This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2662688, IEEE Transactions on Smart Grid

Synchrophasor Data Correction under GPS Spoofing Attack: A State Estimation Based Approach

Xiaoyuan Fan[1], *Member, IEEE*, Liang Du[2], *Member, IEEE*, and Dongliang Duan[3], *Member, IEEE*

***Abstract*—GPS spoofing attack (GSA) has been shown to be one of the most imminent threats to almost all cyber-physical systems incorporated with the civilian GPS signal. Specifically, for our current agenda of the modernization of the power grid, this may greatly jeopardize the benefits provided by the pervasively installed phasor measurement units (PMU). In this paper, we consider the case where synchrophasor data from PMUs are compromised due to the presence of a single GSA, and show that it can be corrected by signal processing techniques. In particular, we introduce a statistical model for synchrophasor-based power system state estimation (SE), and then derive the spoofing-matched algorithms for synchrophasor data correction against GPS spoofing attack. Different testing scenarios in IEEE 14-, 30-, 57-, 118-bus systems are simulated to show the proposed algorithms' performance on GSA detection and state estimation. Numerical results demonstrate that our proposed algorithms can consistently locate and correct the spoofed synchrophasor data with good accuracy as long as the system observability is satisfied. The accuracy of state estimation is significantly improved compared with the traditional weighted least square method and approaches the performance under the Genie-aided method.**

NOMENCLATURE

GSA	GPS Spoofing Attack
N	Total number of Buses
p	Total number of PMUs
k	Index of PMU, or Location of GSA
θ_{spf}	Phase shift introduced by GSA
V_a	Voltage phasor at bus a
I_{ab}	Current phasor from bus a to bus b
σ^2	Variance of the measurement noise
$\boldsymbol{I}$	Identity Matrix
$\boldsymbol{m}$	PMU measurement vector
$\boldsymbol{A}$	Transition Matrix
$\boldsymbol{G}$	GSA Matrix
$\boldsymbol{s}$	System State Vector
$\boldsymbol{e}$	Measurement Error Vector
$\boldsymbol{C}_e$	Covariance Matrix of $\boldsymbol{e}$
$\boldsymbol{Y}$	Residual Sensitivity Matrix
$\mathcal{CN}(\boldsymbol{\mu}, \boldsymbol{C}_e)$	Complex multi-variate Gaussian distribution with mean $\boldsymbol{\mu}$ and covariance matrix $\boldsymbol{C}_e$

This work was in part supported by the Department of Energy under grants DE-OE0000657 and DE-SC0012671.

[1]Electricity Infrastructure, Pacific Northwest National Laboratory, Richland, WA 99354. Email: xiaoyuan.fan@pnnl.gov.

[2]Pressure Pumping and Chemistry Product Group, Schlumberger, Sugar Land, TX 77478. Email: ldu3@slb.com.

[3]Department of Electrical and Computer Engineering, University of Wyoming, Laramie, WY 82071. Email: dduan@uwyo.edu.

I. INTRODUCTION

As one of the most important functions performed in the grid control center, power system state estimation (SE) provides static system state estimates. Traditional SE is done by collecting power measurements generated by current and voltage transformers, which may include real and reactive power flow, voltage magnitude, line current magnitude, and turns ratio of transformers. These measurements are usually collected asynchronously with a communication rate of one sample per 1-4 s [1]. Increasingly pervasive installation of the phasor measurement unit (PMU) in the last decade has dramatically changed the landscape of power grid monitoring and control [1], [2], [3]. To date, there are about 2,000 PMUs installed at key locations of North American power grid, such as major transmission inter-connections, key generation plants, substations, and major load centers [4], [5]. Wide deployment of PMUs can provide the so-termed synchrophasor measurements at a reporting rate of 30 to 120 samples per second, time-stamped using the global positioning system (GPS) signals to capture the grid dynamics, which is much faster than the legacy supervisory control and data acquisition (SCADA) measurements at a rate of a sample every 1 to 4 seconds [6]. Therefore, a new, better, accurate, and faster procedure for SE will be enabled by incorporating GPS-synchronized PMU measurements [7].

One fundamental feature of synchrophasor data is the grid-wide synchronization. PMU measurements are sampled synchronously at selected locations throughout the entire grid based on a Coordinated Universal Time (UTC). Therefore, a grid-wide snapshot with high accuracy and fine resolution can be obtained by combining the highly synchronized measurements across the entire system. Currently, there are many timing protocols available and their accuracy and coverage vary [8].

Considering the huge geographical span of power grid, GPS signal is suggested as the best choice [9] due to its high accuracy and wide accessability. More specifically, GPS-based synchronization can provide the accuracy better than $1\,\mu s$ in time tagging over a huge area [10]. With such a good accuracy in synchronization, one can simply treat all the phasor measurements as perfectly synchronized and model the measurement error caused by the less-than-$1\mu s$ synchronization offsets as part of the small random additive noise. However, it is no longer true when the GPS signal received by PMUs is compromised by intentional attacks, which usually introduce significant synchronization offsets [11], [12]. The loss of accuracy of GPS synchronization signal directly

affects the reliability of the synchrophasor data provided by PMUs, which further impacts all the high-level applications supported by these data in the wide-area monitoring systems (WAMS). This brings new challenges to the system operations and protection, especially with the increasing installations of PMUs.

In general, synchrophasor data generated by PMUs are subject to more different types of attacks due to their heavy reliance on cyber infrastructure, compared with the traditional power measuring instruments which have limited alteration capability. Network connection and GPS synchronization are two major potential targets of the adversary [12]. As PMUs may be connected through open network interfaces and lack tamper-resistance hardware, data received by the control center must be verified before utilized by further applications. More importantly, it is well known that the GPS signal received by PMU is the civilian GPS signal [1], which is publicly-known and readily predictable. This makes GPS-based time-stamp synchronization more vulnerable to GPS spoofing attack (GSA), which hijacks the PMU by faking the GPS signal and compromises the reliability of all the synchrophasor data from this PMU. GSA has been declared as an imminent threat by the U.S. Department of Transportation in 2001 [13] and by the North American Electric Reliability Corporation in 2012 [14]. Furthermore, recent studies have shown that the spoofer can successfully modify the timestamp of PMUs' measurements and negates their effectiveness by forging a matched version of the signal [8], [15], [16], [17]. Northrop Grumman Information Systems and the University of Texas Radio Navigation Laboratory also jointly conducted a real-world field test to evaluate the effects that spoofed GPS timing signals can have on synchrophasor data from PMUs [18]. When the GPS signal is spoofed, the corresponding synchrophasor data becomes unreliable and thus must be fixed by either removal or correction after being detected. Otherwise, the state estimate based on the spoofed data would be wrong and misleading and might initiate unnecessary and possibly destabilizing remedial control actions from the control center. For example, the spoofer could cause control schemes in a currently operational system at Mexico to trip a generator automatically, which could lead to a cascaded failure or even system collapse throughout the grid with high possibility [18].

