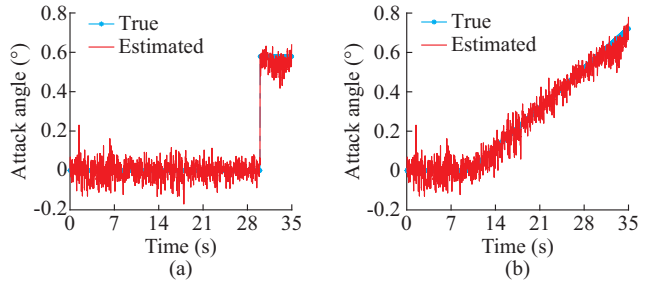

Fig. 4. True and estimated Type I and Type II attack angles at bus 7 in IEEE 118-bus network across time horizon. (a) Type I. (b) Type II.

The relative voltage error is defined as $\|\hat{\boldsymbol{v}}_k - \boldsymbol{v}_k\|_2 / \|\boldsymbol{v}_k\|_2$, where $\hat{\boldsymbol{v}}_k$ and $\boldsymbol{v}_k$ are the state vector estimated with Algorithm 1 and its true value at period k, respectively. The relative voltage error for the IEEE 14- and 118-bus networks across the time horizon is depicted in Fig. 5. The relative error is of the order of 10^{-3} and 10^{-4} for the IEEE 14- and 118-bus networks, respectively. The error in attack angles is defined as $\|\Delta\hat{\boldsymbol{\theta}}_k - \Delta\boldsymbol{\theta}_k\|_2 / P$, where $\Delta\hat{\boldsymbol{\theta}}_k$ and $\Delta\boldsymbol{\theta}_k$ are the attack angle vector resulting from Algorithm 1 and its true value at period k, respectively. Figure 6 depicts the attack angle errors for Type I and Type II attacks in the IEEE 14-bus network. Likewise, Fig. 7 shows the attack angle errors for both types of attacks in the IEEE 118-bus network.

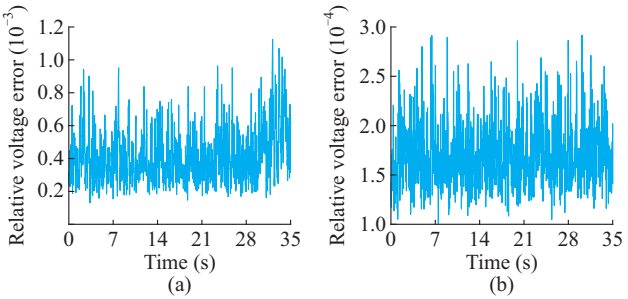

Fig. 5. Relative voltage errors for IEEE 14- and 118-bus networks across time horizon. (a) IEEE 14-bus network. (b) IEEE 118-bus network.

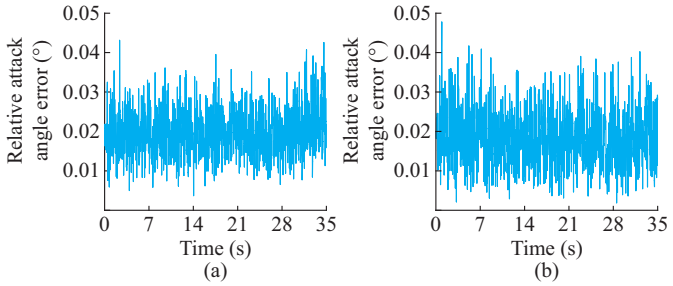

Fig. 6. Type I and Type II attack angle errors for IEEE 14-bus network across time horizon. (a) Type I. (b) Type II.

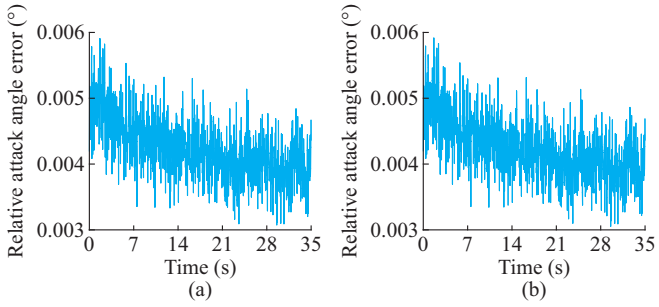

Fig. 7. Type I and Type II attack angle errors for IEEE 118-bus network across time horizon. (a) Type I. (b) Type II.

