Assessment of Cyber Vulnerabilities and Countermeasures for GPS-Time Synchronized Measurements in Smart Grids

Imtiaj Khan

Dissertation submitted to the Faculty of the
Virginia Polytechnic Institute and State University
in partial fulfillment of the requirements for the degree of

Doctor of Philosophy
in
Electrical Engineering

Virgilio Centeno, Chair
Chen-Ching Liu
Jaime De La Reelopez
Yuhao Zhang
Vimal Biswanath

June 24, 2024
Blacksburg, Virginia

Keywords: PMU, GPS-spoofing, Hankel-matrix, Cyberattack, Testbed

Assessment of Cyber Vulnerabilities and Countermeasures for GPS-Time Synchronized Measurements in Smart Grids

Imtiaj Khan

(ABSTRACT)

We aim at expanding the horizon of existing research on cyberattacks against the time-syncrhonized devices such as PMUs and PDCs, along with corresponding countermeasures. We develop a PMU-PDC cybersecurity testbed at Virginia Tech Power and Energy Center (PEC) lab. The testbed is able to simulate real-world GPS-spoofing attack (GSA) and false data injection attack (FDIA) scenarios. Moreover, the testbed can incorporates cyberattack detection algorithm in pseudo real-time. After that, we propose three stealthy attack scenarios that exploit the vulnerabilities of time-synchronization for both PMU and PDC. The next part of this dissertation is the enhancement of Hankel-matrix based bad data detection model. The existing general Hankel-matrix based bad data detection model provide satisfactory performance. However, it fails in differentiating GPS-spoofing attack from FDIA. We propose an enhanced phase angle Hankel-matrix model that can conclusively identify GPS-spoofing attack. Furthermore, we reduce the computational burden for Hankel-matrix based bad data and cyberattack detection models. Finally, we verify the effectiveness of our enhanced Hankel-matrix model for proposed stealthy attack scenarios.

Assessment of Cyber Vulnerabilities and Countermeasures for GPS-Time Synchronized Measurements in Smart Grids

Imtiaj Khan

(GENERAL AUDIENCE ABSTRACT)

Modern power systems incorporate numerous smart metering devices and communication channels to provide better resiliency against hazardous situations. One such metering device is Phasor Measurement Device (PMU), what provides GPS time-synchronized measurements to the system operator. The time-synchronized measurements are critical in ensuring the cyber and physical security of grids. However, like other smart devices, PMUs are susceptible to conventional cyberattacks. In addition to conventional cyberattacks, PMUs are also vulnerable to attacks against its time-synchronization. In this work, we dig deep into the realm of cyberattacks against time-synchronization of PMUs. We propose novel stealthy attacks against PMU time synchronization. Furthermore, we enhance existing attack detection model to conclusively identify such stealthy attacks and implemented the model in cybersecurity testbed that we developed at Virginia Tech.

Dedication

My parents and my beloved wife Monika.

Acknowledgments

I am thankful to all of those who have been with me along the perilious PhD journey. Special thanks to my academic advisor Dr Virgilio Centeno whose guidance and supervision has made this work possible. I cannot thank him enough. I would love to thank Dr Chen-Ching Liu for his support and collaboration that resulted in significant portion of this work. I also thank Dr Jaime De La Ree, Dr Yuhao Zhang, and Dr Vimal Biswanath for their critical assessment and constructive analysis of my work. Furthermore, I thank my lab partners. Alok Kumar, my perfect teammate during my earlier works on synchrophasor. Markus Zimmerman, whose contribution in the enhancement of VT testbed was of tremendous help. Suiksha Gautam, and Vishal Dixit, the friendly environment in room 422 and the brainstorming conversations regarding our research was pivotal for the later part of my PhD journey. My wife Monika, the support I got from you made my PhD possible. Last but not the least, I would love to show my gratitude toward my friends and family, especially my elder brother Imran Khan. He has always been the safety net and motivation during hard times.

Contents

List of Figures

List of Tables

List of Abbreviations

BDD Bad Data Detection

DFT Discrete Fourier Transform

DKF Deviation based Kalman Filtering

FDIA False Data Injection Attack

FO Forced Oscillation

GPS Global Positioning System

GSA GPS-Spoofing Attack

HIL Hardware-In-Loop

IED Intelligent Electronic Device

PDC Phasor Data Concentrator

PMU Phasor Measurement Unit

PPS Pulse Per Second

WLS Weighted Least Square

Chapter 1

Introduction

The recent trend of microgrid demands more emphasis on the development of sophisticated and fast protection mechanism for the smart grid. Microgrid refers to a cluster of interconnected electrical machines, local loads and distributed energy resources (DER) with the ability to function as a standalone system in island-mode as well as to work as grid-connected mode [1]. Penetration of single-phase and unbalanced loads can lead to the increase in power quality issues, that can affect the performance of microgrids (MGs) by causing abrupt changes in the power flow or by violating the operational limit [2]. Data centers in USA, which are considered as microgrid due to its ability to operate in islanding mode during power outage at the main grid, can suffer from voltage sags and harmonics [3]. Charging stations for electric vehicles (EV) can suffer from low order harmonics, causing total harmonic distortion (THD) greater than 1% [4] [5]. Three-phase unbalanced voltage, voltage fluctuation, harmonics etc. can hinder the operation of railway microgrid systems [6]. In addition, conductors breaking down and falling onto grounds/ physical objects can cause line to ground (LG) and phase to phase (PP) faults and subsequently increase the rate of rise of current and/or cause over-currents, over-voltage, under-voltage etc. These consequences can damage the grid performances and pose threats to human and wildlife safety [7]. Among the physical factors causing power quality issues in MG, LG faults are considered to be the most common type [8] - [11].

Integration of microgrids with smart infrastructure including communication, monitoring

and metering devices has pioneered the idea of smart grid (SG) that provides more reliable, resilient and robust operation [12]. The modern smart grid emerged from the interconnection of communication technology, metering devices, and all components of traditional power system. The smart grid shifted the conventional one-way communication system based radial distributed system into two-way communication interconnected meshed structure. On top of enhancing communication between the utility and consumers, smart grids provide better situational awareness, asset maximization, increased resiliency, higher market efficiency etc. The main shortcoming of this enhancements is the increased susceptibility to cyberattacks.

A conventional smart grid is comprised of two major parts: the physical power system layer and the cyber system layer. The physical power system is the electrical grid with its generators, transformers, transmission lines, and protective components. The cyber system layer includes smart metering devices, communication channels, and monitoring schemes. Using a Wide Area Network (WAN), the system operator (SO) at the control center receives measurements from the Intelligent Electronic Devices (IEDs) installed at strategic locations of the grid. Using this Supervisory Control and Data Acquisition (SCADA) based infrastructure, the SO obtains system information that allow them to implement optimal power flow, unit commitment, economic dispatch etc.[13]. The cyber layer is built on top of the physical layer, thereby making the whole SG a cyber-physical system (CPS) [14].

An important component of SG is phasor measurement units (PMU), which provides more reliable and relatively secured system-monitoring along with a faster reporting rate than that of conventional supervisory control and data acquisition (SCADA) system [15]. Another aspect of PMU is its ability to provide accurate timestamps for the measurements using precise time-reference. However, penetration of smart devices such as PMUs into the smart grids increase the dependence on communication links between the different layers of CPS and requires secured data storage and analysis methods. Such dependencies on com-

Table 1.1: PMU reporting rates

System Frequency	50Hz	60Hz
Reporting Rate F_s (frame/second)	10, 25, and 50	10, 12, 15, 20, 30, and 60

munication channel and data storage system raise the risk of cyberattack, particularly for critical infrastructures such as hospitals, military bases, data centers etc [16], [17].

To ensure precise time synchronized data transfer, it is important to assess the existing vulnerabilities of PMU based smart grids against cyberattacks. Furthermore, it is also critical to provide robust detection model against cyberattacks that are unique to PMU time synchronization.

1.1 Phasor Measurement Unit (PMU)

Phasor Measurement Unit (PMU), a relatively newer type of metering device, provides time-synchronized voltage and current magnitudes and phase angles, frequency, and Rate of Change of Frequency (ROCOF) data [18]. The measurement data provided by PMUs are time-tagged with a reliable time-source, most commonly the Global Positioning System (GPS). Widespread installation of PMU, and use of faster communication channels in the smart grid created a new horizon in terms of measurement accuracy and data transmission speed [19] [20]. For example, in conventional SCADA based system, data transfer rate is one frame per second, where in PMU based system, this rate is 30 to 120 frame per second (table 1) [20] [21].

PMUs provide time synchronized phasor data. Phasors are computed from digitized voltage or current waveforms $x(t)$, expressed as:

$$x(t) = X_m cos(\omega t + \phi) = \left(\frac{X_m}{\sqrt{2}}\right) e^{j\phi} = X_m cos(2\pi f_0 t + \phi) \tag{1.1}$$

where X_m is the magnitude of the signal, f_0 is the nominal frequency of the system, and ϕ, the phase angle, is the temporal position of instantaneous signal from the reference time ($t = 0$) synchronized with a reliable time reference (fig. 1.1). Most common time reference is provided by GPS receivers in the form of a one pulse per second (1 PPS) and corresponding timestamps.

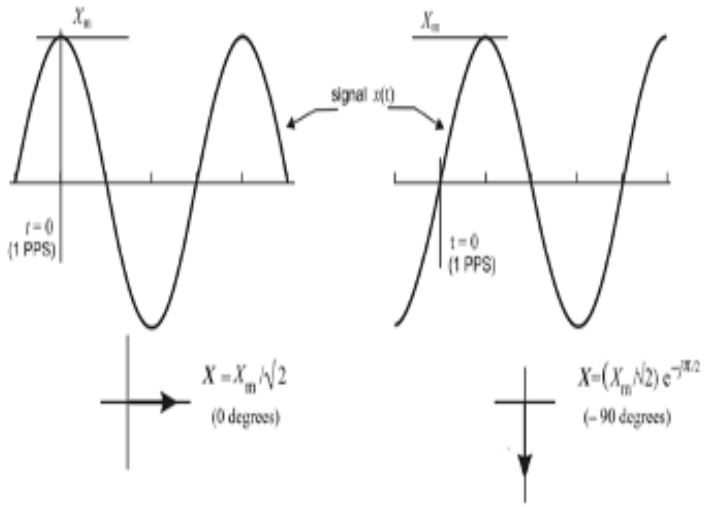

Figure 1.1: Synchrophasor representation [22]

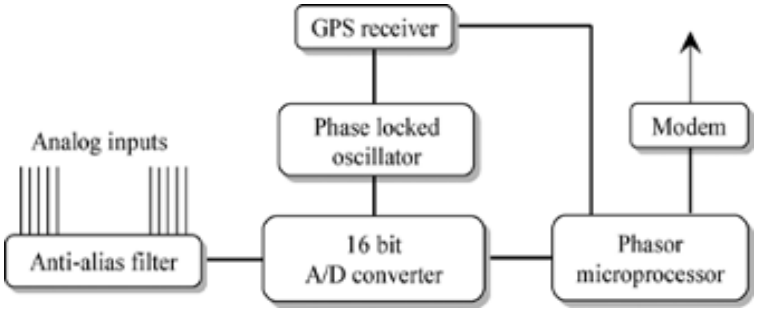

Figure 1.2: PMU functional block diagram [22]

In addition to GPS receiver, a PMU contains the following functional blocks (fig. 1.2):

- a signal processing block;
- a precise Analog to Digital Converters (ADC) for processing synchrophasor data;
- a phase locked oscillator to lock the devise sampling pulse to the 1 PPS;
- a microprocessor to implement the required algorithms to extract phasor information;
- communication channel to send the measurements to PDC or next step of the cyber layer.

The microprocessor block performs synchrophaosor calculation using Discrete Fourier Transform (DFT). For a set of singe phase signal x_i , the synchrophasor estimate for i^{th} sample time can be expressed as:

$$X(i) = \sqrt{2} \times \sum_{k=-\nu/2}^{\nu/2} x_{i+k} \times W e^{-j(i+k)\Delta t \omega_0} \tag{1.2}$$

where, $\omega_0 = 2\pi f_0$ (f_0 is nominal frequency), $\nu =$ FIR filter order, $\Delta t = 1/$ sampling frequency, $x_i = i^{th}$ sample, $W_k =$ low-pass filter coefficient.

Synchrophasor algorithm, as described in ref [22], can estimate N^{th} sample using the sample x_n as in eqn. 1.3.

$$\begin{aligned} x_n &= X_m cos(n\theta + \phi); \\ n &= 1, 2, ..., N-1 \end{aligned} \tag{1.3}$$

For sampling rate N, the complete voltage/current phasor can be calculated using non-recursive method (eqn. 1.4).

$$X_N = \sqrt{2} \times \sum_{n=0}^{N-1} x_{n+1}[cos(n\theta) - jsin(n\theta)] \tag{1.4}$$

Phasor magnitude and phase angles are obtained using eqn. 1.4. Magnitude data reflects the amplitude of original voltage/current signal. The phase angle data is a periodic time series and wrap at 180^o for non-recursive implementation of synchrophasor algorithm (fig. 1.3), described in eqn. 1.2 to 1.4. The phase angle is referenced to the device 1 PPS. The common 1 PPS at all PMUs gives a common time reference for all PMU angles, allowing for the accurate measurement of angle differences.

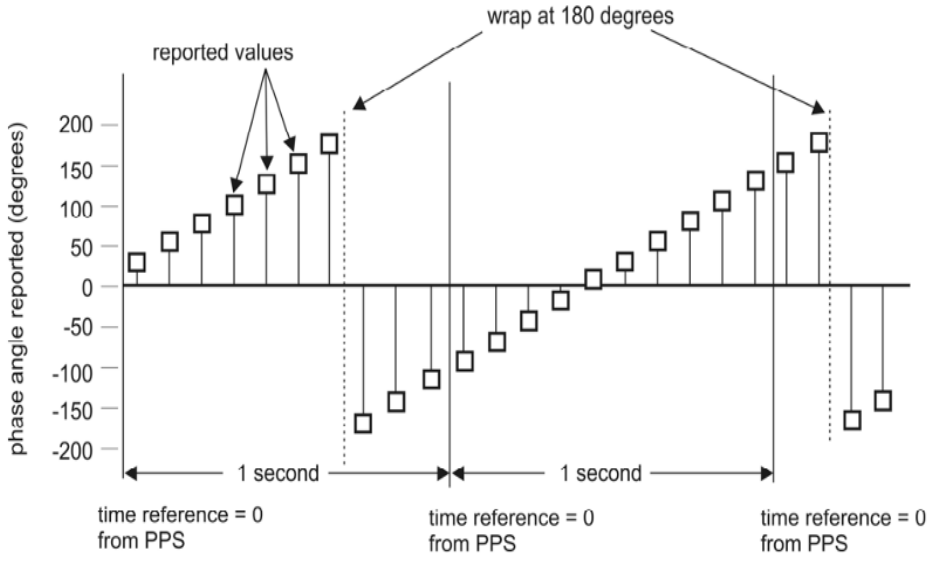

Figure 1.3: Phase angle variation for non-recursive synchrophasor algorithm [6]

1.1.1 Phasor Data Concentrators (PDCs

An integral part of PMU based cyber system is Phasor Data Concentrator (PDC). PMUs located at the nearby nodes in the grid need their timestamps aligned with a common time reference to enable the system operator analyze phasor measurements and look for possible faults/ data anomaly. This time alignment of multiple PMUs is done at the PDCs. PMUs send their measurements to the local PDC using secure communication channel. The most commonly used communication protocol for synchrophasor data transmission is IEEE C37.118.2-2011 (IEEE Standard for Synchrophasor Data Transfer for Power Systems) [23]. PDCs align the phasor measurements from all connected PMUs with UTC timestamps, and aggregate the PMU data to a centralized PDC. Furthermore, PDC can provide additional functionalities such as data visualizations, data analyses, and real-time response to data anomaly or time synchronization loss. Also, PDCs can perform quality check, disturbance check, data storage for off-line analysis, and work as a SCADA interface.

For a small-scale PMU infrastructure, a single PDC can receive, analyze and transmit measurements from all PMUs. However, in large scale cyber-physical system, multiple PMUs are connected to local ore regional PDCs. Power grid substations also require PDCs that aggregate the measurements of substation PMUs. Substation PMUs include the measurements from protection relays, with an addition of timestamp and ROCOF information. The substation PDC align the timestamps of the measurements from substation relays and aggregate to central PDCs. The output stream from the local, regional, and substation PDCs are fed into another central PDC using the same IEEE C37.118.2 protocol. All PMUs and PDCs function in a radial architecture as depicted in fig. 1.4.

Like PMUs, PDCs also can be either individual devices capable of performing user defined tasks, or combination of separate software and hardware modules. As PDC performs time

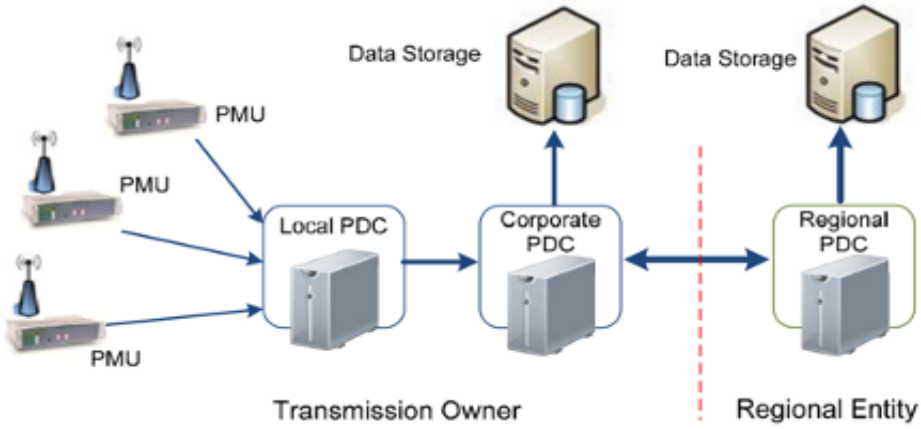

Figure 1.4: PMU-PDC network [23]

alignment of PMU data, it is considered as time-synchronized devices as PMUs. PDCs have been proven to be very useful for ensuring cybersecurity of PMU based infrastructure.

1.2 Cyberattacks against PMUs

PMUs are similar to other IEDs of the smart grids, therefore have similar advantages and limitations of conventional IEDs, such as vulnerabilities against cyberattacks. Cyberattack against PMU, just like IEDs, is a widely discussed topic in literature [24] - [31]. The major cyberattacks against PMU, as for other Intelligent Electronic Devices (IEDs) are:

- False Data Injection Attack (FDIA)
- Man-in-the-middle (MITM) Attack
- Replay attack
- Data-drop attack
- Denial of Service (DOS) Attack

Among these attacks, the most documented attack is the FDIA [27]. In this type of attack, the attacker injects malicious data into PMU datastream received by the System Operator (SO) at control center. The malicious data change the outcome of state estimation, which may eventually lead the SO take wrong or unwanted restorative action. For example, the attacker can modify the power flow measurement through a branch, and change the measurements to a value that crosses normal operational limit. The SO, after performing load flow analysis and optimal power flow, may consider it as a case of operational limit violation, even though the actual power flow is still under the limit. The SO may take unnecessary preventive action, such as tripping out the branch, leading to unwanted load-shedding at critical infrastructures. A carefully crafted FDIA can attack the PT measurements read by PMUs (as for the case of other IEDs), therefore can modify the phase angle measurements directly. The aforementioned cyberattacks against PMUs are similar to the cyberattacks against other IEDs, and in literature these FDIA against PMU measurements are analyzed in a similar way as those attacks against IEDs. However, there is another type of attack that exploits the time synchronization of PMUs. This type of attack is unique to PMUs and also other time synchronized devices such as PDCs. The most common attack against time synchronization is GPS-spoofing attack. In this dissertation, our focus is on the cyberattacks targeting the time-synchronization of PMUs, and other time-synchronized devices.

1.3 Cyberattacks Specific to PMUs: GPS-Spoofing Attack

Global Positioning System (GPS) is one of Global Navigation Satellite Systems (GNSS) and provides position, navigation and time information using four or more GPS satellites [23]. GPS provides accurate locations and time references using the data obtained by at

least four GPS satellites. The GPS signal is widely used in time synchronization of Phasor Measurement Units (PMUs). PMUs require precise time reference to keep the timing error within the limit of 26µs, standardized by IEEE C37.118.2 protocol [32].

