GPS Spoofing Attack Characterization and Detection in Smart Grids

Parth Pradhan, Kyatsandra Nagananda, Parv Venkitasubramaniam, Shalinee Kishore and Rick S. Blum
Department of Electrical and Computer Engineering
Lehigh University, Bethlehem, PA 18015
Email: {pap212,kgn209,pav309,skishore,rblum}@lehigh.edu

***Abstract*—The problem of global positioning system (GPS) spoofing attacks on smart grids endowed with phasor measurement units (PMUs) is addressed, taking into account the dynamical behavior of the states of the system. First, it is shown how GPS spoofing introduces a timing synchronization error in the phasor readings recorded by the PMUs and alters the measurement matrix of the dynamical model. Then, a generalized likelihood ratio-based hypotheses testing procedure is devised to detect changes in the measurement matrix when the system is subjected to a spoofing attack. Monte Carlo simulations are performed on the 9-bus, 3-machine test grid to demonstrate the implication of the spoofing attack on dynamic state estimation and to analyze the performance of the proposed hypotheses test.**

***Index Terms*—GPS spoofing, PMU, hypotheses testing.**

I. Introduction

A modern wide area monitoring system (WAMS) supporting the future grid will include a vastly improved information and communications functionality that allows service providers to sense, monitor, and manage electricity flows throughout the grid [1]. While the cyber physical integration improves the performance and efficiency of the grid, it increases its vulnerability to potential cyber-attacks. Security of cyber-physical systems in the context of the power grid has received significant attention [2] - [4]. In this paper, we address the problem of cybersecurity in smart grid networks involving PMUs taking into account the dynamical nature of the power system.

A PMU can record synchrophasors at a high sampling rate, and the measurements are synchronized to an absolute time reference provided by the GPS. In general, a GPS spoofing attack refers to deception of the GPS receiver by transmitting spurious signals resembling the normal GPS signals, leading to timing synchronization errors [5]. In an electric grid with PMUs, GPS spoofing results in counterfeit time stamps at the synchrophasors and is referred to as a timing synchronization attack (TSA) [6]. While a TSA only alters the time stamps without inducing changes in the actual measurements, it results in confusing the grid command center with erroneous system operation status. Evaluating the threat to synchrophasor measurements and the countermeasures to combat TSAs have received considerable attention in the existing literature [7]-[10].

In this paper, we first analyze the implications of a TSA on the *dynamical behavior* of the power system. We consider the dynamical model of the power system [11], and for simplicity of explanation assume that voltage magnitude and phase are observable by PMUs at all the generator nodes in the network. We show how a TSA alters the phasor readings of one or more PMUs by transforming the system matrix in the measurement equation. Next, we develop a generalized likelihood ratio-based hypotheses testing procedure to detect changes from the normal operating behavior when the system is subjected to a TSA. Monte Carlo simulations are performed to demonstrate (a) the implication of the TSAs on the dynamic state estimation (DSE) and (b) the performance of the proposed test. To the best of our knowledge, this is the first instance where a characterization of the impact of TSAs on the dynamic behavior of power systems and its detection is reported in the literature. These studies are important for efficient wide area monitoring and to initiate timely action in the event of a security threat to the grid.

II. Dynamic Model of the Power System

The power system comprising generators, electrical loads and the transmission network is modeled using differential and algebraic equations. At the ith generator, the rotor angle (δ_i), the rotor speed (ω_i) and the internal voltage (E_i) of the synchronous generator are the state variables of the system governed by differential equations, while the nodal voltage magnitudes (V_i) and the phasor angles (θ_i) are the algebraic variables. To analyze the system's behavior we consider the 3[rd]-order differential equations, which can sufficiently capture the dynamics of state variables [11].

We consider an n-bus, m-generator system where the state vector of the linearized model for synchronous generator $i = 1, \ldots, m$ is denoted by $\boldsymbol{x}_i = [\Delta\delta_i \ \Delta\omega_i \ \Delta E_i]^{\mathrm{T}}$. The state $\boldsymbol{x}_i$ captures the change of the i^{th} generator's variables around an operating point, which depends on the network topology, generator parameters and the load. In the absence of a control mechanism, a perturbation caused by a change in these components can alter the system stability. We model the evolution of the $3m \times 1$ state vector $\boldsymbol{x}_t = (\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_i, \ldots, \boldsymbol{x}_m)$ by

$$\boldsymbol{x}_t \quad = \quad \boldsymbol{A}\boldsymbol{x}_{t-1} + \boldsymbol{v}_t, \tag{1}$$

where $\boldsymbol{A}$ is the $3m \times 3m$ (for the 3[rd]-order model) state transition matrix. The modes given by the eigenvalues of $\boldsymbol{A}$ are assumed to be sufficiently damped for the system to be stable. In other words, a stable open loop system is considered so a zero control input can be employed for simplification. The entries of $\boldsymbol{A}$ are given by the following sub-matrices each of size $m \times m$: $\boldsymbol{A}_{11} = \boldsymbol{0}$ (zero matrix), $\boldsymbol{A}_{12} = \boldsymbol{I}$ (identity matrix),

