5-1-2018

Reliability Test for the Proposed GPS Spoofing Attack Detection Scheme

Alireza Famili
Lehigh University, afamili93@gmail.com

Reliability Test for the Proposed GPS Spoofing Attack Detection Scheme

by

Alireza Famili

A Thesis

Presented to the Graduate and Research Committee

of Lehigh University

in Candidacy for the Degree of

Master of Science

in

Electrical and Computer Engineering

Lehigh University

(May 2018)

Alireza Famili THESIS SIGNATURE SHEET

This thesis is accepted and approved in partial fulfillment of the requirements for the Master of Science.

_____

Date

Rick S. Blum

_____

Thesis Advisor

Chengshan Xiao

_____

Chair of ECE Department

Acknowledgement

I hope to recognize all the people to whom I am faithfully grateful and owe a grave gratitude and appreciation for their efforts and contributions towards my development.

First and foremost, I express my utmost gratitude to my advisor, Professor Rick S. Blum who always been extremely supportive and kind to me during my life here at Lehigh. Getting to know and work with him is one of the greatest experience I've ever had. I learned about many important topics under the direct supervision of Prof. Blum but I think the indirect lessons I learned through observing his honesty, supporting, and selflessness were perhaps the more valuable thing I got that I will never forget in rest of my life.

I would like to express my sincere and special appreciation to Prof. Kishore and Prof. Venkitasubramaniam for their useful guide that ease the path of research for me. Prof. Kishores great knowledge helped me dive deeper into the different topics I studied with purpose and excitement.

I extend my appreciation to my senior Ph.D. student, Parth Pradhan, for our ample of conversations on different topics from smart grids and GPS Spoofing attack to many other topics we discussed. My thanks go to my friends and colleagues at SPCRL Lab for their support and enjoyable conversations: Basel Alnajjab, A. K. Karthik, Jake Perazzone, Ananth Narayan, Yichung Chen, Yongjun Liu, and Zisheng Wang. I am also grateful for our staff members David Morrisette, Diane Hubinsky, and Ruby Scott who were always very helpful and caring.

The importance of the support and encouragement I received outside of Lehigh could not be overstated. All the great experiences and opportunities I was able to

enjoy and take advantage of throughout my life would be impossible without my parents. Their love, encouragement, and dedication have shaped much of who I am today. I am grateful for their endless life-enriching contributions forever and I hope I can make them proud of my character and actions.

Contents

List of Figures

1 Abstract

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 Master's Thesis, we provide two sets of tests for the existing detection scheme which address the problem of cybersecurity in smart grid networks involving PMUs (Phasor Measurement Units) taking into account the dynamical nature of the power system [5].

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 [6]. 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) [7]. 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 [8]- [11].

In this Master's Thesis, we propose two sets of tests for the existing GPS spoofing attack detection scheme [5] to check the performance of the scheme under

different circumstances. In the first sets of test (α test), we simulate the 9−bus, 3−generator IEEE power system in MATLAB and using this simulated system, we apply our test for checking the performance of detection scheme. In the other word, in the α test, we use the simulated data and test the detection scheme. We will investigate the performance of the detection scheme due to changes in attack parameter (which is the time delay made by attacker to spoof the authenticated GPS signal), window size (which is the number of sample in a window we want to check), and examine the performance in the case of unknown time of attack (which means that the time of attack is not known in the detection scheme). The second half of the thesis is dedicated to the second sets of test (β test), in which we use the data from Real-Time Renewable Microgrid Test-bed lab at Lehigh University. The key difference between α and β testing is the data used for the test. In the α test, data comes from the simulated power grid in MATLAB and in the β test, the data comes from one of the labs at Lehigh.

2 Introduction on α Testing

In this section, we document the alpha testing on our algorithm for detecting the time synchronization attack on phasor measurement units (PMUs). First, we will describe the system we used for the testing. Then, the performance of our algorithm will be analyzed for the different attack parameters (β) and window sizes (number of samples). With larger β or larger window sizes, the detection algorithm performs better. Our goal is to show that even with small β and small windows, our algorithm can detect the attack with the large probability. In particular, we find the minimum window size for which the detection algorithm provides acceptable detection performance for the smallest value of β we must consider. We also provide performance for cases where the time of attack is unknown and we need to estimate both β and time of attack.

3 System Description

We conduct experiments on the 9−bus 3−machine Western System Coordinating Council (WSCC) test case with the state space model specified in [12] to demonstrate the effect of a TSA and to verify the performance of the hypotheses test. Figure 1 is a block diagram of this system. We assume a PMU is located at each of the generator nodes. 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 $500,000$ Monte Carlo simulations. First we linearize our system model around an operating point as described in [13]. Let S_0 denote the output matrix of this linearized state space model [14]. In the linearized state space model, we choose

the covariance matrices $C_{w,t}$ (the covariance matrix for the noise vector in input-output equation) and $C_{v,t}$ (the covariance matrix for the noise vector in dynamical equation) to be diagonal with identical diagonal elements of $(0.01)^2$. The dynamic state estimation (DSE) procedure is implemented by employing the discrete-time Kalman Filter (KF) for $t = 0.1$ to $10s$ at a sampling rate of 100 $samples/s$.