Next, the algorithm is tested with attacks at buses 2, 4, 6, and 14 of the IEEE 14-bus network, and buses 7, 50, 60, and 80 of the IEEE 118-bus network. Only one bus is attacked in each run. The mean relative error is defined as the average of the relative error across the time horizon, that is, $\frac{1}{K}\sum_{k=1}^{K} \|\hat{\boldsymbol{v}}_k - \boldsymbol{v}_k\|_2 / \|\boldsymbol{v}_k\|_2$. The mean voltage phase angle is the average of the voltage phase angle of a bus across the time horizon, computed from the random walk model of the voltage state. Tables II and III list the mean voltage phase angle for the attacked bus and the resulting mean relative voltage error for the IEEE 14-bus network with Type I attacks of 0.5787° and 5°, respectively. The corresponding values for the IEEE 14-bus network with Type II attack are given in Table IV. Tables V-VII list the mean voltage phase angle for the attacked bus and the resulting mean relative voltage error for the IEEE 118-bus network under Type I and Type II attacks. The values for the mean voltage phase angle and mean relative voltage error in Tables II-VII are computed from single run of the algorithm. However, these values vary only slightly across multiple runs of the algorithm. The results in Tables II-VII reveal that the performance of the algorithm is not sensitive to the location of the attack, the voltage phase angle of the attacked bus, or the attack size.

TABLE II
MEAN RELATIVE VOLTAGE ERROR AND MEAN VOLTAGE PHASE ANGLE FOR IEEE 14-BUS NETWORK WITH TYPE I ATTACK OF 0.5787°

Attacked bus number	Mean voltage phase angle (°)	Mean relative voltage error
2	−5.0255	0.00044492
4	−10.1426	0.00044767
6	−14.0238	0.00045789
14	−15.8632	0.00042576

TABLE III
MEAN RELATIVE VOLTAGE ERROR AND MEAN VOLTAGE PHASE ANGLE FOR IEEE 14-BUS NETWORK WITH TYPE I ATTACK OF 5°

Attacked bus number	Mean voltage phase angle (°)	Mean relative voltage error
2	−5.3773	0.00043858
4	−10.1261	0.00044767
6	−14.7917	0.00044817
14	−17.5053	0.00044040

TABLE IV
MEAN RELATIVE VOLTAGE ERROR AND MEAN VOLTAGE PHASE ANGLE FOR IEEE 14-BUS NETWORK WITH TYPE II ATTACK

Attacked bus number	Mean voltage phase angle (°)	Mean relative voltage error
2	−5.3774	0.00044050
4	−8.9737	0.00040892
6	−14.5895	0.00044480
14	−16.1468	0.00043225

The quality of the state and attack angle estimation is compared to that of [18], which performs estimation in a single period and does not account for the dynamic network model. Figures 8-10 depict results from Algorithm 1 (single-period SE) and [18] (multi-period SE) plotted every 5$^{\text{th}}$ sample for the setup corresponding to the IEEE 14-bus network and attack on bus 14. The relative voltage error and attack angle error have been previously defined, while the state er-

ror norm depicted in Fig. 9 is defined as $\|\hat{\boldsymbol{v}}_k - \boldsymbol{v}_k\|_2$. In the Type I attack error plots, the error in single-period SE is higher than that in multi-period SE before the attack occurs (at 30 s). Due to the step attack, the error in multi-period SE increases, but remains overall less than that in single-period SE. In Type II attack error plots, the error in single-period SE is greater than that in multi-period SE.

TABLE V
MEAN RELATIVE VOLTAGE ERROR AND MEAN VOLTAGE PHASE ANGLE FOR IEEE 118-BUS NETWORK WITH TYPE I ATTACK OF 0.5787°

Attacked bus number	Mean voltage phase angle (°)	Mean relative voltage error
7	14.1334	0.00017028
50	20.8352	0.00016969
60	24.2264	0.00017338
80	29.0855	0.00016888

TABLE VI
MEAN RELATIVE VOLTAGE ERROR AND MEAN VOLTAGE PHASE ANGLE FOR IEEE 118-BUS NETWORK WITH TYPE I ATTACK OF 5°

Attacked bus number	Mean voltage phase angle (°)	Mean relative voltage error
7	12.7141	0.00016947
50	18.9251	0.00017090
60	23.4543	0.00017410
80	27.3213	0.00017176