978-1-5090-3065-1/16/$31.00 ©2016 IEEE

$\boldsymbol{A}_{13} = \mathbf{0}$, $\boldsymbol{A}_{21} = g_a(\delta_o, E_o, \theta_o, V_o, Y_L)$, $\boldsymbol{A}_{22} = -\text{diag}(D_i)$, $\boldsymbol{A}_{23} = g_b(\delta_o, E_o, \theta_o, V_o, Y_L)$, $\boldsymbol{A}_{31} = g_c(\delta_o, E_o, \theta_o, V_o, Y_L)$, $\boldsymbol{A}_{32} = \mathbf{0}$, $\boldsymbol{A}_{33} = g_d(\delta_o, E_o, \theta_o, V_o, Y_L)$, where D_i is the damping of the i^{th} generator, Y_L is the load admittance, and $(\delta_o, E_o, \theta_o, V_o, Y_L)$ is the operating point around which the system is linearized to make it viable for small signal analysis. The functions $g_a(\cdot)$, $g_b(\cdot)$, $g_c(\cdot)$ and $g_d(\cdot)$ can be written in matrix form [12] and are not presented here for the sake of brevity. The $3m\times 1$ state transition noise vector $\boldsymbol{v}_t$ is assumed to be independently and identically distributed (i.i.d.) and gaussian with $3m \times 1$ zero mean vector and $3m \times 3m$ covariance matrix $\boldsymbol{C}_{v,t}$.

The ith PMU records the voltage magnitude V_i and the phasor angles θ_i, while the rotor speed ω_i is typically measured using a separate sensor and is incorporated into the measurement equation [13]. The $3m \times 1$ measurement vector at time t is the deviation of the measurements from steady state measurement values denoted by $\boldsymbol{y}_{ti} \triangleq [\Delta V_{ri}, \Delta\omega_i, \Delta V_{j_i}]$ where $V_{ri} = V_i\cos(\theta_i), V_{j_i} = V_i\sin(\theta_i)$ and is given by

$$\boldsymbol{y}_t \;=\; \boldsymbol{S}\boldsymbol{x}_t + \boldsymbol{w}_t, \tag{2}$$

where $\boldsymbol{w}_t$ is the $3m \times 1$ measurement noise vector assumed to be i.i.d. and Gaussian with $3m \times 1$ zero mean vector and $3m \times 3m$ covariance matrix $\boldsymbol{C}_{w,t}$. The measurement matrix $\boldsymbol{S}$ is given by

$$\boldsymbol{S} \;=\; \begin{bmatrix} S_{11} & \mathbf{0} & S_{13} \\ \mathbf{0} & \boldsymbol{I} & \mathbf{0} \\ S_{31} & \mathbf{0} & S_{33} \end{bmatrix}, \tag{3}$$

Here, $\boldsymbol{S}$ is $3m\times 3m$ square block matrix of 9 entries with each entry a matrix of size $m \times m$ given by
S_{11}=$(-Y_{f_r}\text{diag}_{1:m}(E_{oi}\text{sin}(\delta_{o_i})) - Y_{f_j}\text{diag}_{1:m}(E_{oi}\text{cos}(\delta_{o_i})))$,
$S_{12} = (Y_{f_r}\text{diag}_{1:m}(\text{cos}(\delta_{o_i})) - Y_{f_j}\text{diag}_{1:m}(\text{cos}(\delta_{o_i})))$,
$S_{21} = (Y_{f_r}\text{diag}_{1:m}(E_{oi}\text{cos}(\delta_{o_i})) - Y_{f_j}\text{diag}_{1:m}(E_{oi}\text{sin}(\delta_{o_i})))$,
$S_{22} = (Y_{f_r}\text{diag}_{1:m}(\text{sin}(\delta_{o_i})) + Y_{f_j}\text{diag}_{1:m}(\text{cos}(\delta_{o_i})))$ where $\text{diag}_{1:m}(u_i)$ denotes a square diagonal matrix of size m having u_i at diagonal entry i. Y_{f_r} and Y_{f_j} are the real and imaginary part of the matrix $(Y_G + Y_L + Y_{bus})^{-1}Y_G$ where Y_G and Y_N are the generator and bus admittance matrices [12].