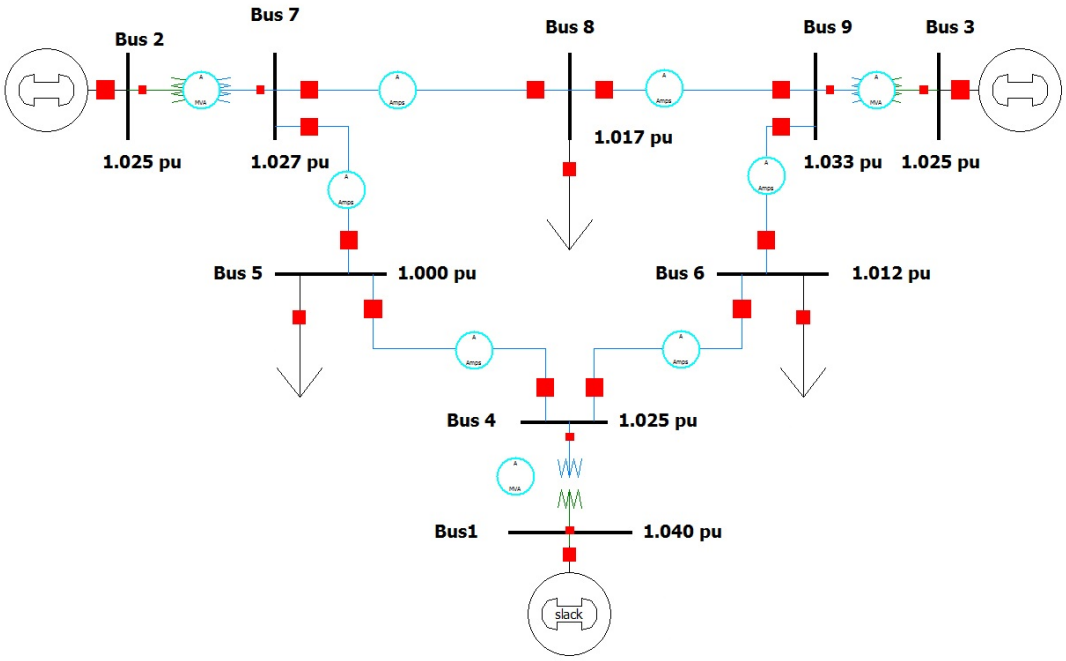

Figure 1: This WSCC 3 Machine, 9 Bus Test Case (known as P.M Anderson 9 Bus) represents a simple approximation of the Western System Coordinating Council (WSCC) actual implementation.

4 Effect of the attack parameter, β

At the time instant $t = 5$s, we induce a TSA by setting the attack parameter at node 1 equal to $8.33ms$ and the attack parameter for all other nodes equal to 0 ($\beta_i(t_c) = b_1 = 1/2f_c = 8.33ms$ for $i = 1$ and $\beta_i(t_c) = 0$ for i not equal

to 1, where $f_c = 60$Hz is the grid frequency, β_i represents the attack parameter at the i^{th} node, and t_c is the time instance in which attack happened), which alters the measurement matrix of the model. After the attack, the KF continues to update the state estimate on receiving a new observation y_t as $\hat{x}_{t|t} = x_{t|\hat{t-1}} + K_t(y_t - S_0\hat{x}_{t|t-1})$ (K_t: Kalman gain) when the output matrix S_0 has changed to $S_c = MS_0$ where M is described in [ref to our conf paper]. 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

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

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 2, we plot the RMSE of the rotor angle of the synchronous generator at node 1 as a function of time. It can be seen that, at $t = 5$s there is a clear jump in RMSE which is not present under normal operating conditions. These jumps may be dangerous, rendering the state estimation useless. A similar behavior is observed in the plot of the RMSE of the internal voltage of the generator at node 1 as shown in Fig 3. 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 2, Fig 3) the change in the state estimates is hard to perceive, and still we

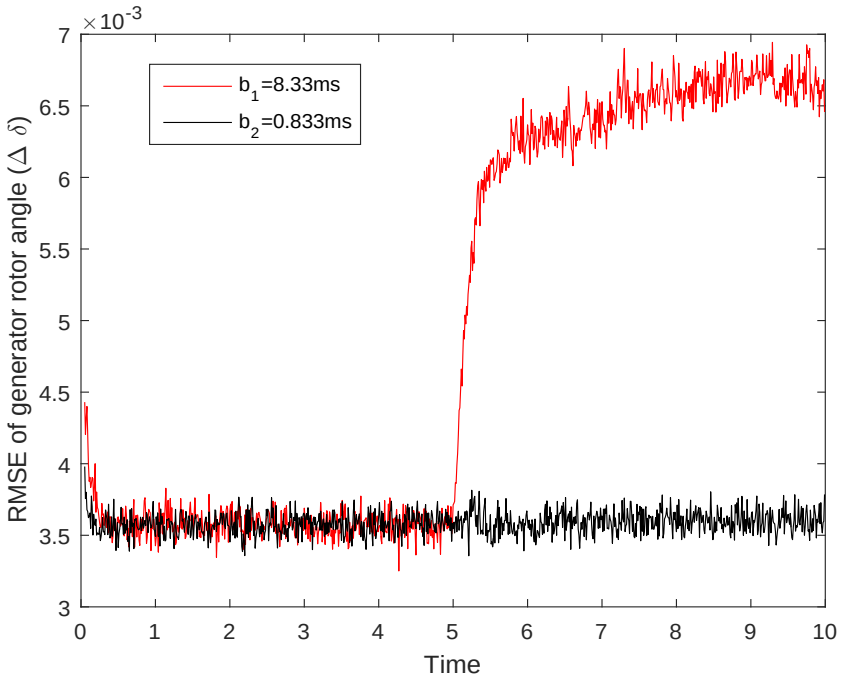

Figure 2: RMSE of the rotor angle $\Delta\delta_1$ of the synchronous generator 1 when the TSA is induced at time of attack equal to 5s ($t_c = 5$s). $\beta_1(t_c) = b_1$ or b_2 where $b_1 = 8.33ms$ and $b_2 = 0.833ms$ are chosen as two TSA parameters.

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

To evaluate the performance of the proposed detection scheme, we generate the receiver operating characteristics (ROC) shown in Fig 4. To plot the ROC, we choose a range of false alarm rates equally spaced within $[0, 0.1]$. 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 and the false alarm rate are tabulated. The ROCs are plotted for some different attack parameters, $\beta_1(t_c) = b_3 = 0.133ms$, $\beta_1(t_c) = b_4 = 0.186ms$, $\beta_1(t_c) = b_5 = 0.239ms$, and $\beta_1(t_c) = b_6 = 0.292ms$ to demonstrate that

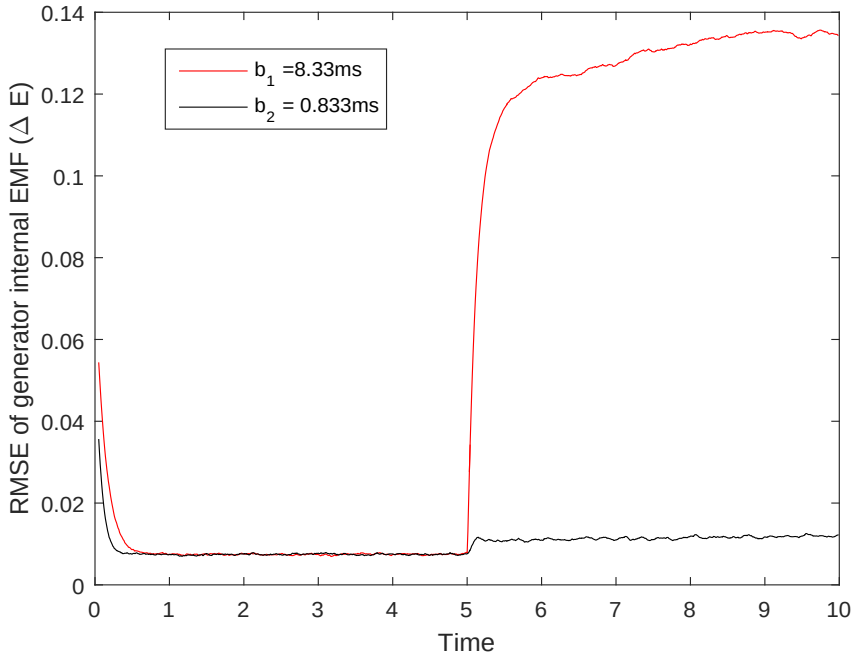

Figure 3: RMSE of the internal voltage ΔE_1 of the synchronous generator 1 when the TSA is induced at $t_c = 5$s. $\beta_1(t_c) : b_1 = 8.33ms$ or $b_2 = 0.833ms$ are chosen as two TSA parameters.

