Online Pattern Recognition and Data Correction of PMU Data Under GPS Spoofing Attack

Ancheng Xue, Feiyang Xu, Jingsong Xu, Joe H. Chow, Shuang Leng, and Tianshu Bi

***Abstract*—Smart grids are increasingly dependent on data with the rapid development of communication and measurement. As one of the important data sources of smart grids, phasor measurement unit (PMU) is facing the high risk from attacks. Compared with cyber attacks, global position system (GPS) spoofing attacks (GSAs) are easier to implement because they can be exploited by portable devices, without the need to access the physical system. Therefore, this paper proposes a novel method for pattern recognition of GSA and an additional function of the proposed method is the data correction to the phase angle difference (PAD) deviation. Specifically, this paper analyzes the effect of GSA on PMU measurement and gives two common patterns of GSA, i.e., the step attack and the ramp attack. Then, the method of estimating the PAD deviation across a transmission line introduced by GSA is proposed, which does not require the line parameters. After obtaining the estimated PAD deviations, the pattern of GSA can be recognized by hypothesis tests and correlation coefficients according to the statistical characteristics of the estimated PAD deviations. Finally, with the case studies, the effectiveness of the proposed method is demonstrated, and the success rate of the pattern recognition and the online performance of the proposed method are analyzed.**

***Index Terms*—global position system (GPS); GPS spoofing attack (GSA), phasor measurement, pattern recognition, data correction, line parameter.**

I. Introduction

PHASOR measurement units (PMUs) are one of the important data sources of smart grids and are even called as the "grid-eye". A large number of applications have been developed based on PMU data for power system situation awareness, analysis and even control [1]-[3] such as parameter identification [4]-[6], state estimation enhancement [7], [8], system monitoring and control [9]-[11].

With the development of smart grids, the grid monitoring and control are dependent on the real-time PMU data heavily, thus making PMU data potential attack targets [12]. For attackers, it is attractive to attack the grid and drive the grid away from the optimal dispatch to gain potential economic benefits or cause grid security issues. For power systems, attacks have serious effects on many applications such as line parameter identification, state estimation, disturbance location, real-time voltage stability detection, system security control, etc., and could even lead to cascading faults and large-scale blackouts [13]-[17].

Currently, the attacks against PMU data can be divided into two types: one is the cyber attacks and the other is the global position system (GPS) spoofing attacks (GSAs). The former needs to access the physical network of the system. Besides, to bypass the existing detection mechanism of bad data, attackers need a full knowledge of the system which makes the implementation of cyber attacks more difficult. In contrast, the latter does not need to access the physical network, which makes GSAs more feasible. On the other hand, the PMU maintains synchronization via the clock signal provided by the GPS satellites. The phase angle errors can be introduced by time synchronization problem [18], [19] which makes the GPS signal vulnerable to attacks. The PMU receives a civilian GPS signal, which is easier to predict than an encrypted military signal, making the attacks less difficult. Therefore, GSAs are easier to be implemented. It can be exploited by portable devices without the need to access the system network, and it is difficult for existing GPS receivers to detect forged GPS signals [14]-[17]. In addition, it should be noted that bad weather can interfere the receiver of GPS signal and result in timing error in PMU device [20]. Because of the deviation of the crystal oscillator frequency, a linear deviation in the phase angle measurement could be introduced when GPS signal is lost [21].

The detection of GSA attracts a lot of research interests due to its high risk. Currently, the research on the detection of GSA can be divided into two categories: one is the methods based on GPS receiving device or GPS signal (physical level), and the other is the methods based on measurement data of power system (data level).

The first category of methods starts from the GPS receiver or GPS signal, and detects the GSA by analyzing the GPS carrier-to-noise ratio (C/No), the number of visible satellites,

Manuscript received: June 4, 2019; accepted: December 13, 2019. Date of CrossCheck: December 13, 2019. Date of online publication: June 2, 2020.

This work was supported by the National Key Research and Development Program of China (No. 2017YFB0902900, No. 2017YFB0902901), National Natural Science Foundation of China (No. 51627811, No. 51725702) and the Fundamental Research Funds for the Central Universities (No. 2018ZD01).

A. Xue (corresponding author), F. Xu, J. Xu, S. Leng, and T. Bi are with State Key Laboratory of Alternate Electrical Power System with Renewable Energy Sources, North China Electric Power University, Beijing 102206, China, and J. Xu is also with State Grid Ningxia Yinchuan Electric Power Company, Yinchuan 750001, China (e-mail: acxue@ncepu.edu.cn; xufeiyangxj@126.com; jansenr@126.com; s.leng@foxmail.com; tsbi@ncepu.edu.cn).

J. H. Chow is with the Department of Electrical, Computer, and Systems Engineering, Rensselaer Polytechnic Institute (RPI), Troy, NY 12180, USA (e-mail: chowj@rpi.edu).

DOI: 10.35833/MPCE.2019.000365

and the observed signal statistics [22], [23]. Most of these methods require improvements to the existing GPS receiver or additional equipment.

The second category of methods takes the GSA as one type of false data injection attack from the viewpoint of power system. Compared with the first category of methods, the second category of methods generally only needs to embed the program in the wide area measurement system (WAMS) or the control center, which is convenient to implement. In this category, the detection methods for the PMU data attacks and the bad data can be divided into four types according to the data used: ① the methods using individual PMU measurement data [24], [25]; ② the methods using PMU data at both ends of the line [26]-[28]; ③ the methods using multi-terminal PMU data [29]-[32]; ④ the methods based on system modeling or state estimation [33]-[37].

The first type of methods detects the attacks and bad data by analyzing the statistical features of individual PMU data [24], [25] and generally does not require the system topology and parameters. It should be noted that the effect of GSA is mainly reflected in the change of the relative amount for the phase angle between different buses. Local phase angle data could not reflect the change of the relative amount. Therefore, this type of methods is not suitable for the detection of GSA.

The second type of methods generally detects the attacks and bad data through the relationship between electrical quantities of the two ends of the transmission line based on the line model [26]-[28]. In detail, [26] solves the correction factors of PMU measurements based on the line model, thus realizing the detection and correction of PMU error, but it requires accurate line parameters which are difficult to acquire in practice [28]. Reference [27] proposes a detection schedule based on the screening of equivalent impedances of the transmission line. However, the data correction after the detection of attacks is not considered. Reference [28] proposes a density-based spatial clustering approach for online detection, classification, and data recovery for the manipulation attacks to PMU measurements. However, this type of attacks could not be automatically classified since only some criteria instead of specific steps are given. The advantage of this type of methods is that it is independent of system topology as the line is decoupled from the system by installing PMUs at the both ends. However, in this case, high observability redundancy is needed for the monitor system.

