GPS Spoofing-Resilient Voltage Phasor Estimation for the Power Grid

Shubhendra Vikram Singh Chauhan\textsuperscript{1} and Grace Xingxin Gao\textsuperscript{2}

University of Illinois at Urbana-Champaign\textsuperscript{1} and Stanford University\textsuperscript{2}

Abstract—Installation of Phasor Measurement Units (PMUs) is a step towards achieving wide-area situational awareness as PMUs provide synchronized measurements using GPS time. GPS signals are susceptible to GPS Spoofing Attacks (GSAs) due to its unencrypted signal structure and low signal power, making PMUs vulnerable to such attacks. We propose a novel method for voltage phasor estimation in the power grid that is resilient to single or multiple GSAs. In this method, we simultaneously detect GSA and correct PMU measurements. Our proposed method consists of two algorithms, residual-based GSA detection and iterative PMU measurement correction. We derive a necessary condition for detecting GSAs using residuals. We refer our proposed method as Spoofing-Resilient Snapshot State Estimation (SR-SSE) that consists of GSA detection and measurement correction algorithms. We perform Monte-Carlo simulations to verify our derived necessary condition. We further simulate the IEEE 14 test bus case to validate our SR-SSE algorithm against single and multiple GSAs.

Keywords—Snapshot State Estimation, PMU, GPS Spoofing Attacks

I. INTRODUCTION

Traditionally, a power grid network is monitored using Supervisory Control and Data Acquisition (SCADA) measurements [1]. These measurements include injection power, power flow and voltage magnitudes at the buses. State estimation is essential for monitoring the power grid. Complex voltage phasors at each bus are the states of the power grid. The state estimation routine involves estimating complex voltage phasors at every bus of the grid using the measurements. Unsynchronized measurements with low update rates are the main disadvantages of SCADA measurements that make it unsuitable for real-time monitoring of the wide-area network.

The Grid Modernization Initiative (GMI) is an initiative to create a modern grid that has greater resilience, improved reliability, enhanced security, additional affordability, superior flexibility, and increased sustainability [2]. Under this initiative, a large number of Phasor Measurement Units (PMUs) are being installed throughout the North American Power Grid. According to North American Synchro-Phasor Initiative (NASPI), roughly 2500 PMUs have been installed throughout the grid [3]. This is a step towards achieving wide-area situational awareness.

Compared to SCADA measurements, PMU measurements are 100 times faster [4] and are synchronized using GPS time. PMU measures voltage magnitude, voltage phase angle, line current magnitude and line current phase angle. Synchronized measurements with faster update rate make PMUs suitable for real-time monitoring of the power grid.

GPS plays a critical role in the synchronization of PMU measurements. GPS provides microsecond level timing [5]. However, GPS civilian signals are susceptible to external attacks due to unencrypted signal structure and low signal power [6]–[8] making PMUs vulnerable to external attacks as well. Spoofing is one such external attack in which, a GPS lookalike malicious signal is broadcasted at a higher power. Due to higher power, conventional GPS receiver architectures [6], [9] lock onto the malicious signal and provide incorrect position and time. GPS Spoofing Attacks (GSAs) are an imminent threat to the power grid. Various studies, [10]–[12], show the feasibility of different GSAs. Humphreys et al. [10] provide exhaustive scenarios of GSAs. Record and replay are some of the simplest GSAs [13]. In this attack, an attacker replays a pre-recorded GPS signal at a higher power. The traditional receiver locks on to the malicious signal and provides the time and position corresponding to the pre-recorded GPS signal. Transmitting GPS signals from a GPS simulator would be another type of GSA. Humphreys et al. [10] explored the feasibility of various spoofing attacks, developed a portable receiver spoofer and provided a few countermeasures for various GSAs.

The impact of GSAs on fault location and voltage stability monitoring algorithm is illustrated in [11], [14]. IEEE C37.118.1-2011 describes a standard for phase angle accuracy. According to this standard, timing error should always be less than 26.5 \( \mu \)s to ensure the phase error is less than 0.01 radian. This standard has been used to study power grid stability analysis [15]. Shepard et al. [12] conducted hardware experiments with PMUs and GPS signals. The group showed that the PMU phase angle can be arbitrarily changed using the portable spoofer device. The incorrect phase angle severely degrades the performance of the state estimation algorithm. This study showed that GSAs is capable of violating IEEE C37.118.1-2011 standard. GSA detection and mitigation are critical to ensure the safe operation of the power grid. The remainder of this section provides a review of prior work, our objectives, approach and contribution.

