Effects of Pseudo-Measurements on GPS Spoofed Power System State Estimation

Mahdi Mahzouni Sani[1], Paresh Risbud[2], Amrusha V. Aryasomyajula[1], and Nikolaos Gatsis[1]

[1]Department of Electrical and Computer Engineering, The University of Texas at San Antonio
[2]IIT Bombay

***Abstract*—Increased visibility of the power grid has been the motivating force for deployment of advanced sensing technologies such as phasor measurement units (PMUs). PMUs are equipped with GPS receivers for time synchronization of the voltage and current measurements. GPS receivers are susceptible to spoofing attacks, which alter the PMU timing information. This work develops an algorithm for power system state estimation and attack angle reconstruction with GPS spoofed PMU measurements aided by pseudo-measurements. Numerical tests performed on the standard IEEE test networks indicate improvement in the state estimation accuracy.**

***Index Terms*—Pseudo-measurements, State Estimation, Phasor Measurement Unit, Global Positioning System**

I. Introduction

There is continuous effort by various stakeholders to modernize the power grid and equip it with technologies that enable an array of advanced Wide Area Monitoring, Protection and Control (WAMPAC) functionalities. Phasor Measurement Units (PMUs) are among such sensing technologies being deployed. PMUs measure the nodal voltages and line currents and utilize the Global Positioning System (GPS) to time-stamp measurements with very high precision. The aforementioned feature enables PMU measurements to be time synchronized across the network. Furthermore, higher sampling rates of PMUs compared to the traditional Supervisory Control and Data Acquisition (SCADA) systems make the grid more visible and assist the network operator in real-time WAMPAC services.

As PMUs generally utilize unencrypted GPS signals to achieve synchronization,they are susceptible to cyber-threats known as GPS spoofing attacks [1]. GPS spoofing entails malicious agents transmitting unauthorized GPS signals that mislead the timing information obtained by the PMUs. Such attacks are also known as Time Synchronization Attacks (TSAs) [2]. In our previous work, [3]–[5] we have developed novel measurement models and static or dynamic state estimation (SE) algorithms for GPS-spoofed PMU-instrumented smart power grids. This work extends our previous efforts to evaluate the effect of available pseudo-measurements on the GPS spoofed power system state estimation.

Several approaches for state estimation under GPS spoofing attacks have been developed in the previous years—see e.g., [6]–[8]—though pseudo-measurements are not readily included. Pseudo-measurements amount to additional information used to increase the redundancy and improve the quality of power system state estimation. In the literature, use of pseudo-measurements to aid the state estimation is seen in the transmission as well as distribution networks. Some examples of pseudo-measurements are surveyed next.

Historical profiles of network data, such as loads, can be used to provide additional information for the state estimation. The survey paper [9] outlines two sets of approaches for including such pseudo-measurements in the distribution system state estimation, namely, probabilistic and statistical approaches on one hand, and learning-based approaches on the other hand. The probabilistic and statistical approaches use temporal/spatial correlation and historic load distribution data to generate the pseudo-measurements—see e.g., [10], [11]. The learning-based approach uses machine learning based modeling for pseudo-measurement generation, e.g., [12], [13].

Furthermore, zero-injection buses—that is, buses with no generation and no load—yield equations based on Kirchhoff's current law (KCL) that constrain the unknown state that is being solved for. In case of transmission networks, representative papers from the classical literature on power system state estimation such as [14]–[17] and a survey paper [18] describe the pseudo-measurements arising from zero-injection buses and the resulting equality constraints. The classical literature is concerned with solving the non-linear power system state estimation problem, because the measurements typically arise from SCADA systems and are nonlinearly related to the unknown network state. Thus, the classical literature focuses on numerical issues arising in the state estimation problem.

It is also worth mentioning that SCADA measurements can be used as pseudo-measurements [19] in the case of PMU based state estimation, where appropriate weights must be assigned to the pseudo-measurements via the SCADA measurement covariance matrix.

This paper contributes to the domain of static power system state estimation affected by GPS spoofing attacks in the presence of pseudo-measurements arising from zero-injection buses. Such pseudo-measurements are the focus of the present

Corresponding author: Nikolaos Gatsis (nikolaos.gatsis@utsa.edu).

This material is based upon work supported by the National Science Foundation under Grants No. ECCS-1719043, CAREER-1847125, ECCS-2115427 as well as the Lutcher Brown Endowed Fellowship at UTSA.

978-1-6654-7902-8/22/$31.00 ©2022 IEEE

2022 IEEE Texas Power and Energy Conference (TPEC) | 978-1-6654-7902-8/22/$31.00 ©2022 IEEE | DOI: 10.1109/TPEC54980.2022.9750738

work because they are *always* present as an extra set of measurements, helping to improve the redundancy and hence the state estimation routine. The resulting pseudo-measurements yield a set of equality constraints that enter the objective function in the form of a weighted quadratic penalty term. The weight can be adjusted to assign relative importance in fitting the model to the PMU measurements versus satisfying the KCL equations resulting from the pseudo-measurements.

Although the PMU measurement model is linear, the GPS spoofing attack renders the overall measurement model non-convex. The developed algorithm jointly solves for the state and spoofing-induced attack angle estimates building on the alternating minimization approach of our previous work [4]. The algorithm developed in this paper is applied on the standard IEEE 14-, 30-, and 118-bus networks and yields improved state and attack angle estimates evaluated by various metrics, compared to previous work in [4].