The third type of methods uses the multi-terminal PMU data in the system to mine the similar features between the normal PMU data to detect attacks and bad data. For example, [29] and [30] detect PMU bad data using the local outlier factor algorithm based on spatiotemporal similarity, which is made up by the standard deviation of different measurements. Reference [31] achieves the detection of GSAs based on the difference of frequency measurements of PMUs. Reference [32] utilizes the artificial neural network in association with the feature extraction technique based on principal component analysis to classify the bad data. The key of this type of methods is to use appropriate similar features to distinguish the normal data from the bad data or attacks. Thus, it may be difficult to detect the ramp attack with a small slope using the similar feature based on standard deviation.

The fourth type of methods detects the data attacks at the system level. It generally detects the bad data or attacks by state estimation or system modeling. For example, [33] and [34] develop the PMU data detection methods based on state estimation. Besides, [35] uses the cumulative sum algorithm to detect network attacks based on system modeling and state estimation. Reference [36] uses the supervisory control and data acquisition (SCADA) data, load forecasts, generation schedules, and PMU data to achieve online anomaly detection. However, the accuracy of the method is heavily based on the load forecasting which has high uncertainty itself. Reference [37] realizes the detection of GSAs by constructing a measurement matrix and using hypothesis tests to judge the detection. In summary, this type of methods generally requires a full knowledge of system configuration, which is difficult in practice. On the other hand, this type of method is difficult to be adaptive to the constantly changed topology and the state of power system.

In this paper, a method for recognizing the pattern of GSAs which belongs to the second type is proposed. The additional function of the method is the data correction of phase angle difference (PAD) of phasors. Specifically, this paper analyzes the effect of GSAs on PMU measurement and introduces two common patterns of GSA and the problem of GSA detection. Then, the method for estimating the PAD deviation introduced by GSA is proposed. Using the π-equivalent model of the transmission line, an estimation model suitable for time-varying deviation cases is established, which does not require the line parameters. Based on the estimation model, the PAD deviations can be obtained and the correction of PAD data can be realized. Based on the estimated PAD deviations, the pattern of GSAs can be automatically recognized by the hypothesis tests and correlation coefficients according to the statistical characteristics of PAD deviations.

The main contributions of this paper are summarized as follows:

1) A data correction method for the PAD deviation introduced by GSA is proposed using the PMU measurements from both ends of the transmission line.

2) An automatic pattern recognition method of GSA is proposed based on the hypothesis tests and correlation coefficients.

3) The proposed method does not require the knowledge of line parameters, which is more practical.

II. GSA and Problem Statement

This section briefly presents the effect of GSAs on PMU and introduces two common patterns of GSA and the problem of GSA detection.

When a GPS receiver of PMU is spoofed, the GPS receiver would track the forged GPS signal instead of the real signal. The existing research has shown that GSA can be implemented in two steps with low-cost and portable devices [14]-

[17]. In the first step, the GPS spoofer sends certain interference causing the GPS receiver to lose track of the real signal. Then, when the GPS receiver searches for signal, it sends a forged GPS signal. Since the characteristics of forged GPS signal is initially consistent with those of real GPS signal, the GPS receiver will track the forged GPS signal when the power of the forged signal increases. Thus, the GPS receiver has been spoofed. The effect of GSAs can be stated as follows.

A. Effect of GSAs on PMU

The synchronization of PMU is maintained via the clock signal provided by the GPS satellites. The phase angle errors can be linearly introduced by time synchronization deviation [18], [19]. If a PMU is subjected to GSA, the time stamp of the PMU could be modified and it will cause a mismatch with other PMUs. For a transmission line with PMUs installed at both ends, if a GSA is launched on one of the PMUs, it can cause a synchronization deviation Δt_{GSA} between PMUs, and the PAD deviation δ across the line can be obtained.

$$\delta = \delta_U = \delta_I = 2\pi f \Delta t_{\mathrm{GSA}} \tag{1}$$

where δ_U is the PAD deviation of voltage measurements; δ_I is the PAD deviation of current measurements; and f is the frequency of power system.

B. Two Patterns of GSA

In this paper, two patterns of GSA are considered: the step attack and the ramp attack.

1) Step attack: when the GPS receiver is subjected to a step attack, the PAD deviation will suddenly increase from 0 to a certain value, and then remain approximately unchanged. This attack pattern can be described as follows:

$$\delta = \begin{cases} 0 & t < t_1 \bigcup t > t_2 \\ a & t_1 \le t \le t_2 \end{cases} \tag{2}$$

where t_1 and t_2 are the start time and end time of the attack; and a is a constant PAD bias error introduced by the attack.

2) Ramp attack: when the GPS receiver is subjected to a ramp attack, the PAD deviation will increase or decrease linearly with time. This attack pattern can be described as follows:

$$\delta = \begin{cases} 0 & t < t_1 \bigcup t > t_2 \\ b(t - t_1) & t_1 \le t \le t_2 \end{cases} \tag{3}$$

where b is the slope of PAD deviation.

C. Problem Statement

The mathematical formulation of the pattern recognition and data correction of GSAs using PMU data at both ends of the transmission line, could be stated as follows. For a transmission line with PMUs installed at both ends, given the measured PMU data (current and voltage phasors), the PAD deviation caused by GSAs is estimated and the GSA is recognized if one of the PMUs is subjected to GSA.

III. Estimation and Correction of PAD Deviation

In [38], a method for estimating constant PAD bias error is proposed. This section extends the proposed method in [38] to obtain the time-varying PAD deviation which may be caused by a ramp attack.

A. Brief Review of Estimation Model of Constant PAD Deviation

The positive-sequence π-equivalent model of a transmission line is shown in Fig. 1, where Z is the impedance of the transmission line; Y is the admittance of the transmission line; and $\dot{U}_m$, $\dot{I}_m$, $\dot{U}_n$ and $\dot{I}_n$ are the positive-sequence voltage and current phasors at both ends of the transmission line, respectively. The voltage and current phasors of the two ends of the transmission line satisfy (4) and (5).

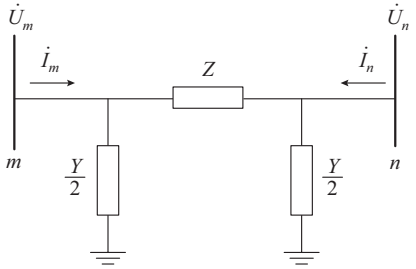

Fig. 1. π-equivalent model using lumped parameters.

$$\dot{I}_m = \frac{(\dot{U}_m - \dot{U}_n)}{Z} + \dot{U}_m \frac{Y}{2} \tag{4}$$

$$\dot{I}_n = \frac{(\dot{U}_n - \dot{U}_m)}{Z} + \dot{U}_n \frac{Y}{2} \tag{5}$$

From (4) and (5), the admittance can be expressed as (6). Note that in general, the double-circuit transmission line can be equivalent to two parallel π-equivalent models through some simplifications. Therefore, the admittance calculation formula for single-circuit lines is applicable to double-circuit lines in most cases.