TABLE VII
MEAN RELATIVE VOLTAGE ERROR AND MEAN VOLTAGE PHASE ANGLE FOR IEEE 118-BUS NETWORK WITH TYPE II ATTACK

Attacked bus number	Mean voltage phase angle (°)	Mean relative voltage error
7	13.0204	0.00016892
50	20.8746	0.00017052
60	22.0586	0.00017233
80	27.8337	0.00017249

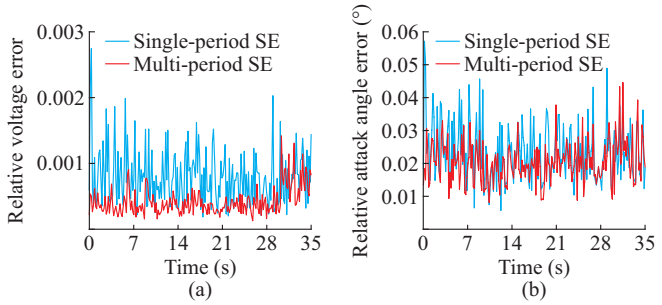

Fig. 8. Relative voltage error and attack angle error for Type I attack in IEEE 14-bus network across time horizon. (a) Relative voltage error. (b) Attack angle error.

Finally, a comparison between Algorithm 1 and the Kalman filter is performed for the IEEE 14-bus network with Type I and Type II attacks at bus 14. The Kalman filter is run according to [28]. Both the Algorithm 1 and the Kalman filter take the sequence of measurements $\boldsymbol{z}_{n,k}^{\text{atk}}$ as input and produce the sequence of state estimates $\hat{\boldsymbol{v}}_k$. Figure 11 depicts the resulting state error norm for the Kalman filter and Algorithm 1. It is observed that at the onset of the attack and thereafter, the Kalman filter yields larger state error norm than Algorithm 1 for both of the attack types. This is to be expected, as the Kalman filter is not designed to mitigate spoofing attacks.

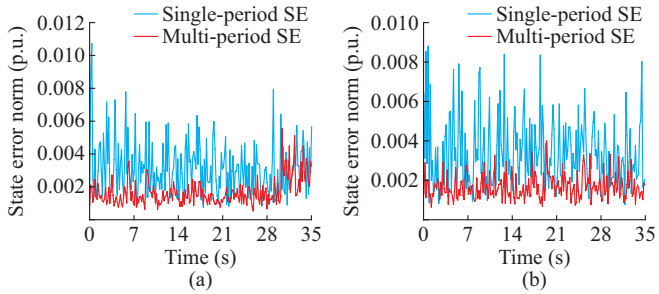

Fig. 9. State error norms for Type I and Type II attacks in IEEE 14-bus network across time horizon. (a) Type I. (b) Type II.

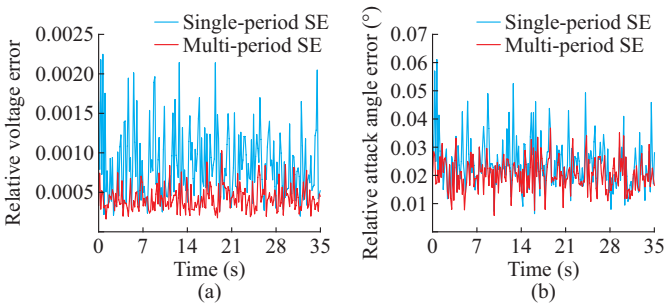

Fig. 10. Relative voltage error and attack angle error for Type II attack in IEEE 14-bus network across time horizon. (a) Relative voltage error. (b) Attack angle error.

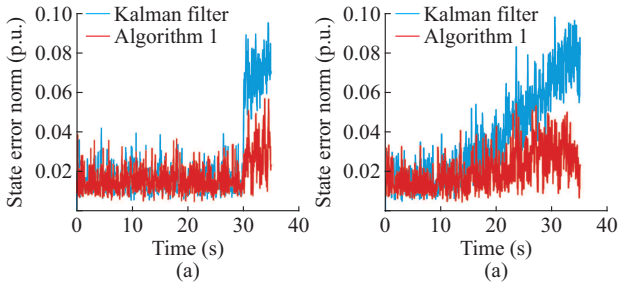

Fig. 11. State error norms for Type I and Type II attacks in IEEE 14-bus network across time horizon using Algorithm 1 and Kalman filter. (a) Type I. (b) Type II.