The structure of this paper is as follows. Section II formulates the PMU measurement and zero-injection bus pseudo-measurement models. Section III develops the algorithm for GPS spoofed state estimation including pseudo-measurements. Numerical tests are detailed in Section IV. Conclusions and future work are provided in Section V.

II. PMU Based State Estimation

This section describes the network and measurement model, with and without TSAs and pseudo-measurements.

A. Network Model and PMU Measurements

Let us consider a network with N_b buses connected with N_l transmission lines. The state vector is the set of nodal voltages in rectangular co-ordinates defined as $\mathbf{v} = [\mathbf{v}_r{}^\top \ \mathbf{v}_i{}^\top]^\top \in \mathbb{R}^{2N_b \times 1}$ where $\mathbf{v}_r$ and $\mathbf{v}_i$ collect the real and imaginary parts $V_{n,r}$ and $V_{n,i}$ of the complex voltages at buses $n = 1, \ldots, N_b$. PMUs are installed at predefined locations in the network [19]. Binary vector $\mathbf{a}$ denotes the presence or absence of a PMU on a given bus such as $\mathcal{N}_{\text{PMU}} = \{i \in \{1, 2, \ldots, N_b\} | a_i = 1\}$. The set of buses connected to bus n is denoted by $\mathcal{N}_n$ and the number of lines connected to bus n is defined as $L_n = |\mathcal{N}_n|$. The PMU installed at a bus measures the voltage phasor at that bus along with the complex currents on the line directly connected to that bus. These PMU measurements are represented by the vector $\mathbf{z}_n \in \mathbb{R}^{2+2L_n}$. Also, define $M_n = 2 + 2L_n$ as the number of distinct real quantities measured by the PMU at bus n. The noiseless measurement vector $\mathbf{z}_n \in \mathbb{R}^{M_n}$ is given as follows:

$$\mathbf{z}_n^{\text{true}} = \begin{bmatrix} V_{n,r} \\ V_{n,i} \\ \{I_{nk,r}\}_{k \in \mathcal{N}_n} \\ \{I_{nk,i}\}_{k \in \mathcal{N}_n} \end{bmatrix} = \begin{bmatrix} |V_n| \cos(\theta_n) \\ |V_n| \sin(\theta_n) \\ \{|I_{nk}| \cos(\theta_{I_{nk}})\}_{k \in \mathcal{N}_n} \\ \{|I_{nk}| \sin(\theta_{I_{nk}})\}_{k \in \mathcal{N}_n} \end{bmatrix} \tag{1}$$

where $I_{nk,r}$ and $I_{nk,i}$ are the real and imaginary parts of the complex current injected into line (n, k). Furthermore, V_n and I_{nk} generically denote the voltage and current phasors at bus n and line (n, k) respectively; and let θ_n and $\theta_{I_{nk}}$ denote the corresponding phasor angles. The noiseless quantities measured at bus $n \in \mathcal{N}_{\text{PMU}}$ comprise the real and imaginary parts of the nodal complex voltage, appended by the real and imaginary parts of the complex currents injected to all lines connected to bus n. Compactly, the measurement vector is given by $\mathbf{z}_n^{\text{true}} = \mathbf{H}_n \mathbf{v}$, where $\mathbf{H}_n \in \mathbb{R}^{M_n \times 2N_b}$ is a regression matrix constructed from the bus admittance matrix [3], [19]. To make this paper self-contained, details about $\mathbf{H}_n$ are provided in Appendix A. Consequently, the noisy version of $\mathbf{z}_n^{\text{true}}$ is denoted as

$$\mathbf{z}_n = \mathbf{z}_n^{\text{true}} + \mathbf{w}_n = \mathbf{H}_n \mathbf{v} + \mathbf{w}_n$$

where $\mathbf{w}_n \sim \mathcal{N}(0, \mathbf{\Sigma}_n)$ represents an additive Gaussian noise vector that is assumed independent across PMUs and has a known positive definite covariance $\mathbf{\Sigma}_n$.

The TSA impacted measurement vector with the phase angle error $\Delta\theta_n$ can be written as follows [2]:

$$\mathbf{z}_n^{\text{atk}} = \begin{bmatrix} |V_n| \cos(\theta_n + \Delta\theta_n) \\ |V_n| \sin(\theta_n + \Delta\theta_n) \\ \{|I_{nk}| \cos(\theta_{I_{nk}} + \Delta\theta_n)\}_{k \in \mathcal{N}_n} \\ \{|I_{nk}| \sin(\theta_{I_{nk}} + \Delta\theta_n)\}_{k \in \mathcal{N}_n} \end{bmatrix} + \mathbf{w}_n \tag{2}$$

Consequently, combining (2) with (1) yields a bilinear relationship which can be formulated as given below [3]:

$$\mathbf{z}_n^{\text{atk}} = \mathbf{\Gamma}_n \mathbf{z}_n^{\text{true}} + \mathbf{w}_n = \mathbf{\Gamma}_n \mathbf{H}_n \mathbf{v} + \mathbf{w}_n \tag{3}$$

where $\mathbf{\Gamma}_n \in \mathbb{R}^{M_n \times M_n}$ is a block diagonal matrix consisting of $1 + L_n$ blocks and each diagonal block is the 2×2 matrix $\left[\begin{smallmatrix} \cos\Delta\theta_n & -\sin\Delta\theta_n \\ \sin\Delta\theta_n & \cos\Delta\theta_n \end{smallmatrix}\right]$. The attacked measurement equation (3) highlights the fact that measurement is bilinear in trigonometric functions of the attack angle and in the state vector.