A. Prior Work

Prior work is broadly divided into two parts: GSA detection and GSA mitigation. A significant work is available for GSA detection [16]–[20]. Various spoofing attacks and recommended countermeasures for commercial receivers are elucidated in [19]. The countermeasure strategies include drift
monitoring, encryption-based defenses, signal-geometry-based defenses, etc. Mina et al. [16] use the presence of encrypted military P(Y) code in authentic signals to detect GSA. The group performs cross-correlation between a wide network of power stations to identify the spoofed node. This method is effective in detecting GSAs that transmit malicious GPS signals. Bhamidipati et al. [17] use multiple receivers with novel GPS receiver architecture to detect and locate a spoofer. The group utilizes the cross-correlation properties of GPS signals across multiple receivers to detect GSA. The method developed in [20], comes under signal-geometry-based defenses. Zhu et al. [20] use the static location of a sub-station and predict visible satellites. A GSA is detected if there is a mismatch between the predicted visible satellites with the actual visible satellites. The generalized likelihood ratio-based hypothesis testing is the basis of the spoofing detection algorithm developed in [21].

After GSA detection, the effect of GSA needs to be mitigated to ensure the safe operations of the power grid. Limited literature is available for GSA mitigation. Fan et al. [22] developed an algorithm to detect and mitigate the effect of GSA on power grid state estimation. The algorithm was tested with simulated data and showed to be resilient against GSA. However, the developed algorithm assumes single GSA and is not capable of mitigating the effect of multiple GSAs on PMU measurements.

Risbud et al. [23] developed a joint state estimation and attack reconstruction algorithm. This work formulates the joint estimation as an optimization problem. The developed algorithm is capable of simultaneously estimating attack angles and states of a power grid network. The phase shift in PMU measurement due to a spoofing attack is referred to as an attack angle. Bias in the state estimate is utilized to detect GSA.

Silva et al. [24] developed a PMU data correction algorithm under GSA. The group utilizes the sparseness of attacked PMUs to correct PMU data. The developed method is applicable for correcting PMU data under multiple attack scenarios. However, state estimation was not performed. This allowed the group to relax the assumption of observability of the power grid network.

B. Our Objectives

The prior work either develop an algorithm for GSA detection or GSA mitigation for the power grid. The exception of this is [23]. However, to the best knowledge of authors, a theoretical analysis for detecting single or multiple GSAs using residuals has not been provided in the literature. The objectives of our work are as follows

1) Provide a theoretical analysis for detection single or multiple GSAs using PMU measurement residuals.
2) Provide an algorithm for correcting PMU measurements under multiple GSAs.
3) Provide a method to perform simultaneous GSA detection and mitigation.

Overall goal of above objectives is to develop a spoofing resilient state estimator that is resilient to single or multiple GSAs with similar signal structure.

C. Our Approach and Contributions

Various spoofing attacks are outlined in [19]. In this paper, we consider a specific GSA that poses a threat to the safe operation of power grid. In this attack, a malicious GPS lookalike signal is transmitted at higher power such that the traditional receiver is locked on to the malicious signal. The malicious signal is created to alter user time and not location. This is one of the advanced attacks that is difficult to detect. A GSA that alters user position would be detectable as PMUs are static with a known location.

In our approach, we utilize PMU measurement residuals to detect GSAs. In prior work, it has been shown that the considered GSA only affects the phase of all the measurements at the attacked node [11], [14], [23]. This unique characteristic of GSA modifies the residual of the measurements at attacked nodes. The contributions of our work are as follows

1) We propose a novel method for voltage phasor estimation in the power grid that is resilient to single or multiple GSAs. Our proposed method simultaneously detects and mitigates single or multiple GSAs. This method consists of two algorithms, one for GSA detection and the other for PMU measurement correction.
   - We develop a GSA detection algorithm, referred as Spoofing Detection, that utilizes measurement residuals for detecting single or multiple GSAs. We utilize the change in the distribution of residuals to detect GSAs.
   - We develop an iterative minimization algorithm, referred as Measurement Correction, to correct PMU measurements under GSAs. In this algorithm, we minimize expected residuals iteratively to correct measurements.

We refer our proposed method as Spoofing-Resilient Snapshot State Estimation (SR-SSE).