VI. CONCLUSION

This paper puts forth a dynamic model which relates the measurement, state vector, and GPS spoofing attacks. The resulting nonconvex multi-period SE problem is solved by an AM algorithm that jointly estimates the state and reconstructs the attack. Two realistic attack scenarios are considered to validate the aforementioned algorithm on standard IEEE transmission networks. The numerical tests indicate that the estimation quality under GPS spoofing attacks is improved by considering the dynamic model of the network, as opposed to static estimation approaches.

The developed dynamic model and resulting algorithm are

applicable to networks whose dynamics are slow enough compared to the sampling period, while relying on the condition that the delay induced by spoofing attack is smaller than the sampling period. It is an interesting direction to develop models for dynamic SE under spoofing attacks in more general setups. Furthermore, power networks may have available readings from SCADA and PMU systems. Developing algorithms for mitigating spoofing attacks in networks where both types of measurements are combined is an additional research direction.

REFERENCES

[1] T. Popovic, C. Blask, M. Carpenter *et al*., "Electric sector failure scenarios and impact analyses – version 3.0," Electric Power Research Institute, Washington, Tech. Rep., Dec. 2015.

[2] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen *et al*., "GPS vulnerability to spoofing threats and a review of anti spoofing techniques," *International Journal of Navigation and Observation*, vol. 2012, pp. 1-16, May 2012.

[3] D. Schmidt, K. Radke, S. Camtepe *et al*., "A survey and analysis of the GNSS spoofing threat and countermeasures," *ACM Computing Surveys*, vol. 48, no. 4, pp. 1-31, May 2016.

[4] B. Moussa, M. Debbabi, and C. Assi, "Security assessment of time synchronization mechanisms for the smart grid," *IEEE Communications Surveys Tutorials*, vol. 18, no. 3, pp. 1952-1973, Feb. 2016.

[5] L. Heng, J. J. Makela, A. D. Dominguez-Garcia *et al*., "Reliable GPS-based timing for power systems: a multi-layered multi-receiver architecture," in *Proceedings of Power and Energy Conference at Illinois*, Champaign, USA, Feb. 2014, pp. 1-7.

[6] D. Chou, L. Heng, and G. Gao, "Robust GPS-based timing for phasor measurement units: a position-information-aided approach," in *Proceedings of 27th International Technical Meeting of the Satellite Division of the Institute of Navigation*, Tampa, USA, Sept. 2014, pp. 1261-1269.

[7] D.-Y. Yu, A. Ranganathan, T. Locher *et al*., "Short paper: detection of GPS spoofing attacks in power grids," in *Proceedings of ACM Conference on Security and Privacy in Wireless & Mobile Networks*, Oxford, United Kingdom, Jul. 2014, pp. 99-104.

[8] F. Zhu, A. Youssef, and W. Hamouda, "Detection techniques for data level spoofing in GPS-based phasor measurement units," in *Proceedings of International Conference on Selected Topics in Mobile Wireless Networking*, Cairo, Egypt, Apr. 2016, pp. 1-8.

[9] Y. Fan, Z. Zhang, M. Trinkle *et al*., "A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart grids," *IEEE Transactions on Smart Grid*, vol. 6, no. 6, pp. 2659-2668, Nov. 2015.

[10] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," *International Journal of Critical Infrastructure Protection*, vol. 5, no. 3, pp. 146-153, Dec. 2012.

[11] I. Akkaya, E. A. Lee, and P. Derler, "Model-based evaluation of GPS spoofing attacks on power grid sensors," in *Proceedings of Workshop Modeling and Simulation of Cyber-Physical Energy Systems*, Berkeley, USA, May 2013, pp. 1-6.

[12] X. Jiang, J. Zhang, B. J. Harding *et al*., "Spoofing GPS receiver clock offset of phasor measurement units," *IEEE Transactions on Power Systems*, vol. 28, no. 3, pp. 3253-3262, Aug. 2013.

[13] Z. Zhang, S. Gong, A. D. Dimitrovski *et al*., "Time synchronization attack in smart grid: impact and analysis," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 87-98, Mar. 2013.