Section II-B develops matrix models for the pseudo-measurements. A three-bus network is provided as an example.

B. KCL Equations from Pseudo-Measurements

Buses with no load and no power generation provide pseudo-measurements. These buses are also called *zero-injection buses* and comprise the set $\mathcal{N}_{\text{pseudo}}$. Consider for example the 3-bus system depicted in Fig. 1. For every line, there is a from and to bus. In this example, line 1 is from bus 1 to bus 2, line 2 is from bus 1 to bus 3, and line 3 is from bus 2 to bus 3. This nomenclature follows MATPOWER [20]. Let $\mathbf{i}_f = [i_{f_1}, i_{f_2}, i_{f_3}]^\top$ collect the complex currents leaving the *from* buses and let $\mathbf{i}_t = [i_{t_1}, i_{t_2}, i_{t_3}]^\top$ collect the complex currents leaving the *to* buses. Assuming bus 2 is a zero-injection bus, the following KCL equation holds: $i_{t_1} + i_{f_3} = 0$. This is a complex equation, yielding two linear equalities—one for the real and one for the imaginary parts—which can be written in a form $\mathbf{C}_2 \mathbf{v} = \mathbf{0}$, where $\mathbf{v}$ is the state vector and $\mathbf{C}_2$ is an appropriate matrix corresponding to bus 2. Constraints of this form can be added to the SE problem formulation to improve the estimate accuracy. This section gives an example of how to formulate the KCL equations using network matrices.

Supposing that m is a zero injection bus, a binary matrix $\mathbf{S}_m$ is defined to select the line currents leaving that bus. The corresponding dimensions are $L_m \times 2N_l$, where L_m is the

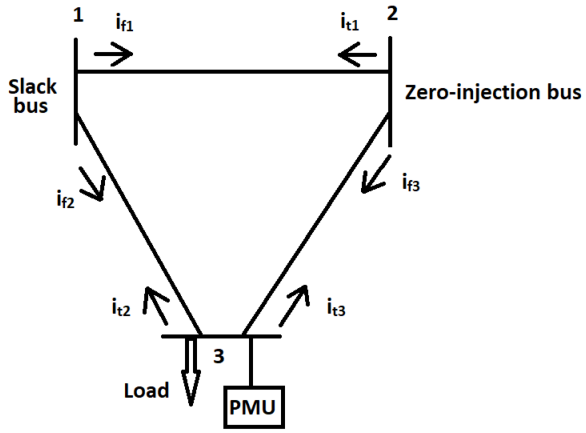


Fig. 1: An example of 3-bus system

number of lines connected to bus m. The $2N_l \times 1$ complex network flow vector is defined as follows:

$$\mathbf{i}_{\text{fl}} = \begin{bmatrix} \mathbf{i}_f \\ \mathbf{i}_t \end{bmatrix} = \begin{bmatrix} i_{f_1} & i_{f_2} & i_{f_3} & i_{t_1} & i_{t_2} & i_{t_3} \end{bmatrix}^\top \tag{4}$$

Then, the vector of currents leaving bus 2 is given as follows:

$$\mathbf{S}_2 \mathbf{i}_{\text{fl}} = \begin{bmatrix} i_{f_3} & i_{t_1} \end{bmatrix}^\top, \text{where } \mathbf{S}_2 = \begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix} \tag{5}$$

For each zero-objection bus, two KCL equations are derived corresponding to the real and imaginary parts of the currents leaving the bus:

$$\mathbf{1}^\top \mathbf{S}_2 \mathbf{i}_{fl,r} = 0 \tag{6}$$

$$\mathbf{1}^\top \mathbf{S}_2 \mathbf{i}_{fl,i} = 0 \tag{7}$$

where $\mathbf{1}$ denotes vector of all ones. Section II-C describes how to write the KCL equations in terms of the state vector.

C. Pseudo-Measurement Linear Constraints

In this section, the KCL equations for all zero-injection buses in the network are cast in the form $\mathbf{C}\mathbf{v} = \mathbf{0}$. Specifically, the complex $2N_l \times N_b$ line-to-bus admittance matrix is $\mathbf{Y}_{\text{fl}} = \begin{bmatrix} \mathbf{Y}_f^\top & \mathbf{Y}_t^\top \end{bmatrix}^\top$, where $\mathbf{Y}_f$ and $\mathbf{Y}_t$ are the from and to branch admittance matrices that can be easily extracted from MATPOWER. The $N_b \times 1$ complex state vector is denoted by $\tilde{\mathbf{v}} = \mathbf{v}_r + j\mathbf{v}_i$. The complex network flow vector $\mathbf{i}_{\text{fl}}$ is given as follows:

$$\mathbf{i}_{\text{fl}} = \begin{bmatrix} \mathbf{i}_f \\ \mathbf{i}_t \end{bmatrix} = \begin{bmatrix} \mathbf{Y}_f \\ \mathbf{Y}_t \end{bmatrix} \tilde{\mathbf{v}} \tag{8}$$

Separating real and imaginary parts of $\mathbf{i}_{\text{fl}}$, it follows that

$$\begin{bmatrix} \mathbf{i}_{\text{fl},r} \\ \mathbf{i}_{\text{fl},i} \end{bmatrix} = \begin{bmatrix} \text{Re}(\mathbf{Y}_{\text{fl}}) & -\text{Im}(\mathbf{Y}_{\text{fl}}) \\ \text{Im}(\mathbf{Y}_{\text{fl}}) & \text{Re}(\mathbf{Y}_{\text{fl}}) \end{bmatrix} \begin{bmatrix} \mathbf{v}_r \\ \mathbf{v}_i \end{bmatrix} \tag{9}$$