Motivated by the data reliability requirements originated from PMUs in current power grid, in this paper, we first study the potential impacts of GPS spoofing attacks and then propose detection and correction algorithms to fix the spoofed synchrophasor data. Numerical simulations are implemented to demonstrate that while GPS spoofing attack can greatly deteriorate the performance of SE, our algorithm could provide a reliable correction on the spoofed synchrophasor data with high precision and hence improve the accuracy of SE.

Literature Review: Existing related research works in the literature can be classified into two categories in general: the navigation community mainly focuses on addressing the timing issues of GPS-synchronized PMUs [19], [20], while the power society pays more attention on neutralizing the bad effects introduced by those erroneous measurements [21]. In [19], three different types of GSA are described and the proposed countermeasures rely on multiple networked GPS receivers to guarantee the security of one PMU. The configuration schemes of these countermeasures have relatively high complexity, and the cost-effectiveness and the robustness of those countermeasures are yet to be tested and reported. The authors of [20] also confirm that the spatial-processing-based anti-spoofing techniques relying on multiple receiver channels/antennas are more effective for spoofing mitigation, but its applicability in practice, especially for power systems is yet to be verified. In [21], the authors aim to compensate the imperfect GPS synchronization by considering small phase mismatch with Gaussian distribution, which enables several key approximations and therefore, makes the close-form solution tractable.

Comparing with the existing research, our main contributions are given as follows. First of all, our proposed method does not require any hardware enhancement at the substation level, and thus it can be readily utilized in real-time applications or offline studies. More importantly, our methods provide not only the detection of GSA, but also the correction of those spoofed synchrophasor data. On the other hand, our solution utilizes the special property of GSA instead of the assumption of random gross errors. That is, the GSA on one PMU impacts all the synchrophasor measurements from this PMU with the same GSA phase shift. It should also be noted that the statistical properties of the GSA phase shift as well as the location of the GSA is unknown, and hence classical approximations to simplify the problem formulation are not applicable. Lastly, our algorithm could detect the presence of GSA based on the data within one snapshot, which makes it more efficient and enables the detection of GSA as quickly as possible.

The rest of this paper is organized as follows. Section II provides the operational paradigm of GPS spoofing attack and its potential impact on the synchrophasor data and SE. Section III introduces a statistical model for the synchrophasor-based SE under the impact of GPS spoofing attacks. The corresponding correction algorithm for GPS-spoofed synchrophasor data for a single GSA is proposed in Section IV and numerical results of different algorithms under multiple testing scenarios are given in section V. Conclusive remarks and future work discussions are provided in Section VI.

II. Impact of GPS Spoofing Attack on SE

Compared with the encrypted military GPS signal, the civilian GPS signal can be predicted by any GPS receiver [17]. Hence, it is possible to forge a matched version of corresponding GPS signal by an attacker. Existing work has shown that GSA can be implemented by a common two-stage scheme with low-cost hardwares [15], [16], [18], [22], [23]. Worse still, GSA can be launched covertly with some mobility as long as the target is within certain range (about hundreds of meters), which makes the detection and protection of the physical presence of attacks more difficult, if not impossible. Furthermore, it has been shown that GSA could seriously deteriorate the effectiveness of power grid control, especially on the voltage stability monitoring, transmission line fault detection, and regional disturbing event location [15].

As discussed above, PMUs based on the civilian GPS timing signal are vulnerable to GSA. When GSA occurs, the timestamp of PMU measurements could be modified, which leads to a mismatch between the measured phasors and the true phasors, or equivalently a modification on the phase angles of these synchrophasor data [9], [16]. Mathematically, for any single snap shot, the spoofed voltage and current synchrophasor data are affected by the GSA as follows:

$$\begin{aligned} V_{\text{spf}} &= V_{\text{true}} \times e^{j\theta_{\text{spf}}} \\ I_{\text{spf}} &= I_{\text{true}} \times e^{j\theta_{\text{spf}}} , \end{aligned} \tag{1}$$

where θ_{spf} denotes the phase shift introduced by the GSA at the current time instant to the true measurements.

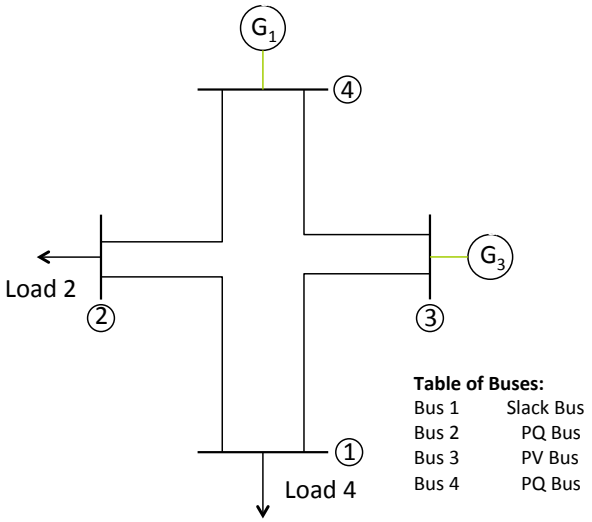

Fig. 1. A 4-bus power system to demonstrate the impact of GSA on SE.

To better illustrate the impact of GSA on power system operations, especially the SE, a tutorial example based on a 4-bus power system is given in Fig. 1 with the line parameters listed in Table I. Assume that bus 1 and bus 4 are installed with PMUs, and accordingly the synchrophasor data generated by these two PMUs are bus voltages V_1, V_4, and line currents $I_{12}, I_{13}, I_{42}, I_{43}$. The system states to be estimated are S_1, S_2, S_3, S_4, which are the voltage phasors at these four buses. Assume that a GSA is present at bus 4 and causes an offset of $833.4\,\mu s$ on the synchronization clock of the PMU installed there, which is equivalent to a GSA phase shift $\theta_{spf} = 0.1\pi$ on the voltage and current synchrophasor data for a 60-Hz system. Traditional weighted least square (WLS) method is employed to estimate the system state. The signal-to-noise ratio (SNR) is set as 20 dB, the numerical results are averaged over 200 Monte Carlo simulations, and the detailed results are listed in Table II.

It should be noted that this GSA can impact not only the states related to bus 4, but also all other states. All four estimated states are affected significantly, especially the phase angle. Under this circumstance, bus 1 can no longer be treated as slack bus due to its nonzero phase. More importantly, corresponding control actions may need to be taken on generators and loads due to the misleading information saying the unbalance of power flow analyzed with these estimated state. In summary, under this circumstance, SE can no longer provide reliable and accurate system state estimation results for higher-level applications.