For a stationary GPS-receiver, such as the case for PMUs in power grids, after getting the initial location information, the position and time-reference can be accurately measured using only one GPS-satellite which transmits the strongest signal for the particular location. If attacker spoofs the GPS signal with a stronger Electro-Magnetic (EM) signal, it is possible for them to disrupt the time synchronization of PMUs. The change in time synchronization leads to wrong synchrophasor calculation, which in turn creates falsified phasor measurements or bad data depending on the degree of loss of synchronization. PMU generally uses public GPS which is vulnerable to cyber-attacks.

GPS signals are prone to jamming and spoofing [33]. Jamming is accomplished by using a jammer device that creates a Radio Frequency (RF) signal to deny the valid signals from the satellites [34], and at the same time providing a fake GPS signal for the receiver, as illustrated in fig. 1.5 [35]. The fake signal can be implemented using one of the three methods: open-loop simulator, repeater or hardware injection [36]. The open-loop simulator generates the EM signal based on historical knowledge of the signal parameters. The spoofed signal, which is asynchronous with legitimate GPS signal, leads to failure in locking the legitimate GPS signals. This particular type of spoofer causes reaquisition of tracking signal, however it does not provide desired spoofed position, and time-reference. The repeater system has a receiver module to receive authentic GPS signals directly from satellites. The spoofer modifies the authentic GPS signal and retransmits it to the target (in this case, PMU GPS receiver). The repeaters synchronize its signals to GPS time and location to the target antenna. A spoofing attack using repeaters is hard to detect by analyzing synchronization, constellation, and signal properties.

Once the receiver is locked with the fake GPS-signal, it estimates the location at an altered position. Position error is not a problem for PMUs since they are static devices but alterations of the valid 1 PPS signal change the phase angle reference for the spoofed PMU. Since PMUs use GPS signal for time synchronization, the PMU as well as the whole power grid operation relies on the authenticity of GPS signal. GPS-Spoofing Attack (GSA) on PMU integrated smart grid can either be performed by manipulating the GPS timestamp or modifying GPS propagation time [37]. In [38], researchers performed a GPS-spoofing field test on PMUs and it has been demonstrated that the attacker can introduce a time-reference error more than tens of microseconds. In conventional GPS-spoofing attack, the attackers' goal is to damage the GPS time-synchronization of PMUs, which in turn make the PMU data useless to the utility. However, in sophisticated GPS-spoofing attack, the attacker can manipulate the spoofed signal to create an undetectable and coordinated time-synchronization error that misinforms the operator and affects the operation of power system. Time synchronization error due to sophisticated GSA can impact the transmission line fault detection, voltage stability monitoring and identification of fault location [39].

Previous works on GPS-spoofing attack can be classified into two parts: 1) Detection and mitigation of the attack, and 2) Creating stealthy GPS-spoofing attack.

1.3.1 Detection and Mitigation of GPS-Spoofing Attack

Cryptographic authentication methods such as public key infrastructure, signal authentication sequence, navigation message authentication etc [40] [41] are few examples of GPS-spoofing attack detection algorithms. Y. Fan et. al. [42] proposed a GPS carrier-to-noise raio (C/No) based GSA detection mechanism for PMUs, which are installed in the physical layer of the cyber-physical system. The suspicious PMUs are identified by calculating a

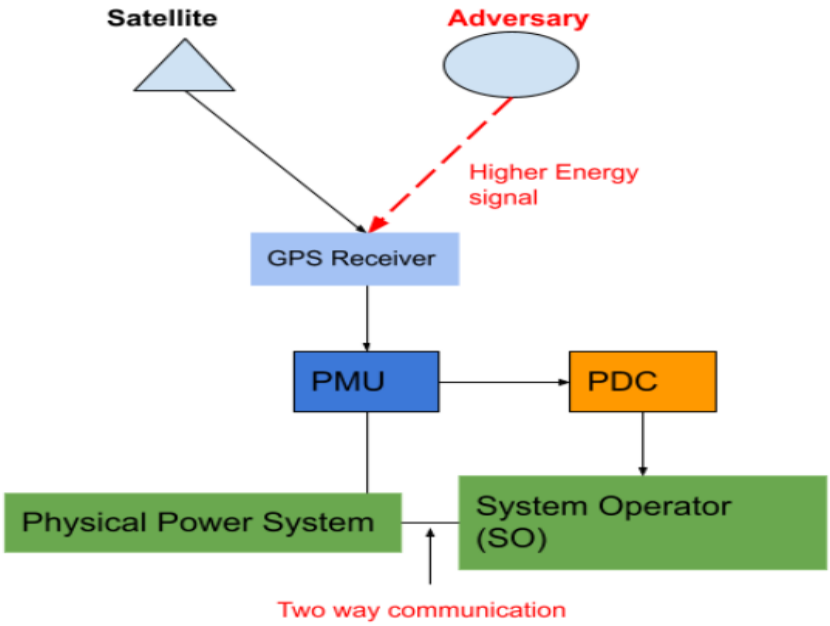

Figure 1.5: GPS-spoofing attack model

priori probability of spoofing. The autocorrelation among multiple GPS-signals can also be a useful tool for the detection of GSA. The p-score thresholds of statistical runs test are used to classify the GPS signal as safe or unsafe. Supervised machine learning techniques can be applied to train the signals based on their classifications [43]. PMUs in power grid uses civilian GNSS and the sophisticated GSA detection methods are not utilized in the current smart grid infrastructure. This limitation has made the PMUs vulnerable to GSAs. However, as GSA creates a modification in the time-reference of PMU, it leads to a phase angle shift in the measurements. Therefore, GSA can be analyzed similarly as conventional FDIA, where the phase angle measurements is falsified by the attackers. From the above discussion, we can infer that a stealthy GSA can be modeled in a similar way of creating a stealthy FDIA, with attacking the phase angle measurements only. The attacker runs the stealthy FDIA algorithm to figure out the most optimal attack a value to the phase angle measurements, then apply the corresponding time shift $\Delta t = a2\pi f = g(a)$ to the 1 PPS

reference signal of the GPS receiver [44]. Several researchers developed GPS-spoofing attack detection model as FDIA detection, and the most commonly used FDIA detection is residual based Bad Data Detection (BDD) method [28]. If the residuals of estimated measurements and the measurements received from PMU are greater than a threshold, the measurement is considered as bad data. For time variant PMU measurement, Kalman Filtering (KF) [29] can be a useful tool to detect FDIA against phase angle measurements. Mousavian et. al. [30] proposed a Mixed-Integer Linear Programming (MILP) based attack prevention scheme where threat level of various PMUs connected to the grid is assessed. The objective function minimizes the maximum threat level of existing PMUs in the system. If the threat level is still higher after first minimization step, the corresponding PMU is disconnected from the system. Vulnerability due to cyber-attack was analyzed for conventional measurements and data-format of PMUs [31]. Independent Component Analysis (ICA) based signal separation model is utilized to create attack on PMU measurements. The authors also proposed a Cognitive Radio (CR) based network topology to ensure secure PMU data transmission, where the network is not directly connected to the backbone network [31]. Cyberattack can cause cascading failure by triggering the failure in the interconnected parts of the physical power system. Rui Ma et. al. [45] proposed a Recovery-based Model Predictive Control scheme (RMPC) to tackle the cascading failure caused by cyberattack. This model takes into account the modified operating conditions and tempered measurements after attack. The control action is determined by solving an optimization algorithm over finite time horizon. The state variables at state k is computed with the historical state variable data in the event of attack. If the power system has been compromised for consecutive N states, the RMPC will predict the k^th state variables using the state variable from k-N state. The incorrect state data are then replaced by the predicted state data. Detection of successive observable cyberattacks can be considered as a matrix decomposition problem of a low-rank matrix plus a transformed column-sparse matrix [46] [47]. Another widely used method to counter

FDIA is to secure the measurements by placing the PMUs to critical locations, for example the greedy based PMU placement as in [48]. Since PMU measurements are time-series data, Hankel-matrix is effective in detecting anomaly in PMU datastream by exploiting the temporal and spatial correlation among the measurements from multiple PMU channels [49]. In this dissertation, we exploit Hankel-matrix to identify bad data, and enhance the existing Hankel-matrix model to provide a method to identify GPS-spoofing attack accurately.

1.3.2 Creating Stealthy GPS-Spoofing Attack

Despite the detection and mitigation models against GPS-spoofing attacks, it is possible to create attack that is undetectable by existing detection approach. As GPS-spoofing attack can be considered similar to an FDIA targeting phase angle measurements, attacker can initiate a shift in GPS 1 PPS signal to create a deviation in phase angle measurements $\Delta\theta$. If this deviation in phase angle caused by GPS-spoofing attack can be kept under the limit dictated by the bad data detection (BDD) threshold, it is possible that the attack goes undetected [50] [51] [52]. In all the attack schemes discussed above, the attacker is assumed to have the sufficient knowledge of the whole network topology of the cyber-physical system. If the complete topology of the grid is unknown, it is difficult for the attackers to formulate stealthy attack. Nevertheless, a Kernel Independent Component Analysis (ICA) based attack construction model has been developed [53]. X. Liu and Z. Li [54] proposed an optimal attack vector using the partial knowledge about network topology. The attack vector is obtained by solving the optimization equation which minimizes an introduced non-negative slack variable. The constraints are real and reactive power flow limits throughout the branches.

1.4 Dissertation Organization

GPS-spoofing attack against time-synchronized measurements is a widely explored research area in recent times. In this dissertation, we dig deeper into the realm of the attack against PMU time synchronization. In chapter II, we develop a PMU-PDC testbed to simulate and transmit synchrophasor measurements. We use the previously developed PMU simulator at Virginia Tech Power and Energy Center (PEC) laboratory. The simulator receives PMU measurements and transmit it as IEEE C37.118.2 protocol to the PDC. This PMU simulator provides the advantage of feeding measurements during several attack conditions, such as GPS-spoofing attack, FDIA, replay attack, data drop attack as demand. In addition to the PMU simulator, we use OPAL-RT synchrophasor module as another source of PMU measurements with the ability to simulate electric grids in real time. For PDC, we use OpenECA, an open-source software platform developed by Grid Protection Alliance (GPA) that has the functionality of real-world PDCs. Moreover, OpenECA can be integrated with user defined algorithms for fault/ cyberattack detection.

In chapter 3, we create three novel coordinated attacks on time-synchronization. These attacks are good representations of possible sophisticated attacks on time synchronized devices that are not detectable by existing algorithms. First of which is a stealthy GPS-spoofing attack with slow incremental shift in GPS 1 PPS signal, resulting in slow incremental deviation in phase angle measurements. In this stealthy attack model, the attacker targets the power flow measurements between two buses, and make the perceived power flow measurements exceed line flow limit. The second attack is spoofing driven FO attack and corresponding detection method. Forced Oscillation (FO) can hamper power grid stability and limit power transfer capability. General cause of FO is periodic external variation in the system, and in real-world cases the FOs are detected with PMU measurements [55]. However, a periodic

GPS-spoofing attack can also add oscillation to PMU measurements that behave similar to an actual FO event caused by physical sources. In the fourth chapter, we develop such attack model by injecting periodic variation in time reference in the synchrophasor algorithm. It is possible to create an additional oscillation in the PMU measurements with a frequency resonant with inter-area mode frequencies, even though there is no actual FO in the physical system. The system operator, considering it as an actual FO event, may take unwanted restorative actions. The third attack scenario is coordinated PDC data-drop attack. Generally, a PDC waits for a specific time-period for PMU data to arrive. If the attacker keep one PMU data arriving earlier than normal arrival time, the PDC is forced to start counting wait-period earlier than normal. As a result, the wait-period ends earlier than normal. At the second step, the attacker targets a second PMU and creates a small delay in the communication channel of second PMU data. Since the PDC wait-time ends earlier during the attack scenario, even a small delay of second PMU data arrival cause its data discarded by PDC. In this coordinated PDC data-drop attack, the delay of second PMU measurements is small enough to be detected by conventional delay attack detection methods.

In chapter 4, with a goal of developing a generalized algorithm to detect attacks on time-synchronization, we enhance the existing Hankel-matrix model to differentiate cyberattack from physical event, and to accurately identify GPS-spoofing attack. Moreover, we propose a sequential event classification and GPS-spoofing attack detection model in the PMU-PDC testbed.

In chapter 5, we analyze the performance of our enhanced Hankel-matrix algorithm for the individual and generalized detection of sophisticated GPS spoofing attacks. Using both simulation data and real-world PMU data provided by PNNL, we show the feasibility of enhanced phase-angle-only Hankel-matrix to detect GPS-spoofing attack. We also implement the sequential event classification algorithm developed in chapter 4. We then proceed to

apply our enhanced Hankel-matrix algorithm to detect novel coordinated attacks on time synchronization and verify the utility of our enhanced algorithm.

In chapter 6, we summarized the dissertation and provide future research guidance.

Chapter 2

PMU-PDC Enhanced Cybersecurity Testbed

Phasor Data Concentrators (PDC) receive synchrophasor measurements from individual PMUs, time-aligns the measurements by their time tags and transmit time-tagged cluster of measurements to the next layer of communication channel or to another central PDC. In addition to the conventional cyberattacks that affect all intelligent electronic devices (IEDs), there are attacks that target the time-synchronization of PMUs, PDCs and other time synchronized devices. The most common attack against time synchronization is the GPS-spoofing attack, where the attacker spoof the GPS signal received by PMUs' GPS receiver with a relatively stronger signal that those of the GPS satellites. False Data Injection Attack (FDIA), the most common type of cyberattacks against IEDs, that are in some way similar to a as GPS-spoofing attack if the FDI attacker targets the phase angle portion of the measurements.

For any cyber-physical systems such as smart grids, it is necessary to have platforms to test and analyze the communication infrastructure as well as to assess the effectiveness of security measures. These platforms enable the researchers to verify developed theories in a process that can be replicated at different locations/ settings. The need for smart grid wide-area monitoring, control, and cybersecurity paved the way of integrating the communication infrastructure with conventional computer simulation and physical hardware-in-loop

simulation-based testing platforms. These interconnected testing platforms are technically termed as "cyber-physical testbed". The cyber-physical testbeds are comprised of complete or partial components of actual substations and control centers. They are vital in testing new applications and control systems in a control environment that allows for reproducible results [56].

As part of cyber-physical system, time synchronized devices such as PMUs and PDCs are prone to conventional cyberattacks such as FDIAs and man-in-the-middle (MITM) attacks. On top of conventional attacks, PMUs and PDCs are also vulnerable to attack against time-synchronization such as GPS-spoofing attack. Since different cyberattack against time synchronized devices demand different restorative actions, and demonstrate unique or common behavior for various network and device settings, it is very critical to analyze and observe the behavior of the grid for different cyberattack scenarios against PMUs. This requirement necessitates a PMU-PDC testbed for cybersecurity purposes. PMUs use dedicated communication protocol such as IEEE C37.118.2 to transmit synchrophasor measurements, and PDCs receive measurements from PMUs using same protocol. Therefore, a PMU-PDC testbed must include:

- multiple PMUs that are able to communicate using IEEE C37.118.2 protocol,
- one or multiple PDCs that receive real-time synchrophasor measurements, and
- a system that observes the existence of data anomaly and can communicate with different layer in the cyber system with updated status flag regarding system states.

2.1 Existing PMU-PDC Testbeds

Ref [57] proposed a four-layer architecture for cyber-physical testbeds embedded with physical network module. Physical components are integrated with wide-area applications using a configurable network. The proposed testbed achieved low-latency with a data broker setup in distributed messaging environment.

The real-time cyber-physical testbed for wide-area application developed by [58] (fig. 2.1) includes comprehensive infrastructure of a PMU-PDC system. It consists of both IEEE C37.118.2 and IEC 61850-90-5 Routable Sample Values communication protocol aimed at transmitting timestamped synchrophasor measurements. The IEC 61850-90-5 also incorporate status and feedback signal in a two-way communication channel between the control center and substations. The key components of this testbed are:

- PMUs,
- Phasor Data Concentrator (PDC),
- IEDs,
- Global Positioning System (GPS) clock,
- software application module, and
- IEC 61850 emulator tools

Ref [59] developed a vendor agnostic PMU real-time simulation and hardware-in-the-Loop (PMU-RTS-HIL) testbed with a goal of integrating multiple PMUs. The proposed testbed includes real and virtual PMU network along with an emulated communication channel layer. The communication channel in the testbed has the ability to replicate bandwidth

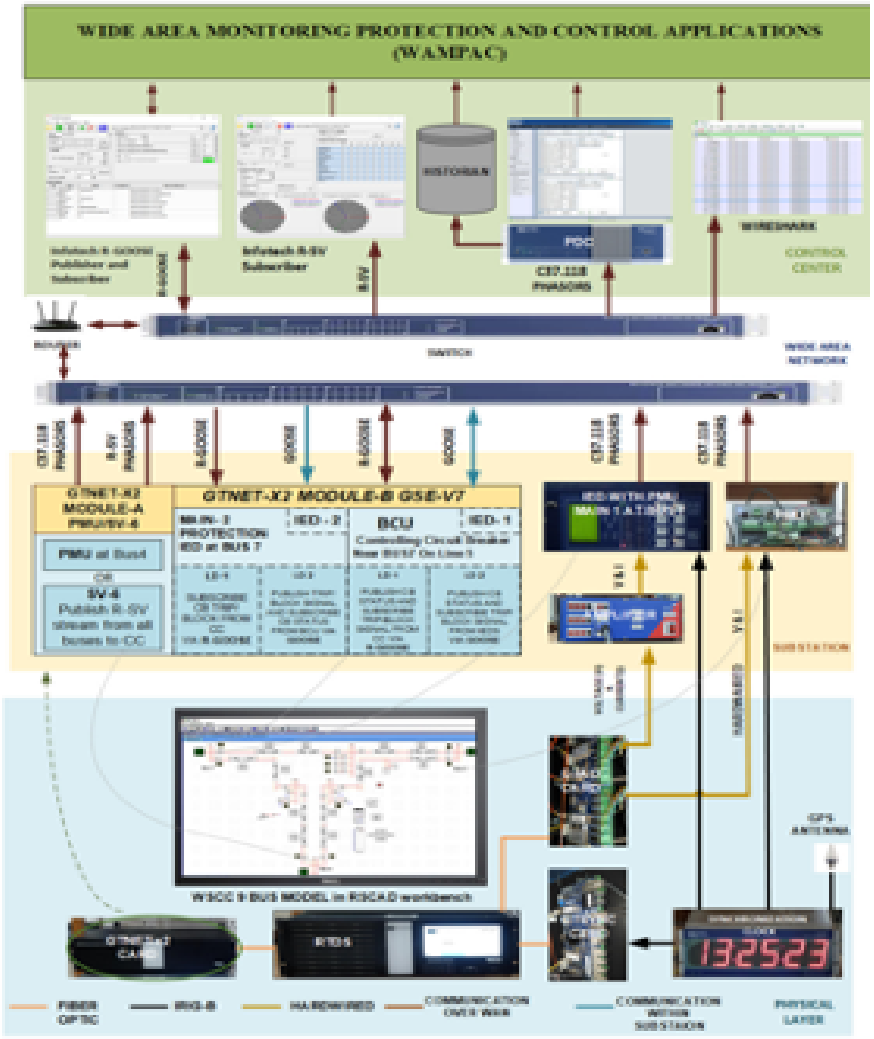

Figure 2.1: The wide-area cyber-physical system testbed developed in [3]

management, data loss and communication loss caused by physical PMU devices. The PMU-RTS-HIL testbed developed by [59] (fig. 2.2) offers flexibility and scalability under different contingency conditions. Another advantage of this testbed is the data mining and data analysis using openPDC as data concentrator and SQL database.