the detection scheme fares better with the increase in the magnitude of attack parameter. In the literature time shifts smaller than $0.013ms$ are said to occur due to normal operation and they do not cause significant problems. Thus such small changes do not be detected. We also compare the ROC performance of the proposed test with the unrealizable (since β unknown) Likelihood Ratio Test (LRT). 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. In all the tests shown in Fig 4, the ROCs for the GLRT are close to those for the LRT.

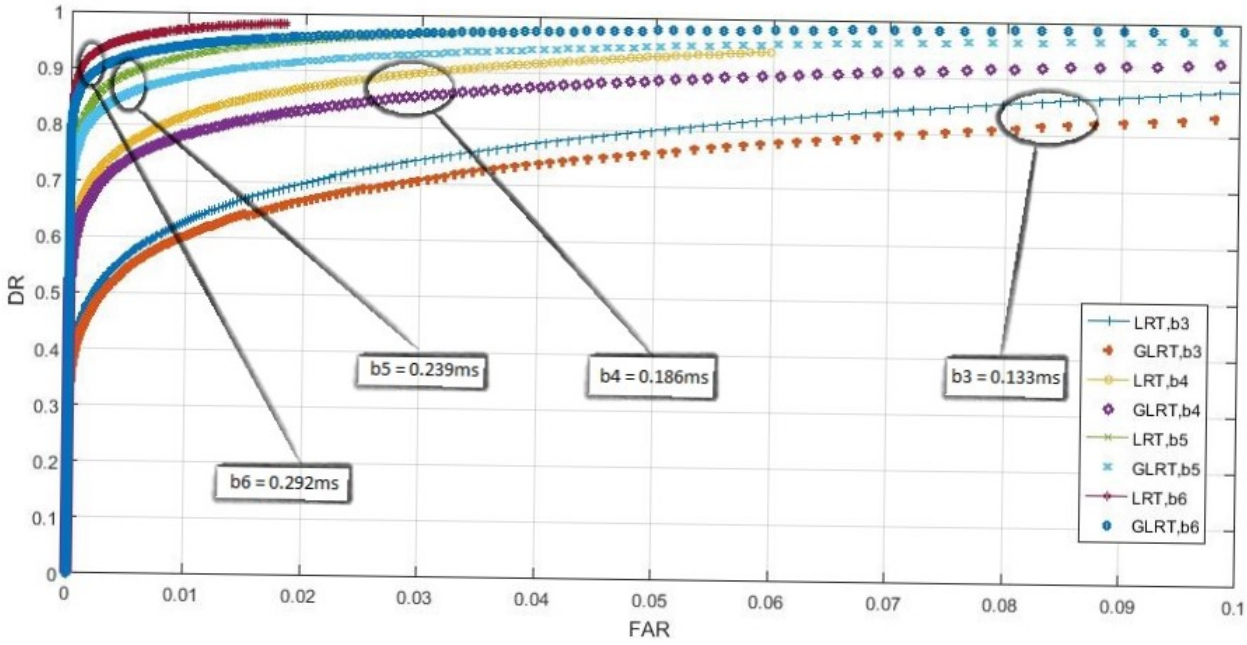

Figure 4: The ROCs for the proposed GLRT compared to the ROCs for the unrealizable LRT for attack parameters, b3 < b4 < b5 < b6

5 Effect of the Window Size

By increasing the window size, more samples will become available to better characterize the attack and reduce the impact of noise. On the other hand, there is a trade off between having a better detection and needing more samples that consumes a delay in making the decision. In this section, our goal is to find the minimum window size for which the algorithm can detect TSA even with small β. Therefore, we provide the ROCs for a different window sizes.

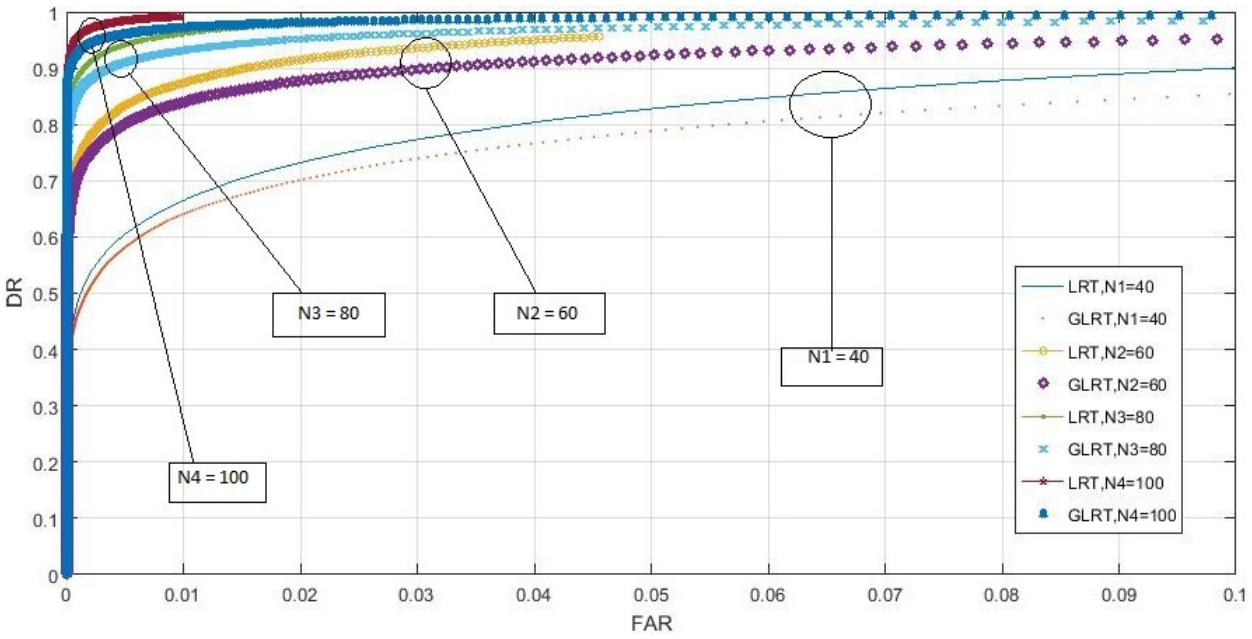

Figure 5: The ROCs for the proposed GLRT compared to the ROCs for the unrealizable LRT for attack parameter equal to $0.278ms$ and different window size: $N_1 = 100$, $N_2 = 80$, $N_3 = 60$, $N_4 = 40$

6 Unknown Time of Attack

In all the work we have done so far for detecting the TSA on smart grid, we assume that the time of attack is known and the only unknown parameter is β. In this section, we provide simulations in which time of attack is also unknown; thus, the algorithm should estimate β and time of attack. It is not surprising that the results show the unknown attack time will degrade performance but the degradation is not very large.