III. Characterization of TSA

In this section, we show how a TSA alters the measurement matrix $\boldsymbol{S}$ in (2). The voltage represented in complex phasor form at generator i is given by $\tilde{V_i} = V_{ri} + jV_{j_i}$, where V_{ri} and V_{j_i} denote the real and imaginary components, respectively. A time synchronization attack on a PMU at node i, denoted by $\beta_i(t_c)$, modifies the instantaneous nodal voltage signal by introducing a phase change as follows:

$$\tilde{V_i}(t + \beta_i(t_c)) = V_i(t + \beta_i(t_c)) \times \cos\left[2\pi f_c(t + \beta_i(t_c)) + \theta_i(t + \beta_i(t_c))\right], \tag{4}$$

where t_c denotes the time instant of the spoofing attack. Assuming normal steady state operation before attack so that the unattacked version of (4) is a sinusoid (constant V_i and θ_i over time), the synchronization delay attack changes the model by adding a factor $2\pi f_c\beta_i(t_c)$ to the phase at time t_c, where f_c denotes the operating frequency of the system. The voltage phasor after a TSA can be written as $\tilde{V_i} = V_i\angle(\theta_i + 2\pi f_c\beta_i(t_c)) = \bar{V}_{ri} + j\bar{V}_{ji}$, where $\angle(\cdot)$ denotes the phase. We thus have

$$\begin{aligned} \bar{V}_{ri} &= V_i\cos(\theta_i + 2\pi f_c\beta_i(t_c)) \\ &= V_i\cos(\theta_i)\cos(2\pi f_c\beta_i(t_c)) \\ &\quad -V_i\sin(\theta_i)\sin(2\pi f_c\beta_i(t_c)) \\ &= V_{ri}\cos(2\pi f_c\beta_i(t_c)) - V_{j_i}\sin(2\pi f_c\beta_i(t_c)) \qquad (5) \\ \bar{V}_{ji} &= V_i\sin(\theta_i + 2\pi f_c\beta_i(t_c)) \\ &= V_i\sin(\theta_i)\cos(2\pi f_c\beta_i(t_c)) \\ &\quad +V_i\cos(\theta_i)\sin(2\pi f_c\beta_i(t_c)) \\ &= V_{ji}\cos(2\pi f_c\beta_i(t_c)) + V_{ri}\sin(2\pi f_c\beta_i(t_c)), \qquad (6) \end{aligned}$$

which is compactly written as follows:

$$\begin{bmatrix} \bar{V}_{ri} \\ \bar{V}_{ji} \end{bmatrix} = \begin{bmatrix} \cos(2\pi f_c\beta_i(t_c)) & -\sin(2\pi f_c\beta_i(t_c)) \\ \sin(2\pi f_c\beta_i(t_c)) & \cos(2\pi f_c\beta_i(t_c)) \end{bmatrix} \begin{bmatrix} V_{ri} \\ V_{ji} \end{bmatrix}. \tag{7}$$

The small signal approximation of the variables in (7) results in

$$\begin{bmatrix} \Delta\bar{V}_{ri} \\ \Delta\bar{V}_{ji} \end{bmatrix} = \begin{bmatrix} \cos(2\pi f_c\beta_i(t_c)) & -\sin(2\pi f_c\beta_i(t_c)) \\ \sin(2\pi f_c\beta_i(t_c)) & \cos(2\pi f_c\beta_i(t_c)) \end{bmatrix} \begin{bmatrix} \Delta V_{ri} \\ \Delta V_{ji} \end{bmatrix}. \tag{8}$$