2) We provide theoretical analysis for GSA detection using measurement residuals. We derive a mathematical necessary condition for detecting single or multiple GSAs using measurement residuals.

3) We validate our proposed method by simulating the IEEE 14 test bus case for various GSA scenarios. We verify our derived necessary condition by performing Monte-Carlo simulations.

The remainder of the paper is organized as follows, a generic snapshot state estimator algorithm for the power grid is presented in section II along with the spoofing attack measurement model. In section III, we provide details of our theoretical analysis for GSA detection using measurement residuals. We derive a necessary condition to detect single or multiple GSAs using measurement residuals.

The proposed method is explained in section IV. In this section, we provide details of simultaneously detecting and mitigating GSAs. Details for the simulation environment and implementation are also presented in this section. Experimental results are shown in section V and finally, the conclusions of the work are provided in section VI.
II. BACKGROUND

State estimation plays a critical role in the power system control center. The state of the power grid network is defined by the voltage magnitudes and angles at all buses (nodes of the network). The state estimator determines the complex voltages of the buses based on a set of redundant measurements. Traditionally, Snapshot State Estimation (SSE) algorithm is used for state estimation due to the slow variation of voltages. Depending on the type measurements there are different SSE algorithms available in the literature [25]. SCADA based SSE algorithm is provided in [1]. PMU based SSE algorithm is developed in [26]. Apart from having a faster update rate and synchronized measurements, PMUs have one more advantage over SCADA measurements. PMUs directly measures voltage and current phasor for a grid. This results in a linear relationship between states of the network and the PMU measurements. SSE based on SCADA and PMU measurements is explored in [27].

In this work, our primary focus is to develop the GSA detection and mitigation algorithm based on PMU measurements. The rest of this section provides details for PMU based SSE and spoofing attack model.

A. PMU-based SSE

Consider a power grid network of \(N\) nodes. In this network, a total of \(m\) PMUs have been installed to ensure observability. The system state \(x \in \mathbb{R}^{2N \times 1}\) consists of

\[
x = [Re(v_1), \ldots, Re(v_N),
Im(v_1), \ldots, Im(v_N)]^T
\]

where \(Re()\) denotes real part, \(Im()\) denotes imaginary part and \(v_i\) denotes the complex voltage of the node. The PMU measurement at node \(i\) that is connected to \(k\) different nodes, is given by

\[
z_i = [Re(v_i), Im(v_i), Re(I_{i1}), \ldots,
Re(I_{ik}), Im(I_{i1}), \ldots, Im(I_{ik})]^T
\]

where \(Re(I_{ik}), Im(I_{ik})\) are real and imaginary parts of the complex current injected into line \((i, k)\). The measurement model for PMU at node \(i\) is written as

\[
z_i = H_{i}x + \eta_i
\]

where \(z_i\) denotes PMU measurements at node \(i\), \(H_{i}\) denotes admittance matrix associated with a bus at node \(i\) and \(\eta_i\) is assumed to be zero-mean Gaussian noise. In MATPOWER [28], a branch line is approximated using a \(\pi\) model. The admittance matrix relates the complex current flowing in a line with the complex voltages at the nodes of the \(\pi\) model. The construction of the admittance matrix is given in [28], [29].

In order to have a concise representation, we stack all PMU measurements vertically to create a total measurement vector \(z\). The overall PMUs’ measurements are given by

\[
z = Hx + \eta
\]

where \(z = \begin{bmatrix} z_1 \\ \vdots \\ z_m \end{bmatrix}\), \(H = \begin{bmatrix} H_1 \\ \vdots \\ H_m \end{bmatrix}\) and \(\eta = \begin{bmatrix} \eta_1 \\ \vdots \\ \eta_m \end{bmatrix}\) is assumed to be i.i.d. Gaussian noise.

In state estimation, the problem is to determine the unknown states \(x\) using \(z\). This a classic least-squares problem. Under the assumption of full observability, the least square solution is given by

\[
\hat{x} = (H^TH)^{-1}H^Tz
\]

where \(\hat{x}\) is the estimated state of the network.