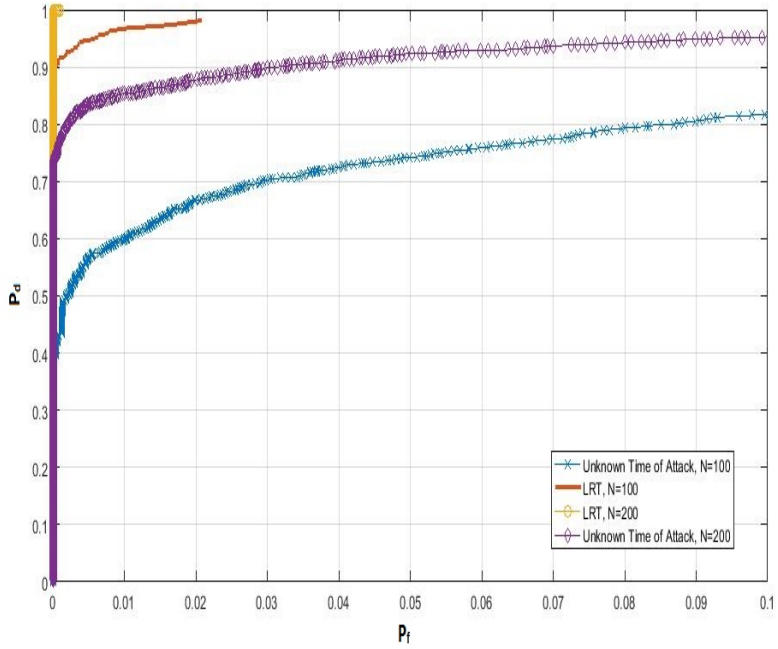

Figure 6: ROC for the proposed GLRT for Unknown Time of Attack compared to the ROC for the unrealizable LRT for attack parameter $\beta = 0.236ms$ and window size = 200 , 100

7 Introduction on β Testing

In this section, we document the beta testing of our algorithm for detecting a time synchronization attack (TSA) on phasor measurement units (PMUs). In this section we explain the theoretical background of the algorithm which will be tested. Then, in the following sections, we will describe the testbed, our scenario for testing, metric of the successful test, and finally in the last section provide the results to show the algorithm passes this beta testing successfully.

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 [5], [15]. We consider an n-bus, m-generator system (in our testing we use $9-$bus, $3-$generator) where the state vector of the linearized model for synchronous generator $i = 1, \ldots, m$ is denoted by $\Delta \boldsymbol{x}_i = [\Delta\delta_i, \Delta\omega_i, \Delta E_i]^{\mathrm{T}}$. The state $\Delta \boldsymbol{x}_i$ 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. We model the evolution of the $3m \times 1$ state vector $\Delta \boldsymbol{x}_t = [\Delta \boldsymbol{x}_1, \Delta \boldsymbol{x}_2, \ldots, \Delta \boldsymbol{x}_i, \ldots, \Delta \boldsymbol{x}_m]^{\mathrm{T}}$ by

$$\Delta \boldsymbol{x}_{t+1} \;=\; \boldsymbol{A}\Delta \boldsymbol{x}_t + \boldsymbol{v}_t, \tag{2}$$

where $\boldsymbol{A}$ is the $3m \times 3m$ (for the 3^{rd}-order model) state transition matrix. 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 $\boldsymbol{C}_{v,t}$. Noise is present in most sensor measurements but we can model accurate sensors with very small noise power also.

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. Thus, before subtracting out the steady state, we have $V_{ri} = V_i \cos(\theta_i)$ and $V_{ji} = V_i \sin(\theta_i)$. The $3m \times 1$ measurement vector at time t is the deviation of the measurements from steady state measurement values denoted by $\Delta \boldsymbol{y_t} = [\Delta \boldsymbol{y_1}, \Delta \boldsymbol{y_2}, \ \ldots \ , \Delta \boldsymbol{y_n}]^{\mathrm{T}}$ where $\Delta \boldsymbol{y}_i \triangleq [\Delta V_{ri}, \Delta \omega_i, \Delta V_{ji}]^{\mathrm{T}}$. The measurements are related to state by the model

$$\Delta \boldsymbol{y}_t \ = \ \boldsymbol{S} \Delta \boldsymbol{x}_t + \boldsymbol{w}_t, \tag{3}$$

where $\boldsymbol{w}_t$ is the $3m \times 1$ measurement noise vector assumed to be $i.i.d$ and Gaussian with zero mean vector and $3m \times 3m$ covariance matrix $\boldsymbol{C}_{w,t}$. We will detect the TSA based on observing $\Delta \boldsymbol{y_t}$ over a window.

In this section, we show how a TSA alters the measurement matrix $\boldsymbol{S}$ in (3). The voltage represented in complex phasor form at generator i is given by $\tilde{V}_i = V_{ri} + jV_{ji}$, where V_{ri} and V_{ji} denote the real and imaginary components, respectively. A time synchronization attack on a PMU at node i, with time change denoted by $\beta_i(t_c)$, modifies the instantaneous nodal voltage signal by introducing

a phase change

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

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) can be approximated as narrow-band (slowly varying 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 nominal 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

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

which is compactly written as

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

Subtracting out the steady state of (7) results in

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

So, the new measurement equation after a TSA is given by

$$\Delta \boldsymbol{y}'_t \;=\; \boldsymbol{M}\boldsymbol{S}\Delta \boldsymbol{x}_t + \boldsymbol{w}_t, \tag{9}$$

where M is the matrix shown in (8).