Using $[\Delta V_r\ \Delta V_j]^T = [\Delta V_{r1}, \ldots, \Delta V_{rm}, \Delta V_{j1}, \ldots, \Delta V_{jm}]^T$

$$\begin{bmatrix} \Delta V_r \\ \Delta V_j \end{bmatrix} \;=\; \begin{bmatrix} S_{11} & S_{13} \\ S_{31} & S_{33} \end{bmatrix} \begin{bmatrix} \Delta\delta \\ \Delta E \end{bmatrix}, \tag{9}$$

we can write

$$\begin{bmatrix} \Delta\bar{V}_r \\ \Delta\bar{V}_j \end{bmatrix} = \begin{bmatrix} M_1 & M_2 \\ M_3 & M_4 \end{bmatrix} \begin{bmatrix} S_{11} & S_{13} \\ S_{31} & S_{33} \end{bmatrix} \begin{bmatrix} \Delta\delta \\ \Delta E \end{bmatrix}, \tag{10}$$

where, $M_1 = \text{diag}_{1:m}(\text{cos}(2\pi f_c\beta_i(t_c)))$,
$M_2 = \text{diag}_{1:m}(-\text{sin}(2\pi f_c\beta_i(t_c))$,
$M_3 = \text{diag}_{1:m}(\text{sin}(2\pi f_c\beta_i(t_c)))$
and $M_4 = \text{diag}_{1:m}(\text{cos}(2\pi f_c\beta_i(t_c)))$.
The new measurement equation after a TSA is given by

$$\boldsymbol{y}'_t \;=\; \boldsymbol{M}\boldsymbol{S}\boldsymbol{x}_t + \boldsymbol{w}_t, \tag{11}$$

where

$$\boldsymbol{M} = \begin{bmatrix} M_1 & \mathbf{0} & M_2 \\ \mathbf{0} & \boldsymbol{I} & \mathbf{0} \\ M_3 & \mathbf{0} & M_4 \end{bmatrix}. \tag{12}$$

In effect, the GPS attack under small signal assumptions can be modeled as modification of the observation matrix based on the attack parameters $\beta_i(t_c)$.

IV. Detection of Spoofing Attack

In this section, we present a statistical hypotheses testing procedure to detect changes in the measurement matrix in the event of a TSA. We denote before attack $\boldsymbol{S}$ from (3). Let us suppose that a TSA has been initiated at the time instant t_c, leading to an alteration of the measurement matrix $\boldsymbol{S}_0$. We denote the resulting measurement matrix by $\boldsymbol{S}_c \triangleq \boldsymbol{M}\boldsymbol{S}_0$ (see (11)). Given the set $\boldsymbol{y}^t \triangleq \{\boldsymbol{y}_1, \ldots, \boldsymbol{y}_t\}$ of measurements, the

problem is formulated as one of devising a statistical testing procedure to detect the change - owing to an attack - in the measurement matrix as reliably as possible. More precisely, we need to devise a test to distinguish between the following two hypotheses:

$$\begin{cases} H_0: \text{ Given } \boldsymbol{y}^t, \boldsymbol{S} = \boldsymbol{S}_0, \quad t = 0, \ldots, T-1 \\ H_1: \text{ Given } \boldsymbol{y}^t, \boldsymbol{S} = \begin{cases} = \boldsymbol{S}_0, & t = 0, \ldots, t_c - 1 \\ = \boldsymbol{S}_c \neq \boldsymbol{S}_0, & t = t_c, \ldots, T-1. \end{cases} \end{cases}$$

The hypotheses test involves comparing a test statistic to a threshold and is of the form $\Lambda \underset{H_0}{\overset{H_1}{\gtrless}} \rho$ where Λ is the test statistic and ρ is the test threshold. We adopt the Neyman-Pearson criterion which maximizes the probability of detection for a fixed probability of false alarm [14]. The likelihood ratio test statistic is given by

$$\Lambda = \frac{p(\boldsymbol{y}_T|\boldsymbol{y}_{T-1}; \boldsymbol{S}_c) \times \cdots \times p(\boldsymbol{y}_{t_c+1}|\boldsymbol{y}_{t_c}; \boldsymbol{S}_c)}{p(\boldsymbol{y}_T|\boldsymbol{y}_{T-1}) \times \cdots \times p(\boldsymbol{y}_{t_c+1}|\boldsymbol{y}_{t_c})}. \quad (13)$$

In this work, we assume knowledge of the time instant t_c when the spoofing attack is launched. Therefore, the results presented in this paper provide upper bounds on the performance of hypotheses tests where t_c is unknown and has to be estimated. To estimate t_c, one can consider a finite time-window and look for a value of t_c which maximizes the likelihood function. The measurement matrix $\boldsymbol{S}_c$ after TSA is unknown and will have to be estimated; therefore, the test is a generalized likelihood ratio test (GLRT). From (11) and (12), we see that estimating the matrix $\boldsymbol{S}_c$ is equivalent to estimating the unknown scalar attack parameter β, which results in GPS spoofing. The GLRT statistic is given by

$$\Lambda = \frac{\max\limits_{\beta} \left[p(\boldsymbol{y}_t|\boldsymbol{y}_{t-1}; \boldsymbol{S}_c) \times \cdots \times p(\boldsymbol{y}_{t_c+1}|\boldsymbol{y}_{t_c}; \boldsymbol{S}_c)\right]}{p(\boldsymbol{y}_t|\boldsymbol{y}_{t-1}) \times \cdots \times p(\boldsymbol{y}_{t_c+1}|\boldsymbol{y}_{t_c})}. \quad (14)$$