B. Spoofing Attack Model

The considered GSA in this work introduces a time delay in GPS time. A phase delay in PMU measurement is introduced due to induced time delay. This phase delay is referred to as an attack angle. Let’s assume PMU at node \(i\) is spoofed. Under the considered GSA, the PMU measurements at node \(i\) are modified as

\[
z_{i}^{spf} = \begin{bmatrix} |v_i|\cos(\theta_i + \Delta \theta_i) \\ |v_i|\sin(\theta_i + \Delta \theta_i) \\ |I_{i1}|\cos(\theta_{i1} + \Delta \theta_{i1}) \\ |I_{i1}|\sin(\theta_{i1} + \Delta \theta_{i1}) \\ \vdots \\ |I_{ik}|\cos(\theta_{ik} + \Delta \theta_{ik}) \\ |I_{ik}|\sin(\theta_{ik} + \Delta \theta_{ik}) \end{bmatrix}
\]

where \(z_{i}^{spf}\) denotes spoofed measurements, \(\theta_i\) is the phase angle at bus \(i, \theta_{ik}\) is the phase angle for the line \((i, k)\) and \(\Delta \theta_i\) is the attack angle. Zhang et al. [14] have shown that the considered GSA introduces a constant attack angle to all the PMU measurements as shown in equation (6). The attack angle at node \(i\) is related to the induced time delay by the following equation

\[
\Delta \theta_i = 2\pi f \Delta t_i
\]

where \(f\) denotes the frequency of the current and \(\Delta t_i\) is the time delay introduced by the considered GSA. Using the cosines identities, a linear relationship is derived between spoofed and authentic measurements [23]

\[
z_{i}^{spf} = \gamma_i H_{i}x + \eta_i
\]

where \(\gamma_i\) is a block diagonal matrix of appropriate size consisting of the following submatrix

\[
R = \begin{bmatrix} \cos(\Delta \theta_i) & -\sin(\Delta \theta_i) \\ \sin(\Delta \theta_i) & \cos(\Delta \theta_i) \end{bmatrix}
\]

We can stack all the PMU measurements vertically and rewrite the equation (8) as

\[
z^{spf} = \Gamma Hx + \eta
\]
where $z^{spf} = \begin{bmatrix} z^{spf}_1 \\ \vdots \\ z^{spf}_m \end{bmatrix}$ and $\Gamma$ is given by
\[
\Gamma = \begin{bmatrix} I_1 & \cdots & 0 \\ \vdots & \ddots & \vdots \\ 0 & \cdots & I_p \end{bmatrix}
\] (11)

where $I$ denotes an identity matrix of appropriate size. Under this GSA, without the knowledge of the structure of $\Gamma$, the state estimation algorithm will produce the following state estimate
\[
\hat{x}^{spf} = \left( H^T H \right)^{-1} H^T z^{spf} = \left( H^T H \right)^{-1} H^T \Gamma z
\] (12)

where $z$ denotes the PMU measurements under nominal condition and $H^\dagger$ denotes $\left( H^T H \right)^{-1} H^T$. The PMU measurements under nominal and spoofed condition are related by following relation
\[
z^{spf} = \Gamma z
\] (13)

In the next section, we provide theoretical derivation for GSA detection using PMU measurement residuals.

III. RESIDUAL-BASED GSA DETECTION

A significant amount of literature is available on detecting bad data using measurement residuals [30]–[33]. The majority of the literature assumes the bad data to be of additive nature. However, the GSA introduces bad data of multiplicative nature. There has been work on the types of attacks that can not be detected by residual-based bad data detection algorithm [30]. Given that certain additive attacks are not detectable, in this section we come up with a necessary condition to show when a GSA is detectable using measurement residuals. The motivation behind using the residuals is that researchers use residuals for detecting bad data in the power grid.

We start with measurement residuals to see if residuals can be used to detect GSA. We analyze residuals for two conditions as enumerated below.

1) Nominal condition: The residual under nominal condition is given by
\[
r = z - H \hat{x} = z - H H^\dagger z
\] (14)

where $r$ denotes PMU measurement residual vector. From equation (4), the expectation of $z$ is $H x$. Using this, taking the expectation of the above equation
\[
E[r] = E[z] - H H^\dagger E[z]
\]
\[
= H x - H H^\dagger H x = H x - H \left( H^T H \right)^{-1} H^T H x = 0
\] (15)

The above equation shows that under nominal condition, the expectation of residual vector is zero.