Now, we describe how to detect a TSA. We present a statistical hypotheses testing procedure to detect changes in the measurement matrix in the event of a TSA. We denote the before attack matrix $\boldsymbol{S}$ as $\boldsymbol{S_0}$. Let us suppose that a TSA has been initiated at the time instant t_c, leading to an alteration of the measurement matrix $\boldsymbol{S}_0$. Initially assume t_c is known. We denote the attacked measurement matrix as $\boldsymbol{S}_c \triangleq \boldsymbol{M}\boldsymbol{S}_0$ (see (9)). Given the set $\Delta\boldsymbol{y}^t \triangleq \{\Delta\boldsymbol{y}_1, \ldots, \Delta\boldsymbol{y}_t\}$ of measurements, the problem is formulated as one of devising a statistical testing procedure to detect the change in the measurement matrix as reliably as possible. More precisely, we need to devise a test to distinguish between the following two hypotheses:

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

The hypotheses test involves comparing a test statistic Λ to a threshold ρ.

We adopt the Neyman-Pearson (NP) criterion which maximizes the probability of attack detection for a fixed probability of attack false alarm. Let $p(\Delta \boldsymbol{y}_t|\Delta \boldsymbol{y}_{t-1}; \boldsymbol{S}_0)$ denote the probability density function of observing $\Delta \boldsymbol{y_t}$ in (9) at time given t. Given $\Delta \boldsymbol{y_{t-1}}$ was observed at time $t-1$ when the measurement matrix $\boldsymbol{S}$ is $\boldsymbol{S_0}$. We use similar notation when $\boldsymbol{S} = \boldsymbol{S}_c$. The NP test statistic, called the likelihood ratio, is given by

$$\Lambda \;=\; \frac{p(\Delta \boldsymbol{y}_T|\Delta \boldsymbol{y}_{T-1}; \boldsymbol{S}_c) \times \cdots \times p(\Delta \boldsymbol{y}_{t_c+1}|\Delta \boldsymbol{y}_{t_c}; \boldsymbol{S}_c)}{p(\Delta \boldsymbol{y}_T|\Delta \boldsymbol{y}_{T-1}; \boldsymbol{S}_0) \times \cdots \times p(\Delta \boldsymbol{y}_{t_c+1}|\Delta \boldsymbol{y}_{t_c}; \boldsymbol{S}_0)}. \tag{10}$$

If we assume knowledge of the time instant t_c when the spoofing attack is launched, there results provide upper bounds on the performance of hypotheses tests where t_c is unknown and has to be estimated. If t_c is unknown, one can consider a finite time-window and look for a value of t_c which maximizes the likelihood function. This is like using a maximum likelihood estimator for t_c. This is an accepted approach called the generalized likelihood ratio (GLRT) approach. The GLRT statistic is given by

$$\Lambda = \frac{\max\limits_{\beta} \left[p(\Delta \boldsymbol{y}_t|\Delta \boldsymbol{y}_{t-1}; \boldsymbol{S}_c) \times \cdots \times p(\Delta \boldsymbol{y}_{t_c+1}|\Delta \boldsymbol{y}_{t_c}; \boldsymbol{S}_c)\right]}{p(\Delta \boldsymbol{y}_t|\Delta \boldsymbol{y}_{t-1}; \boldsymbol{S}_0) \times \cdots \times p(\Delta \boldsymbol{y}_{t_c+1}|\Delta \boldsymbol{y}_{t_c}; \boldsymbol{S}_0)}. \tag{11}$$

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

$$p(\Delta \boldsymbol{y}_t|\Delta \boldsymbol{y}_{t-1}; \boldsymbol{S}_c) = \frac{\exp\left\{-\frac{1}{2}(\Delta \boldsymbol{y}_t - \boldsymbol{\mu}_t)^{\mathrm{T}} \boldsymbol{\Sigma}_t^{-1} (\Delta \boldsymbol{y}_t - \boldsymbol{\mu}_t)\right\}}{(2\pi)^{K/2} |\boldsymbol{\Sigma}_t|^{1/2}}, \tag{12}$$

where $\boldsymbol{\mu}_t \triangleq \mathbb{E}[\Delta \boldsymbol{y}_t|\Delta \boldsymbol{y}_{t-1}] = \boldsymbol{S}_c \boldsymbol{A} \boldsymbol{S}_c^{-1} \Delta \boldsymbol{y}_{t-1}$ is the mean vector and $\boldsymbol{\Sigma}_t \triangleq \mathrm{Cov}[\boldsymbol{y}_t|\Delta \boldsymbol{y}_{t-1}] = \boldsymbol{S}_c \boldsymbol{A} \boldsymbol{S}_c^{-1} \boldsymbol{C}_{w,t-1} \left(\boldsymbol{S}_c \boldsymbol{A} \boldsymbol{S}_c^{-1}\right)^{\mathrm{T}} + \boldsymbol{S}_c \boldsymbol{C}_{v,t} \boldsymbol{S}_c^{\mathrm{T}} + \boldsymbol{C}_{w,t}$ is the covariance matrix.

8 Testbed Configuration

We conduct experiments on the 9−bus 3−machine Simulated Power System in the Real-Time Renewable Microgrid Test-bed lab at Lehigh University to demonstrate the effect of a TSA and to verify the performance of the hypotheses test. Figure 8 shows the equipment used. We assume a PMU is located at each of the nine nodes. Although simultaneous TSAs on several PMUs are possible, in the beta tests, only the PMU on node $i = 1$ is attacked. We did test attacks on multiple PMUs in alpha testing.

Figure 7: Real-Time Renewable Microgrid Test-bed lab, Lehigh University

The detailed $IEEE\ 9-bus$ model is shown in Figure 8. A sixth-order state space model is used for the generators. The Pi model is used for transmission lines. As a result, the model can capture the dynamics of the system. [16], [17]