Since the cyberattacks against a real-world PMU-PDC system is difficult to emulate in laboratory setting, it is imperative to develop scalable PMU cybersecurity testbeds. One notable example is the cybersecurity testbed developed by [56], illustrated in fig. 2.3. The testbed

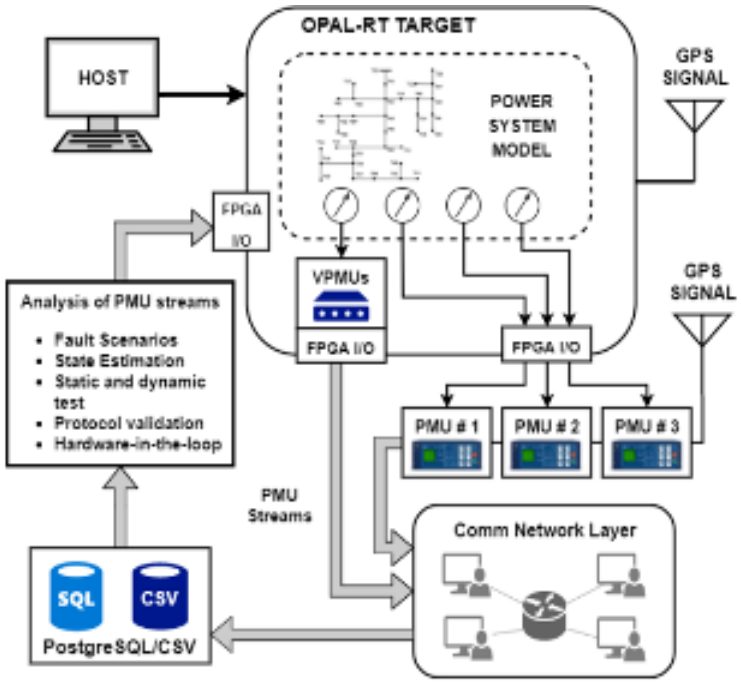

Figure 2.2: The PMU-RTS-HIL testbed [4]

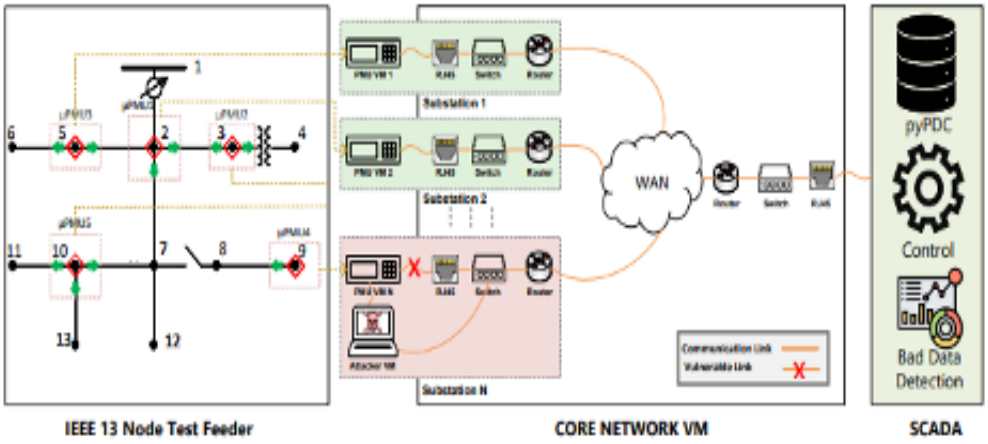

Figure 2.3: VM based PMU cybersecurity testbed [1]

is comprised of script based virtual machine (VM) and a software-based communication network emulator, providing a highly-scalable cyber-physical testbed. Using package manipulator, the testbed is equipped with the capability to run real-world power system under several cyberattack conditions such as Man In The Middle (MITM) attack, Address Resolu-

tion Protocol (ARP) poisoning attack, False Data Injection Attack (FDIA), and Eavesdropping Attack.

As the focus of this dissertation is analyzing attack against time synchronization (such as GPS-spoofing attack) of PMUs and PDCs, it is necessary to have a testbed aimed at analyzing measurements manipulated by attacks against time-synchronization signal. Moreover, we need a scalable testbed that can be reproduced with a low cost in laboratory settings. With this end goal, we have developed and enhanced a PMU-PDC testbed with real-time cybersecurity analysis capability.

2.2 Virginia Tech Enhanced PMU-PDC Testbed

The PMU simulator portion of the testbed was developed at Virginia Tech in 2011 to test the loadability of PDCs up to 300 PMUs [60]. The initial PMU simulator was an enhancement to PMUSim, a small software package used by manufacturers to test PDCs operation by sending garbage data using the C37.118 protocol. The PMUSim code has enhanced to send time tagged data with similar delays and noise level as commercial PMUS while providing the flexibility of sending user generated data. In this work we have enhanced the existing testbed to include PMU simulator that transmit synchrophasor measurements under cyber-attack condition. The VT PMU simulator transmit measurements using IEEE C37.118.2 protocol with at programmable standard rates between 2 to 120 frames per second. The PMU simulator can be fed with real-world PMU measurements, as well as PMU measurements under GPS-spoofing attack condition. The other components of the VT testbed include:

- an Opal-RT: PC/FPGA based real-time HIL simulation,
- a simple ommunication network implemented with ethernet cables, routers, ethernet

switches etc.,

- the OpenECA/ openPDC open source phasor data concentrator (PDCs)

The schematic diagram of the developed testbed is depicted in fig. 2.4.

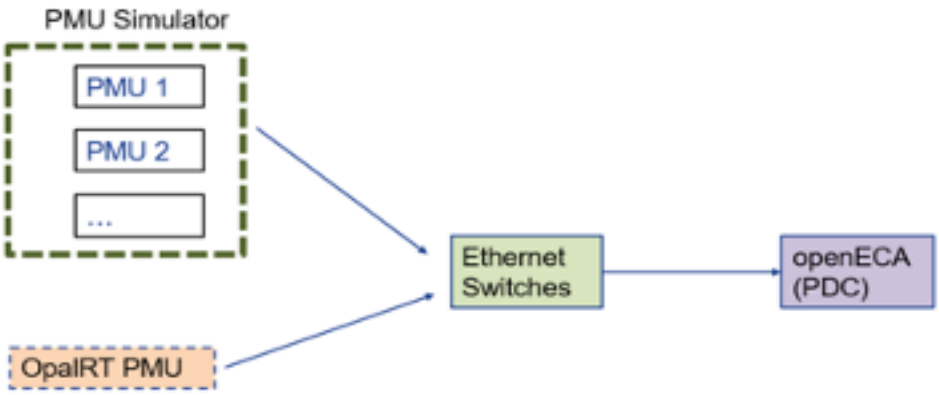

Figure 2.4: VT PMU-PDC Testbed

One advantage of this PMU simulator is its ability to incorporate PMU measurements under GPS-spoofing attack. The enhanced testbed can transmit synchrophasor measurements from a grid to PDCs, as well as measurements under data-manipulation or spoofing.

2.2.1 PMU Simulator

PMU simulator is a Linux based software, that uses a GPS receiver to set the time of the system, provide timestamp in UNIX format. The PMU simulator offers a user-configurable TCP/UDP port as well as IP address and can transmit power system measurements in IEEE C37.118 format. A single PMU simulator can emulate 100 separate PMU channels. Each PMU channel of the simulator consists of timestamp information, phasor measurements, analog signal, frequency, rate of change of frequency (ROCOF), and digital status flags. A single PMU channel can contain a maximum of 20 phasor measurements, 20 analog signals

and 16 digital signals. The Graphics User Interface (GUI), and configuration setup of PMU simulator are depicted in fig. 2.5a-2.5b. The PMU simulator provides the flexibility of user-defined TCP/IP and UDP port, number of phasor measurements for the grid. Furthermore, the PMU simulator incorporates analog and digital channels containing system states and status flags under normal and cyberattack conditions.

(a) User interface

(b) Phasor configuration

Figure 2.5: PMU simulator configuration

2.2.2 OPAL-RT PMUs

The second set of simulated PMUs in the testbed are provided by OpalRT. OpalRT is a hardware-in-loop (HIL) simulation tool [61], which has built-in PMUs with ability to transmit synchrophasor measurements. OpalRT PMUs use TCP communication to transmit measurements to PDC. An advantage of OpalRT is its ability to simulate a power system from a user provided model and transmit the grid measurements as PMU measuremnets to a PDC. The synchrophasor measurements from the user-configurable grid simulated in the OpalRT is sent to OpenPDC, where the measurements are stored and analyzed. The synchrophaosr measurements are timestamped using Opal-RT's internal clock which can be synchronized to an external GPS signal.

2.2.3 OpenECA

The PDC used in this testbed is the OpenECA, an open-source PDC developed by Grid Protection Alliance (GPA) [62]. OpenECA can receives and transmit measurements in various protocols, most significant is the IEEE C37.118 format. OpenECA can be configured with the TCP/UDP ports, IP addresses and PMU IDs of the source PMUs to enable it receive synchrophasor measurements. OpenECA is designed for the user to develop applications for data received by its PDC module. This allow the user to implement applications such as bad data detection, classification, and GPS-spoofing attack identification algorithms on top of the PDC module. This user algorithms can run in quasi-real-time, allowing it to provide bad data flags in millisecond range. The source code of OpenECA is in $C\#$ language, which allows the user to manipulate the measurements received from PMUs in real-time. We can implement state estimation or BDD algorithms in Python/MATLAB and run the algorithm synchronized with real-time measurements received by OpenECA.

The physical VT testbed setup is depicted in fig. 2.6.

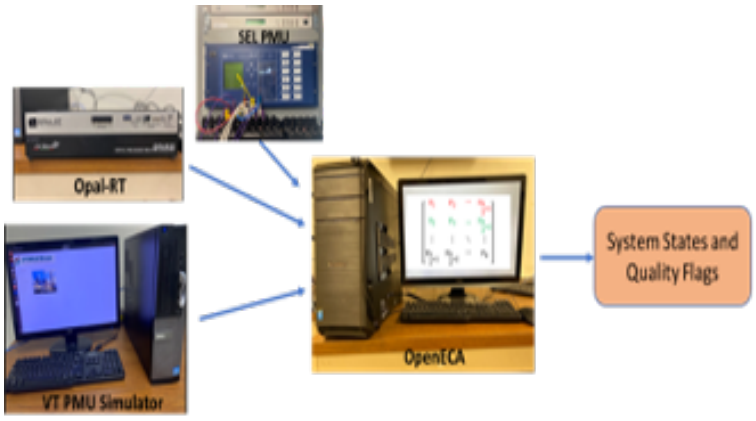

Figure 2.6: Physical testbed of VT

2.3 Communication Delays

Data transmission through any communication channel can be delayed due to any physical conditions or cyberattacks. There is a minimum amount of delay in any communication channel, particularly if the communication channels are poor. For cyberattack analysis, it is important to consider the communication delay due to system's inherent condition. Furthermore, OpenECA has the limitation of a wait-period like any other PDC. OpenECA waits for a user programmable specific period for data from PMUs to arrive, and if the data is not arrived within that period, OpenECA discards it. To tune OpenECA with proper wait-period, the communication delay must be considered. To check the communication delay in the network of VT enhanced PMU-PDC testbed, we observed the communication delay using WIRESHARK [63] for 10,000 sample synchrophasor measurements sent from Opal-RT and PMU Simulator, and subsequently received by the PC with OpenECA.

The communication delay from PMUs to PDCs in the testbed ranges from 0.0225 sec. to 0.0366 sec., with a mean communication delay of 0.029 sec. Fig. 2.7 shows communication

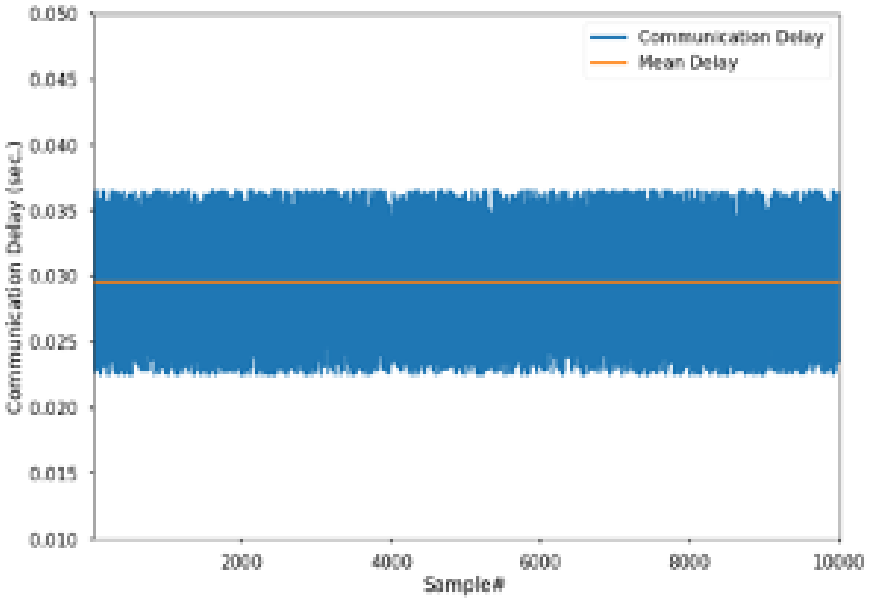

Figure 2.7: Communication delay in the VT PMU-PDC network

delay from PMU to PDC in the testbed.

2.4 Advantage of Virginia Tech Enhanced PMU-PDC Testbed

The enhanced PMU-PDC testbed has the ability to run any state-estimation or BDD algorithms in real-time. The ultimate output of the PMU/PDC testbed is the system states as required by any Intrusion Detection Scheme (IDS) implemented within the cyber-layer of the cyber-physical system. Moreover, the proposed testbed can provide Bad data/ cyberattack flags and corresponding timestamps to the IDS system. The main goal of the enhancement is to detect any anomaly in the measurements in real-time, so that the IDS model can use the information from PDCs as a base case that is already flagged "trusted/untrusted". If any portion of measurements is identified as anomaly, the PDC flags it as "untrusted" mea-

surements, and will send the information of last trusted measurements to the IDS. On top of that, the simulator output also contains estimated measurements from last trusted measurements. The VT enhanced PMU-PDC testbed's PMU simulator can be fed with PMU measurements from a large-scale grid configuration, and the opal-RT can simulate large scale power girds in real-time.

Finally, VT enhanced testbed can be reproduced in university laboratory settings with a very low cost. Since the OpenECA is an open source PDC model, and PMU simulator was implemented using open source LINUX based tool, the total cost of the testbed is incurred by the implementation computer, Opal-RT simulator, ethernet cables, routers, and switches.

Chapter 3

Novel Cyberattacks Targetting Time-Synchronized Devices

3.1 Details of Publications

Co-authors: Virgilio Centeno

Reference [64]: I. Khan, and V. Centeno, "Undetectable gps-spoofing attack on time series phasor measurement unit data". arXiv: 2206.12440 [eess.SY], Sep 2023. Retrieved from: https://arxiv.org/abs/2206.12440.

3.2 Introduction

Since PMU relies on GPS signal for time synchronization, it opens the possibility of GPS-spoofing attack, the most prominent attack on time-synchronization. PMU generally uses public GPS which lacks the sophisticated protection scheme used for military GPS. GPS-spoofing attack poses very serious concern over the cybersecurity of the cyber-physical systems (CPSs) [65]. It may affect the magnitude and the phase angle, however the phase angle is the most susceptible portion, because shifts in the GPS 1 PPS, the common time reference for all PMUs, reflect as shift in the relative phase angle [66]-[68]. Gradual change of phase

angle of a particular node with respect to the other nodes in the grid can, in some scenarios, provide incorrect information to a system operator (SO) at control center that may lead the SO take unnecessary actions. Moreover, the gradual shift in phase angle measurements due to the GPS-spoofing attack has the potential to impact any PMU base transmission line fault detection and identification of event location [65].

Several researchers focused on the protection of the PMU-integrated smart-grid against cyberattacks. Most of these works are based on detecting FDIA. Detection of FDIA is similar to conventional Bad Data Detection (BDD) method [69] [70]. Conventional BDD algorithms observe the residuals between the measured and expected variables and do statistical test to find the outliers. GPS-spoofing attack (GSA), by changing the time-reference, impacts the phase angle measurements more severely than the other PMU measurements. The change in phase angle measurements due to GSA is similar to FDIA targeting phase angle measurements only. As a result, GSA can be considered similar to a FDIA with only the phase angle data modified. Considering the defense strategy taken by control centers, it is possible to create attacks that are stealthy by BDD algorithms [71] [72]. This statement is also true for GPS-spoofing attack if the attack is considered as a variation of FDIA targeting phase angle data only [73]. These types of stealthy attacks can still be prevented by placing PMUs into optimal locations of the grid [74].

However, it is possible to create stealthier GPS-spoofing attacks, which cannot be prevented by optimal PMU placement or by BDD algorithms. Moreover, time-synchronization of PMUs, as well as of PDCs, can be prone to additional type of vulnerabilities such as PDC data-drop attack and periodic GPS-spoofing attack causing Forced Oscillation (FO) in the measurements.

In this chapter, we aim at expanding the horizon of cyberattacks targeting the time-synchronization of PMUs and PDCs. We propose three novel cyberattack types that exploit the vulnerabil-

ities of time-synchronization of time-synchronized devices such as PMUs and PDCs.

3.3 Proposed Attack Scenarios

The first and simplest type of attack is the stealthy incremental GPS-spoofing attack, where the attacker injects a slow incremental shift in the phase angle reference by creating and maintaining an effective delay in time reference of an individual PMU. Doing so, the attacker will be able to change the phase angle difference between the spoofed PMU and any other monitored PMU in the system. If small changes accumulate over time, the attacker may eventually cause a significant impact on the SO's perceived angle differences and computed power flow after the time period T. Assuming that during off-peak hour, the power flow in the line under attack is well below its limit, as indicated by the angle difference of the PMUs at the both ends of the line. By small manipulation of the phase angle measurements of a PMU at one end of the line, attackers can create a very small change in the power flow calculation performed by the SO. This very small change in power flow calculation at single instance is insignificant, however as the attackers keep manipulating the phase angle measurement using GSA over a long time, the accumulative effect of the increases in calculated power flow grows larger. After time T, which can be made to coincide with the peak load, if performed correctly, the line power flow as determined by the phase angle difference from PMU measurements exceeds the line's limit.

At peak load-hour, the SO at the control center is prepared for possible operational limit violations in the physical grid, therefore if the calculated power flow exceeds the line low limit at that time, the SO, considering a physical cause for the event, may then take the protocols required for operational limit violation despite the operational limit is not actually violated. Therefore, load-shedding or other restorative measures may be taken, which may

lead to a hamper in the supply of power to the critical points of the grid.

The second type of attack is GPS-spoofing driven Forced Oscillation (FO) attack. Forced Oscillation (FO) in power grids can hamper system stability, cause power swing, damage equipment, limit power transfer capability etc, especially for the system with poor damping condition [75] [76]. The effect of FO event is much severe for the case when the FO frequency frequency approaches resonant or natural frequency of the system, in this case the entire system might suffer from a complete blackout [77]. FOs are mainly caused by external periodic disturbances, such as periodic variation in loads or malfunction in Power System Stabilizers (PSS) [78]. FOs are predominantly detected using time synchronized data [75] [79]-[82]. There are several real-world cases such as: the oscillation events of the western interconnect in 2005 [75], in 2022 [83], FO of eastern interconnect in 2019 [83], where the occurrence of FOs were identified with PMU data. For the cases in reference [75] and [83], the oscillation frequencies were approximately resonant with NS-A mode ($0.25Hz$) [84].

In this work we show that it is possible to carefully craft a periodic GPS-spoofing attack that adds forced oscillations to the PMU measurements, mimicking an actual FO event in the system. If the attacker can spoof the GPS signal and shift the 1 PPS signal periodically, it is possible to inject an additional oscillation in the phasor measurements. Proper tuning of the periodic shift in 1 PPS enables the attacker to create an oscillation with a frequency close to inter area frequency modes, such as $0.25Hz$ [84].

Attacker can initiate such attack at multiple locations and make it sustain over a long time. The system operator will detect the additional oscillations using PMU measurements, and can interpret it as an actual FO event caused by a periodic physical fault in the system. As a restorative method, the system operator may remove the possible sources of FO such as battery banks and loads, which will incur financial losses and/or unwanted changes in system states. Attacker can create this GPS-spoofing driven FO attack with a very small

deviation in PMU phase angle measurements, and creating such attack does not require detailed insider information of the system. Knowledge regarding only the inter area modal frequencies is enough for the attacker to carry out such attack.

The third type of attack targets the Phasor Data Concentrator (PDC) time-synchronization, instead of PMUs directly. PDCs receive time-tagged measurements from PMUs, align all the PMU measurements, and send the time-tagged measurements to the next stage of the cyber-layer. As the decisions of system operator (SO) rely on the timestamped information provided by PDCs, it is necessary to ensure the security of PDCs against possible cyber threats that targets the time-synchronization.