$$\frac{\dot{I}_m + \dot{I}_n}{\dot{U}_m + \dot{U}_n} = \frac{Y}{2} \tag{6}$$

Assume that there is a constant PAD bias error δ of the PMUs and the measurements are noiseless. By compensating the PAD deviation on the measured PMU data of bus m, the current and voltage phasor measurements satisfy:

$$\begin{cases} \dot{U}_m = \dot{U}_{m\mathrm{M}} \mathrm{e}^{-\mathrm{j}\delta} \\ \dot{I}_m = \dot{I}_{m\mathrm{M}} \mathrm{e}^{-\mathrm{j}\delta} \\ \dfrac{\dot{I}_{m\mathrm{M}} \mathrm{e}^{-\mathrm{j}\delta} + \dot{I}_{n\mathrm{M}}}{\dot{U}_{m\mathrm{M}} \mathrm{e}^{-\mathrm{j}\delta} + \dot{U}_{n\mathrm{M}}} = \dfrac{Y}{2} \end{cases} \tag{7}$$

where $\dot{U}_{m\mathrm{M}}$, $\dot{I}_{m\mathrm{M}}$, $\dot{U}_{n\mathrm{M}}$ and $\dot{I}_{n\mathrm{M}}$ are the measured voltage and current phasors, respectively. Furthermore, assume that the admittance is constant in a short time, with the data of two snapshots, we have:

$$\frac{\dot{I}'_{m\mathrm{M}} \mathrm{e}^{-\mathrm{j}\delta} + \dot{I}'_{n\mathrm{M}}}{\dot{U}'_{m\mathrm{M}} \mathrm{e}^{-\mathrm{j}\delta} + \dot{U}'_{n\mathrm{M}}} = \frac{\dot{I}''_{m\mathrm{M}} e^{-\mathrm{j}\delta} + \dot{I}''_{n\mathrm{M}}}{\dot{U}''_{m\mathrm{M}} e^{-\mathrm{j}\delta} + \dot{U}''_{n\mathrm{M}}} = \frac{Y}{2} \tag{8}$$

where $\dot{U}'_{m\mathrm{M}}$, $\dot{I}'_{m\mathrm{M}}$, $\dot{U}'_{n\mathrm{M}}$, $\dot{I}'_{n\mathrm{M}}$ and $\dot{U}''_{m\mathrm{M}}$, $\dot{I}''_{m\mathrm{M}}$, $\dot{U}''_{n\mathrm{M}}$, $\dot{I}''_{n\mathrm{M}}$ are the PMU measurements at two snapshots.

Equation (8) contains the PMU measurements and the constant PAD bias error δ which could be estimated.

B. Estimation Model for Time-varying PAD Deviation at Different Time

The PAD deviation introduced by GSA could be time-varying. Assume the PAD deviations at snapshots t_1 and t_2 are δ_1 and δ_2, respectively. The PAD deviations δ_1 and δ_2 satisfy:

$$\delta_2 = \delta_1 + \Delta p \tag{9}$$

where Δp is a constant, i.e., the difference between δ_1 and δ_2.

Let $\delta_1 = \delta$, and assume that the line admittance Y does not change in a short time. Thus, with the PMU measurement data of t_1 and t_2 with GSA, (10) can be obtained when the active power and reactive power do not change abruptly within the synchronization time frame.

$$\frac{\dot{I}'_{m\mathrm{M}}\mathrm{e}^{\mathrm{j}\delta} + \dot{I}'_{n\mathrm{M}}}{\dot{U}'_{m\mathrm{M}}\mathrm{e}^{\mathrm{j}\delta} + \dot{U}'_{n\mathrm{M}}} = \frac{\dot{I}''_{m\mathrm{M}}\mathrm{e}^{\mathrm{j}(\delta+\Delta p)} + \dot{I}''_{n\mathrm{M}}}{\dot{U}''_{m\mathrm{M}}\mathrm{e}^{\mathrm{j}(\delta+\Delta p)} + \dot{U}''_{n\mathrm{M}}} = \frac{Y}{2} \tag{10}$$

Note that in order to ensure that (10) can be solved, the PMU data of two snapshots should not be same. It is recommended to use PMU data with different operation conditions at t_1 and t_2. Equation (10) can be rewritten as:

$$\begin{aligned}&(\dot{I}'_{m\mathrm{M}}\dot{U}''_{m\mathrm{M}} - \dot{I}''_{m\mathrm{M}}\dot{U}'_{m\mathrm{M}})\mathrm{e}^{\mathrm{j}(2\delta+\Delta p)} + (\dot{I}'_{n\mathrm{M}}\dot{U}''_{m\mathrm{M}} - \dot{I}''_{m\mathrm{M}}\dot{U}'_{m\mathrm{M}})\mathrm{e}^{\mathrm{j}(\delta+\Delta p)} + \\ &(\dot{I}'_{m\mathrm{M}}\dot{U}''_{n\mathrm{M}} - \dot{I}''_{n\mathrm{M}}\dot{U}'_{m\mathrm{M}})\mathrm{e}^{\mathrm{j}\delta} + (\dot{I}'_{n\mathrm{M}}\dot{U}''_{n\mathrm{M}} - \dot{I}''_{n\mathrm{M}}\dot{U}'_{m\mathrm{M}}) = 0\end{aligned} \tag{11}$$

Then, the real and imaginary parts of (8) can be rewritten as (12) and (13).

$$\begin{aligned}f_1 = {} & k_1\cos(2\delta+\Delta p) - k_2\sin(2\delta+\Delta p) + k_3\cos(\delta+\Delta p) - \\ & k_4\sin(\delta+\Delta p) + k_5\cos\delta - k_6\sin\delta + k_7 = 0\end{aligned} \tag{12}$$

$$\begin{aligned}f_2 = {} & k_1\sin(2\delta+\Delta p) + k_2\cos(2\delta+\Delta p) + k_3\sin(\delta+\Delta p) + \\ & k_4\cos(\delta+\Delta p) + k_5\sin\delta + k_6\cos\delta + k_8 = 0\end{aligned} \tag{13}$$

where k_1 to k_8 are coefficients given by:

$$\begin{cases} k_1 = real(\dot{I}'_{m\mathrm{M}}\dot{U}''_{m\mathrm{M}} - \dot{I}''_{m\mathrm{M}}\dot{U}'_{m\mathrm{M}}) \\ k_2 = imag(\dot{I}'_{m\mathrm{M}}\dot{U}''_{m\mathrm{M}} - \dot{I}''_{m\mathrm{M}}\dot{U}'_{m\mathrm{M}}) \\ k_3 = real(\dot{I}'_{n\mathrm{M}}\dot{U}''_{m\mathrm{M}} - \dot{I}''_{m\mathrm{M}}\dot{U}'_{m\mathrm{M}}) \\ k_4 = imag(\dot{I}'_{n\mathrm{M}}\dot{U}''_{m\mathrm{M}} - \dot{I}''_{m\mathrm{M}}\dot{U}'_{m\mathrm{M}}) \\ k_5 = real(\dot{I}'_{m\mathrm{M}}\dot{U}''_{n\mathrm{M}} - \dot{I}''_{n\mathrm{M}}\dot{U}'_{m\mathrm{M}}) \\ k_6 = imag(\dot{I}'_{m\mathrm{M}}\dot{U}''_{n\mathrm{M}} - \dot{I}''_{n\mathrm{M}}\dot{U}'_{m\mathrm{M}}) \\ k_7 = real(\dot{I}'_{n\mathrm{M}}\dot{U}''_{n\mathrm{M}} - \dot{I}''_{n\mathrm{M}}\dot{U}'_{m\mathrm{M}}) \\ k_8 = imag(\dot{I}'_{n\mathrm{M}}\dot{U}''_{n\mathrm{M}} - \dot{I}''_{n\mathrm{M}}\dot{U}'_{m\mathrm{M}}) \end{cases} \tag{14}$$

With the measured data containing measurement noise, the nonlinear quantities $(\bar{f}_1, \bar{f}_2)$ will not be exactly zero, where the symbol "-" indicates that the variable considers measurement noise.

