Detection Techniques for Data-Level Spoofing in GPS-Based Phasor Measurement Units

Fu Zhu[1], Amr Youssef[2] and Walaa Hamouda[1]
[1]Department of Electrical and Computer Engineering
[2]Concordia Institute for Information Systems Engineering
Concordia University, Montreal, QC, Canada
email: {fu_zh, youssef, hamouda}@encs.concordia.ca

***Abstract*—To face the ever growing demand of electricity, the smart power grid, which includes a variety of operational and energy measures, aims at providing safe and reliable power supply, effective use of renewable energy, and better efficiency of the overall power grid. Phasor Measurement Units (PMUs) are important components of the smart grid Wide Area Measurement Systems (WAMS). A PMU is a transducer that converts the three-phase analog voltage or current signals into synchronized phasor measurements, known as synchrophasors. Typically, PMUs utilize Global Positioning System (GPS) reference source to provide the required synchronization across the wide geographical areas. On the other hand, civil GPS receivers are vulnerable to a number of different attacks such as jamming and spoofing, which can lead to inaccurate PMU measurements and consequently compromise the state estimation in the electric power grid. In this paper, we propose two countermeasures against GPS spoofing attacks in PMUs. In particular, we utilize the fact that in GPS-based PMUs, unlike most of the GPS applications, the position of the PMU receivers are already fixed and known. Our first technique employs an algorithm that accurately predicts the number of theoretically visible GPS satellites from a given position on earth; if the GPS receiver detects satellites which should not be visible at the time, this signifies a spoofing attempt. The second technique is an anomaly-based detection method which assumes that the malicious errors in GPS time solution are unlikely to be consistent with the expected statistics of the typical receiver clock. The effectiveness of the proposed techniques are confirmed by simulations.**

I. Introduction

The smart power grid technology provides two way dialogue where electricity and information can be exchanged between the utility station and its customers [1]. It integrates advanced sensing and measurement technology, networks of communication, control, computers and automation to achieve more efficient, reliable, secure and greener targets. Efficient power transmission and distribution in the smart grid benefit from the measurements collected by a phasor network which consists of Phasor Measurement Units (PMUs) distributed throughout the grid [2]. These PMUs are transducers that convert the three-phase analog voltage or current signal into synchronized phasor measurements, known as synchrophasors. Traditionally, Supervisory-Control And Data-Acquisition (SCADA) systems feed measurements to state estimators every 3-5 seconds, which is not frequent enough to capture the system dynamics. The utilization of PMUs has revealed a promising capability for tracking power system state in real-time [3]. PMUs can measure 50/60 Hz AC waveforms typically at a rate of 2880 samples per second for 60Hz systems [4]. To achieve such a global time reference, time synchronization across PMUs is crucial for maintaining an accurate measurement of phase. Samples from PMUs are time-stamped with a Global Positioning System (GPS) reference source with 1 microsecond accuracy which allows capturing a wide area snapshot of the power system [7].

Unencrypted civil GPS signals are publicly available with weak received power, which renders the GPS receivers vulnerable to jamming and spoofing attacks. The signals sent by the GPS satellites at the GPS receiver will be affected by the jammers high power interfering signal at the same frequency. Another security threat could arise if the attacker manages to spoof the GPS signals. In this case, the GPS receiver will provide an inaccurate time stamp for the PMU which will affect the phasor measurements of the power system. Incorrect time stamping of phasor measurements data impacts the reliability of applications such as distance line protection and voltage stability monitoring [8]. Previous works on the impact of incorrect time stamps of the PMUs show that the attacks could cause erroneous estimates of the actual power load and trigger false warnings of power instability [9]. Therefore, in order to improve the robustness of power grid monitoring, security measures are needed to protect the GPS receiver from theses attacks.

Previous countermeasures against GPS spoofing are based on signal strength [10], incorporation of external hardware such as an inertial measurement unit [11], use of multiple antennas [12], moving the receiver antennas [13], or cryptographic techniques [14]. However, according to the peculiarities of GPS-based PMU, the positions of the receivers are already known. Here we propose two spoofing detection techniques to enhance the robustness of the GPS-based receiver of PMUs; namely prediction of the visible satellites and anomaly-based detection.

The remainder of this paper is organized as follows. Section II explains the basic background of the GPS-based PMU. Section 4 introduces our first proposed countermeasure against the attack from the GPS simulator. Section IV presents the second algorithm which we refer to as joint checking algorithm. Finally, conclusions are presented in the last section.

978-1-5090-1743-0/16/$31.00 ©2016 IEEE

II. Overview of GPS-based PMU

A. Phasor Measurement Units

PMUs are power system devices, which use synchronization signals from the GPS satellites to provide real-time positive sequence phasor voltages and currents measured at a given station [15], [16]. Figure 1 shows a basic hardware block diagram of the PMU. The analog inputs are the voltages and currents obtained from the secondary winding of the three phase voltage and current transformers. The GPS receiver provides 1-PPS (Pulse per second) to the phase lock oscillator of PMU, the l-PPS signal is usually divided by the oscillator into the required number of pulses per second for sampling of the analog signals [15]. This GPS system is designed primarily for navigational purposes, but it furnishes a common-access timing pulse, which is accurate to within 1 microsecond at any location on earth [15]. The phasor microprocessor calculates the phasor using digital signal processing techniques.