At each timestamp, each PDC waits for a specified time period (termed as wait period) so that measurements from all PMU channels connected to that particular PDC arrive. If measurements from a one or more than one PMU channels do not arrive within that wait period, the PDC discards those measurement from that PMU and sends the remaining measurements. An attacker can create enough delay in the communication channel connecting a specific PMU channel and PDC with the goal of causing the measurements from that specific PMU channel to arrive later than the wait-period of the PDC. As a result, the PDC discards measurements from the target PMU and aggregates the measurements from remaining PMUs to transmit to next layer of cyber system. However, creating such significant delay of one PMU channel will be easy to detect by Bad Data Detection (BDD) algorithms. We propose a coordinated data-drop attack, which aims at creating a two-step attack scenario. In the first step, the attacker targets one PMU and make the measurements from this PMU arrive little earlier than actual arrival time to PDC and keep doing so for the attack duration. Since the PDC starts the wait-period counter at the moment of first PMU data arrival, the early arrival from one PMU forces the PDC to start the wait-period counter little earlier than expected for normal communication delays. Since the wait-period for a PDC is constant, an

early start causes the wait-period ends earlier than normal.

For the second step, the attacker targets a second PMU and causes a small delay in the communication channel to the PDC. Since the PDC wait-period has been forced to earlier than normal, a small delayed measurement from second PMU will be enough to make it arrive later than the PDC wait-period window, subsequently causing PDC to drop the measurement from second PMU due to the assumed communication delay. Since both the arrival of first PMU measurements and the delay of second PMU measurements are small and are carefully chosen, it is more difficult for the SO to detect the actual reason behind PDC data-drop.

This chapter describes the formulations of three cyberattack models to illustrate the specific exploitation of the time-synchronization feature of time-synchronized devices (PMUs and PDCs) that are not detected by existing BDD algorithms. The three attack models can be be summarized as follows:

- a relentless small incremental GPS-spoofing attack model targeting the power flow calculations. We develop an optimization criterion to create an attack that is undetectable against conventional bad data detection schemes. The optimization algorithm calculates the phase angle deviations required at each 1 PPS, starting from off-peak hour, to cause the significant on the perceived power flow calculation between two nodes during peak load-hours by assuming an angle stability limit in the constraint, even though the actual flow through the same branch remain unchanged;
- a GPS-spoofing driven FO attack where the attacker does not require detailed system information. The attacker creates a false oscillation in the measurement with periodic small shift in time reference (1 PPS) using GPS-spoofing attack;
- an attack targeting the limitation of real-time operation PDCs. The attacker causes one PMU measurements to arrive earlier than its normal arrival time to force the

PDC start the wait-period counter earlier. The attacker then targets a second PMU and introduces a small delay in the data arrival for this PMU. The delay is carefully engineered to make the second PMU data arrive after the wait-period of PDC, causing PDC drop the data from the second PMU. This attack is termed as "PDC data-drop attack".

These three attacks are not the only possible GPS spoofing attacks but are a good representation of the various ways in which GPS spoofing can be used to perform attacks not detected by existing bad data algorithms.

3.4 Attack 1: Stealthy GPS-Spoofing Attack Modelling

The attacker starts the attack at the initial time t_0. The phase angle shift a_0 generated by the spoofed signal will be derived by solving optimization equation which aims at enabling the attack to be undetectable by commonly used detection techniques that are discussed in chapter 4. The attacker creates a spoofed GPS signal for the PMU at bus i and/ or j at t_0, introducing a time shift $\Delta t_0 = \frac{a_0}{2\pi f}$ [85], corresponding to the optimal phase angle measurement shift a_0 caused by spoofing and system frequency f.

All the sampled measurements of PMU following the timestamp t_0 will be manipulated carry on this time shift in their measurements and the corresponding phase angle measurements will be phase shifted by $\Delta\theta_0 = 2\pi f \Delta t_0 = a_0$. The next step of the attack is initiated at time t_1, after S number of samples. At time $t_1 - T_s$, the attacker estimates the phase angle measurements θ_{i1} and θ_{j1} for timestamp t_1. At t_1, the attacker solves the optimization equation using previously estimated phase angle measurements, (θ_{i1} and θ_{j1}), to compute the new attack value a_1. The corresponding time shift that the attacker needs to introduce

by GPS-spoofing will be $\Delta t_1 = \frac{a_1}{2\pi f}$. The overall phase angle shift in the PMU measurement for the next S number of samples becomes $\Delta\theta_1 = 2\pi f \Delta t_1 + \Delta\theta_0$. The computed power flow through the branch $i-j$ will also deviate accordingly. The attacker keeps instigating the spoofing attack for the following timestamps $t_2, t_3, ...$until T, at which the power flow through the branch $i-j$ reaches the peak value. The tempered extimated power flow, which kept increasing from the actual power flow in the previous timestamps, suffers from an enhanced deviation due to the attack and crosses the power flow limit of the line $i-j$.

The main difference between the GPS-spoofing attack of the proposed model and FDIA is that, in the conventional FDIA the attacker needs to get into the cyber layer or breach network security to initiate the attack. In this model the attacker is not required to breach network security, the attack is launched by spoofing the GPS signal received by the PMU, and the attack is outside of the cyber-physical system of the smart grid. In FDIA, the attacker injects the false data into the cyber layer; however, in the GPS spoofing attack model discussed in this work, the attacker doesn't inject any falsified measurement, rather s/he forces the PMU algorithm to introduce a phase shift in the computed phasor by disrupting GPS signal received by the PMU's GPS receiver. Instead of altering the phase angle measurement directly, the GPS spoofing attack shifts the 1 Pulse-Per-Second (PPS) signal used by the PMU for time reference, and this shift in 1 PPS reference signal reflects as a small change in phase angles for the phasors computed until the next 1 PPS is received. The overall topological structure of the GPS-spoofing attack considered in this work can be depicted in fig 3.1.

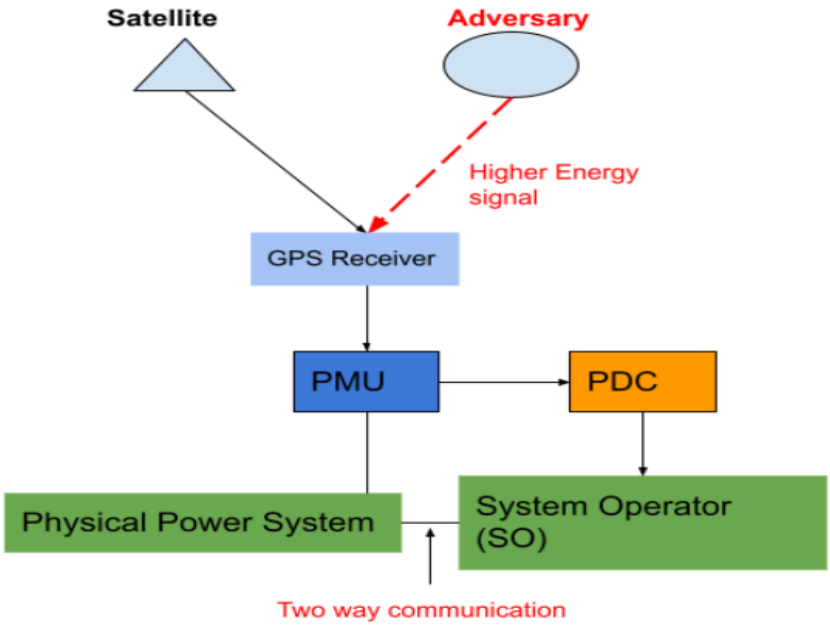

Figure 3.1: GPS spoofing attack structure

3.4.1 Formulation of Stealthy GPS-Spoofing Attack

During GPS-spoofing attack, the time synchronization with GPS signal is distorted and the PMUs start sending measurements of shifted time reference to the PDCs. Due to the change in the time reference, the most affected part of phasor measurement under GPS-spoofing attack is the phase angle; in contrast to only a slight change in the measured magnitude. The SO looks for anomalies in phasor measurements, using state estimation and other bad data detection techniques. SO uses snapshots of phase angle measurements over moving time window and look for any estimation residuals exceeding threshold. As discussed in previous section, the attacker needs to shift the time reference by a very small amount, which causes very small deviation in phase angle measurements, subsequently making the estimation residual by conventional bad data detection models less than threshold. Such carefully crafted stealthy attacks are undetected by the SO. If the attacker keeps shifting

the time reference by this small amount at each 1 PPS signal over a long period of time, there will be a significant amount of shift in time reference after the whole period. From the perspective of SO, it is not possible to detect this shift in GPS 1 PPS time reference by performing state estimation based bad data detection on phasor measurements after each millisecond or fractions of second, since the shift in GPS 1 PPS time reference satisfies the undetectability constraints of state estimation based method.

3.4.2 Optimizing Attack Vector

The most common bad data detection method employed at the control center is Weighted Least Squared Error (WLSE) based state estimation. The undetectable attack model in this work focuses on circumventing the WLS based state estimation technique.

For an n bus system, the state variable at a specific time instance can be represented as the vector $\mathbf{x} = [x_1, x_2, ...x_n]$ and the measurement variables can be represented with the vector $\mathbf{z} = [z_1, z_2, ...z_m]$. Here m is the number of meters (m>>n). The relation between $\mathbf{z}$ and $\mathbf{x}$ can be expressed as

$$\mathbf{z} = \mathbf{H}\mathbf{x} + e \tag{3.1}$$

H is the Jacobian matrix that represents the non-linear relation between the state variable and the measurement variable. $e = [e_1, e_2, ...e_m]$ is the measurement error vector. An FDIA will go undetected if $||z - H\hat{x}||_2$ is less than threshold τ^r, $\hat{x}$ being the estimated state variable which can be calculated from the Weighted Least Square (WLS) method $\hat{x} = (H^T R^{-1} H)^{-1} H^T R^{-1} z$. R is the measurement error covariance matrix. If the attack $\mathbf{a}$ vector is applied during FDIA, the measurement vector under attack will be $z_a = z + a$ and

the estimated state variables under attack will be $\hat{x_a} = \hat{x} + c$. The estimated attack vector is $c = (H^T H)^{-1} H^T a$. After injecting the attack vector, $||z_a - H\hat{x_a}||_2 = ||z + a - H\hat{x} - Hc||_2$ $\leq ||z - H\hat{x}||_2 + ||a - Hc||_2$. For a carefully crafted attack vector, such as $a = Hc$, the estimation residual becomes $||z_a - H\hat{x_a}||_2 \leq \tau^r$. As the estimation residual becomes less than threshold τ^r, the SO fails detect FDIA [24].

The attacker goal is to make the term $||a - Hc||_2$ as small as possible so that $||z_a - H\hat{x}_a||_2$ remains less than the threshold τ^r. $a - Hc$ can be written as Fa, where the term $F = (H(H^T H)^{-1} H^T - I)$. The attacker needs to satisfy the following criterion:

$$\min_a \quad ||Fa||_2 \tag{3.2}$$

To avoid getting detected, the term $||Fa||_2$ needs to be between τ^r and $||z - H\hat{x}||_2$ and the attacker must satisfy the following optimizer:

$$\begin{aligned} \min_a \quad & ||Fa||_2 \\ \text{s.t.} \quad & ||Fa||_2 \leq \tau^r - ||z - H\hat{x}||_2 \end{aligned} \tag{3.3}$$

Assume the impact threshold of attack vector is ζ, implying if the attack vector is greater than this value, there will be a significant impact on the system, else the attacker cannot inflict any damage to the grid. To avoid detection, the attack vector **a** must be less than impact threshold during each time instance, however the total impact, after the phase angle deviation at every time instance being added up, will be significant at the end of total time period **T**. The attacker targets the branch connecting bus i and j, corresponding attack vectors are a_i and a_j respectively ($a_i, a_j \in \mathbf{a}$). Attacker only inject non zero values as a_i and a_j, keeping all other elements of the array **a** as 0. For each time instance, the attacker has to satisfy the following:

$$\begin{aligned} \min_{a} \quad & ||Fa||_2 \\ \text{s.t.} \quad & ||Fa||_2 \leq \tau^r - ||z - H\hat{x}||_2 \\ & ||a_i - a_j|| < \zeta \end{aligned} \tag{3.4}$$

Each time instance can be depicted as index t; t = 1,2,....,T. T = total time period. We need to add the suffix t to indicate the optimization criterion at each time instance. Therefore for the whole time period the optimization criteria becomes:

$$\begin{aligned} t = 1:T \quad & \{ \\ \min_{a_t} \quad & ||Fa_{:,t}||_2 \\ \text{s.t.} \quad & ||Fa_{:,t}||_2 \leq \tau^r - ||z_t - H\hat{x}_t||_2 \\ & ||a_{i,t} - a_{j,t}|| < \zeta \\ \} & \end{aligned} \tag{3.5}$$

$$\sum_{t=1}^{T} ||a_{i,t} - a_{j,t}|| > \zeta$$

The next challenge is to find the impact threshold ζ. The ζ must be less than the ℓ_1 norm of the attack vector for single time instance to avoid detection, but it must be greater than the sum of the ℓ_1 norm of the attack vector over the total T period of time to incur damage to grid operation. Since the $||a||_1$ can takes the value between 0 to ζ at each time instance, it should be between ζ/T and ζ so that the $\sum_{t=1}^{T} ||a_{i,t} - a_{j,t}|| > \zeta$ condition is satisfied.

The optimizer 3.5 becomes:

$$\begin{aligned} \min_{a_t} \quad & ||Fa_{:,t}||_2 \\ \text{s.t.} \quad & ||Fa_{:,t}||_2 \leq \tau^r - ||z_t - H\hat{x}_t||_2 \\ & \zeta/T < ||a_{i,t} - a_{j,t}|| < \zeta \end{aligned} \tag{3.6}$$

In the optimization criteria 3.6, if the attack vector at each time instance satisfies $\zeta/T < ||a_i||_1 < \zeta$, the cumulative impact will be automatically greater than threshold over the whole time period T. Additionally, ζ/T can be replaced as ζ'. Since the eqn 3.6 is a convex, there exists a global minima that corresponds to the attack vector satisfying undetectability constraint. For the second inequality constraint, the solver needs to search the point in a wide range of values between ζ' and ζ, depending on the size of time period T. The second inequality constraint can be computationally simplified by making the attack vector within the range ζ' to $\zeta' + \epsilon$, where ϵ is a small positive integer. In this case, the solver needs to search for the optimum attack vector within small range of constraints.

3.4.3 Determining Impact Threshold

The next challenge is to find the impact threshold ζ', which is defined by the amount of change in power flow calculation incurred by relentless small GPS-spoofing attack. The attacker has to ensure that, the impact must not exceed the operating limit of the power system during off-peak hour. The SO does not expect any operating limit violation during off-peak hour, as a result a very large change in power flow calculation will make the SO suspicious of possible cyberattack. The attacker targets the peak-hour, when the SO generally expect the contingencies due to operating limit violation due to large load demand. If calculated power flow breaches the limit, system operator will consider it as high load demand instead of possible cyberattack. In this way, attacker can enforce the SO take unnecessary restoration

action.

Branch current limit between the bus i and bus j,

$$-I_{lim} \leq I \leq I_{lim} \tag{3.7}$$

Power flow limit between the bus i and bus j,

$$-P_{lim} \leq P \leq P_{lim} \tag{3.8}$$

The power flow between two buses generally depends on the voltage magnitudes of the two nodes, the phase angles of two nodes and the line admittance between the nodes. The power flow between the bus i and j in AC power flow model can be denoted as follows:

$$P_{ij} = |V_i||V_j| \left[g_{ij}cos(\theta_i - \theta_j) + b_{ij}sin(\theta_i - \theta_j)\right] \tag{3.9}$$

In the attack model described in the previous subsection, the attacker creates an incremental deviation of a_i to the phase angle measurement θ_i of bus i, and a deviation of a_j to the phase angle measurement θ_j of bus j. The new power flow during GPS-spoofing attack becomes:

$$\begin{aligned} P'_{ij} = |V_i||V_j|[&g_{ij}cos(\theta_i - \theta_j + a_i - a_j) \\ &+b_{ij}sin(\theta_i - \theta_j + a_i - a_j)] \end{aligned} \tag{3.10}$$

Applying angle addition and subtraction theorem of trigonometry,

$$\begin{aligned} P'_{ij} = |V_i||V_j|[&g_{ij}cos(\theta_i - \theta_j)cos(a_i - a_j) \\ &+g_{ij}sin(\theta_i - \theta_j)sin(a_i - a_j) \\ &+b_{ij}sin(\theta_i - \theta_j)cos(a_i - a_j) \\ &-b_{ij}cos(\theta_i - \theta_j)sin(a_i - a_j)] \end{aligned} \tag{3.11}$$

As depicted in eqn 3.6, the phase angle deviations a_i and a_j are very small. To comply with the IEEE standard of synchrophasor data transmission [32], phase-angle deviation must be less than 57^o for 60Hz system. For a very small a_i and a_j, the $cos(a_i - a_j)$ term can be approximated as 1. Therefore eqn 3.11 can simplified as,

$$\begin{aligned} P'_{ij} \approx |V_i||V_j|[&g_{ij}cos(\theta_i - \theta_j) \\ &+g_{ij}sin(\theta_i - \theta_j)sin(a_i - a_j) + b_{ij}sin(\theta_i - \theta_j) \\ &-b_{ij}cos(\theta_i - \theta_j)sin(a_i - a_j)] \end{aligned}$$

$$\begin{aligned} = |V_i||V_j|[&g_{ij}cos(\theta_i - \theta_j) + b_{ij}sin(\theta_i - \theta_j) \\ &+g_{ij}sin(\theta_i - \theta_j)sin(a_i - a_j) \\ &-b_{ij}cos(\theta_i - \theta_j)sin(a_i - a_j)] \end{aligned} \tag{3.12}$$

The new AC power flow during attack is the actual power flow added by an additional term as depicted in eqn 3.13.

$$\begin{aligned} &= P_{ij} + |V_i||V_j|g_{ij}sin(\theta_i - \theta_j)sin(a_i - a_j) \\ &-|V_i||V_j|b_{ij}cos(\theta_i - \theta_j)sin(a_i - a_j)] \end{aligned} \tag{3.13}$$

To make the power flow between bus i and bus j within the MVA limit, P'_{ij} must be less than $|P_{lim}|$. If the term $|V_i||V_j|g_{ij}$ is expressed as D_1 and the term $|V_i||V_j|b_{ij}$ is expressed as D_2, the second constraint of the eqn 3.4 can be rewritten as:

$$\begin{aligned} &D_1 sin(\theta_i - \theta_j)sin(a_i - a_j) - D_2 cos(\theta_i - \theta_j)sin(a_i - a_j) \\ &< |P_{lim}| - D_1 cos(\theta_i - \theta_j) - D_2 sin(\theta_i - \theta_j) \end{aligned} \tag{3.14}$$

As the attacker aims at instigating relentless GPS-spoofing attack in real time, the calculation time for optimization of eqn 3.6 must be less than T_s, as discussed in section 5.2. In order to simplify the eqn. 3.14, the $sin(a_i - a_j)$ can be approximated as $a_i - a_j$ for small a_i and a_j. After simplification, eqn. 3.14 becomes,

$$\begin{aligned} &D_1 sin(\theta_i - \theta_j)(a_i - a_j) - D_2 cos(\theta_i - \theta_j)(a_i - a_j) \\ &< |P_{lim}| - D_1 cos(\theta_i - \theta_j) - D_2 sin(\theta_i - \theta_j) \end{aligned} \tag{3.15}$$

The attack term $a_i - a_j$ can be computed with the following equation,

$$a_1 - a_2 < \frac{|P_{lim}| - D_1 cos(\theta_i - \theta_j) - D_2 sin(\theta_i - \theta_j)}{D_1 sin(\theta_i - \theta_j) - D_2 cos(\theta_i - \theta_j)} \tag{3.16}$$

The right hand term of the eqn 3.16 can be approximated as the impact threshold ζ'. The optimization criterion from eqn 3.6 is modified to the following form:

$$\begin{aligned} \min_{a_{:,t}} \quad & ||Fa_{:,t}||_2 \\ \text{s.t.} \quad & ||Fa_{:,t}||_2 \leq \tau^r - ||z_t - H\hat{x}_t||_2 \\ & \zeta' < ||a_{i,t} - a_{j,t}|| < \zeta' + \epsilon \\ & \epsilon > 0 \end{aligned} \tag{3.17}$$

$$\text{where}, \zeta' = \frac{|P_{lim}| - D_1 cos(\theta_{i,t} - \theta_{j,t}) - D_2 sin(\theta_{i,t} - \theta_{j,t})}{T \times D_1 sin(\theta_{i,t} - \theta_{j,t}) - D_2 cos(\theta_{i,t} - \theta_{j,t})}$$

3.4.4 Test of undetectability

GPS-spoofing attacks impact the phase angle measurements most, therefore it can be considered as FDIA targeting phase angle measurements only [13]. System Operator (SO) looks for the successive bad data in the measurements to suspect the occurrence of FDIA, which makes FDIA detection similar to Bad Data Detection (BDD). As discussed in section 3.4.1, the most common Bad Data Detection technique is the WLSE based state estimation method [86], where the System Operator (SO) receives the measurements from the physical power system and calculates the residuals between the actual measurement z and the estimated measurement $H\hat{x}$. The notation z, H and x are same as discussed in 3.4.1. The SO considers

the measurements as suspicious if the residual $||r||_2 = ||\hat{z} - H\hat{x}||_2$ is less than a predetermined threshold τ^r.