It will be beneficial to have many measured data to eliminate the effect of the noise. With PMU measurements at $2k$ different time points, k sets of nonlinear equations $(\bar{f}_1^1, \bar{f}_2^1, \ldots, \bar{f}_1^k, \bar{f}_2^k)$ can be obtained. Thus, the estimation of the optimal value of the unknown PAD bias error δ can be formulated as:

$$\begin{cases} \min\limits_{\delta,\Delta p} J_A = \sum\limits_{i=1}^{k}\left((\bar{f}_1^i)^2 + (\bar{f}_2^i)^2\right) \\ \text{s.t. } -\pi < \delta + \Delta p \le \pi \\ \quad -\pi < \delta \le \pi \end{cases} \tag{15}$$

The objective function in (15) is the sum of squares of mismatches due to measurement noises. When the objective function is minimum, the optimal PAD deviation can be obtained. After a lot of tests, we found that the objective function is a unimodal function locally.

C. Process of Estimation and Correction of PAD Deviation

1) Estimation of PAD Deviation Using Moving Data Window

The average PAD deviation of two periods can be obtained separately by the PAD estimation method as stated in Section III-B. Then, when the GSA is detected, the PAD deviation is estimated by using moving data window as shown in Fig. 2.

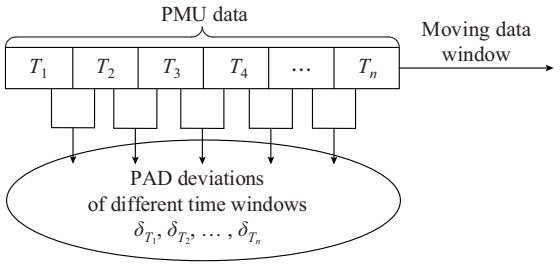

Fig. 2. Estimation of PAD deviation using moving data window.

In Fig. 2, the PAD deviations δ_{T_1} and δ_{T_2} can be estimated separately from the two windows T_1 and T_2, and then the data window will move backward each time after the estimation procedure is executed (the moving distance is the same as the data window length). The average is taken as the final estimated result for the time window which is estimated repeatedly. Finally, the PAD deviations δ_{T_1}, δ_{T_2}, ..., δ_{T_n} can be obtained. For ramp attack, the PAD deviation of each snapshot can be obtained by linear fitting through the mean value of PAD deviation of each period.

2) Start and Stop Criteria of Estimation Algorithm

In order to reduce the amount of calculation, the start and stop criteria of the estimation algorithm are used to avoid the estimation algorithm running all the time.

1) Start criterion. The start criterion can use the existing attack detection methods such as methods in [27], [28] and so on. In this paper, the attack detection method in [28] is used. It can realize the attack detection based on monitoring the change of estimated reactance caused by the attack.

Note that in [28], a check filter is designed based on exponential transformation: $\sigma_c = \mathrm{e}^{X(t+c)-X(t)}$, where $X(t)$ denotes the estimated reactance of transmission line at time t; and c is length of the data window. When there is no attack, the line parameters can be regarded as constants in a reasonably short period of time and the σ_c will be around 1 (0.95-1.05) as $X(t+c) \approx X(t)$. When the attack occurs, the σ_c will be influenced and the attack can be identified when $\sigma_c \neq 1$.

When a GSA occurs, the estimated reactance can be affected by the PAD deviation [13]. It can be detected by the

check filter, and the estimation algorithm for PAD deviation starts.

2) Stop criterion. When the estimated PAD deviations of successive l periods are close to 0, e.g., smaller than 0.1°, the estimation algorithm stops.

3) Process of Estimation of PAD Deviation

According to the above discussion, the flow chart of the online estimation of the PAD deviation is shown in Fig. 3, where l is set to 2.

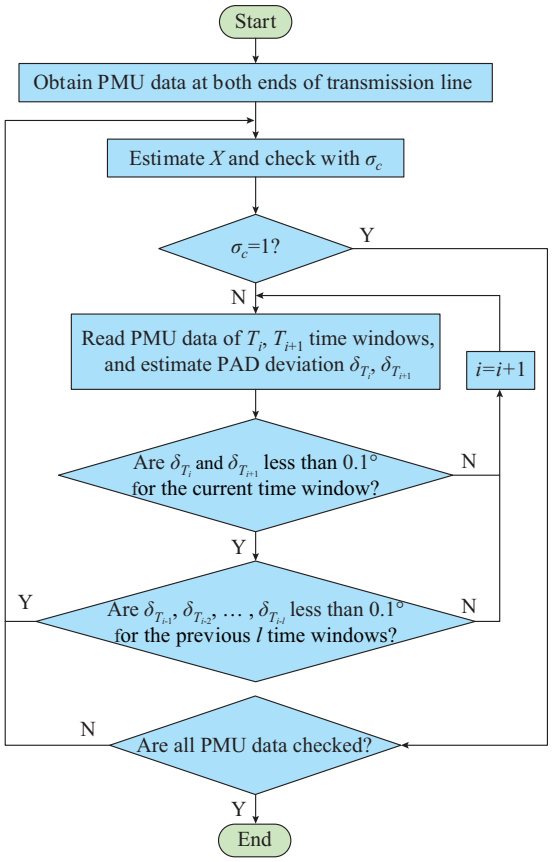

Fig. 3. Flow chart of GSA detection and PAD deviation estimation.

Through the above steps, the PAD deviation can be estimated, and the correction of PAD deviation of the measured data at both ends can be realized.

4) Comments on Proposed Method

The advantage of the proposed method is that it does not need to know the value of transmission line parameters. It only uses the PMU measurements at both ends of the transmission line to estimate the PAD deviations. Thus, the method is practical and simple.

Although the proposed method only shows the case where one of the substations at both ends of the transmission line suffers GSA, it is still effective in the case where the substations at both ends of the transmission line are all attacked, because the amount estimated by the proposed method is the PAD deviation, which is a relative quantity. The phase angle deviation introduced by GSAs at both ends of the transmission line can be converted into PAD deviation which could be estimated.

For the proposed method, it is assumed that the admittance is constant during a short time. However, it will stand for a lot of situations.

In addition, to ensure that (10) can be solved, the PMU data of two snapshots should not be same. It is recommended to use PMU data with different operation conditions, i.e., different operation conditions of t_1 and t_2.