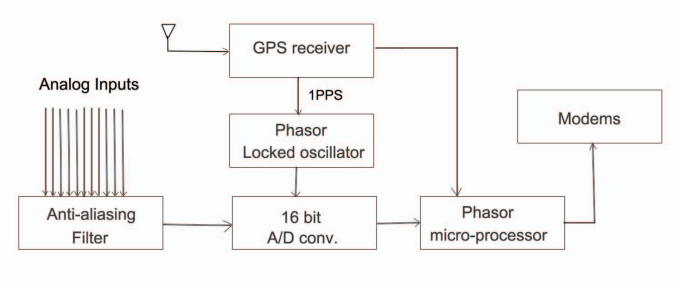

Fig. 1. Block diagram of a PMU [5]

B. Global positioning system

The GPS system is a space-based navigation system that provides location and time information on or near the earth where there is an unobstructed line of sight to four or more GPS satellites out of the 32 operational GPS satellites that are designed to be available 95% of the time [17]. Each GPS satellite contains multiple atomic clocks that provide very precise time data to the GPS signals [19]. These satellites continuously transmit radio ranging signals which contain navigation message and two types of codes: unencrypted C/A (Coarse/Acquisition) code for civil use, and encrypted P(Y) (Precision) code which is reserved for military applications. The information needed by the GPS receiver to calculate the satellite position and clock bias is included in the navigation data.

The GPS receiver must receive at least four satellites signals to solve for the position and time. The distance obtained from this step is referred to pseudo-range as it contains error in the computation. Figure 2 depicts the basic procedure of how the position and time are calculated by the GPS receiver. The preamplifier/down-converter converts the raw radio frequency (RF) signal into intermediate frequency (IF) samples as a preparation for the tracking part. The code and carrier tracking part tracks each visible satellite and generates the local C/A code for the receiver to calculate the pseudo range and further to the decoding module to extract the navigation data.

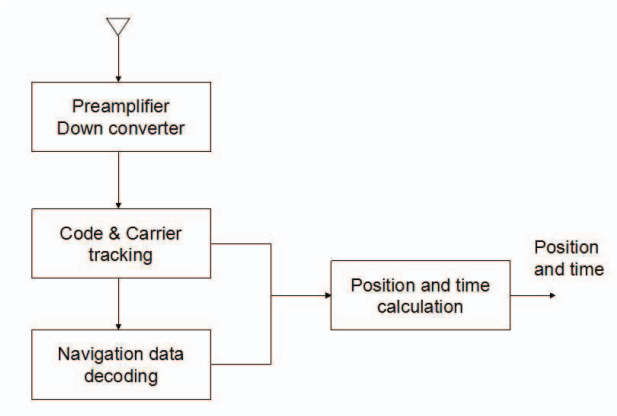

Fig. 2. Block diagram of GPS receiver [6]

Let ρ_i and d_i denote the i^{th} satellite's pseudo range and true range. Let x_i, y_i, and z_i denote the i^{th} satellite's ECEF (Earth-Centered, Earth-Fixed) coordinates Let x_{rec}, y_{rec}, z_{rec}, be the receiver's ECEF coordinates, and let b_i denote the receiver clock offset. Then, we have

$$\begin{aligned} \rho_i &= d_i + c(b_{rec} + b_i) + \varepsilon_i \\ d_i &= \sqrt{(x_i - x_{rec})^2 + (y_i - y_{rec})^2 + (z_i - z_{rec})^2} \end{aligned} \tag{1}$$

where the true range between GPS satellite and receiver (d_i) and receiver clock bias (b_i) are calculated from the navigation message of the i^{th} satellite. c denotes the speed of light, and ϵ_i denotes the range measurement error.

The IEEE C37.118 standard [18] defines the Total Vector Error (TVE) as a vectorial difference between the measured and expected value of the phasor for the measurement at a given instant of time. An error in timing appears identical to an error in phase. Without timing and magnitude errors, a phase error of 0.573 degrees corresponds to a 1% TVE, which is the maximum TVE allowed by the IEEE C37.118 standard. The TVE combines three possible sources of error, namely, magnitude, phase-angle and timing. If only one of these errors exists, the 1% limit would be reached for either a magnitude error equal to 1%, a phase shift of 10 milli-radians or a lack of time synchronization equal to 26.5 μs at 60 Hz.

C. GPS Attacks

There are several types of spoofing attacks. In what follows we list some of the main ones:

- Signal-level spoofing: transmits counterfeit GPS signals that carry the same navigation data as concurrently broadcasted by the GPS satellites.
- Data-level spoofing: modifying several parameters in the navigation data.
- Bent-pipe spoofing: records authentic GPS signals and rebroadcasts them with a time delay.

In this paper, our proposed countermeasures are mainly against those types which change the C/A code and navigation data. According to (1), the data-level spoofing changes the information about satellite's position and further leads to incorrect clock bias b_k. It can also spoof arbitrary number

of satellite signals and introduce a receiver clock offset error without significantly changing the computed receiver position from its pre-attack value.

III. Predicting the visible satellites

Since civilian GPS signals are not authenticated, a well-equipped attacker near the GPS receiver can transmit falsified GPS signals with public GPS parameters, e.g., by using a GPS signal generator with modified C/A codes. Consequently, the front-end of the GPS receiver will receive both the actual satellite signals and the spoofed one.

At the code and carrier tracking part of the GPS receiver, the incoming GPS signals are correlated with the local generated C/A codes in order to identify the satellites associate with the incoming signal. If there are spoofing signals which can complete the C/A code offset search, theses signals will be regarded as real ones by the spoofed receiver. Thus, if the GPS receiver can predict visible satellites at a given position and time period, the receiver local clock can generate only the visible satellites' local C/A code according to the prediction, to prevent the spoofed signal from going into the position and time calculation system. Another approach is to use the mere fact that a match happens with the C/A code of a satellite that is not supposed to be visible at this time and location to trigger an alarm for a possible spoofing attempt.

In what follows we review the process of determining whether a given satellite can be visible at a given location and time [23]. The GPS system is divided into three segments: space segment, control segment, and user segment. The space segment consists of the GPS satellites constellation which are orbiting around the earth. The GPS satellites are placed in six orbital planes, where each orbital plane can contain four or five satellites with 55° inclination to the equatorial plane. The satellites orbit the earth with a circulation time of 11 hours and 58 minutes with an altitude of 20200 km [21]. The high altitude insures that the satellite orbits are stable, precise and predictable.