TABLE I
LINE PARAMETERS FOR THE TESTED 4-BUS SYSTEM

Bus-to-Bus	R (p.u.)	X (p.u.)	B (p.u.)
1-2	0.02	0.06	0.12
1-3	0.08	0.24	0.10
2-4	0.08	0.24	0.10
3-4	0.01	0.04	0.02

TABLE II
AN ILLUSTRATIVE EXAMPLE OF THE IMPACT OF GSA ON THE WLS STATE ESTIMATION

State	SE Error, no GSA		SE Error, under GSA	
	Mag. (p.u.)	Pha. (π)	Mag. (p.u.)	Pha. (π)
$\hat{S}_1$	0.0029	0.0012	0.0102	-0.0467
$\hat{S}_2$	0.0030	0.0012	0.0127	-0.0484
$\hat{S}_3$	0.0013	0.0023	0.0118	-0.0483
$\hat{S}_4$	0.0015	0.0024	0.0159	-0.0473

III. SIGNAL MODEL FOR SYNCHROPHASOR DATA UNDER GSA

Suppose that p PMUs are installed in an N-bus power system and the k-th PMU provides the synchrophasor data as follows [1, Chapter 7]:

$$\boldsymbol{m}_k = \boldsymbol{A}_k \boldsymbol{s} + \boldsymbol{e}_k , \tag{2}$$

with

$$\begin{aligned} \boldsymbol{m}_k &= [m_{k_1}, m_{k_2}, \ldots, m_{k_n}]^T \\ \boldsymbol{s} &= [S_1, S_2, \ldots, S_N]^T , \end{aligned} \tag{3}$$

where $k_1, \ldots, k_n$ are the indices of the measurements provided by the k-th PMU; $\boldsymbol{s}$ denotes the state vector of power grid with S_j denoting the voltage phasor of bus j; $\boldsymbol{A}_k$ can be determined by the relationship between the measurements provided by the k-th PMU and the system states, which can be obtained based on the PMU's location, the network topology and the transmission line parameters [1, Chapter 7]; $\boldsymbol{e}_k$ denotes the measurement noise vector for the k-th PMU. Without loss of generality, we assume that $\boldsymbol{e}_k$ follows identical independently distributed (i.i.d.) complex Gaussian distribution with the same variance σ^2, as they are all originated from the same PMU.

Stacking the measurements provided by all p PMUs together yields a statistical model for the synchrophasor-based power system state estimation

$$\begin{pmatrix} \boldsymbol{m}_1 \\ \boldsymbol{m}_2 \\ \vdots \\ \boldsymbol{m}_p \end{pmatrix} = \boldsymbol{m} = \begin{pmatrix} \boldsymbol{A}_1 \\ \boldsymbol{A}_2 \\ \vdots \\ \boldsymbol{A}_p \end{pmatrix} \boldsymbol{s} + \begin{pmatrix} \boldsymbol{e}_1 \\ \boldsymbol{e}_2 \\ \vdots \\ \boldsymbol{e}_p \end{pmatrix} = \boldsymbol{A}\boldsymbol{s} + \boldsymbol{e} , \tag{4}$$

where $\boldsymbol{m}$, $\boldsymbol{A}$ and $\boldsymbol{e}$ can be appropriately constructed with subblocks $\boldsymbol{m}_k$, $\boldsymbol{A}_k$ and $\boldsymbol{e}_k$ corresponding to different PMUs. Without loss of generality, we assume that the measurement noise of all synchrophasors follow the same distribution, i.e., $\boldsymbol{e} \sim \mathcal{CN}(\boldsymbol{0}, \boldsymbol{C}_e)$ with $\boldsymbol{C}_e = \sigma^2 \boldsymbol{I}$.

Assume that a GSA is present at the k-th PMU with GSA phase shift θ_{spf}, then according to the feature of the effects of GSA on synchrophasor data as discussed in Section II, the spoofed synchrophasor measurement can be modeled as:

$$\boldsymbol{m}_{\text{spf}} = \boldsymbol{G} \cdot \boldsymbol{m} \tag{5}$$
$$= \begin{pmatrix} \boldsymbol{m}_1 \\ \vdots \\ \boldsymbol{m}_k e^{j\theta_{\text{spf}}} \\ \vdots \\ \boldsymbol{m}_p \end{pmatrix} = \begin{pmatrix} \boldsymbol{I}_1 & \dots & \boldsymbol{0} & \dots & \boldsymbol{0} \\ \boldsymbol{0} & \ddots & \boldsymbol{0} & \dots & \boldsymbol{0} \\ \vdots & \vdots & \boldsymbol{I}_k e^{j\theta_{\text{spf}}} & \vdots & \vdots \\ \boldsymbol{0} & \dots & \boldsymbol{0} & \ddots & \boldsymbol{0} \\ \boldsymbol{0} & \dots & \boldsymbol{0} & \dots & \boldsymbol{I}_p \end{pmatrix} \begin{pmatrix} \boldsymbol{m}_1 \\ \vdots \\ \boldsymbol{m}_k \\ \vdots \\ \boldsymbol{m}_p \end{pmatrix},$$

where $\boldsymbol{m}_{\text{spf}}$ denotes the spoofed synchrophasor data vector and $\boldsymbol{I}_k$ denotes an identity matrix with its size determined by the total number of measurements provided by the k-th PMU, or equivalently the size of $\boldsymbol{m}_k$. Without the knowledge of matrix $\boldsymbol{G}$, or equivalently the location k and the phase shift θ_{spf} of this GSA, the system states cannot be estimated accurately.

The GSA process requires specialized equipment as well as thousands of seconds to realize [18]. Due to the huge geographical span of the power grid, especially the long distances between adjacent substations, it is hard for one to coordinately launch GSA in multiple locations or on multiple PMUs. Hence, we will concentrate on the scenario of a single GSA in this paper. Due to the special formation of matrix $\boldsymbol{G}$, we can always treat multiple GSAs as a combination of several independent and uncoordinated single GSAs.

Currently, power system control centers do not differentiate the source of data interference or contamination. In other words, they are all treated as "bad data" in most applications for power system monitoring and control. Bad data removal algorithms such as Largest Normalized Residual Removal (LNRR) are utilized to guarantee the reliability of power measurements [24]. But it may fail to identify the spoofed synchrophasor data under GSA, which can also be verified by our 4-bus illustration example. The main reason is that traditional general-purpose bad data processing algorithms would not utilize the specific feature that GSA will result in same phase angle offset in all spoofed PMU measurements as illustrated in (5).

Moreover, to our best knowledge, most of bad data detection techniques [12], [24], [25], [26] directly remove the bad data once detected due to the fact that there is usually a certain level of redundancy in the measurement set and that the bad data occur individually. However, under GSA, the data are compromised in a *grouped* manner, and removing the spoofed data would mean the loss of a number of measurements rather than a single one, which might lead to system unobservability. Therefore, while handling GSA, simple data removal is not a good option. This is especially so when it is possible to estimate the phase shift introduced to the measurements caused by the GSA and correct the spoofed synchrophasor data accordingly. The estimation and correction of a single GSA only introduce two additional unknowns, which are the location k and the GSA phase shift θ_{spf}. In contrast, traditional removal techniques eliminate all the synchrophasor data generated by the spoofed PMU, which usually include more than two measurements. Therefore, as a more practical and desirable method, GPS spoofed synchrophasor data correction can not only avoid extra loss of data redundancy, but also provide more accurate and robust state estimation. More importantly, the future grid is envisioned to be self-healing under different circumstances such as faults and cyber attacks, and therefore, in this sense, correction of the spoofed synchrophasor measurements is more promising and meaningful.