Kalman Filtering (KF) [87] is an effective tool to detect bad data caused by electrical events and FDIA. For a system, if the state variable is $x(t)$ and the measurement variable is $y(t)$, the state variable at time $t+1$ can be estimated from the previous state $x(t)$ using the following relation:

$$x(t+1) = Ax(t) + w(t) \tag{3.18}$$

KF estimates the state variables $\hat{x}(t)$ at time t using the state variables and measurements upto $t-1$. P(t) is the covariance of estimates at time t. The time updates of state variables and covariance matrix are expressed as:

$$x(t+1|t) = Ax(t) + w(t) \tag{3.19}$$

$$P(t|t-1) = AP(t-1)A^T + Q \tag{3.20}$$

Consequently, the measurements are updated using the following relations:

$$K(t) = P(t|t-1)H^T[HP(t|t-1)H^T + R]^{-1} \tag{3.21}$$

$$P(t|t) = P(t|t-1) - K(t)HP(t|t-1) \tag{3.22}$$

$$\hat{x}(t) = A\hat{x}(t-1) + K(t)[z(t) - H\hat{x}(t|t-1)] \tag{3.23}$$

$$P(t) = [I - K(t)H]P(t|t-1) \tag{3.24}$$

$K(t)$ is the Kalman gain at time t. Starting from an initial condition $\hat{x(0)} = 0$ and $P(0) =$ covariance matrix of: $\hat{x(0)}$, KF provides a recursive calculation of state variables using minimized mean-squared error. The residuals between the measurement $z(t+1)$ and the estimation $H\hat{x}(t+1)$ is tested against predefined threshold τ^k. If the residual exceeds the predetermined threshold, it is perceived as a bad data. The KF estimator generates better estimations of state variables than WLSE based estimator [87]; however conventional FDIA may impact the estimation performance, which can be avoided by updating measurement weighting function $W(t) = R^{-1}$ using the following equation [88] :

$$(W_{new}(t))^{-1} = (W(t))^{-1} \times e^{|z(t)-H\hat{x}(t|t-1)|} \tag{3.25}$$

The updated weighting function in eqn 3.25 increases the FDIA detection probability for the deviation based KF approach compared to the conventional KF estimator [89].

Hankel-matrix based bad data detection is another useful tool to detect the existence of any anomaly in time-series measurements, which looks for bad data over moving time-window [90]. Since the proposed attack scheme initiates a gradual incremental variation in phase angle over time, it is necessary to test the undetectability of the attack model against Hankel-matrix based BDD. However, since the proposed attack model modifies the phase angle measurements very slowly over time, and the phase angle can deviate sharply during load change of peak-hour, it is not sufficient to observe low-rank approximation error of Hankel-matrix alone for the affected node to conclusively determine the occurrence of any attack, since both load change and proposed attack can demonstrate similar change in estimation error for Hankel-matrix low-rank approximation based model.

3.5 Attack 2: Spoofing Driven FO Attack

3.5.1 Attack Formulation

In the proposed attack scenario, the attacker spoofs and shifts the GPS 1 PPS signal by a small time-window t_s, ensuring the phase angle deviation $\theta_s \propto t_s$ remains small enough to go undetected. The 1^{st} 1 PPS signal (at 1s) is unchanged (0 shift). For the 2^{nd} 1 PPS signal (at 2s), the shift is positive t_s. In other words, attacker spoofs the 1 PPS signal and make it arrive t_s later than the actual arrival time. The 3^{rd} 1 PPS signal (at 3s), the shift is again 0 and the 1 PPS signal arrives at the actual arrival time. For the 4^{th} 1 PPS signal (at 4s), the shift is negative t_s, and the attacker spoofs the 1 PPS signal to arrive t_s earlier than the actual arrival time, causing a periodic shift in 1 PPS signal. Since this shift completes one cycle in 4 second, it adds an additional $1/f = 0.25Hz$ frequency oscillation to the original measurements, even though there is no such oscillation in the physical system. The signal contains a FO of $0.25Hz$ which is same as NS-A mode frequency [84]. If the attacker keeps spoofing the 1 PPS signal in this way a over a long time, the voltage and current signals will exhibit similar property of an FO event with a resonant frequency $0.25Hz$. System operator, by performing Fast Fourier transform (FFT) and observing the Power Spectral Density (PSD), will become suspicious of the occurrence of an FO event. The visual demonstration of the periodic shift in GPS 1 PPS signal to initiate the proposed FO attack is depicted in fig. 3.2.

Mathematically, the shift in 1 PPS signal can be modelled as the corresponding phase angle deviation $\Delta\theta$ caused by the shift in time reference. For a voltage or current signal with nominal frequency of f_0, amplitude of X_m, initial phase angle of ϕ and sampling frequency of Nf_0, the signal can be expressed in time domain as $x(t) = X_m cos(2\pi f_0 t + \phi)$. The N sample can be estimated with the $x_n = X_m cos(n\theta + \phi)$ $n = 1, 2, ..., N-1$ [22].

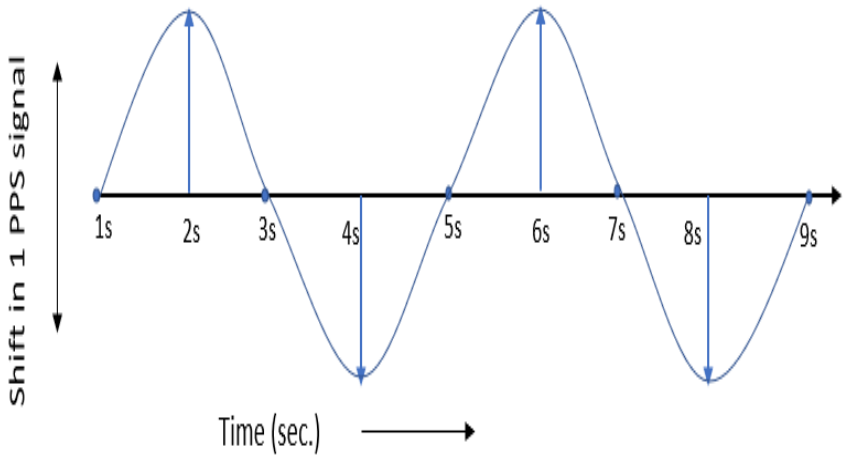

Figure 3.2: Creating a 0.25Hz oscillation by periodic shift of 1 PPS signal with GPS-spoofing

The complete voltage/current phasors are estimated using a non-recursive update method described in [22]:

$$X^N = \frac{\sqrt{2}}{N} \sum_{n=0}^{N-1} x_{n+1} \left[cos(n\theta) - jsin(n\theta) \right] \tag{3.26}$$

For the case of proposed attack model, the time shift t_s will create an angle deviation $\Delta\theta = 2\pi t_s/N$, which will modify the sample value x_{n+1} to x'_{n+1} in eqn. 3.26. The modified sample is,

$$x'_{n+1} = X_m cos((n+1)\theta + 2\pi t_s/N + \phi) \tag{3.27}$$

The attacker initiates the attack at time t_0. As the attacker does not cause any shift at the first 1 PPS at t_0, there is no t_s term in eqn. 3.27 for next Nf_0 samples. At the next or second 1 PPS signal since t_0, attacker causes a shift of t_s, therefore there is a $+t_s$ term

in eqn. 3.27 for next Nf_0 samples. At the third 1 PPS signal since t_0, the t_s is 0 for the next Nf_0 samples. From the fourth 1 PPS signal since t_0, attacker causes a deviation in opposite direction which is $-t_s$. As a result, the next Nf_0 samples will contain a $-t_s$ in eqn. 3.27. This periodic shift in 1 PPS signal due to GPS-spoofing attack will create a periodic variation in the samples of eqn. 3.27. The periodic shift will continue over a long time, for example for few minutes or even hours, so that the system operator will consider it as a sustained FO oscillation event, even though there is no physical FO source in the system. For the attack to emulate a FO, it is assume that the attacker performs similar 1 PPS oscillations at multiple locations.

3.6 Attack 3: Coordinated PDC Data-Drop Attack

The third type of attack is the coordinated PDC data-drop attack. The proposed attack model incorporates a two-step attack scenario. It targets two PMUs, one is the PMU that the attacker wants to get discarded by PDC ($PMU\#2$). The attacker makes another PMU ($PMU\#1$) measurement arrival earlier to the PDC, forcing the PDC to start counting wait period ΔT a little earlier than actual wait-period start. If T_s is the normal arrival time of $PMU\#1$ measurements under no-attack condition, and t_{early} is the amount of time that the attacker makes $PMU\#1$ reach earlier, $PMU\#1$ measurements now reach at $T_s - t_{early}$ and the PDC starts its timer for ΔT at an earlier timestamp $T_s - t_{early}$. The PDC wait period ends at $T_s - t_{early} + \Delta T$, which is earlier than the end time of normal condition $T_s + T_\Delta$. Measurements from $PMU\#2$ coming later than $T_s - t_{early} + \Delta T$ will now get discarded.

After making the $PMU\#1$ measurements reach earlier, even a small delay t_d for $PMU\#2$ is now large enough to get it discarded by PDC. This smaller delay is difficult to be detected by the System Operator.

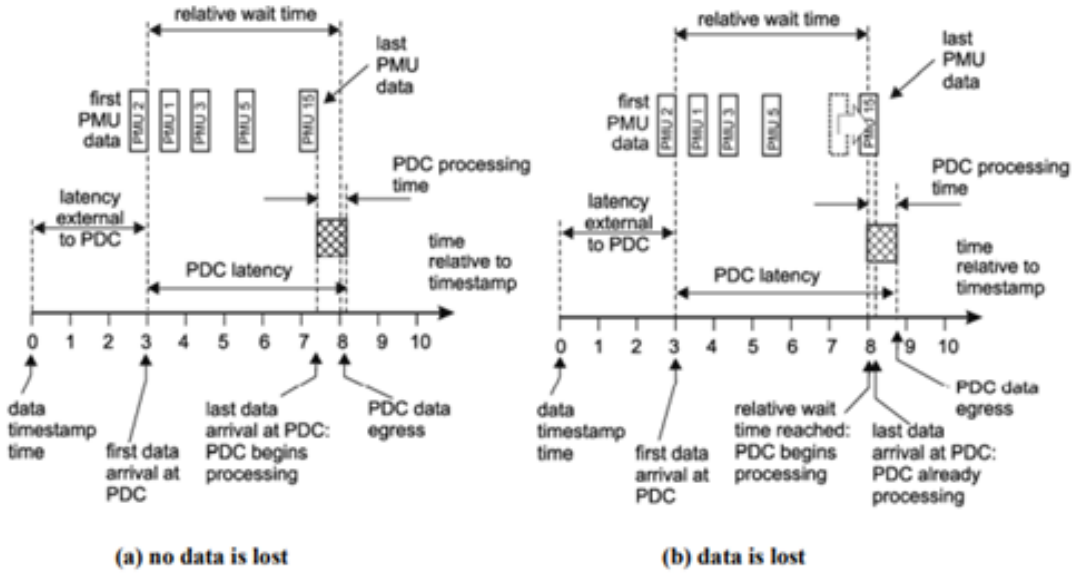

Figure 3.3: PDC wait-period [91]

This coordinated PDC data-drop attack scenario has one obstacle. The attacker cannot speedup communication channels, therefore the hardest part of formulating such attack is creating early arrival of $PMU\#1$ data. To accomplish this, the attacker of our proposed model uses a set of PMU data from consecutive samples to predict the PMU data at half the time of the next reporting rate. This advanced prediction is sent as the first early arrival. At the same time, the actual PMU data corresponding to the first early arrival is saved to be used for the next early arrival. From that point on, the data will arrive early in time but it will be one sample late PMU data.

Assuming $PMU\#1$ data under no-attack arrives at PDC at t_s timestamp. Under no-attack condition, the next data is expected to arrive at t_{s+1}. The attacker needs to have the knowledge regarding a certain number of $PMU\#1$ data upto t_s, which are denoted as $[x_1, x_2, ..., x_s]$. Using the data upto this timestamp, the attacker predicts the next data at t_{s+1}, which can be expressed as x_{s+1}. Under no-attack condition, the x_{s+1} should arrive at PDC at t_{s+1}. In the proposed attack scenario, after t_s the attacker breaches the com-

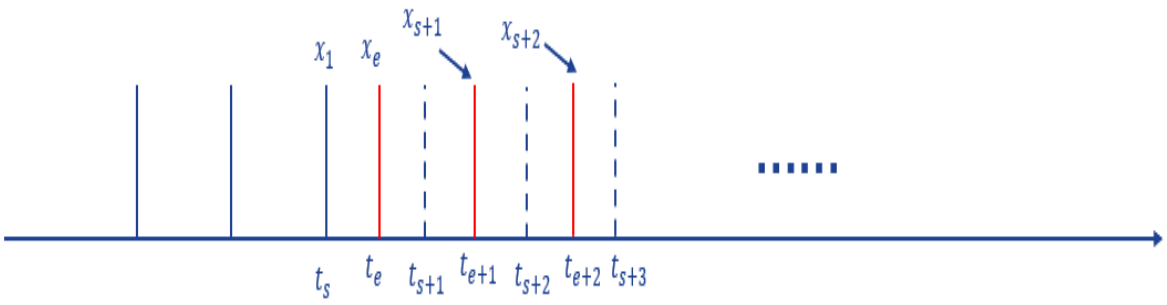

Figure 3.4: Formuating data early arrival

munication network and sends a interpolated data x_e to PDC at a timestamp t_e which is earlier than t_{s+1}. This is the first arrival instance. The attacker needs to ensure that the interpolated data x_e do not deem suspicious by SO. One way to achieve that is to calculate x_e by taking the average of x_s and x_{s+1}. Since under steady-state, the data at consecutive timestamps are not expected to change significantly from each other, the SO accepts x_e as normal data. The attacker saves the x_{s+1} and sends it next early arrival t_{e+1}, which after t_{s+1} but earlier than the following timestamp t_{s+2}. Similarly, the attacker sends x_{s+2} at t_{e+2}, and so on.

Fig. 3.4 illustrate the $PMU\#1$ data early arrival process accomplished by the attacker. Instead of $t_{s+1}, t_{s+2}, ..$, PDC now receives data at a little earlier times $t_{e+1}, t_{e+2}, ...$ As a result, PDC starts counting wait-period at earlier times $t_{e+1}, t_{e+2}, ..$ instead of $t_{s+1}, t_{s+2}, ...$

To detect FDIA or GSA, and to perform state estimation to detect measurement anomaly at each node in the grid, it is important to have measurements from at least two PMUs connected to that particular node. For the data-drop attack causes the loss of measurements from targeted particular PMUs, therefore the anomaly detection algorithms are unable to detect cyberattacks or perform state estimations with the presence of data-drop attack targeting critical PMUs. A graphical demonstration of proposed attack is depicted in fig 3.5.

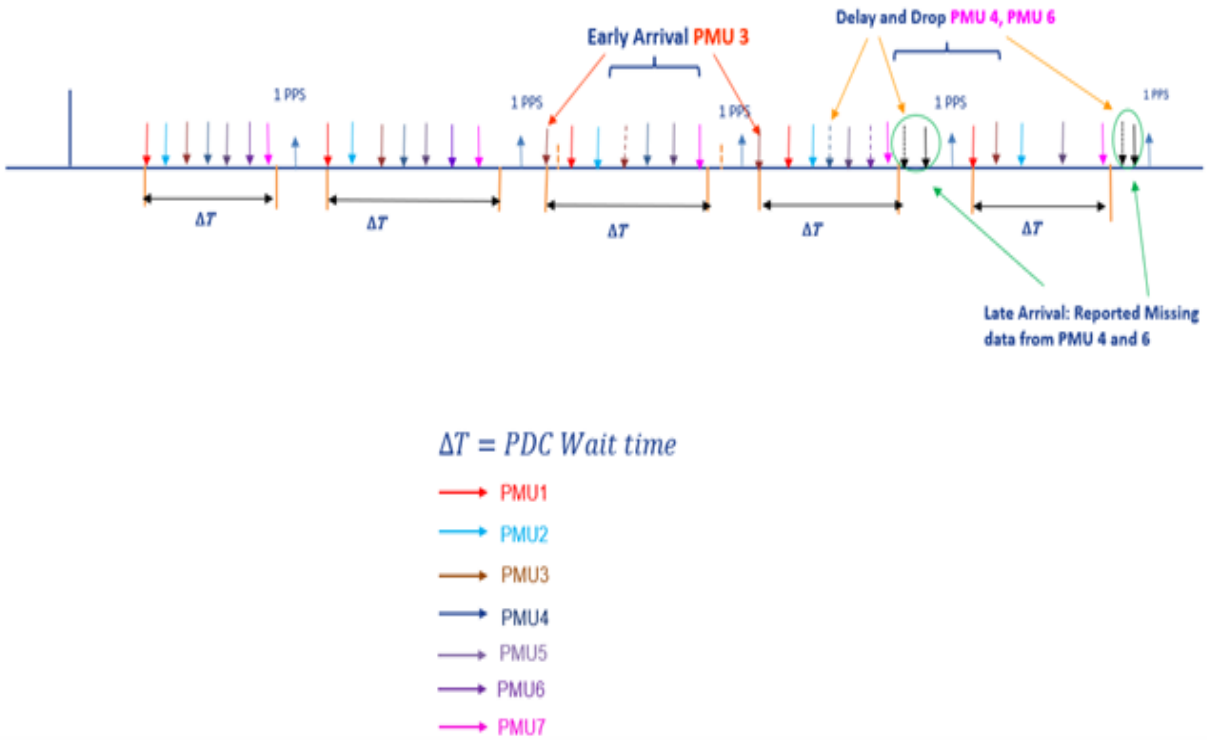

Figure 3.5: Proposed coordinated data drop attack

Chapter 4

Hankel-Matrix Enhancement and Sequential GPS-Spoofing Identification

4.1 Details of Publications

Co-authors: Virgilio Centeno

Reference [92]: © 2022 IEEE. Reprinted, with permission, from I. Khan and V. Centeno, "Detecting GPS-spoofing Attack on PMU Data with Phase Angle Unwrapping Technique and Low-Rank Approximation of Hankel Matrix," in 2022 IEEE Power and Energy Society General Meeting (PESGM), July 2022.

Co-authors: Virgilio Centeno

Reference [93]: © 2023 IEEE. Reprinted, with permission, from I. Khan and V. Centeno, "Realtime Detection of PMU Bad Data and Sequential Bad Data Classifications in Cyber-Physical Testbed," in IEEE Access, July 2023.

4.2 Introduction

There is an increasing penetration of PMU into smart grids that offer superior performance over SCADA based system. However, as discussed in chapter 1, modern PMU integrated smart grids are at risk of sophisticated cyberattacks. Researchers have assessed the vulnerabilities of PMU integrated MGs against cyber-attacks and proposed possible defense mechanism against such attacks. The most common vulnerabilities of PMUs in MGs is the third-party intrusion at the communication channel either between two portions of the cyber layer or between the physical and cyber layers. The third-party, also termed as the *attacker* can modify or take control over the data packets sent over the communication channel, thereby making it a man in the middle attack (MITM) [94] [95]. Of all types of MITM attacks, false data injection attack (FDIA) has been of particular interest among the researchers in recent year. FDIA can be best described as malicious data injection, or modifying the data packets by the intruders having the knowledge of system configuration [96]-[98]. The modified data can lead the system server taking unwanted actions and cause a misoperation in the grid.