The information which is used to calculate the satellites position [23] is broadcast by each GPS satellite. There are two types of navigation data, one referred to as almanac data which includes orbit information, satellite clock correction, and atmospheric delay parameters. The second type of navigation data, referred to as ephemeris data, represents a set of parameters that can be used to accurately calculate the location of the GPS satellite at a particular point in time.

A. Methodology

The preliminaries of calculating the position of GPS satellites are listed below:

- Coordinate system: The Satellite Vehicle (SV) position is expressed in the Earth Centered Earth Fixed (ECEF) coordinate system, which represents positions as an X, Y, and Z coordinate. The ECEF is defined by a standard called the World Geoditic System 1984 (WGS-84). The point $(0, 0, 0)$ is defined as the centre of mass of the earth [24]. As shown in Figure 3, the X_k, Y_k, Z_k axes (at time k) rotate with the earth.

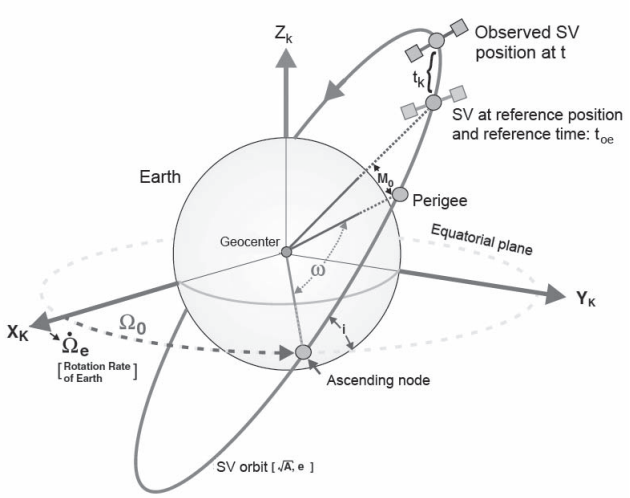

Fig. 3. Description of SV position from orbital parameters [25]

- Time system: In the GPS system, an important parameter is the GPS time, which is also called the Master clock. The SV clock and the user (GPS receiver) clock are running at slightly different rates compared to the GPS time. The goal is to make the corrected user clock and the SV clock read this time as close as possible [25].
- Satellites movement: There are two types of forces on the GPS SV; one is the centripetal force by the earth (under the assumption that the earth is a homogeneous sphere) which keeps the satellite in orbit. The second is the perturbation force which makes the satellite slightly deviate from the orbit (disturbed motion).
- Parameters: The non-disturbed motion of the satellite is based on Newton's laws of motion and gravitation and Kepler's laws for orbits. The following six parameters which are called Orbital elements are required to uniquely identify a specific orbit:
  A: Semi-major axis of the satellite orbit.
  e: Eccentricity of the satellite orbit.
  A and e: determine the shape and size of the Kepler ellipse.
  Ω_0: Longitude of ascending node of orbit plane at weekly epoch.
  i_0: Inclination angle at reference time.
  Ω_0 and i_0: identify the satellite orbit plane and the relative orientation between the earth.
  ω: Argument of perigee which represents the angle within the satellite orbit plane.
  v_k: True anomaly, which is the angle between the direction of periapsis and the current position of the body, as seen from the main focus of the ellipse (the point around which the object orbits) [27].
  The following parameters (which we will explain later) are also contained in the navigation data for the correction of disturbed motion and clock: Δn, a_0, a_1, a_2, t_{oc}, M_0, c_{us}, c_{uc}, c_{rs}, c_{rc}, c_{is}, c_{ic}, $IDOT$, $\dot{\Omega}$,$\dot{\Omega}_e$.

To calculate the satellite position, we proceed as follows [26]: 1. Evaluate the true anomaly of satellite, v_k:

- Compute the mean angle velocity of the satellite:
$$n = n_0 + \Delta n \tag{2}$$
where n_o is given by:
$$n_0 = \frac{\sqrt{\mu}}{\left(\sqrt{A}\right)^3}, \tag{3}$$
μ represents the value of the earth universal gravitational parameter in WGS-84 for the GPS user ($\mu = 3.986005 \times 10^{14} meters^3/sec^2$), and Δn is the mean angle velocity difference between the value calculated from the navigation data and that calculated from the Newton's law and Kepler's law.
- Correct the satellite clock at the observation time t':
$$t = t' - \Delta t \tag{4}$$
$$\Delta t = a_0 + a_1(t - t_{oe}) + a_2(t - t_{oe})^2 \tag{5}$$
Equation (4) represents the conversion of time sent by the GPS satellites to GPS time scale. This step synchronizes the GPS satellite's clock to the Master time. Equation (5) evaluates the SV position for this transmit time t, where we must determine the difference between t and t_{oe}, where t_{oe} denotes the ephemeris reference time (see Figure 3) and a_0, a_1, a_2 denote the clock reference time, 1^{st} order parameter and 2^{nd} order parameter, receptively. Then, we compute the time from ephemeris reference epoch:
$$t_k = t - t_{oe}, \tag{6}$$
where t_k denotes the actual total time difference between the time t and satellite clock correction t_{oe}, and must account for beginning or end of week crossovers.
- Next, we compute the mean anomaly for t_k:
$$M_k = M_0 + nt_k \tag{7}$$
where M_0 represents the mean anomaly of the satellite at reference time t_{oe}.
- Then, we iteratively solve the Kepler's equation for the eccentricity anomaly:
$$E_k = M_k + e \sin E_k \tag{8}$$
where e is the eccentricity of the GPS satellite orbits.
- Compute the true anomaly of GPS satellite v_k:
$$v_k = \arctan\left(\frac{\sqrt{1 - e^2}\sin E_k}{\cos E_k - e}\right) \tag{9}$$