IV. Synchrophasor Data Correction under GSA

Generally, a GPS spoofing attack can be denoted by its location k and phase shift θ_{spf} as GSA(k, θ_{spf}). Hence, the correction of GPS-spoofed synchrophasor data can be tackled by estimating those two parameters, or equivalently estimating the corresponding $\boldsymbol{G}$ matrix. Due to the special construction of the $\boldsymbol{G}$ matrix, the estimated true synchrophasor data can be recovered as follows:

$$\hat{\boldsymbol{m}}_{\text{true}} = \hat{\boldsymbol{G}}^{\mathcal{H}} \boldsymbol{m}_{\text{spf}} , \tag{6}$$

where $\boldsymbol{X}^{\mathcal{H}}$ denotes the Hermitian (conjugate transpose) of $\boldsymbol{X}$.

There are two possible scenarios for the case of a single GSA:

- If the location k is known, only the GSA phase shift θ_{spf} needs to be estimated:

$$\hat{\theta}_{\text{spf}} = \arg\min_{\theta_{\text{spf}}} J(k, \theta_{\text{spf}}) ; \tag{7}$$

- If both parameters are unknown, every PMU will be examined to determine the most likely one under GSA with $\hat{k}$ and $\hat{\theta}_{\text{spf}}$:

$$(\hat{k}, \hat{\theta}_{\hat{k},\text{spf}}) = \arg\min_{k,\theta_{\text{spf}}} J(k, \theta_{\text{spf}}) , \tag{8}$$

where J is a pre-selected cost function and $k \in \{1, \dots, p\}$. A hypothesis test could be employed to detect the presence of GSA, which is given as follows:

$$\begin{aligned} H_0 &: \text{absence of GSA} \\ H_1 &: \text{presence of GSA} \end{aligned} \tag{9}$$

The decision rule is based on $\hat{\theta}_{\hat{k},\text{spf}}$, therefore,

$$\begin{aligned} H_0 &: \hat{\theta}_{\hat{k},\text{spf}} < Thr \\ H_1 &: \hat{\theta}_{\hat{k},\text{spf}} \geq Thr \end{aligned} \tag{10}$$

where Thr is a user-defined threshold for GSA phase shift.

Under the null hypothesis H_0, the Best Linear Unbiased Estimator (BLUE) [27] or the Weighted Least Square (WLS) algorithm [28] can be invoked to implement the state estimation:

$$\hat{\boldsymbol{s}} = (\boldsymbol{A}^{\mathcal{H}} \boldsymbol{C}_e^{-1} \boldsymbol{A})^{-1} \boldsymbol{A}^{\mathcal{H}} \boldsymbol{C}_e^{-1} \boldsymbol{m} . \tag{11}$$

Under the alternative hypothesis H_1, the BLUE can no longer produce a reliable state estimation due to the erroneous measurements in vector $\boldsymbol{m}_{\text{spf}}$:

$$\hat{\boldsymbol{s}}_{\text{spf}} = (\boldsymbol{A}^{\mathcal{H}} \boldsymbol{C}_e^{-1} \boldsymbol{A})^{-1} \boldsymbol{A}^{\mathcal{H}} \boldsymbol{C}_e^{-1} \boldsymbol{m}_{\text{spf}} . \tag{12}$$

However, with the synchrophasor data correction, we can obtain a better state estimate as

$$\hat{\boldsymbol{s}}_{\text{true}} = (\boldsymbol{A}^{\mathcal{H}}\boldsymbol{C}_e^{-1}\boldsymbol{A})^{-1}\boldsymbol{A}^{\mathcal{H}}\boldsymbol{C}_e^{-1}\hat{\boldsymbol{m}}_{\text{true}} \ . \tag{13}$$

Then by (6), (11) and (12), the estimation residual with GPS synchrophasor data correction will be:

$$\boldsymbol{r} = \hat{\boldsymbol{m}}_{\text{true}} - \boldsymbol{A}\hat{\boldsymbol{s}}_{\text{true}} = \hat{\boldsymbol{G}}^{\mathcal{H}}\boldsymbol{m}_{\text{spf}} - \boldsymbol{K}\hat{\boldsymbol{G}}^{\mathcal{H}}\boldsymbol{m}_{\text{spf}} = \boldsymbol{Y}\hat{\boldsymbol{G}}^{\mathcal{H}}\boldsymbol{m}_{\text{spf}} \ , \tag{14}$$

where $\boldsymbol{Y} = \boldsymbol{I} - \boldsymbol{K}$ is the residual sensitivity matrix with $\boldsymbol{K} = \boldsymbol{A}(\boldsymbol{A}^{\mathcal{H}}\boldsymbol{C}_e^{-1}\boldsymbol{A})^{-1}\boldsymbol{A}^{\mathcal{H}}\boldsymbol{C}_e^{-1}$ and $\boldsymbol{I}$ is the identity matrix. Intuitively, a correct estimate of matrix $\boldsymbol{G}$ will lead to a smaller estimation residual. On the other hand, an incorrect estimate of GSA, especially an incorrect estimate on the location of the GSA, is equivalent to add an extra GSA to the system and will lead to an even larger residual. Therefore, the root mean square error (RMSE) of estimation residual can be adopted as the cost function for GSA estimation:

$$J(k, \theta_{\text{spf}}) = \|\boldsymbol{r}(k, \theta_{\text{spf}})\|_2 \ , \tag{15}$$

where $\|\cdot\|_2$ denotes the L_2-norm of a vector.

Based on the previous analysis, the Spoofing-Matched Algorithm for GSA (SpM) is summarized with the following steps:

1) *Initialization*: generate the spoofed synchrophasor data $\boldsymbol{m}_{\text{spf}}$ from (4), (5) based on the obtained measurements and the candidate GSA location and phase shift, and generate the residual sensitivity matrix $\boldsymbol{Y}$ based on the PMU placement profile and the system SNR:

$$\begin{aligned} \boldsymbol{m}_{\text{spf}} &= \boldsymbol{G} \cdot \boldsymbol{m} \\ \boldsymbol{Y} &= \boldsymbol{I} - \boldsymbol{A}(\boldsymbol{A}^{\mathcal{H}}\boldsymbol{C}_e^{-1}\boldsymbol{A})^{-1}\boldsymbol{A}^{\mathcal{H}}\boldsymbol{C}_e^{-1} \end{aligned} \tag{16}$$

2) *Estimation of the GSA Phase Shift*: estimate the best $\hat{\theta}_{\text{spf}}$ for each PMU in the index set, which can be expressed as:

$$\hat{\theta}_{k,\text{spf}} = \arg \min_{\theta_{\text{spf}} \in [0, 2\pi)} \|\boldsymbol{r}(k, \theta_{\text{spf}})\|_2 \ , k \in \{1, \ldots, p\} \tag{17}$$

3) *Identification of GSA Location*: identify the index of the most likely PMU under GSA based on the result of step 2), obtain the following:

$$\hat{k} = \arg \min_{k \in \{1, \ldots, p\}} \|\boldsymbol{r}(k, \hat{\theta}_{k,\text{spf}})\|_2 \tag{18}$$