[14] J. G. Sreenath, S. Mangalwedekar, A. Meghwani *et al*., "Impact of GPS spoofing on synchrophasor assisted load shedding," in *Proceedings of IEEE PES General Meeting*, Portland, USA, Aug. 2018, pp. 1-5.

[15] Y. Wang and J. P. Hespanha, "Distributed estimation of power system oscillation modes under attacks on GPS clocks," *IEEE Transactions on Instrumentation and Measurement*, vol. 67, no. 7, pp. 1626-1637, Jul. 2018.

[16] X. Fan, L. Du, and D. Duan, "Synchrophasor data correction under GPS spoofing attack: a state estimation based approach," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4538-4546, Sept. 2018.

[17] X. Fan, S. Pal, D. Duan *et al*., "Closed-form solution for synchrophasor data correction under GPS spoofing attack," in *Proceedings of IEEE PES General Meeting*, Portland, USA, Aug. 2018, pp. 1-5.

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

[19] S. D. Silva, T. Hagan, J. Kim *et al*., "Sparse error correction for PMU data under GPS spoofing attacks," in *Proceedings of IEEE Global Conference on Signal and Information Processing*, Anaheim, USA, Nov. 2018, pp. 902-906.

[20] Y. Zhang, J. Wang, and J. Liu, "Attack identification and correction for PMU GPS spoofing in unbalanced distribution systems," *IEEE Transactions on Smart Grid*, vol. 11, no. 1, pp. 762-773, Jan. 2020.

[21] P. Pradhan, K. Nagananda, P. Venkitasubramaniam *et al*., "GPS spoofing attack characterization and detection in smart grids," in *Proceedings of IEEE Conference on Communications and Network Security*, Philadelphia, USA, Oct. 2016, pp. 391-395.

[22] P. Castello, C. Muscas, P. Pegoraro *et al*., "Trustworthiness of PMU data in the presence of synchronization issues," in *Proceedings of IEEE International Instrumentation and Measurement Technology Conference*, Houston, USA, May 2018, pp. 1-5.

[23] P. Yang, Z. Tan, A. Wiesel *et al*., "Power system state estimation using PMUs with imperfect synchronization," *IEEE Transactions on Power Systems*, vol. 28, no. 4, pp. 4162-4172, Nov. 2013.

[24] J. Du, S. Ma, Y. Wu *et al*., "Distributed Bayesian hybrid power state estimation with PMU synchronization errors," in *Proceedings of IEEE Global Communications Conference*, Austin, USA, Dec. 2014, pp. 3174-3179.

[25] J. A. Bazerque, U. Ribeiro, and J. Costa, "Synchronization of phasor measurement units and its error propagation to state estimators," in *Proceedings of IEEE PES Innovative Smart Grid Technologies Latin America*, Montevideo, Uruguay, Oct. 2015, pp. 508-513.

[26] M. Todescato, R. Carli, L. Schenato *et al*., "PMUs clock desynchronization compensation for smart grid state estimation," in *Proceedings of IEEE Conference on Decision and Control*, Melbourne, Australia, Dec. 2017, pp. 793-798.

[27] L. Hu, Z. Wang, I. Rahman *et al*., "A constrained optimization approach to dynamic state estimation for power systems including PMU and missing measurements," *IEEE Transactions on Control Systems Technology*, vol. 24, no. 2, pp. 703-710, Mar. 2016.

[28] S. Sarri, L. Zanni, M. Popovic *et al*., "Performance assessment of linear state estimators using synchrophasor measurements," *IEEE Transactions on Instrumentation and Measurement*, vol. 65, no. 3, pp. 535-548, Mar. 2016.

[29] M. B. D. C. Filho and J. C. S. de Souza, "Forecasting-aided state estimation – part I: panorama," *IEEE Transactions on Power Systems*, vol. 24, no. 4, pp. 1667-1677, Nov. 2009.

[30] A. Monticelli, "Electric power system state estimation," *Proceedings of IEEE*, vol. 88, no. 2, pp. 262-282, Feb. 2000.

[31] J. Zhang, G. Welch, G. Bishop *et al*., "A two-stage Kalman filter approach for robust and real-time power system state estimation," *IEEE Transactions on Sustainable Energy*, vol. 5, no. 2, pp. 629-636, Apr. 2014.

[32] N. Zhou, D. Meng, Z. Huang *et al*., "Dynamic state estimation of a synchronous machine using PMU data: a comparative study," *IEEE Transactions on Smart Grid*, vol. 6, no. 1, pp. 450-460, Jan. 2015.