2. Compute the argument of latitude and correction of the perturbations:

- The argument of latitude, which is an angular parameter that defines the position of a satellite moving along the orbit is given by:
$$\Phi_k = v_k + \omega \tag{10}$$
where ω denotes the argument of perigee given by the navigation data.
- Calculate the second harmonic perturbations, namely the argument of latitude correction δu_k, radius correction δd_k and inclination correction δi_k.
$$\begin{aligned} \delta u_k &= c_{us}\sin 2\Phi_k + c_{uc}\cos 2\Phi_k \\ \delta r_k &= c_{rs}\sin 2\Phi_k + c_{rc}\cos 2\Phi_k \\ \delta i_k &= c_{is}\sin 2\Phi_k + c_{ic}\cos 2\Phi_k \end{aligned} \tag{11}$$
where c_{us}, c_{uc} denote amplitude of the sine/cosine harmonic correction term to the argument of latitude.
c_{rs}, c_{rc} denote amplitude of the sine/cosine harmonic correction term to the orbit radius.
c_{is}, c_{ic} denote amplitude of the sine/cosine harmonic correction term to the angle of inclination.

3. Compute the argument of latitude u_k, radial distance r_k, and the inclination i_k:

-
$$\begin{aligned} u_k &= \Phi_k + \delta u_k \\ r_k &= A(1 - e\cos E_k) + \delta r_k \\ i_k &= i_0 + \delta i_k + (IDOT)t_k \end{aligned} \tag{12}$$
where IDOT denotes the rate of inclination angle.

4. Calculate the position of satellite in ECEF:

- The satellite positions in orbital plane is given by:
$$\begin{aligned} x_k{}' &= r_k \cos u_k \\ y_k{}' &= r_k \sin u_k \end{aligned} \tag{13}$$
- Compute the longitude of the ascending node Ω_k with respect to Greenwich, which is the angle from a reference direction, called the origin of longitude, to the direction of the ascending node, measured in a reference plane [28]. This calculation uses the right ascension at the beginning of the current week Ω_0, the correction from the apparent sidereal time (a time scale that is based on the earth's rate of rotation measured relative to the fixed stars rather than the Sun [29]), variation in Greenwich between the beginning of the week and reference time $t_k = t - t_{oe}$, and the change in longitude of the ascending node from the reference time t_{oe}:
$$\Omega_k = \Omega_0 + (\dot{\Omega} - \dot{\Omega_e})t_k - \dot{\Omega_e}t_{oe} \tag{14}$$
where $\dot{\Omega}$ denotes the rate of right ascension and $\dot{\Omega_e}$ is WGS-84 value of the earth's rotation rate ($\dot{\Omega_e} = 7.2921151467 \times 10^{-5} rad/s$).
- Compute the earth-fixed coordinates:
$$\begin{aligned} x_k &= x_k{}' \cos\Omega_k - y_k{}' \cos i_k \sin\Omega_k \\ y_k &= x_k{}' \sin\Omega_k - y_k{}' \cos i_k \cos\Omega_k \\ z_k &= y_k{}' \sin i_k \end{aligned} \tag{15}$$

5. Identify the visible satellites:

- Check which satellites are visible to the test point: As shown in Figure 4, r is the radius of earth and R is the radius of satellites orbit. Given the position of the fixed GPS-receiver location x_{rec}, y_{rec} and the cut-off angle α, the elevation angle of the satellites β can be calculated as:
$$\beta = arctg\frac{\cos(x_k - x_{rec})\cos y_{rec} - 0.15127}{\sqrt{1 - [\cos(x_k - x_{rec})\cos y_{rec}]^2}} \tag{16}$$

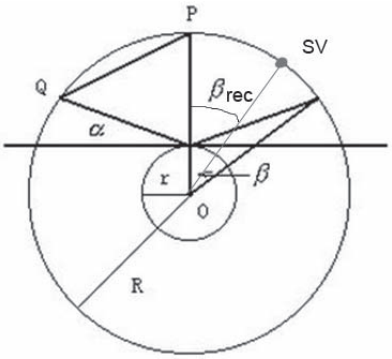

Fig. 4. Visible satellites from a fixed elevation angle

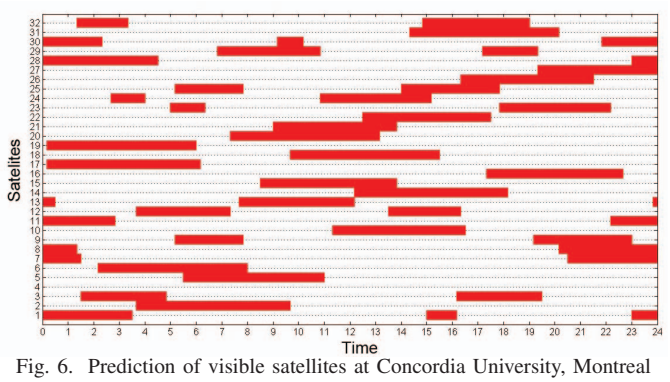

Fig. 6. Prediction of visible satellites at Concordia University, Montreal

If the elevation angle of the GPS satellite β is not larger than the elevation angle of the reference point β_{rec}, the considered satellite is visible.

B. Simulation

The tool we use in our paper as a representative example is named *GPS satellite visibility*. This navigation tool requires the observer's (i.e., GPS-receiver) latitude and longitude, height, cut-off angle and date as well as an almanac file describing the orbits of the GPS satellites. [30] provides the almanac files updated daily for users to download. The program produces comprehensive charts and reports of GPS satellite visibility for a 24-hour period (e.g., see Figure 5). Moreover, as shown in Figure 6, one can also obtain information about which satellites are visible from a fixed location. In our simulation, we choose the coordinates of Concordia University as the tested fixed location, with a cut-off angle of 15 degree at Jan the 13th, 2016.