4) *Decision of GSA Presence*: identify the presence of GSA:

$$\begin{aligned} H_0 &: \hat{\theta}_{\hat{k},\text{spf}} < Thr \\ H_1 &: \hat{\theta}_{\hat{k},\text{spf}} \geq Thr \end{aligned} \tag{19}$$

5) *Correction of the Spoofed Synchrophasor Measurements*: under the null hypothesis H_0, $\hat{\boldsymbol{G}} = \boldsymbol{I}$; under the alternative hypothesis H_1, $\hat{\boldsymbol{G}}$ can be generated to correct the spoofed synchrophasor measurements based on the estimated GSA phase shift from step 2) and the estimated GSA location from step 3), obtain the following:

$$\hat{\boldsymbol{m}}_{true} = \hat{\boldsymbol{G}}^{\mathcal{H}}(\hat{k}, \hat{\theta}_{\hat{k},\text{spf}}) \cdot \boldsymbol{m}_{\text{spf}} \tag{20}$$

6) *System State Update*:

$$\hat{\boldsymbol{s}}_{true} = (\boldsymbol{A}^{\mathcal{H}}\boldsymbol{C}_e^{-1}\boldsymbol{A})^{-1}\boldsymbol{A}^{\mathcal{H}}\boldsymbol{C}_e^{-1}\hat{\boldsymbol{m}}_{\text{true}} \tag{21}$$

And the corresponding flow diagram for the SpM algorithm is given in Fig. 2.

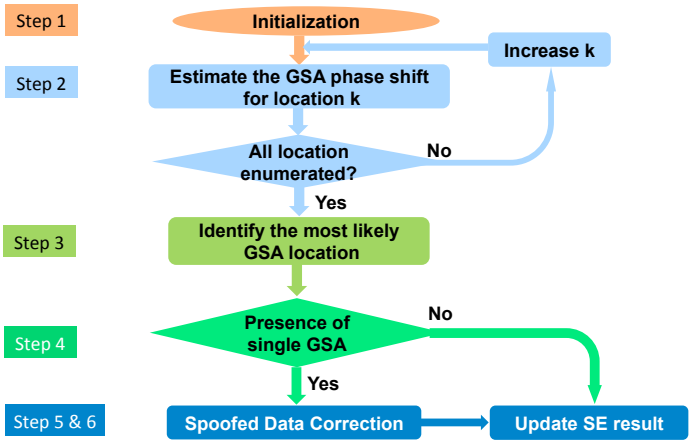

Fig. 2. The flow diagram describing the structure of the SpM algorithm.

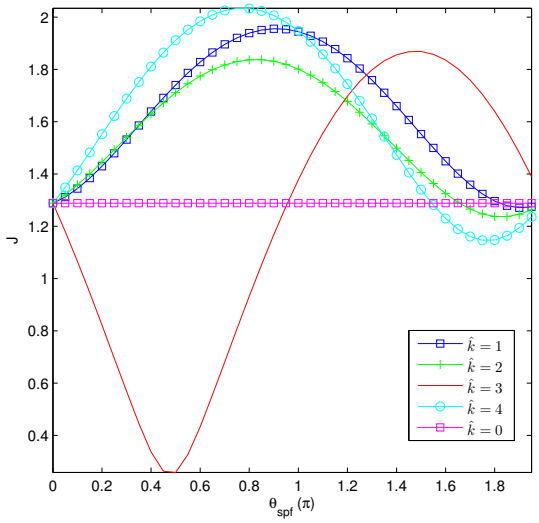

Fig. 3. J vs. θ_{spf} with GSA(3,0.5π) in IEEE 14-bus system.

It should be noted that step 2 is a typical one-dimensional optimization problem that finds the best estimate of the GSA phase shift $\hat{\theta}_{k,\text{spf}}$ over the parameter space $[0, 2\pi)$ for each PMU. The simplest solution to this problem is the exhaustive grid search method, which goes through every possible point exhaustively. However, its disadvantages are also obvious: computationally heavy and time consuming. But the simulation result from the exhaustive grid search method shown in Fig. 3 unveils an important characteristic of $J(k, \theta_{spf})$, namely that it is an unimodal function for θ_{spf}, which means that there is only one global minimizer within the variable's domain. The Golden Section search algorithm is a prevailing solution for this kind of problems by successively narrowing the range of values inside which the extremum is known to exist [29, Chapter 7]. Other one-dimensional search algorithms (see e.g. those introduced in [29, Chapter 7]) can also be applied to solve (17).

Without loss of generality, in this paper, we apply the Golden Section search algorithm to find the best estimation

of the GSA phase shift $\hat{\theta}_{k,\text{spf}}$ in the domain of $[0, 2\pi]$ with the following steps [29, Chapter 7]:

1) *Initialization*: set the iteration index $n = 0$, the start point of range $range_L = a_0 = 0$, the end point of range $range_R = b_0 = 2\pi$, the desired precision $\epsilon = 10^{-5}$, and the reduction factor $\rho = 0.61803$;
2) *Intermediate Points Evaluation*: to evaluate J at two initial intermediate points a_1 and b_1, obtain the following:
$$\begin{aligned} a_1 &= range_L + (1-\rho)(range_R - range_L) \\ b_1 &= range_L + \rho(range_R - range_L)\ , \end{aligned} \tag{22}$$
then with the index of PMU k, compute $J(k, a_1)$ and $J(k, b_1)$.
3) *Iteration Index Update*: if the desired precision is satisfied, or equivalently $|range_R - range_L| < \epsilon$, then do step 6; otherwise $n = n + 1$;
4) *Range Reduction Update & Coincide Point Evaluation*: if $J(k, a_n) < J(k, b_n)$, obtain the following:
$$\begin{aligned} &range_R = b_n, \quad b_{n+1} = a_n, \quad J(k, b_{n+1}) = J(a_n), \\ &a_{n+1} = range_L + (1-\rho)(range_R - range_L)\ , \end{aligned} \tag{23}$$
only $J(k, a_{n+1})$ needs to be recalculated; otherwise obtain the following:
$$\begin{aligned} &range_L = a_n, \quad a_{n+1} = b_n, \quad J(k, a_{n+1}) = J(b_n), \\ &b_{n+1} = range_L + \rho(range_R - range_L)\ , \end{aligned} \tag{24}$$
only $J(k, b_{n+1})$ needs to be recalculated, then go back to Step 3);
5) *Estimation Result*: calculate the final result as follows:
$$\hat{\theta}_{spf} = \arg \min_{\theta \in \{range_L, range_R\}} J(k, \theta)\ . \tag{25}$$

And the corresponding flow diagram for Golden Section search algorithm is given in Fig. 4 as follows:

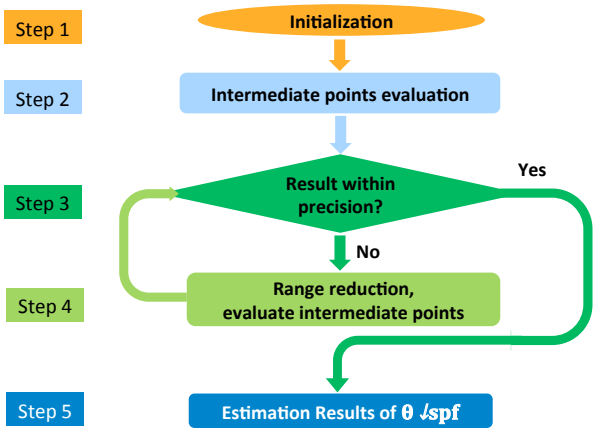

Fig. 4. The flow diagram for Golden Section search algorithm.