In chapter 3 we discussed GPS-spoofing attacks (GSAs) that targets time-synchronization of PMUs. GSA doesn't require the attacker to manipulate a highly secured communication channel or to have internal knowledge of the network parameters. As explained in chapter 3 attackers can spoof the time-reference in the PMU [101] by manipulating the GPS 1 PPS signal [102]. Instead of modifying the measurements directly, GSA changes the reference for measureed phase angles. As a result, the phase angle measurements received by the system operator (SO) are shifted when referenced to the angle measurements of other PMUs. If not detected, these measurements may result in incorrect actions by the SO, such as tripping a line serving critical loads and/or send wrong command back to the IEDs [103].

The the cases of physical fault, FDIA, and GSA, the phasor measurements from PMUs exhibit anomaly in the data. In general, cyberattacks and physical faults require different restoration method, making it critical for SO to differentiate between these two sources of data anomalies. In addition, GPS-spoofing attacker targets the GPS 1 PPS signal and unlike FDIA, the attacker does not need to breach the communication network. To ensure accurate system restoration of real events, it is also imperative for the SO to conclusively identify the GSA and differentiate it from FDIA. Several event detection schemes such as weighted least squares (WLS) [98], Kalman Filtering (KF) [104], software-defined networking model [105], active synchronous model [106], etc. can detect the PMU data anomaly with high precision. Carefully designed FDIA can bypass a WLS based detection model [112]. KF is a more robust detection method to implement in real time. However, since it relies on the measurements from the immediate previous state, a monotonous variation of time-series measurements during faults or cyberattacks may provide wrong detection flag to the SO. Whereas the models proposed in [106] and [107] demonstrate satisfactory performance in terms of anomaly detection for time-series measurements, these models fail to distinguish cyberattack from physical events. The machine learning and big data approaches in [108] - [111] train the model with sensor measurements to compare the expected measurement with actual measurements. Nonetheless, these models suffer similar problem of failing to separate cyberattack from physical events. In addition, it is computationally difficult to implement these models in real-time.

The next challenge of event detection is real-time implementation. The Hankel-matrix based model uses time-series measurements over a moving data-window, therefore it is easily implementable in real-time. Another challenge of algorithms is numerical efficiency. Implementing one algorithm for event detection in the first part and a different one for event classification in the second part is numerically inefficient. This is the case for the online detection model

described in ref [112] and [113], both of them can be implemented in real-time. However, these models are numerically exhaustive and are not scalable to a different grid topology and operating set points. The models need to be re-trained for each change in topology/operating points.

The low rank approximation of Hankel-matrix is able to recover a large volume of missing data, and correct the event that exists in PMU measurements [114] [115] - [117]. The Hankel-matrix structure based models also showed superior performance when implemented in real-time [114] [115]-[118]. However, the general Hankel-matrix algorithms that use phasor measurements (magnitude and raw phase angle measurements) fail to conclusively identify the GSA and differentiate it from FDIA.

Hankel-matrix offers a more efficient real-time implementation than ML based methods, as well as provides superior performance as it exploits temporal and spatial relationship among multiple PMU channels, giving it an edge over KF and WLS based methods. Moreover, recently various utilities and research laboratories utilised existing Hankel-matrix based algorithms for event detection, differentiating events from noise, and missing data recovery. Therefore, it is more efficient to enhance the existing Hankel-matrix based algorithm to differentiate GPS-spoofing attacks from FDIAs, as well as to classify physical events from cyberattacks, since this will provide less data processing and computational burden.

With this advantages in mind, we propose to enhance the event detection and correction models described in [114] [115] - [117] to conclusively identify GSA and differentiate it from FDIA and/or physical faults. The unwrapped phase angle measurements as well as the phase angle difference between target PMU and a reference PMU show contrasting behavior for GSA and for FDIA. Therefore, the enhanced Hankel-matrix based algorithm using unwrapped phase angle measurements or phase angle difference can determine the occurrence of GSA. After enhancing the Hankel-matrix based algorithm, we implement the GSA

identification in a real-time sequential event classification model

The overall real-time sequential implementation has three steps: first of which is the event detection. The Hankel-matrix based model developed in [114] and [117] can detect event when the Hankel-matrix at each timestamp is created using single channel PMU measurements. The Hankel-matrix based model analyzes each PMU channel individually to detect event, therefore it does not depend on grid topology. After detecting the data anomaly, the model goes to second stage which is classification of event among physical faults and cyberattack using multi-PMU Hankel-matrix. Only a very few works in existing literature focused on differentiating between physical events and cyberattacks. A notable example of differentiating cyberattacks and physical events is the online machine learning (ML) based model [107]. Another ML based model that exclusively detects cyberattack and differentiates it from faults for differential relays is proposed in [119]. Both models have limitations of scalability and numerical complexity. ML based model requires training of large volume of measurements for a specific grid topology and operating conditions. A large dataset is required to be trained for any change in grid topology and operating conditions, which is numerically exhaustive. Ref [115] utilizes low rank approximation of Hankel-matrix to distinguish measurement noises from physical events. We exploit similar concept to differentiate between physical events and cyberattacks by creating multi-PMU Hankel-matrix.

The proposed real-time classification model computes the low rank approximation error among the temporal measurements from neighboring PMUs. For each PMU node in the grid, the model uses multi-PMU Hankel-matrix by taking measurements from the PMU nodes that are physically connected to it. As the model computes the low rank approximation error using measurements from only a few physically connected nodes, it is numerically less exhaustive. Additionally, the model does not depend on the grid topology or system operating condition since it analyzes the time-series measurements from only a cluster of physically connected

nodes. For cyberattack, the temporal relation among physically connected nodes is different from the case with physical events, regardless of the grid topology. These attributes make the proposed model scalable to more complex topology and different operating conditions.

The third stage of the sequential classification model is to differentiate GSA from FDIA. Conventionally detection model of GSA can be formulated similarly as FDIA detection approach, with phase angle data used as measurement matrix [99], [120] [121]. Even though GSA can be detected in a similar way of FDIA, these approaches fail to differentiate GSA from FDIA. Our enhanced phase angle Hankel-matrix model, with its low-rank property, can differentiate GSA from FDIA and therefore can conclusively identify GSA.

The contribution of this work is twofold: first, we enhance the general Hankel-matrix algorithm of ref [114], [115] - [117] for conclusive identification of GSA and differentiation of GSA from FDIA. Secondly, we propose and implement a real time detection and subsequent classification of data anomalies in the PMU measurements based on the event types such as: physical events, FDIA and GSA. We have considered a sequential structure of the algorithm where the event is detected in the first step. The event is classified between physical event and cyberattack at the second step. If the cyberattack is identified, the algorithm uses enhanced Hankel-matrix algorithm to classify the attack between FDIA and GSA. The proposed sequential anomaly detection model is tested in the real-time testbed described in chapter 2.

4.3 Enhancement of Hankel-matrix for Efficient Detection of GPS-Spoofing Attack

Matrix low-rank approximation is generally used for matrix completion, a robust method for data recovery and bat data detection for time-series measurements. Ref [122]-[124] demonstrated the effectiveness of low-rank approximation for various real-world cases. The key idea behind the low-rank approximation is, for a matrix Y with small-noisy data, there exist l singular values obtained from Singular Value Decomposition (SVD) that are insignificant or can be approximated as zero. If a new matrix Y^r is formed with remaining significant $r = rank(Y) - l$ singular values, it is a rank-r approximation of the original matrix Y. When the data do not contain any significant noise or anomaly, the low rank form Y^r is a good approximation of the original matrix Y. On the other hand, for noisy data, the singular values that were previously considered insignificant (near zero), are no longer small enough to be approximated as 0. Hence the original matrix can no longer be approximated with low rank r with similar estimation accuracy, and can only be approximated with a rank that is larger than r.

The low rank approximation can identify the existence of data anomaly or measurement noises for power system data, using the spatial and temporal PMU data matrices [125] [126]. Hankel-matrices incorporate temporal and spatial correlation if formed using time-series PMU measurements, and exhibits low-rank property [127]. These attributes make Hankel-matrix a suitable candidate for PMU data anomaly detection.

Hankel-matrix is a skew-diagonal square matrix which is constant on each anti-diagonal element. The $(n, m)^{th}$ element of a Hankel matrix H, given there exists a sequence $s_1, s_2, ...,$ is s_{m+n-1}. Due to its utility in state-space realization or Markov model [128] [129], Hankel-matrix has widespread applications in signal processing, cryptography, quantum mechanics,

medical imaging etc. Particularly, Hankel-matrix is a useful tool for state identification of Linear Time Invariant (LTI) systems [130]. As mentioned before, the low-rank property of Hankel-matrix has been used in PMU missing data recovery [114] - [131]. Ref [132] and [133] investigated the Hankel-matrices' low-rank property for matrix completion and concluded that Hankel-matrix offers superior performance over low-rank approximation of general matrix in terms of numerical efficiency.

In our work, we go beyond the conventional Hankel-matrices' application in event detection and study the utility of Hankel-matrix, specifically its low-rank behavior, in identifying GPS-spoofing attack against PMUs. Moreover, we enhance the Hankel-matrix algorithm that is embedded on general full phasor measurement to a phase-angle based algorithm. The enhanced algorithm can identify the occurrence of attack against time-synchronization of PMU, which the general full phasor based algorithm fails to detect conclusively. Furthermore, we improve the performance of the enhanced Hankel-matrix algorithm by reducing computational time.

4.4 Hankel-Matrix Formulation

Hankel-matrix contains the time-series PMU measurements where the anti-diagonal elements are equal. Each row is one element right shifted from the previous row. For event detection models using Hankel-matrix, the matrix H is created with total W number of PMU measurements, spanning from the timestamp t_1 to the timestamp t_s. The timestamp sequence is $t_1, t_2, t_3, ..., t_w$. W is the Hankel-matrix window length. At each timestamp t_w, the Hankel-matrix is created with the measurement at t_w and previous $W-1$ measurements.

The first row of H is created by slicing the measurements over window W into a smaller portion of $W-k+1$, k being positive integer. In the second row, the first element is the second

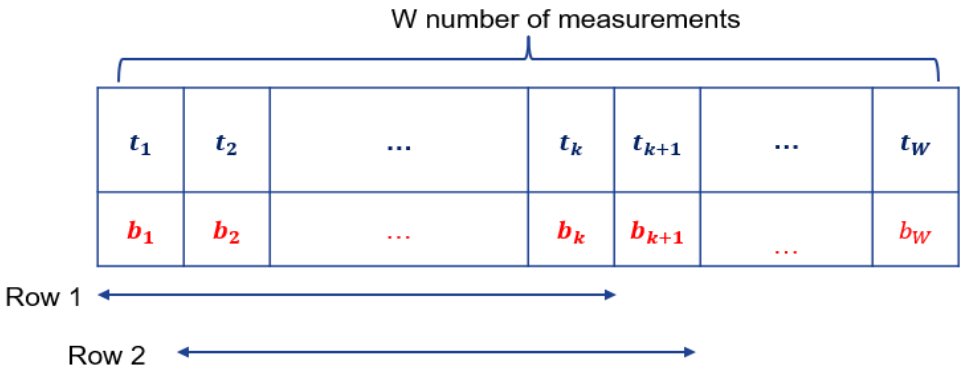

Figure 4.1: Formation of Hankel-matrix using PMU measurements

element of row 1, the second element is the third element of row 3, and so on. Elements of each column is the element from the previous row and next column. In other words, the $(m,n)^{th}$ element is equal to the $(m-1,n+1)^{th}$ element. For a PMU measurements $b_1, b_2, ...b_w$, correspond to the timestamps $t_1, t_2, ..., t_w$ respectively over window W, the Hankel matrix H can be formulated as eqn. 4.1. The elements b_i refers to phasor measurement (voltage or current) received from each PMU channel at timestamp t_i. The visualization for Hankel-matrix formulation with phasor measurements is illustrated in fig. 4.1.

$$H = \begin{bmatrix} y_1 & y_2 & \cdots & y_{W-k+1} \\ y_2 & y_3 & \cdots & y_{W-k+2} \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ y_k & y_{k+1} & \cdots & y_W \end{bmatrix} \tag{4.1}$$

The matrix H, which is a a $k \times (W-k+1)$ matrix, is also referred as a single PMU Hankel-matrix. The single PMU Hankel-matrix can be extended to multi-PMU Hankel-matrix, specifically for the applications where the spatial and temporal correlation among multiple

PMUs or among multiple channels of same PMUs are required. If there exists M number of PMUs which are located M neighboring buses, the M-PMU Hankel-matrix H_{mul} can be expressed as in eqn. 4.2.

In multi-PMU Hankel-matrix, the first row of Hankel-matrix is formed using the measurements over sliced window $W-k+1$ using the phasor measurements $y_{1,i}$ of the 1^{st} PMU. The measurements $y_{m,:}$ for rest of the neighboring $m-1$ PMUs, where $m \in M$ and M is the total number of neighboring PMUs, are put at each of the following $m-1$ in same sequence as the PMUs over same window of $W-k+1$. After measurements from all M neighboring PMUs over first window are stacked vertically, as displayed in fig. 4.2, measurements over the next window of length $W-k+1$ are put at each of the following M rows of multi-PMU Hankel-matrix H_{mul}.

$$H_{mul} = \begin{bmatrix} y_{1,1} & y_{1,2} & \cdots & y_{1,W-k+1} \\ y_{2,1} & y_{2,2} & \cdots & y_{2,W-k+1} \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ y_{M,1} & y_{M,2} & \cdots & y_{M,W-k+1} \\ y_{1,2} & y_{1,3} & \cdots & y_{1,W-k+2} \\ y_{2,2} & y_{2,3} & \cdots & y_{2,W-k+2} \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ y_{M,2} & y_{M,3} & \cdots & y_{M,W-k+2} \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ y_{1,k} & y_{1,k+1} & \cdots & y_{1,W} \\ y_{2,k} & y_{2,k+1} & \cdots & y_{2,W} \\ \cdots & \cdots & \cdots & \cdots \\ \cdots & \cdots & \cdots & \cdots \\ y_{M,k} & y_{M,k+1} & \cdots & y_{M,W} \end{bmatrix} \tag{4.2}$$

4.4.1 Low-rank approximation

Hankel-matrix demonstrates low-rank property. Lets assume the H matrix is to be approximated with rank-r, r is less than the full rank of matrix H. The first step is to perform Singular Value Decomposition (SVD) of the H as $U\Sigma V^*$. The H can be approximated as rank-r by taking the largest r singular values, i.e. approximating the remaining $rank(H) - r$

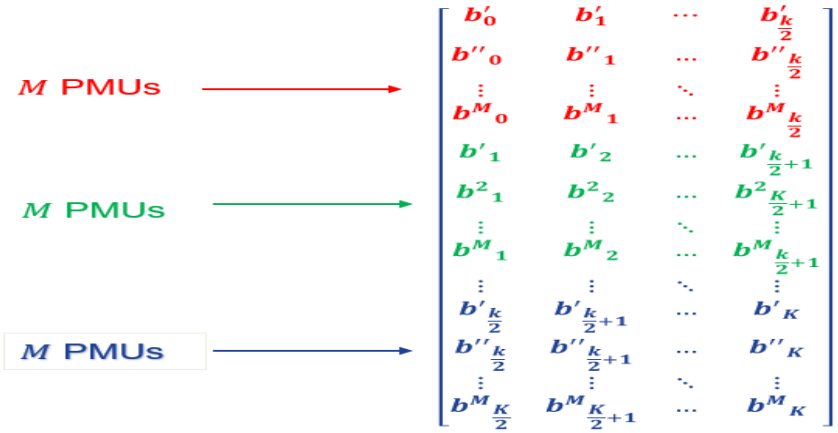

Figure 4.2: Formation of multi-PMU Hankel-matrix

singular values as 0. The approximated rank-r approximation of H is denoted by H^r, as expressed in eqn. 4.3.

$$H^r = U\Sigma^r V^* \tag{4.3}$$

The Σ^r is the singular value matrix taking largest r singular values. The normalized low-rank approximation (LRA) error is calculated with eqn. 4.4.

$$e^r(H) = \frac{||H^r - H||_F}{||H||_F} \times 100\% \tag{4.4}$$

,

At each timestamp, the algorithm creates the corresponding Hankel-matrix H, then calculates the smallest r for which the low-rank approximation error remains under threshold. Ref [117] determined this threshold to be in order of 10^{-2}.

For PMU measurements takedn of a power system in steady state and with small noise, the low-rank approximation error is less than a predetermined threshold. During power system

disturbance or cyberattack, there exist anomalies in the measurements b of H matrix at the corresponding timestamps. If the anomalies are significant enough, the low-rank approximation of corresponding H matrix result in approximation error larger than a predetermined threshold, indicating the occurrence of power system fault or cyberattack.

4.5 Enhancement of Hankel-matrix Algorithm

For event detection and correction of missing data, the Hankel-matrix algorithms in [114] and [117] take phasor voltage and current measurements from PMUs in rectangular format. Full phasor data in rectangular format provide accurate results for conventional event detection or FDIA. However, for GPS-spoofing attack, the full phasor measurements are not sufficient enough to correctly differentiate between an attack on the time synchronization of PMUs or a conventional FDIA/ physical fault in the system. In the following section, we discuss about the feasibility of enhanced Hankel-matrix based algorithm with only the phase angle measurements that can identify the GPS-spoofing attack conclusively.

4.5.1 Hankel-matrix Algorithm with only Phase Angle Data

During a physical fault in the system, such as line-to-ground (LG) or line-to-line (LL) fault, voltage and current phasors can exhibit sharp change in the data pattern. Similar behavior can be observed for FDIA, when the attacker targets a specific PMU channel and manipulates the PMU measurement transmitted to a PDC. The change in data due to physical fault or FDIA can be illustrated as follows:

$$V = V_m\langle\theta = V_m cos(\omega t + \theta) + jV_m sin(\omega t + \theta) \tag{4.5}$$

For a physical faults, assume the voltage magnitude V_m changes to $V_m + \Delta V$ and the voltage angle changes to $\theta + \Delta\theta$. A FDI attacker, targeting the PMU voltage measurement channel, can inject malicious measurements with similar ΔV and $\Delta\theta$ changes in voltage magnitude and angle measurements, respectively. For a GPS-spoofing attack, the attacker changes the GPS 1 PPS signal and cause deviation in time-reference for PMUs. The deviation in horizontal time-reference affects the PMU phase angle measurements most severely, and only a small spike in magnitude measurement. Subsequently, the $\Delta\theta$ is more significant that ΔV change, implying there are different levels of changes in phase angle and magnitude measurements. However, as the full phasor rectangular form of eqn. 4.5 incorporates both voltage magnitude and phase angle, the combined affect due to GPS-spoofing attack will cause a change significant enough to be detected by general Hankel-matrix based algorithms that uses full phasor measurements.

$$\begin{aligned} V' &= (V_m + \Delta V)\langle(\theta + \Delta\theta) \\ &= (V_m + \Delta V)cos(\omega t + \theta + \Delta\theta) + jV_m sin(\omega t + \theta + \Delta\theta) \end{aligned} \tag{4.6}$$

From eqn. 4.6 it is evident that, since all of mentioned three cases: physical faults, FDIA, and GPS-spoofing attack create changes in $\Delta\theta$ and ΔV to different degrees, the voltage phasor suffer from sharp change at the moment of fault/ attack. This change can be detected using general Hankel-matrix based algorithms in [114]-[117]. However, the GPS-spoofing attack is different from FDIA since in GPS-spoofing attack in done at the GPS signal received by

PMU, in contrast with a communication network breach that is done during FDIA. This contradictory behavior require different restoration techniques. The full rectangular phasor form in eqn. 4.6, despite correctly detecting data anomaly, fails to indicate whether the source of data anomaly is due to FDIA or GPS-spoofing attack.