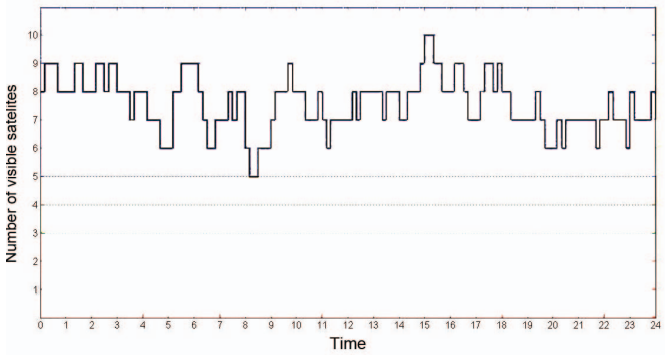

Fig. 5. Prediction of visible satellites at Concordia University, Montreal

As depicted in Figure 5, for the interval and positions used in our simulations, there are at least five visible satellites at the same time. GPS receiver needs at least four satellites to calculate the time and position. Also, there are errors which are called *ephemeris* errors as they affect the satellite's orbit or ephemeris. These errors are caused by gravitational pulls from the moon and sun and by the pressure of solar radiation on the satellites. These kind of errors are usually very slight. However, if higher accuracy is desirable, one can use the data available from the International GNSS (Global navigation satellite system) Service (IGS) which collects, archives, and distributes GPS and GLONASS (Russian Global Navigation Satellite System) observation data sets from varieties of analysis centers for better prediction accuracy.

IV. Anomaly Detection of Data-Level GPS Spoofing

A. Clock Behavior of GPS Receiver

The GPS receiver provides 1 pulse-per-second(PPS) signal for the PMUs. For the reason that the GPS receiver clock may drift apart or gradually desynchronize from the master time, one needs to use the GPS system with highly accurate atomic clocks to synchronize the GPS receiver's clock. Besides, there are other factors which may affect the time solution of the GPS receiver, such as the system noise. Based on the fact that we have already known the fixed position of the GPS receiver, in our approach, we describe the time solution by a simple model:

$$c \times \Delta t_{trans,k} = d_{true,k} + c \times t_{b,k} \tag{17}$$

$$t_{meas,k} = t_{rcv,k} - t_{b,k} \tag{18}$$

where $t_{rcv,k}$ denotes the time provided by the internal clock of the GPS receiver at time k, $\Delta t_{trans,k}$ denotes the signal propagation time from the GPS satellites to the GPS receiver at time k (calculated during the code tracking part), $d_{true,k}$ represents the true range between visible GPS satellite and GPS receiver, $t_{b,k}$ is the time bias between GPS satellites clock system and the GPS receiver internal clock, and $t_{meas,k}$ is the synchronized time solution of the GPS receiver.
The error in time is given by:

$$e_k = t_{meas,k} - t_{true,k} \tag{19}$$

The IEEE C37.118 standard [18] requires that the accuracy of the time solution should be within the range of $e_k \leq 40$ ns for 95% of the values. In what follows, we assume that the random error ε between the time solutions of GPS receiver and the UTC follows a Gaussian distribution $\tilde{e_k} \sim N(0, \sigma^2)$.

B. Error Analysis of GPS Receiver

1) Statistics of the receivers clock: In order to check whether the measurement time solution is within a reasonable range, given the real UTC time and the system noise are unknown, we will induce the pseudo-error $\tilde{e_k}$. Different from the real error between time solution and UTC time, we

randomly choose a start point of the time solutions from GPS receiver, then calculate the pseudo-error as follows:

$$\tilde{e}_k = t_{meas,k} - t_{meas,1} - (k-1) \quad k = 1, 2, 3... \tag{20}$$

According to our simulation results, the distribution of $\tilde{e_k}$ also follows a normal distribution. Then, the sample mean of the pseudo-error is given by

$$\hat{\mu} = \bar{t}_{\tilde{e}_k} = \frac{\sum_{k=1}^{n} (\tilde{e}_k)}{n} \tag{21}$$

2) Models of attacks: Data-level spoofing will modify the navigation data sent by the GPS satellites. According to the structure of the navigation data sent by the GPS satellites [32], the GPS receiver will continuously receive the signal and refresh one sub-frame of navigation information for 30 seconds. As a result, different types of errors may occur. Following are three possible types of spoofing attacks that we consider:

a) Scaling Attack In this type of attack, the error caused by the spoofer will shapely increase (or decrease) and will continue with the same error value,

$$w_k = p, \ k \geq n \tag{22}$$

where w_k denotes the error value at the *ith* epoch and p is the spoofing error value.

b) Ramp Attack: Here, the attacker will gradually increase (or decrease) the error value, rendering the time solution to exceed the threshold. This type of attack is described as follows,

$$w_k = p_k + m \times \Delta p, \quad k \geq n, \quad m = 1, 2, 3... \tag{23}$$

where Δp is the error changing rate. Here the error value is continuous for a time length of integer multiple of 30 seconds.

c) Random Attack: The error will change discontinuously and gradually until it passes the threshold.

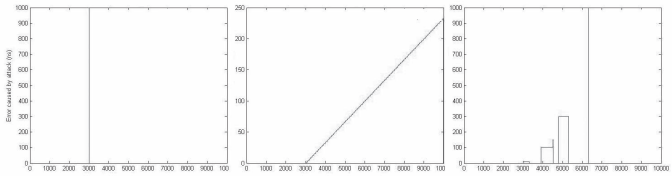

Fig. 7. Example of Scaling attack, ramp attack and random attack

C. The proposed Anomaly Detection Scheme

As mentioned in Section IV-A, we assume that the GPS receiver's time solution follows a normal distribution for a random sample from the entire population. There is enough evidence to infer that the pre-attacked values of pseudo-error also follow a normal distribution. We use binary hypothesis testing in this section to determine that if there is a abnormal value of the time solution caused by a spoofer. There are two types of statistical hypotheses: The null hypothesis, denoted by H_0, represents the hypothesis that the time solution at the moment is consistent with the learnt statistics of the receiver's clock. The alternative hypothesis, denoted by H_1 or H_a, is the hypothesis that the pseudo-error has exceeded the threshold which means the system is influenced by the attacker [31].