Comparing with the exhaustive grid search technique, the Golden Section search algorithm can effectively alleviate the computational burden by finding the approximation of the global minimizer with as few calculations as possible, and the accuracy of results can be controlled by the user defined precision parameter. At every stage of the uncertainty range reduction, the range is reduced by the ratio of ρ, which could greatly improve the speed of convergence. For example, to achieve the desired precision of 10^{-5}, we need guarantee that $(0.61803)^N \leq 10^{-5}/2$, equivalently $N \geq 26$, which means only 26 iterations are needed to find the extremum with the precision of 10^{-5}.

V. Simulation Tests

In this section, we use numerical examples to illustrate the effectiveness of the proposed SpM algorithm for synchrophasor data correction under GSA. The effect of the location of GSA, the value of GSA phase shift and the total number of PMUs installed are of our major concerns.

A. Simulation Setup

TABLE III
PMU Placement Profile under Different Test Scenarios

# of Buses	Sce.	# of PMUs	Indices of Buses with PMUs
14	1	4	2,6,7,9
	2	6	2,4,6,7,9,13
30	3	10	1,7,9,10,12,18,24,25,27,28
	4	16	3,4,5,7,10,11,12,17,19, 22,24,25,26,28,29,30
57	5	17	1,4,6,13,20,22,25,27,29 32,36,39,41,45,47,51,54
	6	28	1,3,4,6,9,12,20,22,24,27,29, 30,32,34,36,38,39,41,43, 44,45,46,48,51,52,53,54,56
118	7	32	2,5,9,12,15,17,21,25,29,34, 37,42,45,49,53,56,62,63,68, 70,71,75,77,80,85,86,91,94, 102,105,110,114
	8	45	2,5,7,9,12,15,17,21,25,29,31, 34,37,39,42,45,47,49,51,53, 56,57,58,62,63,66,68,70,71, 75,77,80,85,86,89,91,94,97, 100,102,105,107,110,112,114

To test the proposed Spoofing-Matched Algorithm (SpM) under different scenarios, we adopt the standard IEEE 14-, 30-, 57-, 118-bus test systems with the system topology and parameters provided in [30] for our simulation setup. For each test system, different scenarios corresponding to different PMU placement profiles are adopted and the details are given in Table III [21], [31]. Concerned about the potential loss of observability due to transmission line outages, we configured that scenario 1, 3, 5, 7 are with the minimum number of PMUs that satisfy the system observability, while scenario 2, 4, 6, 8 are with some randomly selected redundant PMUs based on scenario 1, 3, 5, 7 correspondingly. Under each scenario, GSA is launched on one randomly selected PMU with GSA phase shift θ_{spf}. 1000 Monte Carlo simulations are conducted for each testing scenario. The system signal-to-noise ratio (SNR) is selected as 20 dB, and the precision of Golden Section search algorithm is selected as $\epsilon = 10^{-5}$ for better accuracy. The specifications of the computer running the system test are given as follows: CPU: Quad Core Intel i7-3770 (3.4GHz); Memory: 16GB, 1600MHz, DDR3 SDRAM.

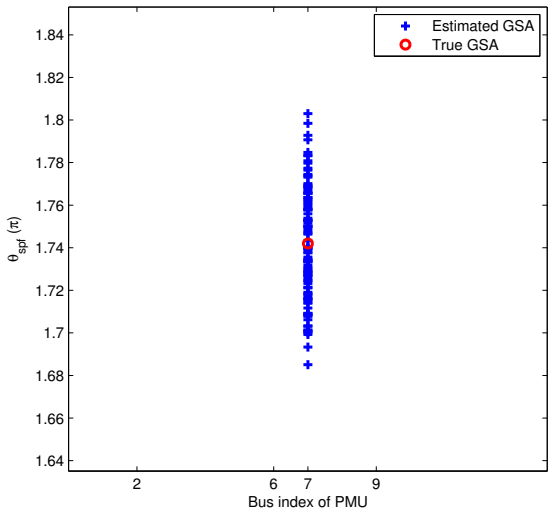

Fig. 5. Numerical result for detection of GSA(3, θ_{spf}) in Scenario 1.

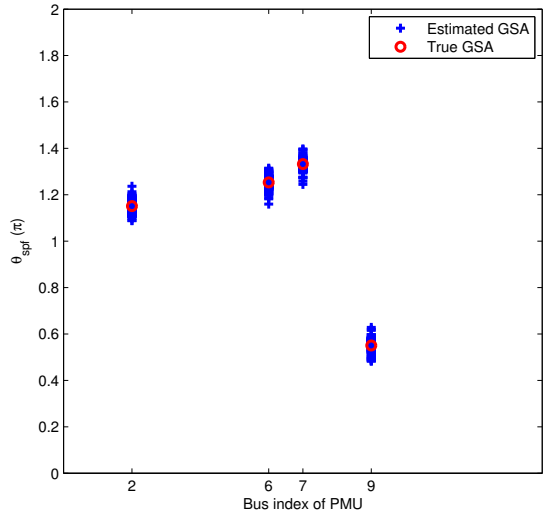

Fig. 6. Combined results for detecting GSA on each PMU in Generalized Scenario 1.

B. Performance of GSA Detection

We first consider the performance of GSA detection, which should cover the following two aspects: the correctness of estimated GSA location and the accuracy of the estimation of GSA phase shift. Here we do not consider the system dynamics and all the synchrophasor data used in a testing case are from the same snapshot.

In Scenario 1, a GSA is launched on the 3rd PMU (installed on bus 7) with one randomly selected phase shift (denoted as GSA(3, θ_{spf})) in IEEE 14-bus system. The detection results of SpM algorithm are shown in Fig. 5, in this case, the GSA location is identified correctly for each iteration, and the estimated GSA phase shift are centralized around the true one.

In order to show that our algorithm is insensitive to the location of GSA, we generalize Scenario 1 by simulating a GSA on one PMU in each simulation and combine their results in Fig. 6, clearly the GSA can be correctly detected no matter

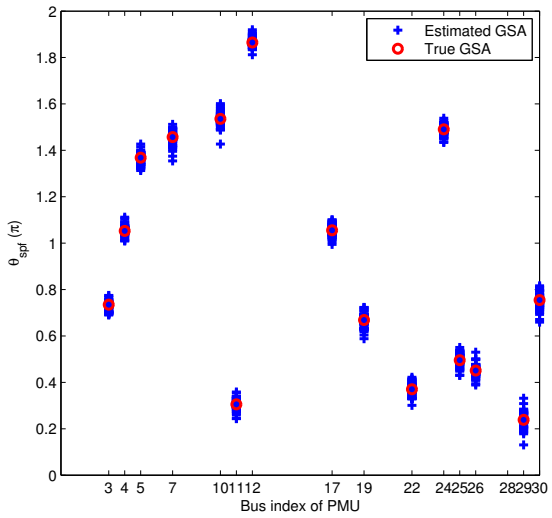

Fig. 7. Combined result for detecting GSA on each PMU in Generalized Scenario 4.

where the GSA is located. Similar results are shown in Fig. 7 for generalized Scenario 4, which verifies that our algorithms is robust when the system order increases.