The conditional probability $p(\boldsymbol{y}_t|\boldsymbol{y}_{t-1}; \boldsymbol{S}_c)$ is given by

$$p(\boldsymbol{y}_t|\boldsymbol{y}_{t-1}; \boldsymbol{S}_c) = \frac{\exp\left\{-\frac{1}{2}(\boldsymbol{y}_t - \boldsymbol{\mu}_t)^{\mathrm{T}} \boldsymbol{\Sigma}_t^{-1} (\boldsymbol{y}_t - \boldsymbol{\mu}_t)\right\}}{(2\pi)^{K/2} |\boldsymbol{\Sigma}_t|^{1/2}}, \quad (15)$$

where $\boldsymbol{\mu}_t \triangleq \mathbb{E}[\boldsymbol{y}_t|\boldsymbol{y}_{t-1}] = \boldsymbol{S}_c \boldsymbol{A} \boldsymbol{S}_c^{-1} \boldsymbol{y}_{t-1}$ is the mean vector and $\boldsymbol{\Sigma}_t \triangleq \mathrm{Cov}[\boldsymbol{y}_t|\boldsymbol{y}_{t-1}] = \boldsymbol{S}_c \boldsymbol{A} \boldsymbol{S}_c^{-1} \boldsymbol{C}_{w,t-1} \left(\boldsymbol{S}_c \boldsymbol{A} \boldsymbol{S}_c^{-1}\right)^{\mathrm{T}} + \boldsymbol{S}_c \boldsymbol{C}_{v,t} \boldsymbol{S}_c^{\mathrm{T}} + \boldsymbol{C}_{w,t}$ is the covariance matrix. The matrix $\boldsymbol{S}_c$ will be replaced by $\boldsymbol{S}_0$ for the likelihood function under hypothesis H_0. Taking logarithms on both sides of (14), and considering $t = T - 1 = t_c$ as an example (which is like considering one product term in (13)), the test is given by

$$\Lambda' \underset{H_0}{\overset{H_1}{\gtrless}} \rho', \quad (16)$$

where $\Lambda' = (\boldsymbol{y}_t - \boldsymbol{\mu}_{t,S_0})^{\mathrm{T}} \boldsymbol{\Sigma}_{t,S_0}^{-1} (\boldsymbol{y}_t - \boldsymbol{\mu}_{t,S_0}) - (\boldsymbol{y}_t - \boldsymbol{\mu}_{t,\hat{S}_c})^{\mathrm{T}} \boldsymbol{\Sigma}_{t,\hat{S}_c}^{-1} (\boldsymbol{y}_t - \boldsymbol{\mu}_{t,\hat{S}_c})$, $\rho' = 2\rho - \ln\left\{\frac{|\boldsymbol{\Sigma}_{t,S_0}|}{|\boldsymbol{\Sigma}_{t,\hat{S}_c}|}\right\}$, and $\boldsymbol{\mu}_{t,S_0} = \boldsymbol{S}_0 \boldsymbol{A} \boldsymbol{S}_0^{-1} \boldsymbol{y}_{t-1}$, $\boldsymbol{\mu}_{t,\hat{S}_c} = \hat{\boldsymbol{S}}_c \boldsymbol{A} \hat{\boldsymbol{S}}_c^{-1} \boldsymbol{y}_{t-1}$,
$\boldsymbol{\Sigma}_{t,S_0} = \boldsymbol{S}_0 \boldsymbol{A} \boldsymbol{S}_0^{-1} \boldsymbol{C}_{w,t-1} \left(\boldsymbol{S}_0 \boldsymbol{A} \boldsymbol{S}_0^{-1}\right)^{\mathrm{T}} + \boldsymbol{S}_0 \boldsymbol{C}_{v,t} \boldsymbol{S}_0^{\mathrm{T}} + \boldsymbol{C}_{w,t}$,
$\boldsymbol{\Sigma}_{t,\hat{S}_c} = \hat{\boldsymbol{S}}_c \boldsymbol{A} \hat{\boldsymbol{S}}_c^{-1} \boldsymbol{C}_{w,t-1} \left(\hat{\boldsymbol{S}}_c \boldsymbol{A} \hat{\boldsymbol{S}}_c^{-1}\right)^{\mathrm{T}} + \hat{\boldsymbol{S}}_c \boldsymbol{C}_{v,t} \hat{\boldsymbol{S}}_c^{\mathrm{T}} + \boldsymbol{C}_{w,t}$. Under hypothesis H_0, the first quadratic term$(\boldsymbol{y}_t - \boldsymbol{\mu}_{t,S_0})^{\mathrm{T}} \boldsymbol{\Sigma}_{t,S_0}^{-1} (\boldsymbol{y}_t - \boldsymbol{\mu}_{t,S_0})$ clearly has central Chi square distribution as $(\boldsymbol{y}_t - \boldsymbol{\mu}_{t,S_0})^{\mathrm{T}} \boldsymbol{\Sigma}_{t,S_0}^{-1/2}$ has zero mean and unit covariance with $3m$ degrees of freedom (d.o.f.). The density of the second non-central quadratic term $(\boldsymbol{y}_t - \boldsymbol{\mu}_{t,\hat{S}_c})^{\mathrm{T}} \boldsymbol{\Sigma}_{t,\hat{S}_c}^{-1} (\boldsymbol{y}_t - \boldsymbol{\mu}_{t,\hat{S}_c})$ can be calculated using either numerical methods or series expansion techniques [15]. Under H_0, the test statistic Λ' is the difference between two random variables (quadratic forms) whose pdf can be obtained by convolution [16]. The general case in (13) can be handled using similar methods.