For the first part of our proposed anomaly detection, we will use the sample mean to estimate the population mean of the pseudo-error, and then compare it to the upcoming values of the pseudo-error. Let n denote the number of samples. According to (21), after n samples, we use upcoming values $\tilde{e_k}$ $(k > n)$ to compare with the sample mean $\hat{\mu}$.

$$H_0\text{: } \tilde{e_k} = 0$$
$$H_1\text{: } \tilde{e_k} \neq 0$$

Let α_1 denote the false alarm rate according to the system design requirements, and λ_1 denote the corresponding threshold calculated from the distribution of pseudo-error. As shown in Figure 8, if $\tilde{e_k}$ is out of the acceptance region, we conclude that the time solution at time *k* is calculated from the spoofed signal.

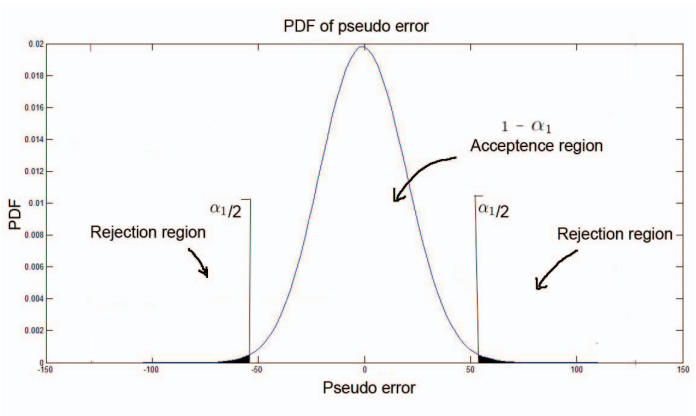

Fig. 8. Hypothesis testing of anomaly detection 1

The second part of the detection allows us to test if the GPS receiver is under the ramp attack following the procedure below.

- As mentioned in the first part, we calculate the sample mean of the pseudo-error.
- Count the number of upcoming pseudo errors that are larger than the sample mean in the considered sliding window analysis:

$$N_{L\_j} = \#\left\{j - N_T < k \leq j | \tilde{e}_k > \hat{\mu}\right\} \tag{24}$$

  where N_{L_j} represents the number of samples larger than the threshold in the shifting window.
- Calculate the ratio of larger samples:

$$r_j = N_{L\_j}/N_T \tag{25}$$

  where N_T is the number of samples in the sliding window.
- Let α_2 denote the false alarm rate for the slope detection system and let λ_2 denote the corresponding threshold. The value of the ratio at time *j* equal r_j.

$$H_0\text{:} r_j = 0.5$$
$$H_1\text{:} r_j \neq 0.5$$

  If the ratio we tested falls in the acceptance region (H_0), then the system has not been spoofed or the influence

of the spoofing attack is not large enough to cause an unacceptable error to the PMU. Note that H_1 represents a warning area in this scenario, if r_j is in the rejection region, the time solution at time j is labelled as being spoofed (Figure 9).

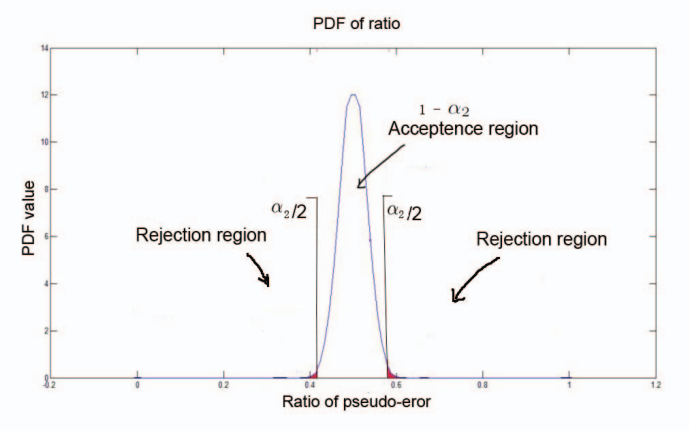

Fig. 9. Hypothesis testing of the anomaly detection 2

The flow chart of the detection algorithm is shown in Figure 10. When the algorithm declares that the GPS receiver has been spoofed, there are different methods to locate the spoofer [34] . Also, there are methods to increase the stability of the PMU clock, for example, according to [35], after disconnecting the link, the PMU can operate stably for a period of 6 hours. In that case, we can restart the GPS receiver, refresh the navigation data and check for spoofing again.

D. Simulation Results

The simulation environment used in our performance investigation is as follow:

- Accuracy of the time solution: $e_k \leq 40$ ns for 95% of the values.
- Number of samples for the sample mean: 300 samples.
- Shifting window for the slope detection: 150 samples.

Figure 11 depicts the Receiver-Operating Characteristics (ROC) curves of our anomaly detection for the scaling attack. From our simulations, it can be seen that the error caused by the scaling attack can be detected when it is larger than about $120ns$, which is smaller than the threshold defined by the IEEE C37.118 standard.

For the ramp attack, the system can detect the attack with a zero miss-detection rate. The simulation results show that our anomaly detection is an effective countermeasure against the data-level spoofing.

The advantage of the anomaly detection is the fast detection time against the different types of data-level spoofing. Figure 12 shows that the detection time of different error increasing/decreasing rate caused by the attacker. The detection time of the algorithm equal to the minimum of the two sub-detection systems.