TABLE IV
GSA DETECTION PERFORMANCE UNDER SINGLE GSA

Scenario	1	2	3	4	5	6	7	8
$p_{\text{CDT}}(\%)$	100	100	100	100	100	100	100	100
$p_{\text{MDT}}(\%)$	0	0	0	0	0	0	0	0
Bias($\hat{\theta}_{\text{spf}}$)	0.0226	0.0213	0.0255	0.0240	0.0310	0.0207	0.0209	0.0190
RMSE($\hat{\theta}_{\text{spf}}$)	0.0266	0.0262	0.0323	0.0309	0.0385	0.0254	0.0270	0.0237
$T_{\text{computing}}$(sec)	0.012	0.018	0.036	0.072	0.095	0.267	0.458	1.088

Numerical simulations have also been implemented under other scenarios, and several metrics are adopted to evaluate the performance of our algorithm. The probability of correct detection (p_{CDT}) and the probability of miss detection (p_{MDT}) are calculated for each scenario. On the other hand, the bias and root mean square error (RMSE) are adopted to evaluate the accuracy of the estimated GSA phase shift $\hat{\theta}_{\text{spf}}$. Details of numerical results for all scenarios are given in Table IV. It should be noted that when the total number of PMUs increases, e.g., from scenario 1, 3, 5, 7 to scenario 2, 4, 6, 8 correspondingly, the performance of our proposed algorithm has been improved due to the additional information from those newly included PMUs. Moreover, the computing time for each scenario provided in Table IV also indicate that the detection, and correction of GPS-spoofed data could be completed in a timely manner based on the proposed SpM algorithm, which guarantees the time requirements for the potential online applications.

C. Performance of State Estimation

The ultimate goal of synchrophasor data correction under GSA is to provide reliable PMU measurements for further applications in power grid control center, where one critical application is the power system SE. Therefore, the SE result based on the synchrophasor-based linear model can be adopted

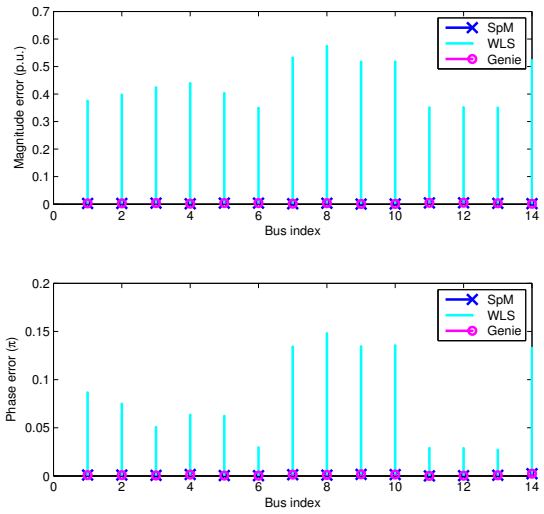

Fig. 8. Comparison of estimation error using SpM, WLS and Genie with GSA(3, θ_{spf}) in Scenario 1.

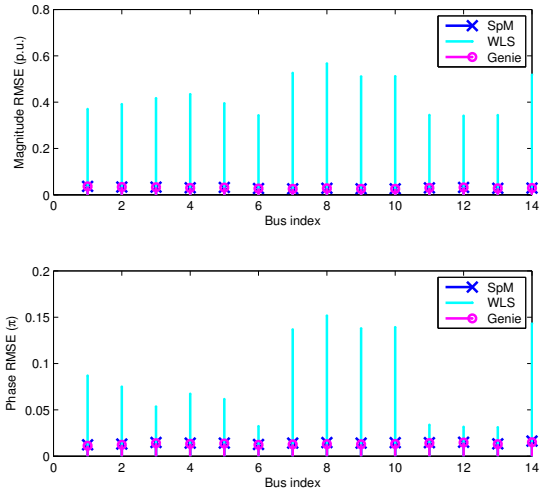

Fig. 9. Comparison of RMSE using SpM, WLS and Genie with GSA(3, θ_{spf}) in Scenario 1.

for comparisons among different algorithms. We compare our SpM algorithm with the traditional weighted least square (WLS) algorithm. Genie-aided solutions with known GSA information are also included as a reference.

In Scenario 1, the estimation error of system states is shown in Fig. 8, where the magnitude and phase of system states are compared separately for different algorithms. We observe that when GSA is present, SpM algorithm can reduce the estimation errors in both magnitude and phase. It should be noted that the errors from SpM are comparable to the Genie-aided algorithm. The RMSE of SpM, WLS and Genie-aided in Scenario 1 is shown in Fig 9. We observe that the performance of SpM is comparable to Genie while WLS is the worst. Numerical simulations have also been implemented under other scenarios and the details of results are given in Table V. Clearly the numerical result for each test is consistent with our previous conclusion. On the other hand, the performance of all three methods improves when the total number of PMUs increases in each testing system as expected.

To further show the relative improvement of our proposed algorithm over WLS, we also calculated another performance metric as $(1 - \frac{\text{RMSE}_{\text{SpM}}}{\text{RMSE}_{\text{WLS}}}) \times 100\%$ for magnitude and phase separately, and it indicates that the SpM has a consistently better performance.

VI. Conclusions and Future Work

It has been shown that GPS spoofing attack is an imminent threat to modern power system monitoring and control, where GPS-synchronized PMUs are pervasively installed. Unlike random gross errors and statistically distributed small phase mismatch, one GSA impacts all the synchrophasor measurements from the same spoofed PMU with the same GSA phase shift. Currently, there exist few effective solutions for synchrophasor data correction under GPS spoofing attack. In this paper, the spoofing-matched algorithm (SpM) is proposed to address this issue. Numerical simulations have been implemented under multiple testing scenarios, and the results show that the proposed algorithm not only can identify the GSA location effectively, but also can recover the GPS-spoofed synchrophasor data accurately with high efficiency, which in turn improves the result of power system state estimation. In the future, extension of our SpM algorithm to the scenario of multiple independent GSAs will be studied. In addition, other anti-GSA strategies will be investigated such as optimal PMU placement and synchronization protocols, etc.; on the other hand, how to utilize the parallel computing techniques to improve the computational efficiency would also be an interesting topic to look into.

References

[1] A. G. Phadke and J. S. Thorp, *Synchronized Phasor Measurements and Their Applications*. Springer, 2010.

[2] V. Terzija, G. Valverde, D. Cai, P. Regulski, V. Madani, J. Fitch, S. Skok, M. Begovic, and A. Phadke, "Wide-area monitoring, protection, and control of future electric power networks," *Proceeding of the IEEE*, vol. 99, no. 1, pp. 80–93, January 2011.