V. Experimental Results & Discussion

We conduct experiments on the 9-bus 3-machine Western System Coordinating Council (WSCC) system with the state space model specified in [11] to demonstrate the effect of a TSA on DSE and to verify the performance of the hypotheses test. Although simultaneous TSAs on several PMUs are possible, in the experiments, only the PMU on node $i = 1$ is attacked. The results are based on 10^4 Monte Carlo simulations. The DSE procedure is implemented employing the discrete-time Kalman Filter (KF) for $t = 0.1$ to 10s at a sampling rate of 100 samples/s. We choose covariance matrices $\boldsymbol{C}_{w,t}$ and $\boldsymbol{C}_{v,t}$ to be diagonal with identical diagonal elements of $(0.01)^2$. At the time instant $t = 5$s, we induce a TSA by setting $\beta_1(t_c) = b_1 = 1/2f_c = 8.33ms$ ($f_c = 60$Hz, the grid frequency) for $i = 1$ and $\beta_i(t_c) = 0$ for i not equal to 1, which alters the measurement matrix of the model as shown in Section III. After the attack, the KF continues to update the state estimate on receiving a new observation y_t as $\hat{x}_{t|t} = x_{t|\hat{t-1}} + K_t(y_t - S\hat{x}_{t|t-1})$ (K_t: Kalman gain) when the output matrix S_0 has changed to $S_c = MS_0$. The performance of the filtering algorithm is assessed by plotting the root mean squared error (RMSE) of the estimated state variable as a function of time. The RMSE for the rotor angle $\Delta\delta_i$ at time t is given by

$$\mathrm{RMSE}_{\Delta\delta_i,t} = \sqrt{\frac{1}{L} \sum_{\ell=1}^{L} \left(\hat{\Delta\delta}_{i,t}^{\ell} - \Delta\delta_{i,t}^{\ell}\right)^2}, \quad (17)$$

where $\hat{\Delta\delta}_{i,t}^{\ell}$ and $\Delta\delta_{i,t}^{\ell}$ denote the estimate and the true value, respectively, of the rotor angle at time t in the ℓ^{th} Monte Carlo simulation, and L is the number of runs used in Monte Carlo simulations. The RMSE for the internal voltage ΔE_i of the i^{th} generator is defined analogously.