For zero-injection bus m, the vectors of complex, real and imaginary parts of currents leaving bus m are respectively given as $\mathbf{S}_m \mathbf{i}_{\text{fl}}$, $\mathbf{S}_m \mathbf{i}_{\text{fl},r}$, and $\mathbf{S}_m \mathbf{i}_{\text{fl},i}$, where $\mathbf{S}_m$ is defined in Section II-B. The two equations stemming from KCL for zero-injection buses are given as follows:

$$\mathbf{1}^\top \mathbf{S}_m \mathbf{i}_{\text{fl},r} = 0 \tag{10}$$

$$\mathbf{1}^\top \mathbf{S}_m \mathbf{i}_{\text{fl},i} = 0 \tag{11}$$

These can be organized in matrix form

$$\begin{bmatrix} \mathbf{1}^\top \mathbf{S}_m & \mathbf{0} \\ \mathbf{0} & \mathbf{1}^\top \mathbf{S}_m \end{bmatrix} \begin{bmatrix} \mathbf{i}_{\text{fl},r} \\ \mathbf{i}_{\text{fl},i} \end{bmatrix} = 0 \tag{12}$$

and invoking (9)

$$\begin{bmatrix} \mathbf{1}^\top \mathbf{S}_m \text{Re}(\mathbf{Y}_{\text{fl}}) & -\mathbf{1}^\top \mathbf{S}_m \text{Im}(\mathbf{Y}_{\text{fl}}) \\ \mathbf{1}^\top \mathbf{S}_m \text{Im}(\mathbf{Y}_{\text{fl}}) & \mathbf{1}^\top \mathbf{S}_m \text{Re}(\mathbf{Y}_{\text{fl}}) \end{bmatrix} \begin{bmatrix} \mathbf{v}_r \\ \mathbf{v}_i \end{bmatrix} = 0 \tag{13}$$

Eq. (13) can be compactly written as follows

$$\mathbf{C}_m \mathbf{v} = 0 \tag{14}$$

Upon concatenating all $\mathbf{C}_m$ matrices for the zero-injection buses in the network, the matrix $\mathbf{C} \in \mathbb{R}^{2|\mathcal{N}_{\text{pseudo}}| \times 2N_b}$ is formulated, yielding the set of KCL equations $\mathbf{C}\mathbf{v} = \mathbf{0}$. Section III develops the GPS spoofed state estimation including pseudo-measurements.

III. GPS Spoofed State Estimation including Pseudo-Measurements

This section formulates and solves the GPS spoofed SE problem including pseudo-measurements. The aim is to solve for a state estimate and attack angle estimates that fit the model in (3) to the PMU measurements $\mathbf{z}_n$ as well as approximately satisfy the pseudo-measurement KCL equations $\mathbf{C}\mathbf{v} \approx \mathbf{0}$.

Introduce first the auxiliary variables $\gamma_{n,1} = \cos\Delta\theta_n$ and $\gamma_{n,2} = \sin\Delta\theta_n$. The model fit to the measurements is captured by the least squares residual

$$\sum_{n=1}^{N_b} a_n (\mathbf{z}_n^{\text{atk}} - \mathbf{\Gamma}_n \mathbf{H}_n \mathbf{v})^\top \mathbf{\Sigma}_n^{-1} (\mathbf{z}_n^{\text{atk}} - \mathbf{\Gamma}_n \mathbf{H}_n \mathbf{v}) = (\mathbf{z} - \mathbf{\Gamma}\mathbf{H}\mathbf{v})^\top \mathbf{\Sigma}^{-1} (\mathbf{z} - \mathbf{\Gamma}\mathbf{H}\mathbf{v}) \tag{15}$$

where $\mathbf{\Gamma}_n$ is a block diagonal matrix that includes 2×2 blocks $\begin{bmatrix} \gamma_{n,1} & -\gamma_{n,2} \\ \gamma_{n,2} & \gamma_{n,1} \end{bmatrix}$ on the diagonal; $\mathbf{z} \in \mathbb{R}^M$ is formulated by concatenating vectors $\mathbf{z}_n$ for all PMUs and M is the total number of measurements defined as $M = \sum_{n \in \mathcal{N}_{\text{PMU}}} M_n = \sum_{n \in \mathcal{N}_{\text{PMU}}} (2 + 2L_n)$; $\mathbf{H}$ is formulated by concatenating matrices $\mathbf{H}_n$ for all PMUs ($n \in \mathcal{N}_{\text{PMU}}$); $\mathbf{\Gamma}$ is an $M \times M$ block diagonal matrix with diagonal blocks $\mathbf{\Gamma}_n$ for all PMUs ($n \in \mathcal{N}_{\text{PMU}}$); and $\mathbf{\Sigma}^{-1}$ denotes an $M \times M$ block diagonal matrix with diagonal blocks $\mathbf{\Sigma}_n^{-1}$ for all PMUs ($n \in \mathcal{N}_{\text{PMU}}$).