[3] J. De La Ree, V. Centeno, J. Thorp, and A. Phadke, "Synchronized phasor measurement applications in power systems," *IEEE Trans. on Smart Grid*, vol. 1, no. 1, pp. 20–27, June 2010.

[4] DOE, *Synchrophasor Technologies and their Deployment in the Recovery Act Smart Grid Programs*. U.S. Department of Energy, August 2013.

[5] P. Overholt, D. Ortiz, and A. Silverstein, "Synchrophasor technology and the DOE: Exciting opportunities lie ahead in development and deployment," *IEEE Power and Energy Magazine*, vol. 13, no. 5, pp. 14–17, September 2015.

[6] G. Giannakis, V. Kekatos, N. Gatsis, S.-J. Kim, H. Zhu, and B. Wollenberg, "Monitoring and optimization for power grids: A signal processing perspective," *IEEE Signal Processing Magazine*, vol. 30, no. 5, pp. 107–128, September 2013.

[7] M. Kezunovic, S. Meliopoulos, V. Venkatasubramanian, and V. Vittal, *Application of Time-Synchronized Measurements in Power System Transmission Networks*. Springer International Publishing, 2014, vol. 1.

[8] J. G. Fletcher, M. Chaluvadi, D. Anand, J. Amelot, Y. Li-Baboud, and J. Moyne, "Smart clocks have a hand in the smart grid," in *2011 IEEE Power and Energy Society General Meeting*, July 2011, pp. 1–6.

[9] IEEE Std, *IEEE Standard for Synchrophasor Measurements for Power Systems, C37.118.1-2011 (Revision of IEEE Std C37.118-2005)*, December 2011.

[10] M. A. Lombardi, L. M. Nelson, A. N. Novick, and V. S. Zhang, "Time and frequency measurements using the global positioning system," *Calibration Laboratory: The International Journal of Metrology*, vol. 1, no. 1, pp. 26–33, July 2001.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TSG.2017.2662688, IEEE Transactions on Smart Grid

TABLE V
RMSE OF STATE ESTIMATION UNDER DIFFERENT SCENARIOS

Scenario	SpM		WLS		Genie		Improvement	
	Mag.(p.u.)	Pha.(π)	Mag.(p.u.)	Pha.(π)	Mag.(p.u.)	Pha.(π)	Mag.(%)	Pha.(%)
1	0.0307	0.0156	0.4355	0.0851	0.0309	0.0134	92.95	81.66
2	0.0250	0.0121	0.3250	0.0622	0.0249	0.0110	92.30	80.55
3	0.0324	0.0158	0.1758	0.0333	0.0324	0.0152	81.57	52.48
4	0.0188	0.0080	0.1082	0.0163	0.0188	0.0078	82.63	50.57
5	0.0430	0.0203	0.1400	0.0536	0.0430	0.0196	69.27	62.13
6	0.0186	0.0081	0.0642	0.0118	0.0186	0.0081	71.06	30.94
7	0.0298	0.0098	0.0629	0.0120	0.0298	0.0096	52.61	18.70
8	0.0182	0.0062	0.0377	0.0075	0.0182	0.0061	51.70	17.78

[11] J. S. Warner and R. G. Johnston, "A simple demonstration that the global positioning system (GPS) is vulnerable to spoofing," *Journal of Security Administration*, 2003.

[12] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *IEEE Trans. on Parallel and Distributed Systems*, vol. 25, no. 3, pp. 717–729, March 2014.

[13] *Vulnerability assessment of the transportation infrastructure relying on the Global Positioning System*. John A. Volpe National Transportation Systems Center Technical Report, August 2001.

[14] Anon., *Extended loss of GPS Impact on Reliability*. North American Electric Reliability Corporation Technical Report, July 2012.

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

[16] I. Akkaya, E. Lee, and P. Derler, "Model-based evaluation of GPS spoofing attacks on power grid sensors," in *2013 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems (MSCPES)*, Berkeley, CA, May 20, 2013, pp. 1–6.

[17] X. Jiang, J. Zhang, B. Harding, J. Makela, and A. Dominguez-Garcia, "Spoofing GPS receiver clock offset of phasor measurement units," *IEEE Trans. on Power Systems*, vol. 28, no. 3, pp. 3253–3262, August 2013.

[18] 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. 1, pp. 134–147, December 2012.

[19] L. Heng, J. Makela, A. Dominguez-Garcia, R. Bobba, W. Sanders, and G. Gao, "Reliable GPS-based timing for power systems: A multi-layered multi-receiver architecture," in *Power and Energy Conference at Illinois (PECI), 2014*, February 2014, pp. 1–7.

[20] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, and G. Lachapelle, "GPS vulnerability to spoofing threats and a review of antispoofing techniques," *International Journal of Navigation and Observation*, vol. 2012, pp. 111–119, May 2012.

[21] P. Yang, Z. Tan, A. Wiesel, and A. Nehora, "Power system state estimation using PMUs with imperfect synchronization," *IEEE Trans. on Power Systems*, vol. 28, no. 4, pp. 4162–4172", November 2013.

[22] S. Gong, Z. Zhang, M. Trinkle, A. Dimitrovski, and H. Li, "GPS spoofing based time stamp attack on real time wide area monitoring in smart grid," in *2012 IEEE Third International Conference on Smart Grid Communications (SmartGridComm)*, November 2012, pp. 300–305.

[23] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, and K. Poolla, "Smart grid data integrity attacks: characterizations and countermeasures," in *2011 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, October 2011, pp. 232–237.

[24] F. Schweppe, "Power system static-state estimation, part I - III," *IEEE Trans. on Power Apparatus and Systems*, vol. PAS-89, no. 1, pp. 120–135, January 1970.

[25] W. Xu, M. Wang, J.-F. Cai, and A. Tang, "Sparse error correction from nonlinear measurements with applications in bad data detection for power networks," *IEEE Trans. on Signal Processing*, vol. 61, no. 24, pp. 6175–6187, December 2013.

[26] L. Liu, M. Esmalifalak, Q. Ding, V. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Trans. on Smart Grid*, vol. 5, no. 2, pp. 612–621, March 2014.

[27] S. M. Kay, *Fundamentals of statistical signal processing : estimation theory*. Prentice Hall PTR, US, 1993, vol. 1.

[28] A. Abur and A. Gomez-Exposito, *Power System State Estimation: Theory and Implementaion*. CRC Press, 2004.

[29] E. K. Chong and S. H. Zak, *An Introduction to Optimization*. John Wiley & Sons, Inc., 2001.

[30] University of Washington, *Power System Test Case Archive*. [Online]. Available: http://www.ee.washington.edu/research/pstca/.

[31] J. Xu, M. H. F. Wen, K.-C. Leung, and V. O. K. Li, "Optimal PMU placement for wide-area monitoring using chemical reaction optimization," in *Proc. IEEE ISGT 2013*, Washington, DC, February 24-27, 2013, pp. 1–6.