In Fig. 1, we plot the RMSE of rotor angle of the synchronous generator as a function of time. It can be seen that, at $t = 5$s there is a clear jump in RMSE which becomes considerably higher when compared to that under normal operating conditions. These jumps may be dangerous rendering the state estimation useless. A similar behavior is observed in the plot of RMSE of the internal voltage of the generator as shown in Fig. 2. When $\beta_1(t_C) = b_1$ these jumps can be easily perceived. However, when the magnitude of the TSA is small, say $\beta_1(t_c) = b_2 = 0.1b_1$, (refer Fig. 1, Fig. 2) the change in the state estimates is hard to perceive, and still we show the

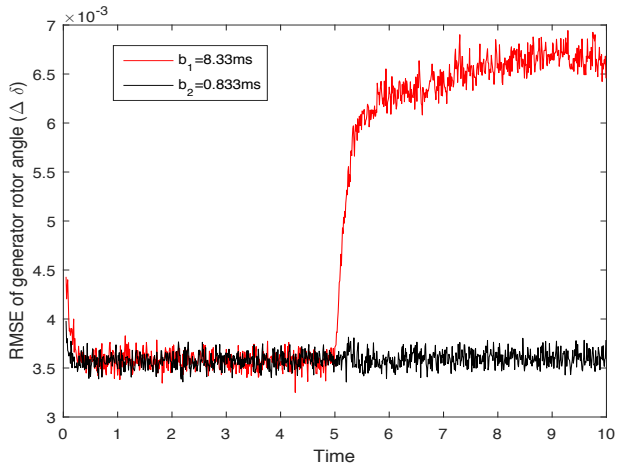

Fig. 1: RMSE of the rotor angle $\Delta\delta_i$ of the synchronous generator i when the TSA is induced at $t_c = 5$s. $\beta_1(t_c) : b_1 = 8.33ms$ or $b_2 = 0.833ms$ are chosen as two TSA parameters.

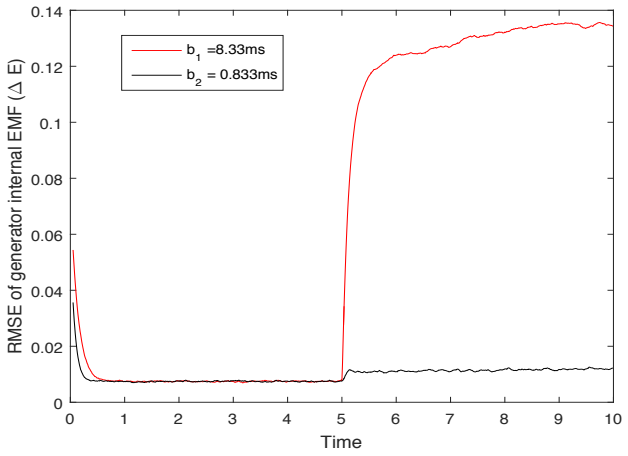

Fig. 2: RMSE of the internal voltage ΔE_i of the synchronous generator i when the TSA is induced at $t_c = 5$s. $\beta_1(t_c) : b_1 = 8.33ms$ or $b_2 = 0.833ms$ are chosen as two TSA parameters.

proposed detection scheme can efficiently decide whether the system is under attack or not.

To evaluate the performance of proposed detection scheme, we generate the receiver operating characteristics (ROC) shown in Fig. 3. To plot the ROC, we choose a range of false alarm rates equally spaced within $[0, 0.088]$. The threshold is picked by inspecting the empirical cumulative distribution function of the test statistic under hypothesis H_0. The threshold then is applied to the test, and the detection rate under hypothesis H_1 and the false alarm rate under H_0 are tabulated. The ROCs are plotted for two different attack parameters, $\beta_1(t_c) = b_2 = 0.833ms$ and $\beta_1(t_c) = b_3 = 0.965ms$ to demonstrate that the detection scheme fares better with the increase in the magnitude of attack parameter. It can be seen that the test succeeds in detecting the change in the measurement matrix from $\boldsymbol{S}_0$ to $\boldsymbol{S}_c$

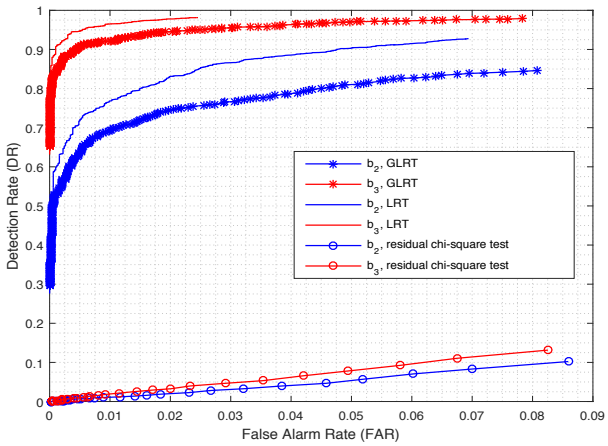

Fig. 3: The ROC curves for the test proposed GLRT compared against LRT and detection using residuals test for attack parameters, $b_2 < b_3$

when the system is subjected to a TSA. We also compare the proposed test with Likelihood Ratio Test (LRT) and chi-square test. The LRT test in which $\beta_1(t_c)$ is assumed to be known gives an upper bound on the ROC of any test, including the GLRT. The test using residual analysis does not perform very well for small time synchronization errors as the errors in the estimation do not change significantly for small model changes. For large values of attack parameter, the residual test performs better while the LRT and GLRT detection rates are one.