Based on our simulation results, we can conclude that the proposed anomaly detection can detect a scaling attack when

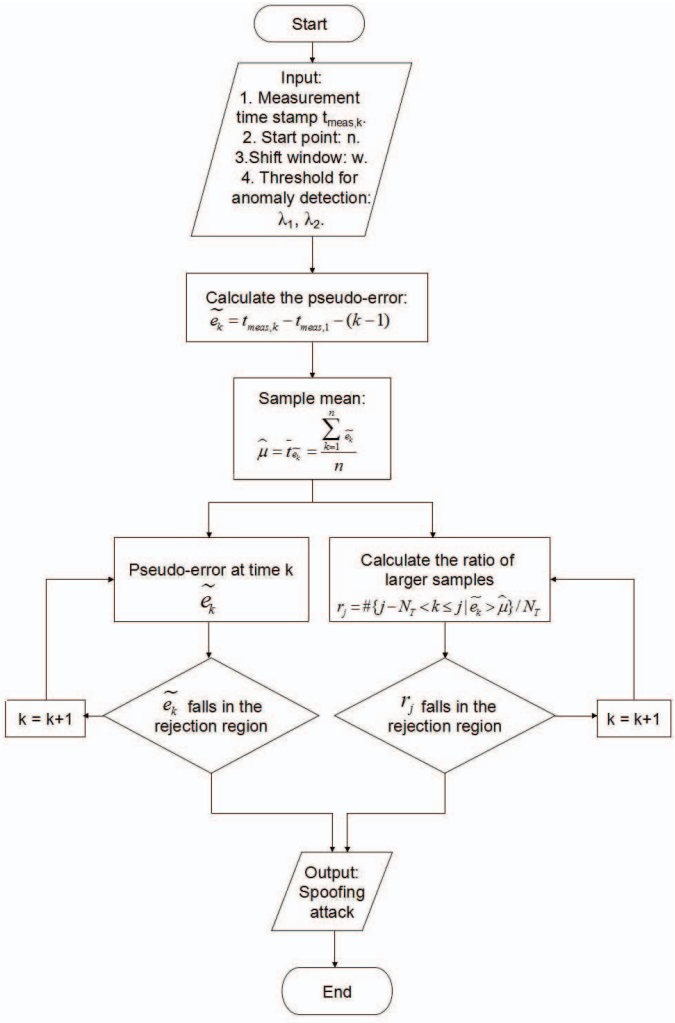

Fig. 10. Flow chart of anomaly detection algorithm

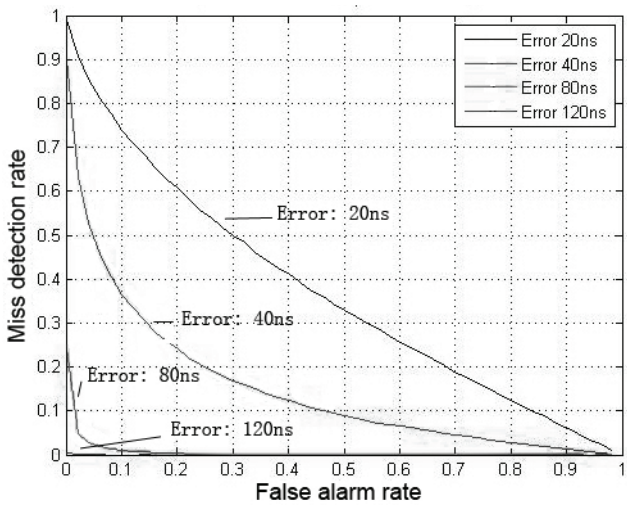

Fig. 11. ROC curve of detect the scaling attack

the error caused by the attacker exceeds the threshold based on the real needs of the system. Also, we can detect a spoofing attack when there is a continuous trend of increase/decrease

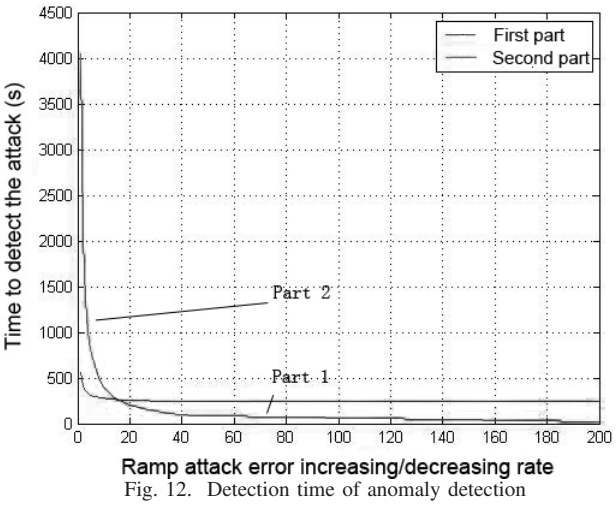

Fig. 12. Detection time of anomaly detection

of the error.

V. Conclusion

Security and reliability of measurements by Phasor measurement unit are vital for power systems. In order to enhance the robustness of the GPS-based PMU, we proposed two methods to detect spoofing attempts. In the first method, we predict the number of visible satellites to prevent the GPS receiver from tracking manipulated signals. The second detection technique utilizes the changes in the observed signal statistics when the system is under attack to detect the presence of spoofing attempts. We have defined three types of error pattern: scaling attack, ramp attack and random attack. Our simulation results confirmed the effectiveness of our proposed solutions against these types of attacks.