The SE problem is thus formulated as a bi-criterion minimization as follows

$$\underset{\mathbf{v}, \{\boldsymbol{\gamma}_n\}_{n \in \mathcal{N}_{\text{PMU}}}}{\text{minimize}} \quad \underbrace{(\mathbf{z} - \mathbf{\Gamma}\mathbf{H}\mathbf{v})^\top \mathbf{\Sigma}^{-1} (\mathbf{z} - \mathbf{\Gamma}\mathbf{H}\mathbf{v})}_{F_1} + \mu \underbrace{||\mathbf{C}\mathbf{v}||_2^2}_{F_2} \tag{16a}$$

$$\text{subject to} \quad \boldsymbol{\gamma}_n^\top \boldsymbol{\gamma}_n = 1, \quad n \in \mathcal{N}_{\text{PMU}}, \tag{16b}$$

The first objective function represents the residuals from fitting the system model to the PMU measurements, while the second

objective ensures that the KCL equations corresponding to zero-injection buses are approximately satisfied. It is worth mentioning that instead of the attack angles $\Delta\theta_n$, the vectors $\boldsymbol{\gamma}_n = [\gamma_{n,1}, \gamma_{n,2}]^\top$ are optimization variables. The notations $\boldsymbol{\gamma}_n$ and $\boldsymbol{\Gamma}_n$ are used interchangeably, as they both collect the unknowns $\gamma_{n,1}$ and $\gamma_{n,2}$. Constraint (16b) ensures that the attack angles $\Delta\theta_n$ can be uniquely recovered from $\gamma_{n,1}$ and $\gamma_{n,2}$. The aforementioned transformation was first introduced in [4].

The second objective is introduced with a weight $\mu > 0$, which is a parameter that can be set by the system operator solving the SE. The present approach gives the freedom to place relative significance on minimizing F_1 or F_2. Specifically, if $\mu = 0$, then the pseudo-measurements are entirely ignored, and the SE only relies on the PMU measurements. As μ becomes larger, emphasis is placed in producing a state estimate $\mathbf{v}$ that also approximately satisfies the pseudo-measurement KCL equations, in addition to minimizing the PMU measurement residuals.

Problem (16) is a nonconvex, but it can be approximately solved by an alternating minimization algorithm, building on our previous work [4]. Specifically, one set of optimization variables (e.g., $\boldsymbol{\gamma}_n$ for $n \in \mathcal{N}_{\text{PMU}}$) is kept fixed and (16) is minimized with respect to the other variable (in this example, $\mathbf{v}$). Then, the latter variable ($\mathbf{v}$) is kept fixed, and the minimization is performed with respect to $\boldsymbol{\gamma}_n$ for $n \in \mathcal{N}_{\text{PMU}}$. The process is repeated and it guarantees that the resulting sequence of objective function values (16a) is non-increasing. The process is terminated when the change in the objective value is less than a prescribed tolerance. The minimizations with respect to each variable are described next.

A. Minimization with Respect to the State

When the variables $\boldsymbol{\gamma}_n$ for $n \in \mathcal{N}_{\text{PMU}}$ are kept fixed, the optimization in (16a) is an unconstrained quadratic minimization written as

$$\underset{\mathbf{v}}{\text{minimize}} \quad (\tilde{\mathbf{z}} - \mathbf{B}\mathbf{v})^\top \mathbf{Q}^{-1} (\tilde{\mathbf{z}} - \mathbf{B}\mathbf{v}) \tag{17}$$

where $\tilde{\boldsymbol{z}} = [\boldsymbol{z}^\top \mathbf{0}^\top]^\top$, $\mathbf{0} \in \mathbb{R}^{2|\mathcal{N}_{\text{pseudo}}|}$, $\mathbf{Q} = \text{blkdiag}(\tilde{\boldsymbol{\Sigma}}^{-1}, \mu\mathbf{I})$ (following MATLAB notation for a block diagonal matrix), and $\mathbf{B} = \begin{bmatrix} \boldsymbol{\Gamma}\mathbf{H} \\ -\mathbf{C} \end{bmatrix}$.

The objective function (17) can be written as a standard quadratic as follows:

$$\underset{\mathbf{v}}{\text{minimize}} \quad \tfrac{1}{2}\mathbf{v}^\top \mathbf{P}\mathbf{v} + \mathbf{q}^\top \mathbf{v} + r \tag{18}$$

where

$$\begin{aligned} \mathbf{P} &= 2\mathbf{B}^\top \mathbf{Q}^{-1} \mathbf{B} \\ \mathbf{q} &= -2\mathbf{B}^\top \mathbf{Q}^{-1} \tilde{\mathbf{z}} \\ r &= \tilde{\mathbf{z}}^\top \boldsymbol{Q}^{-1} \tilde{\mathbf{z}} \end{aligned} \tag{19}$$

The estimated state vector $\hat{\mathbf{v}}$ can be obtained as a solution to the following linear system of equations:

$$\mathbf{P}\hat{\mathbf{v}} = -\mathbf{q} \tag{20}$$

Algorithm 1: State Estimation & Attack Reconstruction with Pseudo-Measurements

Result: State Estimate $\hat{\mathbf{v}}$ and Attack Angle Reconstruction $\widehat{\Delta\boldsymbol{\theta}} = \{\Delta\theta_n\}_{n \in \mathcal{N}_{\text{PMU}}}$
Input: $\mathbf{z}_n^{\text{atk}}$
Initialization: Solve (20) for $\hat{\mathbf{v}}$ upon setting $\boldsymbol{\gamma}_n = [1\ 0]^\top$
repeat
  for $n \in \mathcal{N}_{PMU}$ **do**
    Find the corresponding $\boldsymbol{\gamma}_n$ via eq. (24)
  end
  Update $\hat{\mathbf{v}}$ by solving (20)
until *convergence or maximum iterations reached*;