2) Under GSA: The residual spoofing attack is given by
\[
r^{spf} = z^{spf} - H \hat{x}^{spf} = \Gamma z - H H^\dagger \Gamma z
\] (16)

where $r^{spf}$ denotes PMU measurement residual vector under GSA. To simplify things, let $m_s$ denotes the set of PMUs that are unspoofed and let $m_s$ denotes the set of PMUs that are spoofed. Using this, the attacked measurements can be re-written as
\[
z^{spf} = \begin{bmatrix} I_{m_s} & 0 \\ 0 & \gamma_{m_s} \end{bmatrix} z
\] (17)

where $z_{m_s}$ denotes original measurements corresponding to unspoofed PMUs and $z_{m_s}$ denotes original measurements corresponding to spoofed PMUs. Note that $z = [z_{m_u} \ z_{m_s}]$, which is a nominal case measurement. Using this, the residual equation can further be simplified as
\[
r^{spf} = \begin{bmatrix} z_{m_u} - H \gamma_{m_u} \ z_{m_u} \\ \gamma_{m_s} z_{m_s} \end{bmatrix} - H H^\dagger \begin{bmatrix} z_{m_u} \\ \gamma_{m_s} z_{m_s} \end{bmatrix}
\]
\[
= \begin{bmatrix} z_{m_u} \\ \gamma_{m_s} z_{m_s} + z_{m_s} - z_{m_s} \end{bmatrix} - H H^\dagger \begin{bmatrix} z_{m_u} \\ \gamma_{m_s} z_{m_s} + z_{m_s} - z_{m_s} \end{bmatrix}
\]
\[
= \begin{bmatrix} z_{m_u} - H H^\dagger z_{m_u} \\ \gamma_{m_s} z_{m_s} + z_{m_s} - z_{m_s} \end{bmatrix} - H H^\dagger \begin{bmatrix} z_{m_u} \\ \gamma_{m_s} z_{m_s} + z_{m_s} - z_{m_s} \end{bmatrix}
\]
\[
= r + \begin{bmatrix} -H_{m_u} H_{m_u}^\dagger (\gamma_{m_u} - I_{m_u}) z_{m_u} \\ (I_{m_s} - H_{m_u} H_{m_u}^\dagger) (\gamma_{m_s} - I_{m_s}) z_{m_s} \end{bmatrix}
\] (18)

where $H_{m_u}$ denotes the rows of $H$ corresponding to unspoofed PMUs, $H_{m_s}$ denotes the rows of $H$ corresponding to spoofed PMUs, $H_{m_u}^\dagger$ denotes columns of $H^\dagger$ corresponding to spoofed PMUs. Taking the expectation on last equation will give
\[
E[r^{spf}] = E[r] + \begin{bmatrix} -H_{m_u} H_{m_u}^\dagger (\gamma_{m_u} - I_{m_u}) E[z_{m_u}] \\ (I_{m_s} - H_{m_u} H_{m_u}^\dagger) (\gamma_{m_s} - I_{m_s}) E[z_{m_s}] \end{bmatrix}
\]
\[
= \begin{bmatrix} -H_{m_u} H_{m_u}^\dagger (\gamma_{m_u} - I_{m_u}) E[z_{m_u}] \\ (I_{m_s} - H_{m_u} H_{m_u}^\dagger) (\gamma_{m_s} - I_{m_s}) E[z_{m_s}] \end{bmatrix}
\]
\[
\ne 0
\] (19)

The expectation is non zero since $E[z_{m_s}]$ is non zero (assuming the states are non zero). Therefore a spoofing attack gives rise to a bias in residuals. This change in
the statistic is used in our approach to detect a spoofing attack. We show that the norm of residuals increases under a spoofing attack. We show $\|r^{spf}\|^2 > \|r\|^2$ if $(I - HH^\dagger)$ is semi-positive definite which implies the residual norms increases under spoofing attack. The proof of the inequality is as follows.

Let $b = [(\gamma_m - I_m)z_m]$ to simplify calculations. From equation (18)

$$r^{spf} = r + (I - HH^\dagger)b$$
$$= (I - HH^\dagger)z + (I - HH^\dagger)b$$

Taking square of norm on both sides

$$\|r^{spf}\|^2 = \|r\|^2 + \| (I - HH^\dagger) b \|^2$$
$$+ 2z^T(I - HH^\dagger)^T(I - HH^\dagger)b$$
$$= \| (I - HH^\dagger)b \|^2 + 2z^T(I - HH^\dagger)^Tb$$
$$- 2z^T(I - HH^\dagger)^T(HH^\dagger)b + \|r\|^2$$
$$= \| (I - HH^\dagger)b \|^2 + 2z^T(I - HH^\dagger)^Tb$$
$$- 2z^T(HH^\dagger - HH^\dagger HH^\dagger)^Tb + \|r\|^2$$
$$= \|r\|^2 + \| (I - HH^\dagger)b \|^2$$
$$+ 2z^T(I - HH^\dagger)^Tb$$