In this work, we aim to enhance general full phasor Hankel-matrix algorithm used in ref [114] and [117] to detect GPS-spoofing attack conclusively. The key idea is, instead of using full phasor measurements, the detection algorithm based on the phase angle measurement alone can indicate GPS-spoofing attack occurrence and can differentiate GSA from FDIA. Hankel-matrix algorithm using the unwrapped phase angle demonstrates contrasting behavior during GPS-spoofing attack and FDIA.

The attacker injects falsified measurements into the communication network and changes the data received by SO. Lets assume at the timestamp t, an FDI attacker initiates the attack by targeting a PMU phase angle measurements, and modifies the phase angle measurements from $\theta(t)$ to $\theta'(t)$ by adding an attack value a(t) to the actual phase angle $\theta(t)$. If the attacker initiates consecutive attack, the following measurement $\theta(t+1)$ also change to $\theta'(t+1)$ by being added up by next attack value $a(t+1)$. The new phase angle values will be as follows:

$$\begin{aligned} \theta'(t) &= \theta(t) + a(t) \\ \theta'(t+1) &= \theta(t+1) + a(t+1) \end{aligned} \tag{4.7}$$

Adding an attack vector to the phase angle data, as described in eqn 4.7, causes an increase or a decrease in the phase angle measurement. However, the transition point between $+/-\pi$ to $-/+\pi$ doesn't change with respect to neighboring PMUs. To make the attack stealthy, the attacker tries to make the $a(t)$ small enough as to be undetected by conventional residual based state estimators. As a result, for FDIA, the phase angle data will not demonstrate

any sustain distortion in the graph for a single or few consecutive instances of the attack.

During GPS-spoofing attack (GSA), the spoofing of GPS 1 PPS signal changes the time-reference. The change in time-reference and corresponding shift in timestamps causes deviation in phase angle, which exhibit similar jump in the measurement as it does for FDIA. Therefore, looking into raw phase angle measurements is not enough to differentiate GSA from FDIA and to identify GSA conclusively. However, unwrapped phase angle, which linearizes the raw phase angle to avoid the wrapping around $+/-\pi$ and $-/+\pi$, show a contrasting behavior during GSA. As for GSA, the transition point between $+/-\pi$ to $-/+\pi$, that follows the attack instances, shifts. This transition no longer occurs at the same timestamp as it would be under no-attack scenario. If we unwrap the raw phase angle, this shifts in $+/-\pi$ to $-/+\pi$ transition result in sustained distortion in the unwrap phase angle graph. For a new phase angle measurement after GSA of θ'', it can be expressed as:

$$\theta''(t) = \theta(t + \Delta T) \tag{4.8}$$

ΔT is the timestamp shift caused by the shift in GSA 1 PPS. At each attack moment, due to the time-reference change, phase angle measurements remained changed over next 1 second (or untill next GPS PPS signal is received). Each $+/-\pi$ transition point over the next 1 sec. period will also shifted horizontally, creating a sustained distortion in unwrapped phase angle measurements [92]. Therefore, unwrapped phase angle exhibits contradictory behavior for GSA and FDIA.

If we perform the low-rank approximation analysis using the Hankel matrix in eqn. 4.1 using unwrapped phase angle measurements instead of full phasor in rectangular form, we can correctly identify the GSA and differentiate it from FDIA. Whereas the general full

phasor Hankel-matrix in [114] [117] can detect the event due to cyberattack or physical fault in the system, the unwrapped phase angle Hankel-matrix algorithm are also needed to be implemented alongside to correctly distinguish the GSA from FDIA, and to exclude the possibility of implementing the wrong restoration scheme.

4.5.2 Computational Efficiency of Hankel-matrix Algorithm

As discussed in the previous subsection, unwrapped phase angle can identify GSA and distinguish GSA from FDIA. However, the phase angle measurement provided by PMUs are not by default unwrapped. Most commercial PMUs sends phase angle measurements that are periodically wrapped around 180^o, as displayed in fig. 1.3. To perform our proposed enhanced Hankel-matrix algorithm for the detection of GSA, the raw phase angle measurements are required to be unwrapped at each iteration of event detection. This additional calculation significantly increases computational burden.

The phase angle difference between the target PMU and a reference PMUs have similar characteristics as unwrapped phase angle for the case of GSA. If the phase angle difference between PMU A, and a reference PMU B are observed, the time reference shift in PMU A will be reflected by a sudden deviation in the angle difference.

The effect of GSA on the phase angle difference is better visualized in fig. 4.3 and 4.4. The phase angle difference between PMU A and PMU B does not change significantly under normal condition. However, if a GSA is initiated at the time of sample 200, corresponding time-reference is shift which is reflected by sudden change in phase angle difference between PMU A and PMU B, as illustrated in fig. 4.4.

Similar to unwrapped phase angle measurements, just one instance of GSA causes sustained deviation in phase angle difference $\Delta\theta$ measurement too. It implies that for GSA identifica-

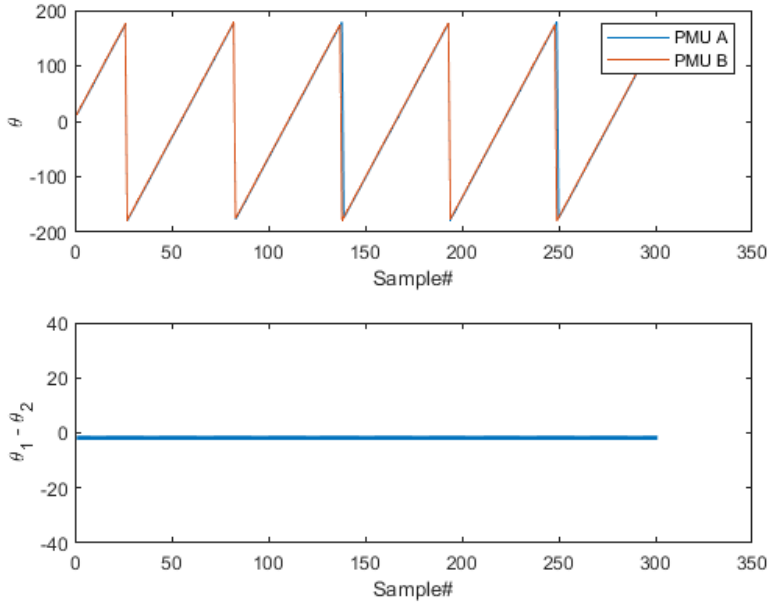

Figure 4.3: Phase angle difference under normal condition

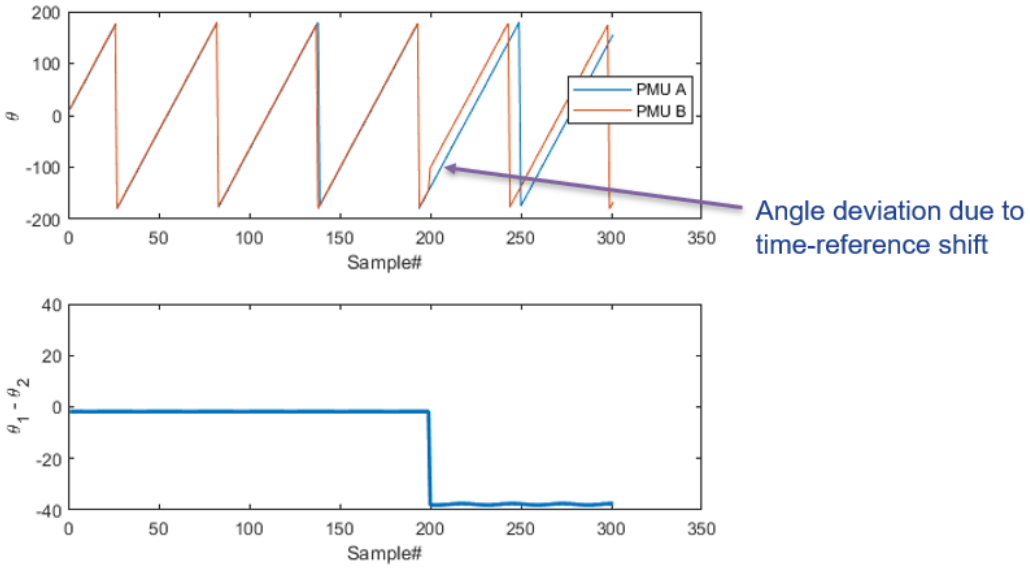

Figure 4.4: Phase angle difference under GPS-spoofing attack

tion, using $\Delta\theta$ instead of unwrapped phase angle measurements in enhanced Hankel-matrix algorithm will give similar accuracy. However, using $\Delta\theta$ measurements instead of unwrapped phase angle has one additional advantage: it requires less computational time to execute.

Using $\Delta\theta$ instead of unwrapped phase angle reduces the computational burden of the algorithm. We can also further increase the numerical efficiency by using a predetermined low rank r instead of calculating the low-rank at every iteration of event detection. In section 4.4.1, we discussed that ref [114] and [117] approximate the Hankel-matrix to the low-rank r during every iteration. In each iteration, the smallest r that gives the low-rank approximation error within threshold is used to detect event. Running the low-rank approximation calculation at every iteration to find most optimum r requires a significant computational time.

The general assumption is, for steady state measurements with a consistent range of noise, the r value after performing low-rank approximation at each iteration remains within a certain range. If we choose steady state measurements under normal condition over a certain period of time, we can run the low-rank approximation calculation at each iteration and obtain a range of r values. After having the range of r values and calculating their mean for a specific PMU phase angle measurements over a chosen time period, we can use this mean r value to detect event and GPS-spoofing attack for future measurements received from the same PMU under same configuration. The Hankel-matrix based event detection algorithm in ref [117] has two segments that are performed at each iteration: first calculating the low-rank r and then estimating the next measurements using Hankel-matrix of previous measurements. If, after the initial chosen time period, we can omit the first part of determining low-rank r by using predetermined low-rank r, we can reduce the computational time as the algorithm only perform new measurement estimation portion at each iteration.

In short, we can reduce the computational time for using phase angle only Hankel-matrix

by:

- using phase angle difference $\Delta\theta$ instead of unwrapping phase angle at each iteration;
- using a predetermined mean value of low-rank r instead of running r value calculation at each iteration.

The proposed numerical efficiency enhancement by reducing computation time assume the measurements received from PMU are already in polar format. If the measurements are received are in Cartesian format, we need to perform addition calculation to separate phase angle measurements to use in enhanced Hankel-matrix algorithm.

4.6 Sequential Real-time Event Classification and Identification of GPS-Spoofing Attack

4.6.1 Event Detection

As mentioned before, most common method to detect event injected by attacker is the state estimation model. The system operator estimates the state variable using AC and DC power flow equations, and flags event if the deviation between measurements and estimations exceeds threshold. The measurements are estimated with Weighted Least Squares (WLS) [98] [112] method. event is detection when the ℓ_2-norm of the residual between actual measurement and estimated measurement, also known as estimation residual, is larger than a predetermined threshold τ^h.

A well-designed FDIA can be stealthy enough to bypass WLS based event detection method [134]. However, more robust techniques such as Kalman Filtering (KF) [135] can be an effec-

tive tool to detect event caused by electrical events and FDIA. The KF estimator generates better estimations of state variables than conventional weighted least square based method [135]. At each time instance, KF estimates the state variable and measurements using measurements from previous timestamps. Furthermore, deviation based KF approach provides better result compared to the conventional KF estimator, particularly during FDIA since the estimation accuracy is impacted by malicious data injected to the measurement stream [136].

One advantage of the deviation based KF method (DKF) is that it incorporates the time-series variation of measurements. A similar advantage is available in the Hankel-matrix based detection method [115], which utilizes both temporal and spatial relation among the measurements from single or multiple PMU channels. The proposed event identification method in this work relies on both spatial and temporal relation of time-series PMU measurements from single and multiple channels. This approach has an edge over DKF method, as even a small deviation in measurements can be identified by comparing the spatial and temporal relations of measurements with neighboring PMU channels. Furthermore, applying Hankel-matrix based method in the first step of event detection reduces the time required to execute the proposed sequential algorithm of event classification in the second and third steps, providing the SO with a faster restoration and mitigation opportunity.

The first step of the Hankel-matrix based event detection method is to exploit the low rank approximation (LRA) of the Hankel-matrix H as illustrated in eqn. 4.1, 4.3 and 4.4.

The low rank approximated equivalent of H is $H^r = U\Sigma^r V^*$. Low rank approximated Hankel-matrix is also have same $k \times W - k + 1$ dimension as original Hankel-matrix $hank(Y_{mul})$.

Each element $\hat{y_{i,j}}$, where i is the index of individual PMU, and $j = 1, 2, ..., W$ comes from the low rank approximated H^r. Using the WLS method, the state variable d is estimated

using the following relation [137]:

$$\hat{d} = (\hat{U^r}^T * \hat{U^r})^{-1} \hat{U^r} * H^r \tag{4.9}$$

where $\hat{U^r}$ is the first r dominant left singular matrix from U. For each PMU i, where $i = 1, 2, ..., M$, the data at timestamp t_{s+1} is considered to be accep Table (not event) if the estimation residual $||y_{i,\hat{t_{s+1}}} - \Gamma_i||_2 \leq \tau^h$. The Γ is defined as $M \times 1$ matrix calculated from $\hat{U^r}\hat{d}$. Here τ^h refers to a predetermined threshold for event detection.

On the contrary, when the estimation residual exceeds the τ^h, it indicates the existence of estimation error at the timestamp t_{s+1}. However, a single occurrence such estimation error doesn't indicate physical event or cyberattack, since measurement noise or data transmission error might provide a discrete outlier in the measurement stream. To ensure the occurrence of event without any false positive case, we consider it as event only if there exists more than three consecutive estimation error over three consecutive moving time window with length T.

The main contribution of this section is the detection of event using low rank approximation of Hankel-matrix. The proposed method is scalable, since it only calculates estimation residuals separately for each individual PMU channel, therefore the size of the power grid does not impact the accuracy of detection. Moreover, the proposed model utilizes both spatial and temporal relationship among the PMU channels, thereby providing the SO with the ability to detect relatively smaller changes in measurements during a physical event or a cyberattack. This attribute gives the proposed model an edge over DKF.

4.6.2 Cyberattack vs Physical Event Classification

As the fault mitigation and system restoration techniques are different for cyberattack and physical events, differentiating these two types of faulty conditions is paramount for the system operator. The proposed Hankel matrix based model for BDD [115] can be extended to distinguish cyberattack and physical events. During physical event, there must exist a time-series correlation among the neighboring PMUs that are physically connected or topologically nearby. On the other hand, since a cyberattack is targeted to particular PMUs, there is no or little time-series correlation among the topologically neighbor PMUs. These differences can be exploited to identify the event type.

Generally under normal condition (without any physical event or cyberattack), random column permutation of Hankel-matrix would cause an increase in the low rank approximation error since the temporal relation among the elements of Hankel matrix is destroyed after column permutation. Since during physical event there exist temporal correlation among the data from neighboring PMU channels, a random column permutation will result in increased low rank approximation error. However, as for cyberattack, there is no or little temporal correlation among the data from neighboring PMU channels, therefore the low rank approximation error is already higher for cyberattack. A random column permutation will not change the low rank approximation error significantly. In short, observing the low rank approximation error before and after random column permutation will help the system server determine the cause of event in the measurements. Mathematically, the proposed cyberattack vs event identification model can be formulated as algorithm described in Algorithm 1.

The proposed algorithm of differentiating physical event from cyberattack has a limitation against PMU calibration error, since despite being a physical event in nature, it lacks the proposed models' assumptions of the existence temporal relation among neighboring PMUs.

However, there are real-time correction method of such events, that can provide PMU measurements with no or very little calibration error to the PDCs [138]. As a result of this pre-processing, the sudden change in measurements during cyberattack/ LG fault data will not be affected by such calibration error.

Algorithm 1 Identifying event Type

Initialization: For a particular PMU channel I that is identified to contain event at timestamp t_s as in section II, O is the number of PMU channels that are physically connected to I. Receive data from all O PMU channels over data-window starting from timestamp t_{s+1} to t_{s+W+1}; W being a positive integer which is referred as data-window length. η is the threshold to identify event type; k is the Hankel matrix parameter representing number of rows.
Step 1: Create a $Ok \times W - k + 1$ Hankel-matrix H_A, similar to eqn 4.2, with voltage phasor measurements from O PMUs over data-window length of W;
Step 2: Calculate the low rank approximation error e^{rz} with varying rank r ($r \leq rank(H_A)$);
Step 3: Do a random column permutation on the Hankel matrix H_A and create a new matrix $\bar{H_A}$;
Step 4: Calculate the low rank approximation error e^{rrz} with varying rank r ($r \leq rank(\bar{H_A})$);
Step 5: If $e^{rrz} > \eta$ for r = 1, it is an electrical event. Go to step 1 with the next data window, starting from timestamp t_{s+2} to t_{s+W+2} data sample;
Step 6: If $e^{rrz} < \eta$ for r = 1, continue from step 2 with moving data-window until the data-window starting from timestamps $t_{s+W/3}$ to $t_{s+W/3+W}$ is covered. If $e^{rrz} > \eta e^{rz}$ is satisfied for any of the previous data-window, it is physical event; **Step 6**: Else, it is cyberattack.

4.6.3 Differentiating FDIA and GSA

After the cause of event is identified as *cyberattack*, the SO tries to restore the breached communication network or use alternate communication medium. However, a GPS-spoofing attack doesn't require the attackers to breach the network communication between measurement devices to PDCs and/or to control center [102] [103]. This type of attack is done by spoofing the GPS signal. The GPS receiver uses the spoofed GPS signal instead of the actual signal. As a result, GPS-spoofing attack needs to be mitigated in a different way than FDIA.

Previous works focused on the detection of GPS-spoofing attacks (GSA) treated this type of attack similar to FDIA, with a difference in measurement matrix $\mathbf{z}$ as in eqn 5.15. For FDIA, the affected matrix can be either voltage or current magnitude or phase angles, however for GSA the affected measurement matrix is generally voltage/ current phase angle [99] [120] [121] since the impact of shift in time-reference due to spoofing of GPS 1 PPS signal is reflected mostly in the phase angle portion of measurements. The phase angle measurements in Algorithm 1 flags the event type as cyberattack for GSA. Similarly, if the FDIA targets phase angle measurements, executing Algorithm 1 with voltage/current phase angle measurements will also classify the event as cyberattack. It is difficult for the SO to determine whether the event is caused by spoofing GPS 1 PPS signal (GSA) or by corrupting the phase angle measurements directly (FDIA).

Generally, Algorithm 1 with the raw phase angle measurements cannot indicate whether it is GSA or FDIA, due to the similar behavior in raw phase angle data during GSA and FDIA. However, our enhanced Hankel-matrix algorithm as described in section 4.3, that uses unwrapped angle measurements or phase angle difference between PMU i (which already demonstrated the data anomaly during first stage of sequential method) and a reference PMU R, demonstrates contrasting behavior for GSA and FDIA.

4.6.4 Proposed Real-time Sequential Event Classification

The real-time sequential event classification relies on the successful implementations of the algorithms described in section 4.6.1 to 4.6.3. At first the algorithm runs Hankel-matrix based model mentioned in section 4.6.1 to detect the event. If the occurrence of event is detected, the event type is identified using multi-PMU Hankel-matrix described in section 4.6.2. Once the cause of event is identified as cyberattack, we apply the single PMU Hankel-

matrix algorithm in section 4.6.3 on the unwrapped phase angle data. The detailed process is described in algorithm in Algorithm 2.