VI. Concluding Remarks

In this paper, we showed how GPS spoofing alters the time synchronization of phasor readings recorded by the PMUs and affects the normal operating behavior of the grid. Erroneous estimates of the state vector could lead to faulty monitoring of the grid. To detect changes in the measurement matrix due to the TSA, we devised a hypotheses test to maximize the probability of detection for a given probability of false alarm assuming that the time instant of the spoofing attack is known exactly. However, in practice, the time of attack is not known *a priori* and has to be estimated as quickly and as reliably as possible. This can be accomplished by sequential testing procedures; this is also relegated to future work. Another future extension of this work is to study how a sequence of wrong decisions made based on compromised measurements may cause instability in a practical feedback based Wide Area Control System (WACS). What is the range of the TSA parameter that causes maximum system disruption under different operating points is also an open question.

VII. Acknowledgement

This material is based upon work supported by the Department of Energy under Award Number DE-OE0000779.

REFERENCES

[1] A.G. Phadke and J.S. Thorp, "Communication needs for wide area measurement applications," in *Proc. IEEE Int. Conf. Critical Infras.*, Sept. 2007, pp. 1–7.

[2] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: Attack strategies and countermeasures," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, Oct. 2010, pp. 220–225.

[3] S. Cui, Z. Han, S. Kar, T. T. Kim, H. V. Poor, and A. Tajer, "Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions," *IEEE Signal Process. Mag.*, vol. 29, no. 5, pp. 106–115, Sept. 2012.

[4] S. Liu, S. Mashayekh, D. Kundur, T. Zourntos, and K. Butler-Purry, "A framework for modeling cyber-physical switching attacks in smart grid," *IEEE Trans. Emerg. Topics Comput.*, vol. 1, no. 2, pp. 273–285, Dec. 2013.

[5] T. E. Humphreys, B. M. Ledvina, M. L. Psiaki, B. W. O'Hanlon, and P. M. Kintner, "Assessing the spoofing threat: Development of a portable GPS civilian spoofer," in *Proc. Int. Tech. Meet. Satellite Div. The Ins. Navigation*, Sept. 2008, pp. 2314–2325.

[6] S. Gong, Z. Zhang, M. Trinkle, A. D. Dimitrovski, and H. Li, "GPS spoofing based time stamp attack on real time wide area monitoring in smart grid," in *Proc. IEEE Int. Conf. Smart Grid Commun.*, Nov. 2012, pp. 300–305.

[7] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to GPS spoofing attacks," *Int. J. Critical Infras. Protect.*, vol. 5, no. 3-4, pp. 146–153, Dec. 2012.

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

[9] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela, and A. D. Domínguez-García, "Spoofing GPS receiver clock offset of phasor measurement units," *IEEE Trans. Power Systems*, vol. 28, no. 3, pp. 3253–3262, Aug. 2013.

[10] Y. Fan, Z. Zhang, M. Trinkle, A. D. Dimitrovski, J. B. Song, and H. Li, "A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart grids," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 2659–2668, Aug. 2015.

[11] P. W. Sauer and M. A. Pai, *Power System Dynamics and Stability*, Prentice Hall, 1998.

[12] A. Chakrabortty and P. P. Khargonekar, "Introduction to wide-area control of power systems," in *Proc. IEEE American Control Conf.*, June 2013, pp. 6758–6770.

[13] Tuomas Rauhala and Pertti Järventausta, "Testing the quality of pmu output data based subsynchronous damping analysis in real-time simulation environment," in *International Conference on Power Systems Transients (IPST07)*, 2007, pp. 1–8.

[14] H. V. Poor, *An Introduction to Signal Detection and Estimation*, Springer-Verlag, 2 edition, 1994.

[15] Arakaparampil M Mathai and Serge B Provost, *Quadratic forms in random variables: theory and applications*, M. Dekker New York, 1992.

[16] Athanasios Papoulis and S Unnikrishna Pillai, *Probability, random variables, and stochastic processes*, Tata McGraw-Hill Education, 2002.