IV. Pattern Recognition of GSA

A. Hypothesis Tests for PAD Deviations

Once the PAD deviations are obtained with the proposed method over a number of time windows, the statistical characteristics of the PAD deviation can be analyzed. As stated in Section II-B, if it is subjected to a step attack, the PAD deviation will be almost constant, thus the obtained PAD deviations will have a mean value deviated from zero and a small variance. If it is subjected to a ramp attack, the PAD deviations can change linearly with time. The mean value and variance of PAD deviations will deviate from zero. If it is subjected to a random attack or hybrid attack, the mean value and/or the variance may be large. In this paper, the traditional t-test and χ^2-test are used to analyze the property of mean and variance, and the correlation coefficient is used to measure the linearity of PAD deviations.

1) Test 1: Test of Mean Value of PAD Deviations (t-test)

From the central limit theorem, the PAD deviations approximate a normal distribution without attack under the condition that the sampled data are sufficiently large. Assume that normal PAD deviations satisfy the normal distribution $N(\mu_0, \sigma_0^2)$, where $\mu_0 = 0$, σ_0 is the standard deviation of normal phase angle measurement determined by PMUs. Then, the t-distribution as (16) can be used to test the mean value. The hypothesis test can be given as (17), and the decision rule is shown in (18) with a determined significance level α.

$$t_s = \frac{\bar{X}_s - \mu_0}{S/\sqrt{n_s}} \tag{16}$$

$$\begin{cases} H_0: \mu = \mu_0 \\ H_1: \mu \neq \mu_0 \end{cases} \tag{17}$$

$$\begin{cases} H_0: |t| = \left| \dfrac{\bar{X}_s - \mu_0}{S/\sqrt{n_s}} \right| < \lambda_1 = t_{\alpha/2}(n_s - 1) \\ H_1: |t| = \left| \dfrac{\bar{X}_s - \mu_0}{S/\sqrt{n_s}} \right| \geq \lambda_1 = t_{\alpha/2}(n_s - 1) \end{cases} \tag{18}$$

where t_s is the test statistic of test 1; $\bar{X}_s$ is the mean value of the PAD deviation samples; S is the standard deviation of the samples; n_s is the number of the samples; μ is the mean value of the t-distribution; and $t_{\alpha/2}(n_s - 1)$ is available in the t-distribution table.

As shown in Fig. 4, if the observation falls into the rejection domain at a certain significance level, the PMU for that period is considered to have a high probability of being attacked. Otherwise, it may not be attacked or is subjected to

other types of attacks with a mean value close to zero.

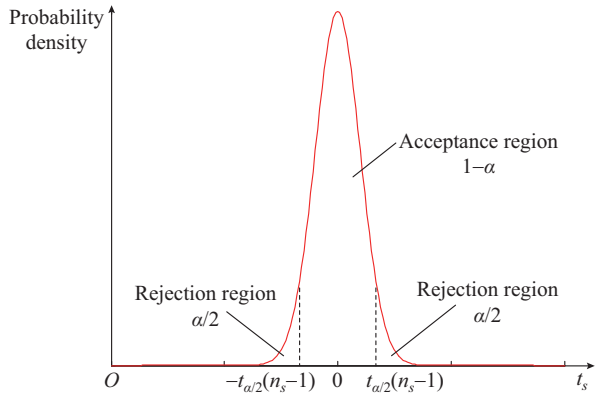

Fig.4. Schematic diagram of test 1.

2) Test 2: Test of Variance of PAD Deviations (χ^2-test)

As mentioned earlier, the variance of normal PAD deviations should be close to a constant σ_0^2 determined by PMUs. When it is not attacked or during a step attack, the variance of PAD deviations will be close to 0 which is quite different from subjecting to ramp attack or hybrid attack. Therefore, a unilateral hypothesis test as (19) can be used to test the variance. The hypothesis test can be given as (20), and the decision rule is shown in (21) with the determined significance level α.

$$\chi^2 = (n_s - 1)S^2/\sigma_0^2 \tag{19}$$

$$\begin{cases} H_0: \sigma^2 < \sigma_0^2 \\ H_1: \sigma^2 \geq \sigma_0^2 \end{cases} \tag{20}$$

$$\begin{cases} H_0: (n_s - 1)S^2/\sigma_0^2 < \lambda_2 = \chi_\alpha^2(n_s - 1) \\ H_1: (n_s - 1)S^2/\sigma_0^2 \geq \lambda_2 = \chi_\alpha^2(n_s - 1) \end{cases} \tag{21}$$

where χ^2 is the test statistic of test 2; σ is the standard deviation of the χ^2-distribution; and $\chi_\alpha^2(n_s - 1)$ is available in the χ^2-distribution table.

As shown in Fig. 5, if the observation falls into the rejection region at a certain significance level, then it is believed that the PAD deviations of PMUs fluctuate greatly. There is a high probability of being subjected to a ramp attack or a hybrid attack; otherwise, it may not be attacked or is subjected to step attack.

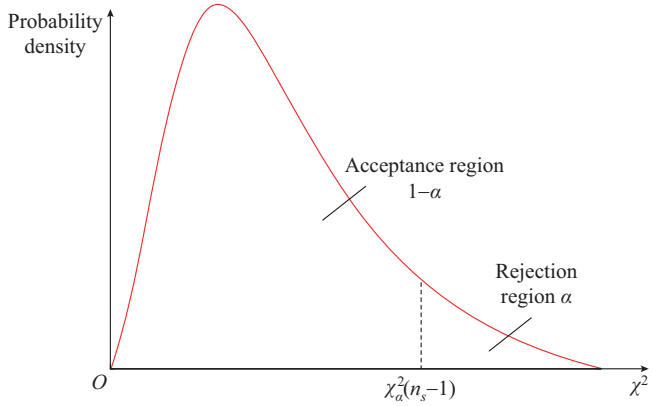

Fig. 5. Schematic diagram of test 2.

3) Test 3: Detection of Linearity of PAD Deviations

With the ramp attack, the PAD deviation linearly correlates with the time. Therefore, the correlation coefficient can be used to test whether the PAD deviation is linear with time. The definition of the correlation coefficient is as follows:

$$\rho(x,y) = \frac{Cov(x,y)}{\sqrt{Var(x)Var(y)}} \tag{21}$$

where $Cov(x,y)$ is the covariance of variables x and y; and $Var(x)$, $Var(y)$ are the variances of x and y, respectively.

In practical problems, when $\rho(x,y)$ is greater than 0.8, there is a linear relationship between the two variables. Therefore, we select 0.8 as the threshold for linearity detection. If the correlation coefficient between PAD deviations and time is greater than 0.8, there is a greater probability be subjected to ramp attack.

B. Process of Pattern Recognition of GSAs

Based on the characteristics of PAD deviations under GSAs in Section II-B, the pattern of GSA can be recognized with the tests. The corresponding results are shown in Table I. The recognition process of GPAs is shown in Fig. 6.