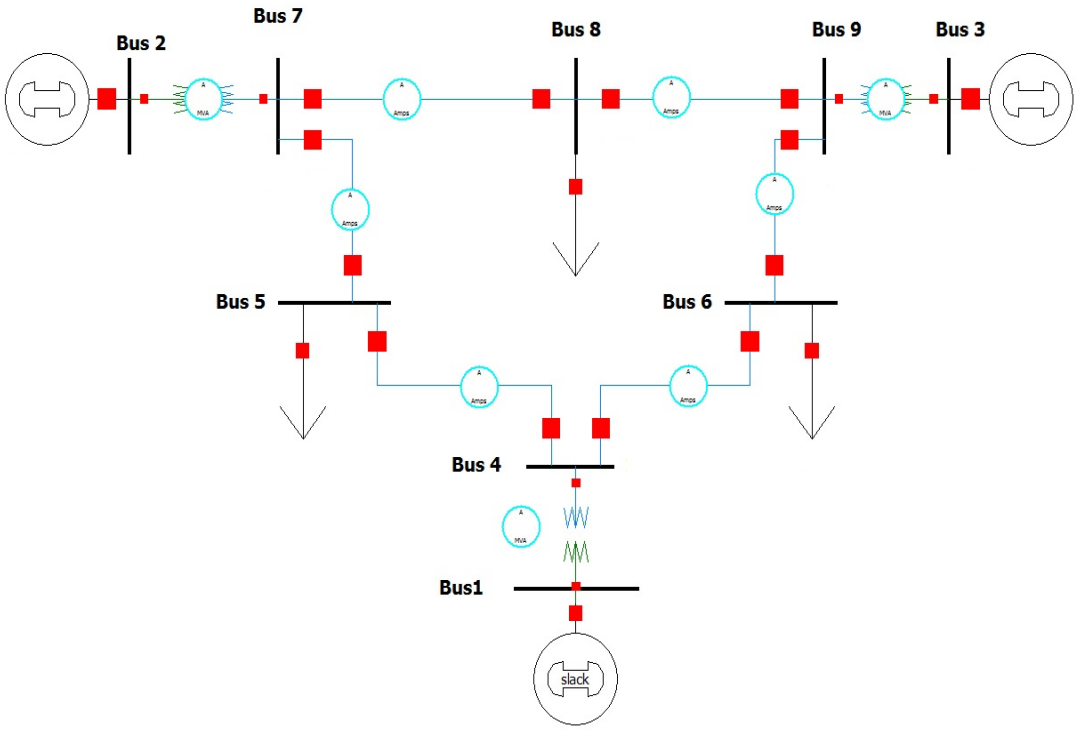

Figure 8: IEEE 9 Bus System

A wide variety of power systems can be simulated using the Real-time simulator at Lehigh University. The simulations can run in real time, generating data that fully captures the dynamics of the system. A wireless communication link is established between the Real-time simulator and a PC, transmitting measurements gathered from the model. Measurements are then received by the PC and fed into the TSA detection algorithm.

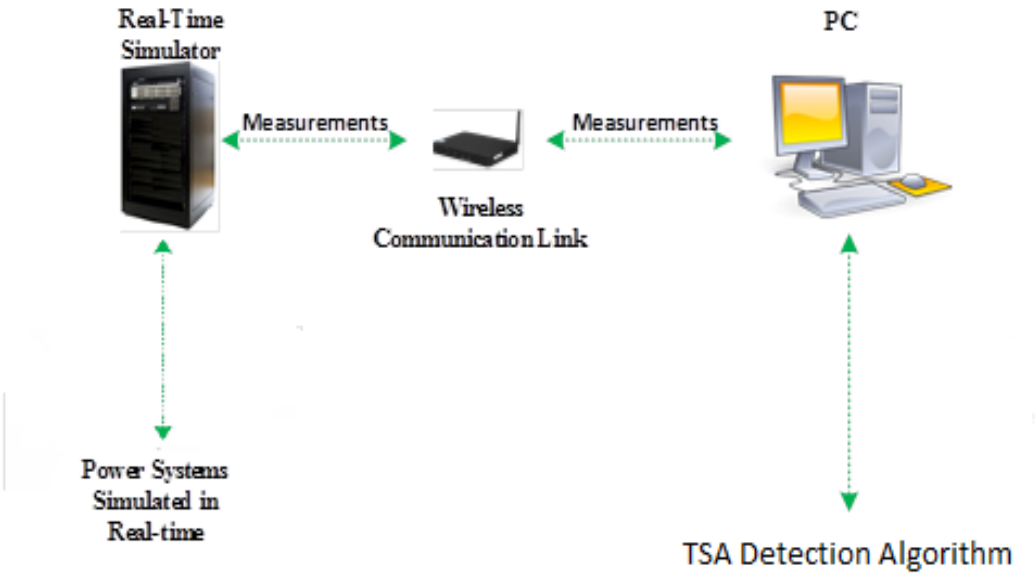

Figure 9: Overview of the Testbed Configuration

9 Testing Scenarios

To apply our testing method, first we received time sampled measurements from the real time simulator where k is the discrete time index. Our measurements are $\boldsymbol{x}_i(k) = [\delta_i(k), \omega_i(k), E_i(k)]^{\mathrm{T}}$, $\boldsymbol{x}_i(k+1) = [\delta_i(k+1), \omega_i(k+1), E_i(k+1)]^{\mathrm{T}}$, and $\boldsymbol{y}_i(k) = [V_{ri}(k), \omega_i(k), V_{im}(k)]^{\mathrm{T}}$. We have 3 generators $i = 1, 2, 3$ and we use 1000 samples in our testing, so $k = 1, ..., 1000$. To fit the data with a state space model, we first subtract the steady state value to obtain $\Delta\boldsymbol{x}_i(k) = [\Delta\delta_i(k), \Delta\omega_i(k), \Delta E_i(k)]^{\mathrm{T}}$, $\Delta\boldsymbol{x}_i(k+1) = [\Delta\delta_i(k+1), \Delta\omega_i(k+1), \Delta E_i(k+1)]^{\mathrm{T}}$, and $\Delta\boldsymbol{y}_i(k)$. Then using 2 and 3, we use a Least-Square method to find $\boldsymbol{A}$ and $\boldsymbol{S_0}$ [18], [19].

10 Metric for Successful Test

To demonstrate our algorithm works correctly, we will plot the probability of detection vs probability of false alarm (attack detected but no attack present) in the next section. We will see the probability of detection is very close to unity for all false alarm probabilities. This is proper for a correctly functioning test. We also compare our performance to the performance for an optimum unachievable test (Likelihood Ratio Test-LRT) which knows the exact attack. We show our performance is close to this unachievable test.

11 Results of Beta Testing

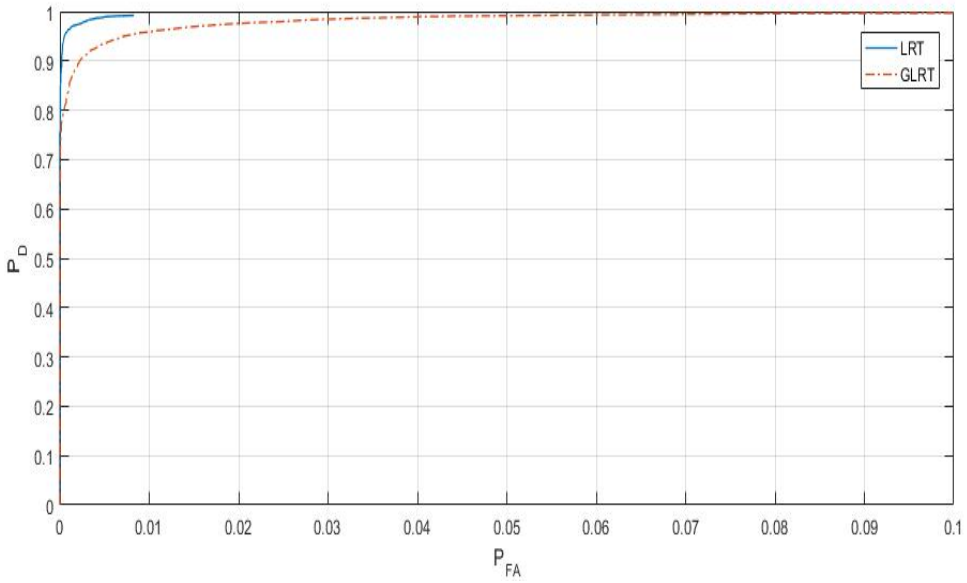

Figure 10: ROC curve when attack parameter is equal to 0.279 ms, the window size is $N = 100$, and the time of attack is $t_c = 5s$.