(21)

as $HH^\dagger = HH^\dagger HH^\dagger$, due to the structure of pseudoinverse matrices. Now, note that RHS contains sum of positive numbers, the last term is positive since $(I - HH^\dagger)$ is semi-positive definite. This implies that

$$\|r^{spf}\|^2 \geq \|r\|^2$$

(22)

The above proof shows that the residual norm under the spoofing attack will be larger than that of the nominal residual norm. Semi-positive definiteness of the matrix $(I - HH^\dagger)$ is the necessary condition for detecting spoofing attacks using residual norms. This observation is used in the measurement correction in the subsequent section.

IV. Spoofing-Resilient Snapshot State Estimation (SR-SSE)

The overall architecture of our proposed method is shown in Figure 1. In the proposed method, we perform the following steps:

1) Initialization: We first estimate states using the provided PMU measurements. This step is performed to calculate the measurement residuals.
2) Spoofing Detection: The measurement residuals are passed to this algorithm to detect if the measurements are spoofed or not. We consider measurements to be spoofed if the measurement residual norm is higher than a predefined threshold.
3) Measurement Correction: Based on the output of the Spoofing Detection algorithm, the measurement correction step is performed. In this algorithm, we estimate the attack angle. Once the attack angle is estimated, we correct the PMU measurements.
4) SSE: The corrected measurements are passed to SSE to estimate power grid states.

The following sub-section provides more details to our Dpoofing Detection and Measurement Correction algorithms.

A. Spoofing Detection

In the previous section, we showed that the characteristic of measurement residual changes under GSA. Essentially, the norm of the measurement residual increases under a single or multiple GSA. We utilize this change of statistic of measurement residuals to detect GSA.

We first perform Monte-Carlo simulations for the nominal scenario to obtain the maximum measurement residual norm. We use this value as a threshold. A GSA is detected if the measurement residual norm is larger than the threshold. The residuals are obtained in our initialization step. These residuals are passed to the Spoofing Detection algorithm, where we compare the measurement residual norm with a predefined threshold. If the measurement residual norm is larger than the threshold we correct measurements in Measurement Correction algorithm, otherwise we use the measurements as it is.

B. Measurement Correction

In this section, we will describe our algorithm to correct PMU measurements and thus provide spoofing resilient states. The flow chart of the algorithm is shown in the right side of Figure 1. The measurement correction is an iterative algorithm that estimates the attack angle for a single or multiple attack scenarios. The following steps are performed in the Measurement Correction algorithm

1) Depending on the output of the Spoofing Detection algorithm, we proceed to estimate the attack angle by minimizing the expected residual norm for a given state estimate in $\text{Minimize } f(\Delta \theta, \bar{x})$.
2) If the measurements are spoofed, we first select the PMU that corresponds to the highest residual norm. In equation (22), we showed that the residual norm increases under a spoofing attack. The PMU with the highest residual norm is more likely to be spoofed. We pass the measurement residuals to the Measurement Correction algorithm.
3) We correct the measurements using the estimated attack angle by using the following equation

$$z_c = \Gamma^T(\Delta \theta)z^{spf}$$

(23)
Fig. 1: Flow chart of SR-SSE. First, we utilize residuals in the Spoofing Detection algorithm to detect GSA. Later, if GSA is detected, we correct PMU measurements in the Measurement Correction algorithm by iteratively minimizing expected measurement residuals. The corrected measurements are used in SSE that provides GSA resilient states.

where $z_c$ denotes corrected measurements.

4) The corrected measurements are used in SSE to estimate states of the power grid once again.

5) The estimated states are passed again to Minimize $f(\Delta \theta, \hat{x})$ and the inside process repeats till the states are converged. We use the norm of the states between two iterations as a criterion for convergence.

6) Once the estimated states are converged, we calculate residual norm. If the residual norm is larger than the predefined threshold, we repeat the process from step 1 of the Spoofing Detection algorithm. This step is necessary if there are multiple attacks.

The minimization of the expected residual norm is a non-convex problem. Our developed iterative algorithm is motivated by alternative minimization. In order to estimate both attack angle and state, we minimize the objective function first with respect to attack angle and then with respect to states.