TABLE I
RECOGNITION OF GSA PATTERNS

Case	Test result	GSA pattern
1	$\mu=\mu_0, \sigma^2<\sigma_0^2$	No attack
2	$\mu=\mu_0, \sigma^2\geq\sigma_0^2$	Other attacks
3	$\mu\neq\mu_0, \sigma^2<\sigma_0^2$	Step attack
4	$\mu\neq\mu_0, \sigma^2\geq\sigma_0^2, \lvert\rho(X,Y)\rvert\geq 0.8$	Ramp attack
5	$\mu\neq\mu_0, \sigma^2\geq\sigma_0^2, \lvert\rho(X,Y)\rvert< 0.8$	Other attacks

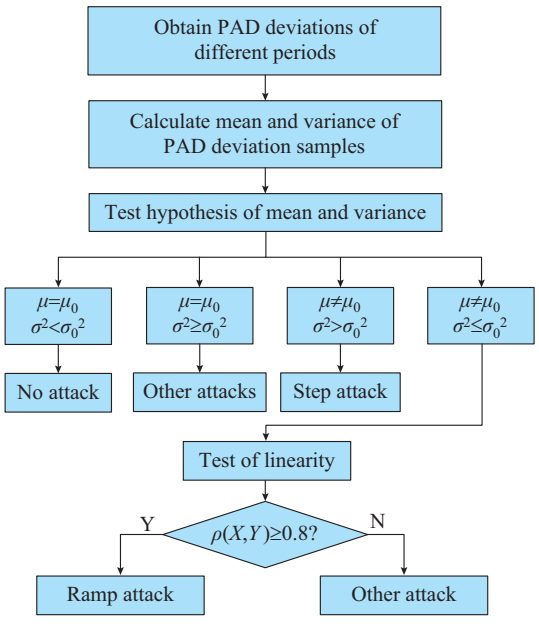

Fig. 6. Flow chart of GSA recognition.

As shown in Fig. 6, in the recognition process, tests 1 and 2 can be performed simultaneously. If the test result is one

of cases 1-3, no subsequent detection is performed and the result can be directly output. If the result is $\mu \neq \mu_0$, $\sigma^2 \geq \sigma_0^2$, the test 3 is performed to determine whether the attack is ramp attack or other attack.

In summary, the recognition of GSA and the correction of PAD deviations can be realized by the proposed method.

V. Case Study

In this section, a 500 kV single-circuit transmission line is modeled in PSCAD. The step attack and ramp attack are performed to verify the proposed method. Besides, the success rate of the pattern recognition with different degrees of attacks and the online performance of the whole scheme are analyzed.

A. Model Setting and Data Acquisition

A 500 kV single-circuit transmission line is modeled in PSCAD where the length is 200 km, the resistance is 2.666 Ω, the reactance is 40.4408 Ω, and the susceptance is 46.542 μS. The system frequency is 50 Hz. The sampling period of PMU data is 20 ms. Multiple sets of steady-state measurements (each set contains 10 s data) under different power flow conditions are obtained by changing the load. The data contains the amplitudes and phase angles of voltage and current at both ends of the transmission line.

B. Estimation of PAD Deviations

For the step attack and ramp attack described in Section II, two cases are set to verify the estimation method. In this paper, the length of the time window is set to 10 s (data of 500 snapshots).

1) Case 1: assume that the PMU at bus m is subjected to step attack with 25 μs synchronization deviation, so the phase angle error 0.450º is added to the phase angles of voltage and current at bus m of the transmission line. Besides, a Gaussian distribution noise with mean value of zero and a standard deviation of 0.2% is added to the amplitude; and a Gaussian distribution noise with mean value of zero and a standard deviation of 0.05° is added to the phase angle. The estimated results in the first 5 time windows, the average, median, and maximum error of the results of all 20 time windows are shown in Table II, and the overall estimated results are shown in Fig. 7.

TABLE II
Estimated Results of PAD Deviations Under Step Attack

Time window	Set value (°)	Estimated result (°)	
		No noise	Noise added
1	0.450	0.450	0.4338
2	0.450	0.450	0.4374
3	0.450	0.450	0.4140
4	0.450	0.450	0.4482
5	0.450	0.450	0.4464
Average value	0.450	0.450	0.4433
Median value	0.450	0.450	0.4455
Maximum error		0	0.0360

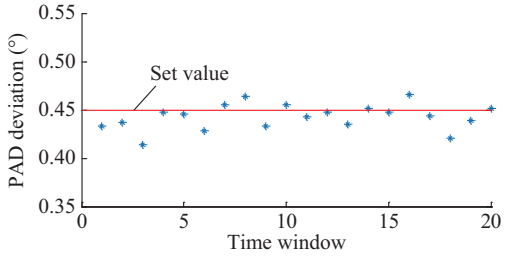

Fig. 7. Estimated result of PAD deviation with noise under step attack.

In Fig. 7, the estimated results of each period are closer to the set value with noise added, i.e., the proposed method can effectively estimate the PAD deviation of PMUs at both ends of the line.

2) Case 2: assume that the PMU at bus m is subjected to ramp attack. The first-snapshot phase angle error ζ at bus m of the time window 1 is 0.252° (14 μs synchronization deviation), the slope of the ramp attack is 0.0036 °/s (0.2 μs/s). Besides, the noise which is the same to that in case 1 is added. The estimated results of the first 5 time windows, the first-snapshot phase angle error ζ and the slope of the attack are shown in Table III and the overall estimated results are shown in Fig. 8. Note that the result of PAD deviations during a time window is the estimation for the average of PAD deviations during the time window.

TABLE III
Estimated Results of PAD Deviation Under Ramp Attack

Time window	Set value (°)	Estimated result (°)	
		No noise	Noise added
1	0.270	0.270	0.251
2	0.306	0.306	0.344
3	0.342	0.342	0.336
4	0.378	0.378	0.371
5	0.414	0.414	0.409
ζ (°)	0.2520	0.2520	0.2384
Slope (°/s)	0.00360	0.00360	0.00348

As shown in Table III, without noise, the PAD deviations can be accurately estimated. With noise added, though the estimated results deviate from the actual value, they are within the acceptable range.

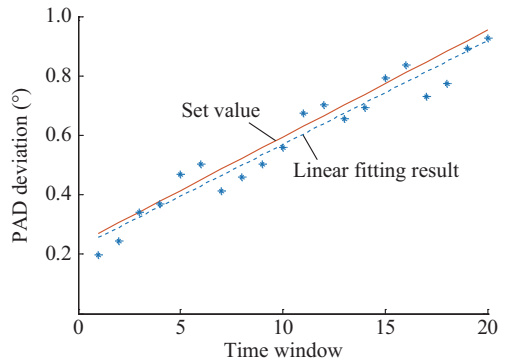

Fig. 8. Estimated results of PAD deviation with noise under ramp attack.

C. Pattern Recognition for GSA

In this subsection, the estimated results of cases 1 and 2 in Section V-B are used to verify the effectiveness of the proposed GSA recognition method.