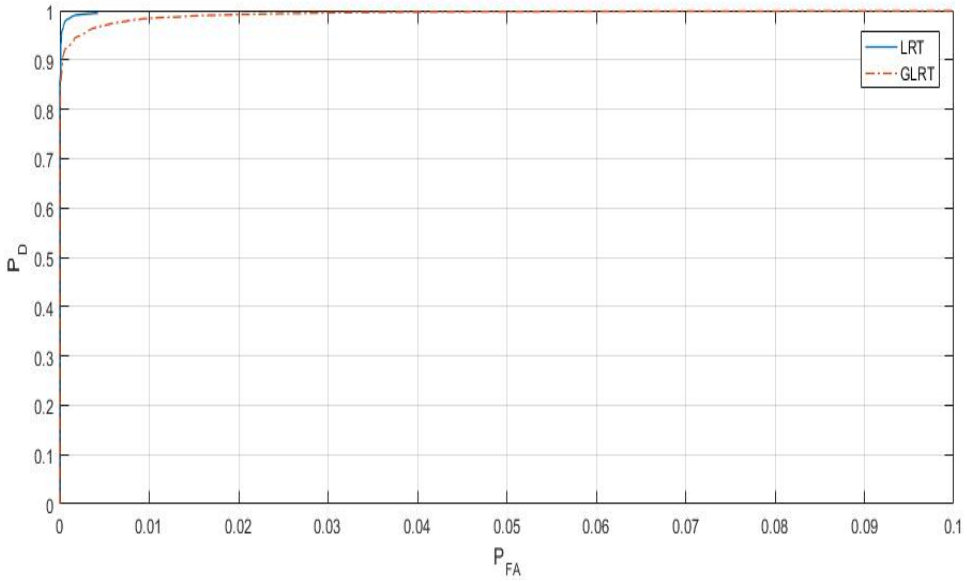

Figure 11: ROC curve when attack parameter is equal to 0.305 ms, the window size is $N = 100$, and the time of attack is $t_c = 5s$.

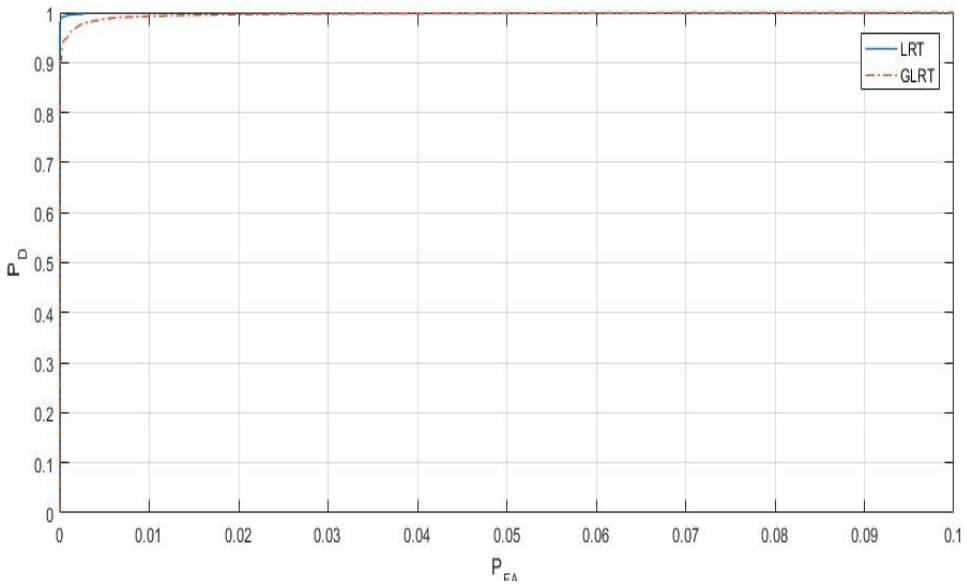

Figure 12: ROC curve when attack parameter is equal to 0.332 ms, the window size is $N = 100$, and the time of attack is $t_c = 5s$.

According to Figures 10, 11, and 12, the algorithm has good performance for small attack parameters ($\beta = 0.279\ ms$). Further, by increasing the attack parameter ($\beta = 0.305\ ms$, $\beta = 0.332\ ms$), the detection performance is even better.

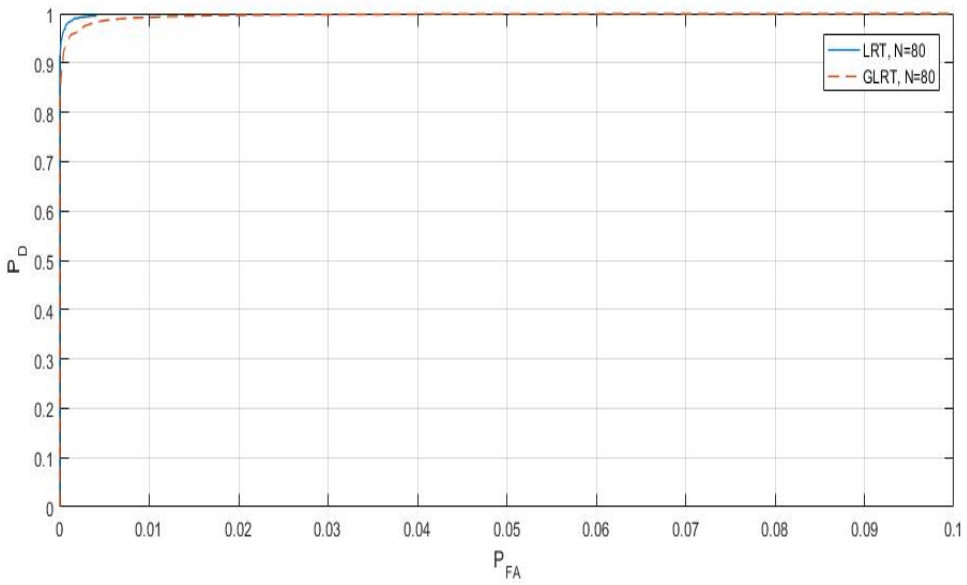

Figure 13: ROC curve when attack parameter is equal to 0.332 ms, the window size is $N = 80$, and the time of attack is $t_c = 5s$.