B. Minimization with Respect to Attack Angle

The minimization with respect to the attack angle for the problem in (16) takes the following form:

$$\begin{aligned} &\underset{\boldsymbol{\gamma}_n}{\text{minimize}} \ \left(\mathbf{z}_n^{\text{atk}} - \mathbf{A}_n\boldsymbol{\gamma}_n\right)^\top \Sigma_n^{-1} \left(\mathbf{z}_n^{\text{atk}} - \mathbf{A}_n\boldsymbol{\gamma}_n\right) \\ &\text{subject to } \boldsymbol{\gamma}_n^\top \boldsymbol{\gamma}_n = 1 \end{aligned} \tag{21}$$

where $\mathbf{h}_{n,i}^\top$ is the i-th row of $\mathbf{H}_n$ $(i = 1, 2, \ldots, M_n)$ and $\mathbf{A}_n \in \mathbb{R}^{M_n \times 2}$ is defined as (note that $\mathbf{v}$ is fixed in this step)

$$\mathbf{A}_n = \begin{bmatrix} \mathbf{h}_{n,1}^\top \mathbf{v} & -\mathbf{h}_{n,2}^\top \mathbf{v} \\ \mathbf{h}_{n,2}^\top \mathbf{v} & \mathbf{h}_{n,1}^\top \mathbf{v} \\ \vdots & \vdots \\ \mathbf{h}_{n,M_n-1}^\top \mathbf{v} & -\mathbf{h}_{n,M_n} \mathbf{v} \\ \mathbf{h}_{n,M_n}{}^\top \mathbf{v} & \mathbf{h}_{n,M_n-1}^\top \mathbf{v} \end{bmatrix} \tag{22}$$

Suppose that the covariance Σ_n is a diagonal matrix with entries $\sigma_{n,i}^2, i = 1, \ldots, M_n$, where

$$\sigma_{n,1} = \sigma_{n,2}, \sigma_{n,3} = \sigma_{n,4}, \ldots, \sigma_{n,M_n-1} = \sigma_{n,M_n} \tag{23}$$

In this case, the closed form solution for attack angle can be calculated as

$$\boldsymbol{\gamma}_n = \left(1/\left\|\mathbf{A}_n^\top \boldsymbol{\Sigma}_n^{-1} \mathbf{z}_n^{\text{atk}}\right\|_2\right) \mathbf{A}_n^\top \boldsymbol{\Sigma}_n^{-1} \mathbf{z}_n^{\text{atk}}. \tag{24}$$

The previous development is based on Lagrangian duality theory thoroughly analyzed in [4], which also deals with the case of nondiagonal covariance $\boldsymbol{\Sigma}_n$. The aim of the present section is to provide a self-contained exposition of the computational steps involved in providing the $\boldsymbol{\gamma}_n$-update. Algorithm 1 summarizes the step to solve the SE problem.

IV. Numerical Tests

The numerical tests are performed on the IEEE 14-, 30-, and 118-bus networks named as Case-14, Case-30, and Case-118, respectively. Table I depicts the PMU locations in the standard IEEE test networks, obtained with the algorithm developed in [19]. The performance of the proposed algorithm is compared to the algorithm in [4] using different values of μ to evaluate the effect of including pseudo-measurements in state and attack angle estimation. Four performance criteria are used for comparison in this paper. The first is the relative state

TABLE I: Optimal PMU location (a) for IEEE test networks.

Test Case	$\lvert\mathcal{N}_{\text{PMU}}\rvert$	Bus number
IEEE 14	6	2,4,6,7,10,14
IEEE 30	13	2,3,6,10,11,12,15,20,23,25,27,28,29
IEEE 118	94	1–5,7–19,21–25,27–36,40,43,44,46,47,48, 50,51,52,53,55–60,64,65,66,67,6870,71,73,75,76, 77,80–83,85–90,92,94–104,106–111,113–118

TABLE II: Performance of algorithms on Case-14 under attack on two PMUs.

Method	**RSEE**	**RAAE**	**NAAE**	**SEN**
Algorithm in [4]	0.0165	0.0473	0.4268	0.0651
$\mu = 0$	0.0165	0.0473	0.4268	0.0651
$\mu = 1$	0.0165	0.0473	0.4268	0.0651
$\mu = 10$	0.0165	0.0473	0.4266	0.0650
$\mu = 100$	0.0165	0.0471	0.4252	0.0648
$\mu = 1000$	0.0162	0.0463	0.4182	0.0636
$\mu = 10000$	0.0159	0.0457	0.4122	0.0625

TABLE III: Performance of algorithms on Case-30 under attack on two PMUs.

Method	**RSEE**	**RAAE**	**NAAE**	**SEN**
Algorithm in [4]	0.0581	0.226	0.944	0.312
$\mu = 0$	0.0581	0.226	0.944	0.312
$\mu = 1$	0.0580	0.226	0.942	0.312
$\mu = 10$	0.0573	0.223	0.931	0.308
$\mu = 100$	0.0524	0.205	0.854	0.282
$\mu = 1000$	0.0436	0.172	0.716	0.235
$\mu = 10000$	0.0406	0.161	0.669	0.218

estimation error (RSEE), which is defined as $\frac{||\hat{\mathbf{v}}-\mathbf{v}||_2}{||\mathbf{v}||_2}$, where $\hat{\mathbf{v}}$ is the estimated state vector and $\mathbf{v}$ is the true state. The second is the relative attack angle error (RAAE), which is defined as $\frac{||\widehat{\boldsymbol{\Delta\theta}}-\boldsymbol{\Delta\theta}||_2}{||\boldsymbol{\Delta\theta}||_2}$, where $\boldsymbol{\Delta\theta}$ collects the true attack angles for all PMU buses. The third is the normalized attack angle error (NAAE), which is defined as $\frac{||\widehat{\boldsymbol{\Delta\theta}}-\boldsymbol{\Delta\theta}||_2}{|\mathcal{N}_{\text{PMU}}|}$. The fourth is state error norm (SEN), which is given by $||\hat{\mathbf{v}}-\mathbf{v}||_2$.