C. Simulation Environment and Implementation

Real-life spoofing experiments can not be performed without proper approval from the US government. It is illegal to broadcast any signal at GPS frequency. Also, it is costly to conduct real-life experiments with PMU and the electric power grid. Due to these reasons, we decided to perform simulations. For our simulation analysis, we use MATPOWER [28] to generate steady-state data for IEEE 14 bus test case. The IEEE 14 bus test case is illustrated in Figure 2. In our simulations, we have assumed the network to be observable. The locations of the PMUs are indicated in Figure 2. The parameters required to create the admittance matrix ($H$) is provided in MATPOWER [28]. The noise covariance ($E[\eta \eta^T]$) is a diagonal matrix with standard deviation of 0.01 and 0.02 for bus voltage and line current measurements respectively. Simulation results are presented in the next section.

V. Experimental Results

We have divided experimental results into two parts: Residual Characteristics and State Estimation. We first performed Monte-Carlo simulations to show the residual characteristics under spoofing and nominal cases. This is done to validate our derived necessary condition and hypothesis that residual norm increases under GSA. In the second part, we present state estimation results for SSE and SR-SSE to verify that our SR-SSE provides spoofing resilient states.
A. Residual Characteristics

For the considered test bus case, the minimum eigenvalue of \((I - HH^\dagger)\) was found to be 0 implying that \((I - HH^\dagger)\) is semi-positive definite. Therefore we expect the residual norm to increase under GSA. We consider two scenarios for GSA: single attack and multiple attacks.

1) Single attack: The PMU measurements at bus 2 are modified according to the spoofing attack model with an attack angle of 20 degrees. We perform 1000 Monte-Carlo simulations. The Monte-Carlo simulation results for residual norms under nominal and spoofing case are shown in Figures 3 and 4.

![Fig. 3: The frequency plot of measurement residual norms under nominal, shown with blue bars, and spoofed, shown with orange bars, scenarios. Nominal and spoofed scenarios are distinctively differentiable due to the change in the distribution of the residual norms.](image)

![Fig. 4: The frequency plot of constituent PMU measurement residual norms. Each color corresponds to an individual PMU measurement residual norms. Spoofed PMU is distinguishable from others due to the largest change in the residual norm distribution, shown in orange bars.](image)

From Figure 3, it is observed that under spoofing, a large amount of bias is introduced in the overall residual norm. A predefined threshold is selected based on the maximum residual norm in the nominal case. This verifies our result proved in equation (22). It is also observed from Figure 4 that the major contribution in the overall residual norm comes from the PMU that is being spoofed. This idea is used in the Measurement Correction algorithm to minimize the nonlinear objective function.

2) Multiple attacks: The PMU measurements at bus 2, 4, and 6 are modified according to the spoofing attack model with an attack angle of 20 degrees. We perform 1000 Monte-Carlo simulations. The Monte-Carlo simulation results for residual norms under the nominal and spoofing case are shown in Figures 5 and 6.

![Fig. 5: The frequency plot of measurement residual norms under nominal, shown with blue bars, and multiple GSAs, shown with orange bars, scenarios. Nominal and multiple GSAs scenarios are distinctively differentiable due to the change in the distribution of the residual norms.](image)

![Fig. 6: The frequency plot of constituent PMU measurement residual norms. Each color corresponds to an individual PMU measurement residual norms. The largest residual norms correspond to the residuals from spoofed PMUs, shown with orange, yellow and green bars.](image)

From Figure 5 and 6, similar observations as that of previous case are made. These results verifies our equation derived in section IV.

B. State Estimation

We implement our SR-SSE method and test it for various scenarios. We consider two attack scenarios as follows:

1) Single attack: The PMU measurements at bus 2 are modified according to the spoofing attack model with an
attack angle of 20 degrees. The results for state estimation using SSE and SR-SSE are shown in Figures 7 and 8.

![Relative absolute error of estimated voltage magnitude of the buses](image)

**Fig. 7**: We compare SSE and SR-SSE under single GSA. The bar plot shows the relative absolute error between estimated states and true states of the power grid. The blue bars correspond to SR-SSE and yellow bars correspond to SSE estimates. The estimated states obtained from SR-SSE are within 1.1% of true states.

![Relative absolute error of phase angles of the buses](image)

**Fig. 8**: We compare SSE and SR-SSE under single GSA. The bar plot shows the relative absolute error between estimated phase angle and true phase angles of the power grid. The blue bars correspond to SR-SSE and yellow bars correspond to SSE estimates. The estimated states obtained from SR-SSE are within 2.5% of true phase angles.