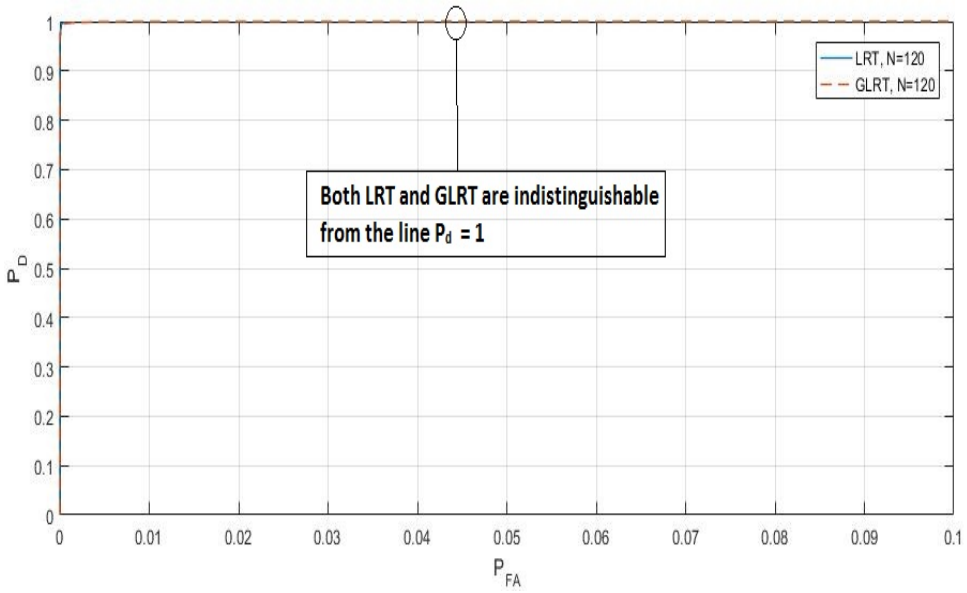

Figure 14: ROC curve when attack parameter is equal to 0.332 ms, the window size is $N = 120$, and the time of attack is $t_c = 5s$.

Figures 13 and 14 show the impact of window size on the detection algorithm. Increasing the number of samples in each case increases the performance of detection algorithm.

According to our previous testing (α *testing*) and also by theory, we know that increasing β or N will increase the detection performance. We observed this in our tests.

In all of the results that we have presented so far, we know the time of the attack. Figure 15 shows the ROC for the case where the time of attack is unknown and we have to estimate it. There is some loss for estimating the time of attack, but the performance is still good.

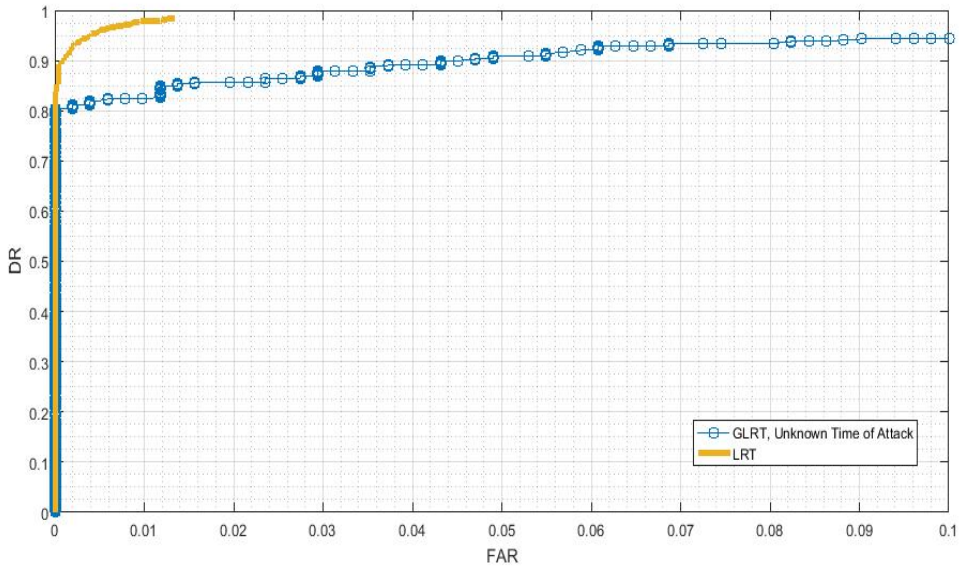

Figure 15: ROC curve when the window size is $N = 100$ and the time of attack is unknown.

References

[1] A. Phadke and J. Thorp, "Communication needs for wide area measurement applications," in *Proc. IEEE Int. Conf. Critical Infras.*, Sep. 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, Sep. 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] P. Pradhan, K. Nagananda, P. Venkitasubramaniam, S. Kishore, and R. S. Blum, "Gps spoofing attack characterization and detection in smart grids," in *2016 IEEE Conference on Communications and Network Security (CNS)*, Oct 2016, pp. 391–395.

[6] 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*, Sep. 2008, pp. 2314–2325.

[7] 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.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] P. Sauer and M. Pai, *Power system dynamics and stability.* Prentice Hall, 1998.

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

[14] P. Pradhan, K. Nagananda, P. Venkitasubramaniam, S. Kishore, and R. S. Blum, "Gps spoofing attack characterization and detection in smart grids," in *2016 IEEE Conference on Communications and Network Security (CNS)*, Oct 2016, pp. 391–395.

[15] P. Sauer and M. Pai, *Power system dynamics and stability.* Prentice Hall, 1998.

[16] J. Duan, H. Xu, and W. Liu, "Q-learning based damping control of wide-area power systems under cyber uncertainties," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–1, 2017.

[17] Opal-rt technologies. [Online]. Available: http://www.opal-rt.com/software-rt-lab/

[18] H. W. Sorenson, "Least-squares estimation: from gauss to kalman," *IEEE Spectrum*, vol. 7, no. 7, pp. 63–68, July 1970.

[19] H. O. J. Olkkonen, "Least squares matrix algorithm for state-space modelling of dynamic systems," *Journal of Signal and Information Processing*, vol. 2, no. 4, pp. 287–291, November 2011.

12 Vita

My name is Alireza Famili. I was born at December 8th, 1993 in Tehran (capital city of Iran). After getting my Bachelor degree in Electrical engineering from University of Tehran, I came to US and joined Lehigh University. Right now, I have been here at Lehigh for almost two years. This is my Master thesis which shows that I am going to graduate with the Master degree from Lehigh University.