In this case study, the number of samples n_s is 20; the significance level α is set to 0.05; μ_0 is set to 0 in test 1; σ_0 is set to 0.10 in test 2. Thus, the threshold of the rejection region can be determined: $\lambda_1 = 2.093$ (test 1), $\lambda_2 = 30.144$ (test 2). The recognition results are shown in Table IV.

TABLE IV
RECOGNITION RESULTS OF GSAS

Test	Threshold	Recognition result	
		Case 1	Case 2
Test 1	2.093	151.01	12.04
Test 2	30.144	0.32	85.71
Test 3	0.800		0.93
Test result		Step attack	Ramp attack

As shown in Table IV, the recognition of step attack only requires tests 1 and 2, and can be completed without test 3. The recognition of ramp attack requires tests 1, 2 and 3. Besides, it is shown that the difference of the statistical characteristics between step attack and ramp attack is obviously distinguishable. The GSA can be recognized by the proposed method accurately.

D. Success Rate Test of Pattern Recognition

In this subsection, the success rate of the pattern recognition with different degrees of GSAs is tested.

The noise which is the same as that in case 1 in Section V-B is added and different degrees of attacks are performed. In order to fully test the success rate, the stop criterion of the estimation algorithm does not work in the test. The setup of the recognition is the same as that in Section V-C. Each attack has been tested 100 times (different noises in the same distribution are added at each time) and the success rate of recognition are shown in Tables V and VI. Note that in the ramp attack, the first-snapshot PAD deviation of the first time window is 0.252° (14 μs synchronization deviation), which is the same as that in case 2 in Section V-B.

TABLE V
SUCCESS RATE OF RECOGNITION UNDER DIFFERENT DEGREES OF STEP ATTACKS

Step value (μs)	Success rate of recognition (%)		
	Ramp attack	Step attack	Other attacks
2	0	100	0
4	0	100	0
6	0	100	0
8	0	100	0

In Tables V and VI, the success rate of the proposed pattern recognition for step attack is 100% even with 2 μs step attack. For the ramp attack, when the slope of the ramp attack is 0.100 μs/s, the deviation of PAD caused by the attack is basically the same as that caused by the noise, resulting in a small standard deviation of some estimation results of PAD deviations. Therefore, some ramp attacks are misrecognized as step attacks. With the increase of the slope, the success rate increases. For the ramp attack with a slope of 0.150 μs/s and above, the success rate reaches 100%. In summary, for the step attacks and most of the ramp attacks whose slope is equal to or greater than 0.15 μs/s, the success rate of the proposed pattern recognition is very high.

TABLE VI
SUCCESS RATE OF RECOGNITION UNDER DIFFERENT DEGREES OF RAMP ATTACKS

Slope (μs/s)	Success rate of recognition (%)		
	Ramp attack	Step attack	Other attacks
0.100	34	66	0
0.125	79	21	0
0.150	100	0	0
0.200	100	0	0

E. Online Performance Analysis

In this subsection, the online application performance of the whole scheme is analyzed.

In the proposed scheme, the time cost can be divided into four parts, i.e., the attack detection delay part, the data acquisition part, the PAD deviation estimation part and the pattern recognition part. Among them, the data acquisition and the PAD deviation estimation can run in parallel.

The simulations are performed on the computer with Intel Core i5-8400 2.8 GHz, running in the environment of MATLAB. Multiple tests show that: the average delay of the attack detection for the ramp attack is about 0.8 s, while it is less than 0.1 s for the step attack; the time cost of data acquisition is equal to the length of the moving time window (500 snapshots) which is 10 s; the average execution time of PAD deviation estimation for each time window is 1.38 s; the average execution time of pattern recognition is about 0.006 s.

As mentioned above, after the attack is detected, the PAD deviation estimation can be completed before the data of next time window come. Thus, the application of the proposed method could be "online" with a time delay of seconds (limited to 2 s in the simulations).

VI. CONCLUSION

For GSAs on the PMU, this paper proposes a method for online pattern recognition of GSAs with the additional benefit of PAD data correction. In the paper, the effect of GSA on PMU measurement is analyzed and two common patterns of GSA are described. Besides, a method for estimating the time-varying PAD deviations introduced by GSA is presented. The value of the parameters of transmission line could be ignored and only the PMU measurements at both ends of the transmission line are used to estimate the PAD deviations. With the estimated PAD deviations of different time windows, the pattern of GSA can be recognized by hypothesis tests and correlation coefficients. In the case studies, the

estimation effectiveness and reliability of the PAD deviation are demonstrated and the success rate of the pattern recognition and the online performance of the method are analyzed. The results show that the success rate of the proposed pattern recognition is high for the step attack whose step value is greater than 2 μs, and also for the ramp attacks whose slope is greater than 0.15 μs/s. The application of the proposed method could be "online" with a time delay of seconds. Besides, the corrected PMU data can be used for the power system analysis and control application such as line parameter identification, state estimation.

In the proposed method, the practically acceptable assumption that the line admittance is unchanged during a short period is assumed. Besides, in the proposed method, the determination of the attack position of GSA could not be achieved by one line as the effect of GSA is measured by PAD, which is a relative value. With other information, e.g., another line without attack connecting the same bus, the attack position of GSA may be determined by comparing the PAD deviations of two lines.

REFERENCES

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

[2] A. G. Phadke and T. Bi, "Phasor measurement units, WAMS, and their applications in protection and control of power systems," *Journal of Modern Power Systems and Clean Energy*, vol. 6, no. 4, pp. 619-629, Jul. 2018.

[3] D. L. R. Jaime, V. Centeno, J. S. Thorp *et al*., "Synchronized phasor measurement applications in power systems," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, Jun. 2010.

[4] S. Gajare, A. K. Pradhan, and V. Terzija, "A method for accurate parameter estimation of series compensated transmission lines using synchronized data," *IEEE Transactions on Power Systems*, vol. 32, no. 6, pp. 4843-4850, Nov. 2017.

[5] M. Asprou and E. Kyriakides, "Identification and estimation of erroneous transmission line parameters using PMU measurements," *IEEE Transactions on Power Delivery*, vol. 32, no. 6, pp. 2510-2519, Dec. 2017.

[6] C. Wang, Z. Qin, Y. Hou *et al*., "Multi-area dynamic state estimation with PMU measurements by an equality constrained extended Kalman filter," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 900-910, Mar. 2018.

[7] A. Rendon, C. R. Fuerte, and J. G. Calderon, "SCADA and PMU measurements for improving power system state estimation," *IEEE Latin America Transactions*, vol. 13, no. 7, pp. 2245-2251, Jul. 2015.

[8] J. Zhao, L. Mili, and F. Milano, "Robust frequency divider for power system online monitoring and control," *IEEE Transactions on Power Systems*, vol. 33, no. 4, pp. 4414-4423, Jul. 2018.

[9] G. C. Patil and A. G. Thosar, "Application of synchrophasor measurements using PMU for modern power systems monitoring and control," in *Proceedings of 2017 International Conference on Computation of Power, Energy Information and Commuincation (ICCPEIC)*, Melmaruvathur, Mar. 2017, pp. 754-760.