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Voltage RMSE (pu)</th>
<th>Phase RMSE (deg)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSE</td>
<td>$1.8265 \times 10^{-2}$</td>
<td>1.1949</td>
</tr>
<tr>
<td>SR-SSE</td>
<td>$6.4098 \times 10^{-2}$</td>
<td>1.3882 \times 10^{-1}</td>
</tr>
</tbody>
</table>

**TABLE I**: SR-SSE provides an order magnitude accurate state estimates under GSA compared to SSE

Table 1 tabulates the Root Mean Squared Error (RMSE) for SSE and SR-SSE. SR-SSE estimates are an order magnitude accurate than that of SSE estimates. This is evident from the RMSE values tabulated in table I.

2) Multiple attacks: The PMU measurements at bus 2, 4, and 6 are modified according to the spoofing attack model with an attack angle of 20 degrees. The results for state estimation using SSE and SR-SSE are shown in Figures 9 and 10.

![Relative absolute error of estimated voltage magnitude of the buses](image)

**Fig. 9**: We compare SSE and SR-SSE under multiple GSAs. The bar plot shows the relative absolute error between estimated voltage magnitude and true voltage magnitude of the power grid. The blue bars correspond to SR-SSE and yellow bars correspond to SSE estimates. Compared to SSE estimates, the SR-SSE estimates are within 0.7% of the true voltage magnitudes.

![Relative absolute error of phase angles of the buses](image)

**Fig. 10**: We compare SSE and SR-SSE under multiple GSAs. The bar plot shows the relative absolute error between estimated voltage magnitude and true voltage magnitude of the power grid. The blue bars correspond to SR-SSE and yellow bars correspond to SSE estimates. Compared to SSE estimates, the SR-SSE estimates are within 2.5% of the true phase angles.

<table>
<thead>
<tr>
<th>Algorithm</th>
<th>Voltage RMSE (pu)</th>
<th>Phase RMSE (deg)</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSE</td>
<td>$2.4204 \times 10^{-2}$</td>
<td>1.0578</td>
</tr>
<tr>
<td>SR-SSE</td>
<td>$3.6936 \times 10^{-3}$</td>
<td>2.3848 \times 10^{-1}</td>
</tr>
</tbody>
</table>

**TABLE II**: SR-SSE provides an order magnitude accurate state estimates under multiple GSAs compared to SSE

Table II tabulates the RMSE for SSE and SR-SSE. Our method provide an order magnitude accurate estimates of states compared to SSE. This is shown in table II.

VI. CONCLUSIONS

We proposed a novel method for voltage phasor estimation in the power grid that is resilient to single or multiple
GSAs. The proposed method consists of two algorithm, one for GSA detection and second for measurement correction. Our Spoofing Detection algorithm is based on measurement residuals. We developed Measurement Correction algorithm to correct the PMU measurements under single or multiple attacks. We mathematically derived a necessary condition for GSA detection. We validated our necessary condition by performing Monte-Carlo simulations. We showed that the residual norm under spoofing always increases and thus is used as the detection criteria. We simulated IEEE-14 test bus case and tested various GSA scenarios. Our SR-SSE estimates are at most 2.5% of the true states under single or multiple GSAs.

ACKNOWLEDGEMENT

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000780. This paper was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use would not infringe privately owned rights. Reference herein to any specific commercial product, process, or service by trade name, trademark, manufacturer, or otherwise does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government or any agency thereof. The views and opinions of authors expressed herein do not necessarily state or reflect those of the United States Government or any agency thereof.

REFERENCES


Shubhendra Vikram Singh Chauhan received his B.Tech. and M.Tech degree in aerospace engineering from Indian Institute of Technology, Bombay, India in 2016. He received the Institute Silver Medal on graduation. He is currently pursuing his Ph.D. degree at the University of Illinois at Urbana-Champaign. His research interests include robotics, controls, state estimation for power grid and sensor fusion.

Grace Xingxin Gao is an assistant professor in the Department of Aeronautics and Astronautics at Stanford University. Before joining Stanford University, she was an assistant professor at University of Illinois at Urbana-Champaign. She obtained her Ph.D. degree at Stanford University. Her research is on robust and secure positioning, navigation and timing with applications to manned and unmanned aerial vehicles, robotics and power systems.