The Gaussian noise vector is random in this simulation thus the results are averaged over 100 realizations. The noise standard deviations of 0.01 for voltages and 0.02 for line currents are used for Case-14 and Case-30; and respectively 0.1 and 0.2 for Case-118.

Tables II and III denote the performance of algorithms on Case-14 and Case-30 under attack on two PMUs. The attack angles for Case-14 are $\Delta\theta_6 = 30^\circ$ and $\Delta\theta_{14} = 45^\circ$, and for Case-30 they are $\Delta\theta_6 = 30^\circ$ and $\Delta\theta_{12} = 45^\circ$.

TABLE IV: Performance of algorithms on Case-118 under attack on two PMUs.

Method	**RSEE**	**RAAE**	**NAAE**	**SEN**
Algorithm in [4]	0.0396	0.401	0.590	0.424
$\mu = 0$	0.0396	0.401	0.590	0.424
$\mu = 1$	0.0388	0.400	0.588	0.416
$\mu = 10$	0.0378	0.398	0.585	0.405
$\mu = 100$	0.0374	0.397	0.584	0.400
$\mu = 1000$	0.0373	0.397	0.584	0.400
$\mu = 10000$	0.0373	0.397	0.584	0.400

TABLE V: Performance of algorithms on Case-118 under attack on 20% of PMUs.

Method	**RSEE**	**RAAE**	**NAAE**	**SEN**
Algorithm in [4]	0.0380	0.361	0.579	0.407
$\mu = 100$	0.0364	0.358	0.575	0.390

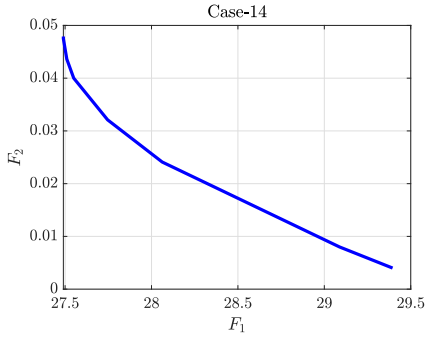
Table IV reports the estimation performance under attack on two PMUs in Case-118. The attack angles are $\Delta\theta_{36} = 30^\circ$ and $\Delta\theta_{50} = 45^\circ$ for Case-118. The algorithm in [4] has identical perfomance with the algortihm in this paper when $\mu = 0$. The overall trend is that all metrics improve when μ increases, that is, when sufficient weight is placed on the pseudo-measurements. This implies that not only the state estimation accuracy is improved, but also the attack angle is more accurately reconstructed.

Furthermore, attacks on 20% of PMUs in Case-118 are considered. Along with the random noise, the location of the attack is randomized using the MATLAB command `randperm`, and the attack angle is also randomly chosen from a uniform distribution in the interval $[-60^\circ, 60^\circ]$. The results in this scenario are presented in Table V, where one representative value of mu is chosen. It is observed again that the performance of SE including pseudo-measurements is better than that of the algorithm in [4].

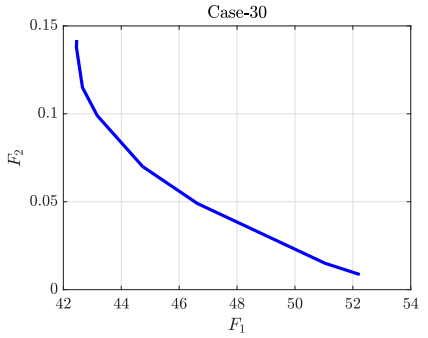
The resulting Pareto frontiers for the various cases are depicted in Fig. 2. These are obtained by varying μ and for one noise realization. Such graphs reveal the tradeoff between the two objectives and can assist the network operator with the selection of μ.

V. Conclusions and Future Work

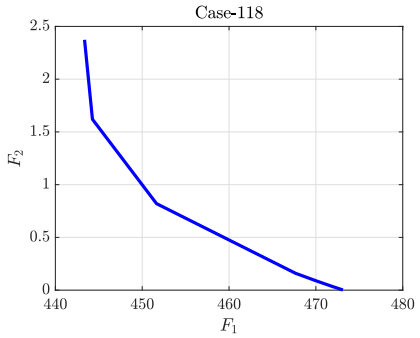
This work develops a state estimation algorithm aided by pseudo-measurements for PMU-instrumented power grids vulnerable to GPS spoofing attacks. The pseudo-measurements come in the form of KCL equations for zero-injection buses, and the always exist in the network due its topology. Future work includes accounting for pseudo-measurements in a dynamic state estimation framework under GPS spoofing attacks,



(a)



(b)



(c)

Fig. 2: The Pareto frontier for (a) Case-14; (b) Case-30; and (c) Case-118. The top left point corresponds to $\mu = 0$ and the bottom right point corresponds to $\mu = 10000$.

as well as considering the improvements from other types of pseudo-measurements, such as historical load data or SCADA measurements.

REFERENCES

[1] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela, and A. D. Dominguez-Garcia, "Spoofing GPS receiver clock offset of phasor measurement units," *IEEE Trans. Power Syst.*, vol. 28, pp. 3253–3262, Aug. 2013.