[10] M. U. Usman and M. O. Faruque, "Applications of synchrophasor technologies in power systems" *Journal of Modern Power Systems and Clean Energy*, vol. 7, no. 2, pp. 211-226, Mar. 2019.

[11] I. Zenelis and X. Wang, "Wide-area damping control for interarea oscillations in power grids based on PMU measurements," *IEEE Control Systems Letters*, vol. 2, no. 4, pp. 719-724, Oct. 2018.

[12] A. Sundararajan, T. khan, A. Moghadasi *et al*., "Survey on synchrophasor data quality and cybersecurity challenges, and evaluation of their interdependencies," *Journal of Modern Power Systems and Clean Energy*, vol. 7, no. 3, pp. 449-467, May 2019.

[13] A. Xue, F. Xu, K. E. Martin *et al*., "Linear approximations for the influence of phasor angle difference errors on line parameter calculation," *IEEE Transactions on Power Systems*, vol. 34, no. 5, pp. 3455-3464, Sept. 2019.

[14] 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, Oct. 2012.

[15] S. Gong, Z. Zhang, M. Trinkle *et al*., "GPS spoofing based time stamp attack on real time wide area monitoring in smart grid," in *Proceedings of 2012 IEEE Third International Conference on Smart Grid Communications*, Tainan, China, Nov. 2012, pp. 300-305.

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

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

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

[19] T. Bi, J. Guo, K. Xu *et al*., "The impact of time synchronization deviation on the performance of synchrophasor measurements and wide area damping control," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1545-1552, Jul. 2017.

[20] T. Gregorius and G. Blewitt. (1998, Jan.). The effect of weather fronts on GPS measurements. [Online]. Available: http://www2. unb. ca/gge/Resources/gpsworld.may98.pdf

[21] W. Yao, Y. Liu, D. Zhou *et al*., "Impact of GPS signal loss and its mitigation in power system synchronized measurement devices," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 1141-1149, Mar. 2018.

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

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

[24] M. Zhou, Y. Wang, A. K. Srivastava *et al*., "Ensemble based algorithm for synchrophasor data anomaly detection," *IEEE Transactions on Smart Grid*, vol. 10 no. 3, pp. 2979-2988, May 2019.

[25] Y. Chen, W. Chen, W. Yao *et al*., "Rapid identification and recovery of wrong WAMS data," *Electric Power Automation Equipment*, vol. 36, no. 12, pp. 99-105, Dec. 2016.

[26] D. Shi, D. J. Tylavsky, and N. Logic, "An adaptive method for detection and correction of errors in PMU measurements," *IEEE Transactions on Smart Grid*, vol. 3, no. 4, pp. 1575-1583, Dec. 2012.

[27] S. Pal, B. Sikdar, and J. H. Chow, "Classification and detection of PMU data manipulation attacks using transmission line parameters," *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 5057-5066, Sept. 2018.

[28] X. Wang, D. Shi, J. Wang *et al*., "Online identification and data recovery for PMU data manipulation attack," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 5889-5898, Nov. 2019.

[29] I. Idehen and T. Overbye, "A similarity-based PMU error detection technique," in *Proceedings of 2017 19th International Conference on Intelligent System Application to Power Systems (ISAP)*, San Antonio, USA, Sept. 2017, pp. 1-6.

[30] M. Wu and L. Xie, "Online detection of low-quality synchrophasor measurements: a data-driven approach," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 2817-2827, Jul. 2017.

[31] A. K. Mattei, W. M. Grady, P. J. Caspary *et al*., "Detection of time spoofing attacks on GPS synchronized phasor measurement units," in *Proceedings of 2016 69th Annual Conference for Protective Relay Engineers (CPRE)*, College Station, USA, Apr. 2016, pp. 1-8.

[32] K. Mahapatra, N. R. Chaudhuri, and R. Kavasseri, "Online bad data outlier detection in PMU measurements using PCA feature-driven ANN classifier," in *Proceedings of 2017 IEEE PES General Meeting*, Chicago, USA, Jul. 2017, pp. 1-5.

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

[34] M. Yasinzadeh and M. Akhbari, "Detection of PMU spoofing in power grid based on phasor measurement analysis," *IET Generation, Transmission & Distribution*, vol. 12, no. 9, pp. 1980-1987, May 2018.

[35] M. N. Kurt, Y. Yılmaz, and X. Wang, "Real-time detection of hybrid and stealthy cyber-attacks in smart grid," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 2, pp. 498-513, Feb. 2019.

[36] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Online detection of stealthy false data injection attacks in power system state estimation," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 1636-1646, May

2018.
[37] P. Pradhan, K. Nagananda, P. Venkitasubramaniam *et al*., "GPS spoofing attack characterization and detection in smart grids," in *Proceedings of 2016 IEEE Conference on Communications and Network Security (CNS)*, Philadelphia, USA, pp. 391-395, Oct. 2016.
[38] A. Xue, F. Xu, J. Xu *et al*., "Correction of phasor measurements independent of transmission line parameters," *IEEE Transactions on Smart Grid*, vol. 11, no. 1, Jan. 2020, pp. 346-356.

Ancheng Xue received the B.Sc. degree in applied mathematics and the Ph. D. degree in electrical engineering both from Tsinghua University, Beijing, China, in 2001 and 2006, respectively. He was a post-doctor at the Institute of System Science, Chinese Academy of Sciences, Beijing, China. Currently, he is a professor with the School of Electrical and Electronic Engineering, North China Electric Power University, Beijing, China, where he joined in March 2008. His research interests include data-driven power system analysis, control and protection.

Feiyang Xu is currently pursuing his Ph.D. degree at North China Electric Power University, Beijing, China, where he obtained the B. Sc. degree in electrical engineering. His research interests include the applications of PMU and the detection and correction of low-quality data.

Jingsong Xu received his M. S. degree from North China Electric Power University, Beijing, China, in 2019. He joined the State Grid Ningxia Yinchuan Electric Power Company, Yinchuan, China, in August 2019. His research interest is the application of PMU in power systems.

Joe H. Chow received the M. S. and Ph. D. degrees from the University of Illinois, Urbana-Champaign, USA. After working in the General Electric power system business in Schenectady, USA, he joined Rensselaer Polytechnic Institute, Troy, USA, in 1987, where he is an institute professor of electrical, computer, and systems engineering. He is a member of the U. S. National Academy of Engineering. His research interests include power system dynamics and control and synchronized phasor data.

Shuang Leng is currently pursuing his M.S. degree at North China Electric Power University, Beijing, China. In the same university, he got his B.S degree in electrical engineering. His research interests are the PMU data quality and PMU application.

Tianshu Bi received the Ph. D. degree from the Department of Electrical and Electronic Engineering, University of Hong Kong, Hong Kong, China, in 2002. She is currently a professor at North China Electric Power University, Beijing, China. Her research interests include power system protection and control, and PMU techniques and application.