[33] J. Zhao, M. Netto, and L. Mili, "A robust iterated extended Kalman filter for power system dynamic state estimation," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3205-3216, Jul. 2017.

[34] Y. Guo, B. Zhang, W. Wu *et al*., "Multi-time interval power system state estimation incorporating phasor measurements," in *Proceedings of IEEE PES General Meeting*, Denver, USA, Jul. 2015, pp. 1-5.

[35] A. Khalajmehrabadi, N. Gatsis, D. Akopian *et al*., "Realtime rejection and mitigation of time synchronization attacks on the global positioning system," *IEEE Transactions on Industrial Electronics*, vol. 65, no. 8, pp. 6425-6435, Aug. 2018.

[36] V. Kekatos, G. Giannakis, and B. Wollenberg, "Optimal placement of phasor measurement units via convex relaxation," *IEEE Transactions on Power Systems*, vol. 27, no. 3, pp. 1521-1530, Aug. 2012.

[37] P. Risbud, N. Gatsis, and A. Taha, "Assessing power system state estimation accuracy with GPS-spoofed PMU measurements," in *Proceedings of 7th IEEE Conference on Innovative Smart Grid Technologies*, Minneapoils, USA, Sept. 2016, pp. 1-5.

[38] A. Gomez-Exposito, A. J. Conejo, and C. Canizares, *Electric Energy Systems: Analysis and Operation*. Boca Raton: CRC Press, 2018.

[39] R. Horn and C. R. Johnson, *Matrix Analysis*, 2nd ed. Cambridge: Cambridge University Press, 2013.

[40] A. Gomez-Exposito, P. Rousseaux, C. Gomez-Quiles *et al*., "On the use of PMUs in power system state estimation," in *Proceedings of*

17th Power System Computation Conference, Stockholm, Sweden, Aug. 2011.
[41] R. Zimmerman, C. Murillo-Saanchez, and R. Thomas, "MATPOWER: steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 12-19, Feb. 2011.
[42] *IEEE Standard for Synchrophasor Measurements for Power Systems*, IEEE Std C37.118.1-2011 (Revision of IEEE Std C37.118-2005), 2011.

Paresh Risbud received the B.E degree in electronics engineering from the University of Mumbai, Mumbai, India, in 2011. He completed the M.S. degree in electrical and computer engineering from the University of Texas at San Antonio, San Antonio, USA, in 2014. Currently, he is working towards the Ph.D. degree in the Department of Electrical and Computer Engineering at the University of Texas at San Antonio, San Antonio, USA, where he is a graduate research assistant. His research interests include statistical signal processing, power system state estimation, and optimization and control of cyber-physical systems.

Nikolaos Gatsis received the Diploma degree in electrical and computer engineering from the University of Patras, Patras, Greece, in 2005 with honors. He completed his graduate studies at the University of Minnesota, Minnesota, USA, where he received the M.Sc. degree in electrical engineering in 2010, and the Ph.D. degree in electrical engineering with minor in mathematics in 2012. He is currently an associate professor with the Department of Electrical and Computer Engineering at the University of Texas at San Antonio, San Antonio, USA. He is a recipient of the NSF CAREER Award. He has co-organized symposia in the area of smart grids in IEEE Global SIP 2015 and 2016. He has also served as a co-guest editor for a special issue of the IEEE Journal on Selected Topics in Signal Processing on Critical Infrastructures. His research interests include optimal and secure operation of smart power grids and other critical infrastructures, including water distribution networks and the global positioning system.

Ahmad Taha received the B.E. and Ph.D. degrees in electrical and computer engineering from the American University of Beirut, Beirut, Lebanon, in 2011 and Purdue University, West Lafayette, USA, in 2015. In Summer 2010, Summer 2014, and Spring 2015, he was a visiting scholar at Massachusetts Institute of Technology (MIT), Cambridge, USA, University of Toronto, Toronto, Canada, and Argonne National Laboratory, USA. Currently, he is an assistant professor with the Department of Electrical and Computer Engineering at The University of Texas, San Antonio, USA. He is an editor of the IEEE Control Systems Society Electronic Letter (E-Letter). He is interested in understanding how complex cyber-physical systems operate, behave, and misbehave. His research interests include optimization, control, and security of cyber-physical systems with applications to power, water, and transportation networks.