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

[3] P. Risbud, N. Gatsis, and A. Taha, "Assessing power system state estimation accuracy with GPS-spoofed PMU measurements," in *Proc. 7th IEEE Conf. Innovative Smart Grid Technologies*, Minneapoils, MN, Sept. 2016, pp. 1–5.

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

[5] P. Risbud, N. Gatsis, and A. Taha, "Multi-period power system state estimation with PMUs under GPS spoofing attacks," *J. Mod. Power Syst. Cle.*, vol. 8, no. 4, pp. 597–606, 2020.

[6] X. Fan, L. Du, and D. Duan, "Synchrophasor data correction under GPS spoofing attack: A state estimation-based approach," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4538–4546, Sep. 2018.

[7] S. D. Silva, T. Hagan, J. Kim, and E. C. Sanchez, "Sparse error correction for PMU data under GPS spoofing attacks," in *Proc. IEEE Global Conf. Signal and Information Processing*, Anaheim, CA, Nov. 2018, pp. 902–906.

[8] P. Pradhan, K. Nagananda, P. Venkitasubramaniam, S. Kishore, and R. S. Blum, "GPS spoofing attack characterization and detection in smart grids," in *Proc. IEEE Conf. Communications and Network Security*, Oct. 2016, pp. 391–395.

[9] K. Dehghanpour, Z. Wang, J. Wang, Y. Yuan, and F. Bu, "A survey on state estimation techniques and challenges in smart distribution systems," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2312–2322, 2019.

[10] A. Ghosh, D. Lubkeman, M. Downey, and R. Jones, "Distribution circuit state estimation using a probabilistic approach," *IEEE Trans. Power Syst.*, vol. 12, no. 1, pp. 45–51, 1997.

[11] R. Singh, B. C. Pal, and R. A. Jabr, "Statistical representation of distribution system loads using gaussian mixture model," *IEEE Trans. Power Syst.*, vol. 25, no. 1, pp. 29–37, 2010.

[12] D. Gerbec, S. Gasperic, I. Smon, and F. Gubina, "Allocation of the load profiles to consumers using probabilistic neural networks," *IEEE Trans. Power Syst.*, vol. 20, no. 2, pp. 548–555, 2005.

[13] E. Manitsas, R. Singh, B. C. Pal, and G. Strbac, "Distribution system state estimation using an artificial neural network approach for pseudo measurement modeling," *IEEE Trans. Power Syst.*, vol. 27, no. 4, pp. 1888–1896, 2012.

[14] F. Aschmoneit, N. Peterson, and E. Adrian, "State estimation with equality constraints," in *Tenth PICA Conference Proceedings*, 1977, pp. 427–430.

[15] A. S. Costa, S. Seleme, and R. Salgado, "Equality constraints in power system state estimation via orthogonal row-processing techniques," *IFAC Proceedings Volumes*, vol. 18, no. 7, pp. 43–49, 1985, iFAC Symposium on Planning and Operation of Electric Energy Systems., Rio de Janeiro, Brazil, 22-25 July.

[16] A. Monticelli and A. Garcia, "Modeling zero impedance branches in power system state estimation," *IEEE Trans. Power Syst.*, vol. 6, no. 4, pp. 1561–1570, 1991.

[17] G. Korres, "A new method for treatment of equality constraints in power system state estimation."

[18] A. Monticelli, "Electric power system state estimation," *Proc. IEEE*, vol. 88, no. 2, pp. 262–282, Feb. 2000.

[19] V. Kekatos, G. Giannakis, and B. Wollenberg, "Optimal placement of phasor measurement units via convex relaxation," *IEEE Trans. Power Syst.*, vol. 27, no. 3, pp. 1521–1530, Aug. 2012.

[20] R. Zimmerman, C. Murillo-Saánchez, and R. Thomas, "MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, Feb. 2011.

APPENDIX A
CONSTRUCTION OF $\mathbf{H}_n$ MATRIX

The construction of $\mathbf{H}_n$ matrix is based on the line-to-bus admittance matrix $\mathbf{Y}_{\text{fl}}$ which is introduced in Section II-C. The vector of complex currents injected to the lines is i_{fl} with the entries of $I_{nk,r} + jI_{nk,i}$. The real and imaginary parts of i_{fl} care given by (9). Comparing the measurement $\mathbf{z}_n^{\text{true}}$ in (1) and the i_{fl} in (9), the $\mathbf{H}_n$ can be written as

$$\mathbf{H}_n = \begin{bmatrix} \mathbf{e}_n^T & 0^T \\ 0^T & \mathbf{e}_n^T \\ \mathbf{S}_n \operatorname{Re}(\mathbf{Y}_{\text{fl}}) & -\mathbf{S}_n \operatorname{Im}(\mathbf{Y}_{\text{fl}}) \\ \mathbf{S}_n \operatorname{Im}(\mathbf{Y}_{\text{fl}}) & \mathbf{S}_n \operatorname{Re}(\mathbf{Y}_{\text{fl}}) \end{bmatrix} \in \mathbb{R}^{M_n \times 2N_b} \quad (25)$$

where $\mathbf{S}_n \in \mathbb{R}^{L_n \times 2N_l}$ is a binary matrix selecting the rows of $\mathbf{Y}_{\text{fl}}$ leaving from bus n, and $\mathbf{e}_n \in \mathbb{R}^{N_b}$ is a vector with 1 in its n-th entry and zero otherwise.