References

[1] https://www.smartgrid.gov
[2] R. E. Wilson, "Uses of precise time and frequency in power systems, Proceedings of the IEEE, vol. 79, no. 7, pp. 10091018, 1991.
[3] Jinghe Zhang, Marjan Momtazpour and Naren Ramakrishnan, "Secure and Adaptive State Estimation for a PMU-equipped Smart Grid", Discovery Analytics Center, Virginia Tech Virginia, USA
[4] https://en.wikipedia.org/wiki/Phasor_measurement_unit
[5] Liang Heng, Jonathan J. Makela, Alejandro D. Domnguez-Garca, Rakesh B. Bobba, William H. Sanders, and Grace Xingxin Gao, "Reliable GPS-Based Timing for Power Systems: A Multi-Layered Multi-Receiver Architecture" , University of Illinois at Urbana-Champaign, Urbana, IL 61801 Email: heng, jmakela, aledan, rbobba, whs, gracegao@illinois.edu
[6] http://www.phasor-rtdms.com/phaserconcepts/phasor_adv_faq.html
[7] KRISH NARENDRA, TONY WEEKES, "Phasor Measurement Unit (PMU) Communication Experience in a Utility Environment", ERL. Phase Power Technologies Ltd.(CAN), Manitoba Hydro(CAN) SUMMARY
[8] Joe-Air Jiang Dept. of Electr. Eng., Nat. Taiwan Univ., Taipei, Taiwan Jun-Zhe Yang ; Ying-Hong Lin ; Chih-Wen Liu ; Jih-Chen Ma, "An adaptive PMU based fault detection/location technique for transmission lines. I. Theory and algorithms ", IEEE Transactions on Power Delivery, (Volume:15 , Issue: 2), Apr 2000.
[9] X. Jiang, J. Zhang, B. Harding, J. Makela, and A.Dominguez-Garcia. "Spoofing GPS Receiver Clock Offset of Phasor Measurement Units." IEEE Trans.Power Systems, 2013.
[10] Jon S. Warner, Ph.D. and Roger G. Johnston, Ph.D., CPP "GPS Spoofing Countermeasures" Vulnerability Assessment Team Los Alamos National Laboratory Los Alamos, New Mexico, 87545
[11] N. White, P. Maybeck, and S. DeVilbiss, "Detection of interference/jamming and spoofing in a DGPS-aided inertial system, Aerospace IEEE Transactions on and Electronic Systems, vol. 34, no. 4, pp. 12081217, 1998.
[12] P. Y. Montgomergy, T. E. Humphreys, and B. M. Ledvina, "Receiver-autonomous spoofing detection: Experimental results of a multiantenna receiver defense against a portable civil GPS spoofer, in Proceedings of the ION ITM, (Anaheim, CA), Jan. 2009.
[13] M. L. Psiaki, S. P. Powell, and B. W. OHanlon,"GNSS spoofing detection by correlating carrier phase with rapid antenna motion, GPS World, vol. 24, pp. 5358, June 2013.
[14] P. Levin, D. De Lorenzo, P. Enge, and S. Lo, "Authenticating a signal based on an unknown component thereof, June 2011. US Patent 7,969,354 B2.
[15] A. G. Phadke, "Synchronized phasor measurements in power systems, IEEE Computer Applications in Power, Vol. 6, Issue 2, pp. 10-15, April 1993.
[16] Phadke A G "Synchronized phasor measurementsa historical overview" IEEE/PES Transmission and Distribution Conference and ExhibitionAsia Pacific20021476-479
[17] Rohini P. Haridas, "GPS Based Phasor Technology in Electrical Power System", Electrical Engineering Department, S.S.G.M.C.E, Shegaon, India International Journal of Electronics and Electrical Engineering, Vol. 3, No. 6, December 2015
[18] $C37.118.1_{WG}$ - Synchrophasor Measurements for Power Systems, "C37.118.1-2011 - IEEE Standard for Synchrophasor Measurements for Power Systems", IEEE Power and Energy Society External Link, C37.118.1a-2014
[19] http://www.gps.gov/applications/timing/
[20] C. Ma, G. Lachapelle, and M.E. Cannon, "Implementation of a Software GPS Receiver", Position, Location And Navigation (PLAN) Group, Department of Geomatics Engineering, University of Calgary, Calgary, Alberta, Canada, T2N 1N4
[21] Ignacio Ginés Fernández, "GPS Space Segment Monitoring", Engenharia Electrotécnica e de Computadores
[22] http://touque.ca/EC/ICS2O/students/2010-09/ICS2O7C/AbidiM/assignment/Mosaic_Project.html
[23] Ryan Monaghan, "GPS Satellite Position Estimation from Ephemeris Data by Minimum Mean Square Error Filtering Under Conditions of Selective Availability", Student Member, IEEE
[24] https://en.wikipedia.org/wiki/ECEF
[25] Dan Doberstein, "Fundamentals of GPS receivers, a hardware approach", DKD Instruments 750 Amber Way Nipomo, CA, USA, dand@dkdinst.com
[26] Navstar GPS space segment/navigation user interfaces, "Global positioning systems directorate systems engineering and integration, interface specification IS-GPS-200", Global positioning systems directorate
[27] https://en.wikipedia.org/wiki/True_anomaly
[28] https://en.wikipedia.org/wiki/Longitude_of_the_ascending_node
[29] https://en.wikipedia.org/wiki/Sidereal_time
[30] http://www.navcen.uscg.gov/?Do=gpsArchives&path=ALMANACS/YUMA&year=2015
http://celestrak.com/GPS/almanac/Yuma/
[31] http://stattrek.com/hypothesis-test/hypothesis-testing.aspx
[32] Heidi Kuusniemi, "User-Level Reliability and Quality Monitoring in Satellite-Based Personal Navigation", Institute of Digital and Computer Systems Tampere University of Technology Finland, 11th June 2005
[33] http://www.radartutorial.eu/01.basics/False\%20Alarm\%20Rate.en.html
[34] Der-Yeuan Yu, Aanjhan Ranganathan, Thomas Locher, Srdjan Capkun, David Basin, "Detection of GPS Spoofing Attacks in Power Grids", Department of Computer Science, ETH Zurich, Switzerland
[35] Wu Ning, PAN Xiaolong, YU Jiexia, "Research and Realization of the High Accuracy GPS Synchronization Clock", Nanjing University of Aeronautics and Astronautics , Nanjing 210016 , China
[36] https://en.wikipedia.org/wiki/Receiver_operating_characteristic