Algorithm 2 Differentiating GSA from FDIA

Initialization: The number of PMU channels M, t_s is the current timestamp, T is the time period from 1^{st} timestamp to timestamp t_s , k is the Hankel matrix parameters, O is the number of PMU channels physically connected to the affected PMU channels, W is the data-window length over total T timestamps;
Step 1: Create a $Mk \times W - k + 1$ Hankel-matrix H, similar to eqn 4.2, with measurement from M PMUs over data-window length of W, the data window starts from the 1^st timestamp and ends at the timestamp T;
Step 2: For every PMU i, calculate the estimation residual for the measurement at timestamp t_{s+1} using $||y_{i,t_{s+1}} - \Gamma_i||_2$, ;
Step 3: If the estimation residual at timestamp t_{s+1} doesnt exceed threshold τ^h, measurement at t_{s+1} is not a event, proceed with the next time window starting from 2^{nd} timestamp and ending at timestamp t_{s+1} and perform BDD method from step 1;
Step 4: If the residual at timestamp t_{s+1} exceeds threshold τ^h, measurement at t_{s+1} is a event, proceed to step 5;
Step 5: Apply algorithm 1 to identify the event type;
Step 6: If identified as cyberattack, proceed to step 7;
Step 7: Unwrap the angular data and create Hankel-matrix H_u similar to step 1, using measrurements with timestamps starting from 2 to the timestamp t_{s+1} ;
Step 8: Calculate the rank-1 approximation error e^{rc};
Step 9: If the gradient of rank-1 approximation error is positive for more than three consecutive timestamp moving time window, then it is a GPS-spoofing attack;
Step 10: Else, it is an FDIA

4.7 Contributions

The major contributions of this chapter are as follows:

- we develop an enhanced Hankel-matrix algorithm to identify GPS-spoofing attack and differentiate it from FDIA. Instead of using PMU full phasor measurements or raw phase angle measurements as in general Hankel-matrix algorithms developed previ-

ously, our enhanced Hankel-matrix algorithm uses unwrapped phase angle measurement and/ or phase angle difference;

- after enhancing the Hankel-matrix based model to correctly identify GSA, we propose and implement a sequential real-time event detection and classification technique. The proposed model identifies the occurrence of event, as well as classifies the event among physical event, FDIA and GSA, in a real-time sequential manner;

- the proposed sequential classification model exploits the previously developed low rank approximation of Hankel-matrix based event detection and correction models by extending its application in differentiating event types, thereby providing the knowledge of event type to the SO to ensure proper system restoration and resiliency;

- the proposed technique utilizes Hankel-matrix based algorithm that is scalable to larger and more complex power grid, with combined detection and classification time being less than 1 sec., providing fast response opportunity for SO.

Chapter 5

Results

5.1 Details of Publications

Co-authors: Virgilio Centeno

Reference [64]: I. Khan, and V. Centeno, "Undetectable gps-spoofing attack on time series phasor measurement unit data". arXiv: 2206.12440 [eess.SY], Sep 2023. Retrieved from: https://arxiv.org/abs/2206.12440.

Co-authors: Virgilio Centeno

Reference [92]: © 2022 IEEE. Reprinted, with permission, from I. Khan and V. Centeno, "Detecting GPS-spoofing Attack on PMU Data with Phase Angle Unwrapping Technique and Low-Rank Approximation of Hankel Matrix," in 2022 IEEE Power and Energy Society General Meeting (PESGM), July 2022.

Co-authors: Virgilio Centeno

Reference [93]: © 2023 IEEE. Reprinted, with permission, from I. Khan and V. Centeno, "Realtime Detection of PMU Bad Data and Sequential Bad Data Classifications in Cyber-Physical Testbed," in IEEE Access, July 2023.

5.2 Introduction

In this chapter, we test the feasibility of our enhanced Hankel-matrix method from chapter 4 against the stealthy GPS-spoofing attack models proposed in chapter 3. In addition, we also analyze the effectiveness of real-time sequential event classification algorithm developed in chapter 4. In this chapter we present the results obtained when:

- we test our enhanced phase angle Hankel-matrix algorithm for the conclusive detection of GPS-spoofing attacks, using PMU-PDC testbed described in chapter 2;

- we verify the numerical efficiency of enhanced Hankel-matrix algorithm using real-world PMU measurements;

- we implement the real-time sequential event classification algorithm using the VT PMU-PDC testbed developed in chapter 2, and analyze the utility of developed testbed using conventional GPS-spoofing attacks;

- we test the effectiveness of the enhanced phase angle Hankel-matrix algorithm for the detection of proposed stealthy incremental GPS-spoofing attack model described in chapter 3. In addition, we test the undetectability of stealthy incremental GSA model against conventional event detection models;

- we apply the enhanced Hankel-matrix model to detect GPS-spoofing driven FO attack described in chapter 3. Additionally, we propose a power flow measurement based GPS-spoofing driven FO detection model and verify its effectiveness using simulated measurements.

5.3 Numerical Results for Enhanced Hankel-matrix Algorithm

In this section, we use simulated and real pmu data to test the proposed enhanced phase angle measurements Hankel-matrix for GPS-spoofing detection, and the numerical efficiency of the enhancements. At first, we observe the feasibility of proposed phase angle Hankel-matrix for detecting GPS-spoofing attack and differentiating it from FDIA. After that, we analyze the accuracy of the enhanced model using both $\Delta\theta$ values and unwrapped phase angle values under different noise level and different degree of time-reference shift. Thirdly, we demonstrate the results of numerical efficiency enhancements using both real-world data and simulation data.

5.3.1 Result with IEEE 13 Bus System

This chapter presents the results obtained using the IEEE 13 bus system to test the Hankel-matrix method. We utilize SIMULINK to run the power system simulation over 30 second, and extracted the voltage and current measurements. We applied the synchrophasor algorithm in eqn. 1.4 to the voltage and current measurements. Assuming attacker target the PMU of Bus 680 as illustrated in fig. 5.1. For GPS-spoofing attack, we consider time-reference deviation of $0.3msec.$ approximately at $5.0sec.$ of the simulation. For FDIA, we performed a separate simulation under same condition and added an angle deviation of 1^o at the same time of $5.0sec.$. We have added a white noise with standard deviation of 1 and mean 0 to the signal to reflect measurement and system noises.

We calculate low-rank approximation error for full-phasor Hankel-matrix, where the phasors are in rectangular form as in [117] and [114]. The results from fig. 5.2 and 5.3 indicate that

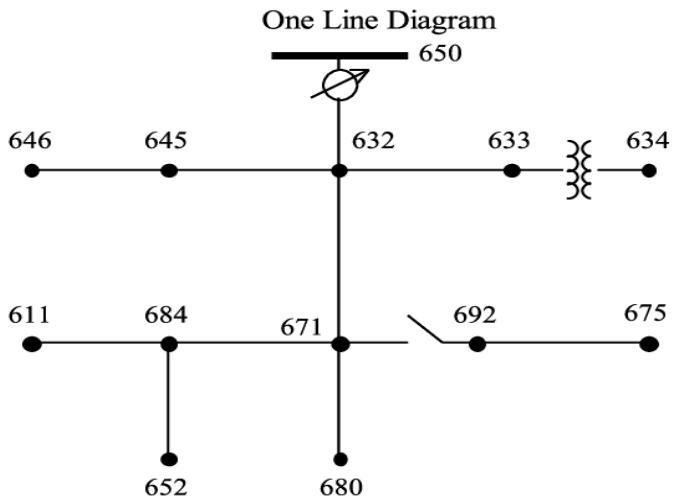

Figure 5.1: IEEE 13 node test feeder

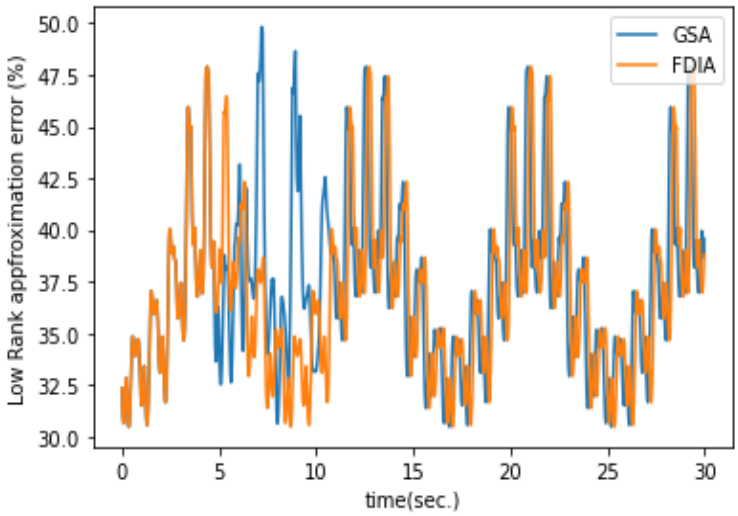

Figure 5.2: Low-rank approximation error for imaginary part of phasor measurements

even though the low-rank approximation error changes for GPS-spoofing attack, it does not show conclusive evidence regarding the type of attack. Similarly, results from fig. 5.4 do not provide conclusive evidence for GSA since it is not sufficient to different GSA from FDIA from the low-rank approximation error result.

However, the unwrapped phase angle Hankel-matrix shows significant difference in the be-

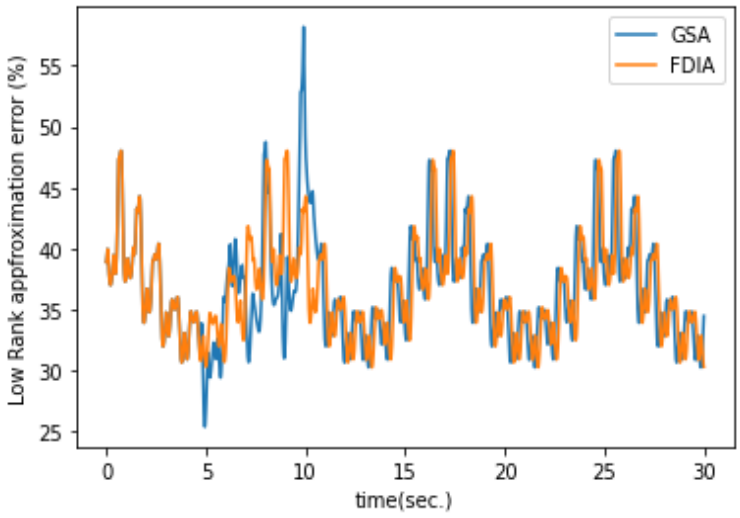

Figure 5.3: Low-rank approximation error for real part of phasor measurements

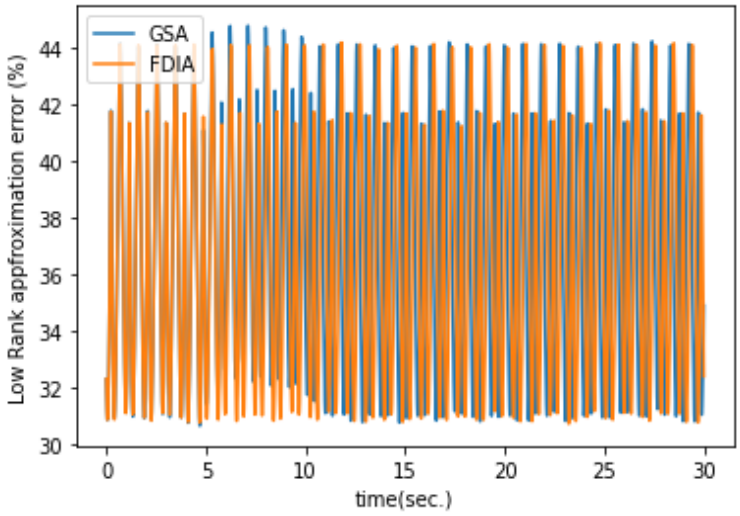

Figure 5.4: Low-rank approximation error for raw phase angle Hankel-matrix

havior of GSA and FDIA. During GSA, the unwrapped phase angle measurements suffer from sustained change, resulting in much higher change in the low-rank approximation error for GSA than it is for FDIA, as discussed in previous section. As illustrated in fig. 5.5, the low-rank approximation error changes significantly at the moment when the change in time-reference is initiated by the GPS-spoofing attacker.

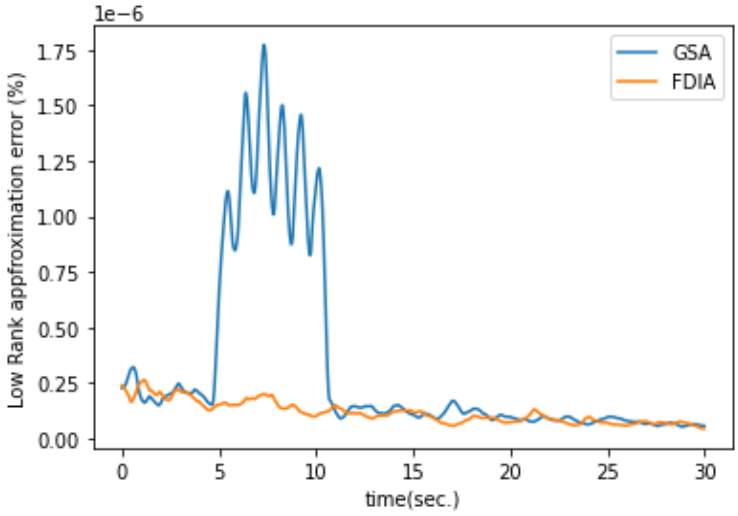

Figure 5.5: Low-rank approximation error for unwrapped phase angle Hankel-matrix

The numerical efficiency can be increased by using $\Delta\theta$ instead of unwrapped phase angle in the Hankel-matrix. Also, for small time-reference deviations, the *jump* in unwrapped phase angle during the time-reference change is harder to detect for high noisy condition. On the other hand, the $\Delta\theta$ is less prone to noisy condition as we create the Hankel-matrix by subtracting phase angle of target PMU from that of a reference PMU. Common portions of the random white noises cancel each other to a certain extent. We have analyzed the accuracy for detecting GSA with unwrapped phase angle Hankel-matrix and with the $\Delta\theta$ Hankel-matrix. We have considered phase angle measurements from bus 692 as reference PMU measurements and fed the $\Delta\theta$ between phase angle of bus 680 and bus 692 into Hankel-matrix. The Hankel-matrix width W is varied from 50 to 150, with an interval of 5; and the noise level is varied with white Gaussian noise of standard deviations 1 to 5. The accuracy and time required to perform each iteration is depicted in table 5.1.

The result demonstrate the perfect accuracy as well as smaller computational time for Hankel-matrix with phase angle difference as opposed for Hankel-matrix with unwrapped phase angle.

Table 5.1: Accuracy and computation time for GPS-spoofing detection

Hankel-matrix input data	Accuracy (%)	Mean Computation time (sec.)
Unwrapped Phase Angle Measurements	96	3.2×10^{-5}
$\Delta\theta$ between bus 680 and reference PMU	100	1.6×10^{-6}

5.3.2 Result with real-world PMU data

We use real-world PMU data from the Western Interconnection transmission grid. In the dataset obtained from the Pacific Northwest National Laboratory (PNNL), the proprietary information such as PMU locations, event locations, and the system topology are unavailable. PNNL provided measurements from 43 PMUs of 3 different interconnects for the year 2016 and 2017. The sampling rates of PMUs are either 30 or 60 fps. In each data file, the measurements from a particular interconnect includes:

- UTC timestamps
- voltage magnitude: three phases and positive sequence
- voltage angle: three phases and positive sequence
- current magnitude: three phases and positive sequence
- current angle: three phases and positive sequence
- frequency, and
- Rate of Change of frequencey (ROCOF)

To test our proposed enhanced Hankel-matrix model, we choose a portion of dataset that is relatively steady state with no events reported for that period. We select PMU measurements

from the anonymous PMU ID: C132 of interconnect C. The timestamps of the portion of data used start from UTC $2017-08-03\ 02:52:00.000$ and end at UTC $2017-08-03\ 02:58:00.000$.

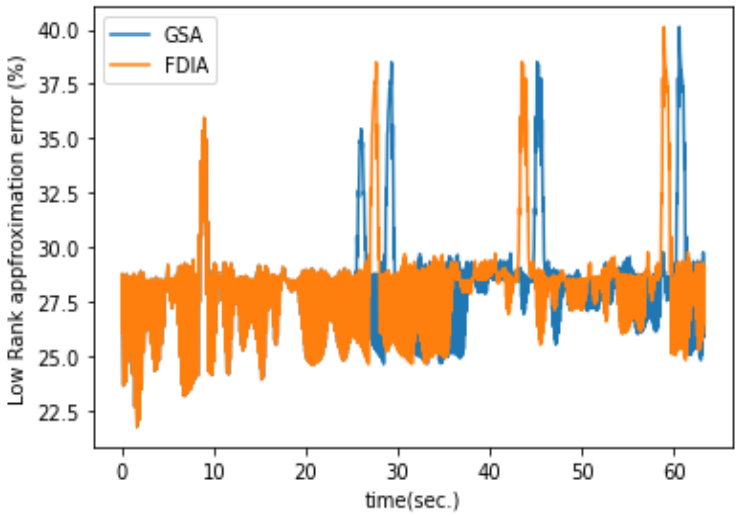

Figure 5.6: Low-rank approximation error for real-world PMU data: real part of full phasor Hankel-matrix

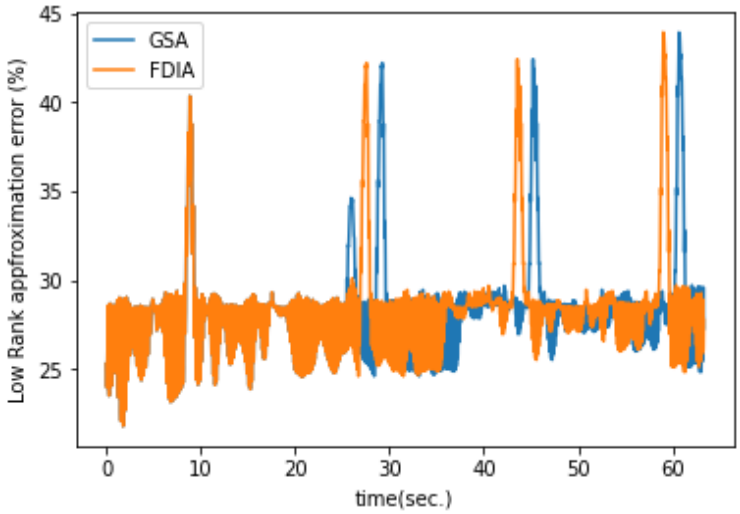

Figure 5.7: Low-rank approximation error for real-world PMU data: imaginary part of full phasor Hankel-matrix

Fig. 5.6 and 5.7 show the inability of full phasor Hankel-matrix in differentiating GSA

from FDIA. The original data provided by PNNL does not contain any cyberattack effect. We have modified the measurement to mimic both GSA and FDIA in separate analysis. For GSA, we time-shift the phase angle measurements starting from the hypothetical GSA attack instances. The FDIA is emulated by adding a deviation in phase angle measurement at the attack instances. We perform both general and enhanced Hankel-matrix algorithm, under GSA and FDIA conditions separately. The low-rank approximation error results do not provide any significant different behavior for GSA and FDIA. We can made similar conclusion for the results obtained from raw phase angle Hankel-matrix low-rank approximation error as displayed in fig. 5.8

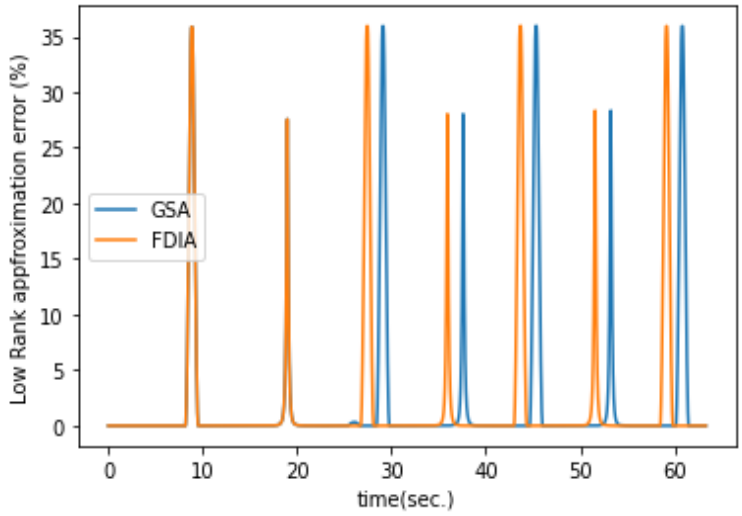

Figure 5.8: Low-rank approximation error for real-world PMU data: raw phase angle Hankel-matrix

The high noisy measurements impact the accuracy for unwrapped phase angle Hankel-matrix based analysis, as depicted in table 5.1. Fig. 5.9 demonstrates the failure of unwrapped phase angle Hankel-matrix to detect GSA conclusively. Therefore, Hankel-matrix with $\Delta\theta$ phase angle difference is the better choice for GSA identification. We use anonymous PMU ID C102 as reference PMU for calculating $\Delta\theta$ of PMU IC C132. The low-rank approximation error results show the effectiveness of phase angle difference Hankel-matrix algorithm for

identifying GSA and differentiating it from FDIA, as demonstrated in fig. 5.10.

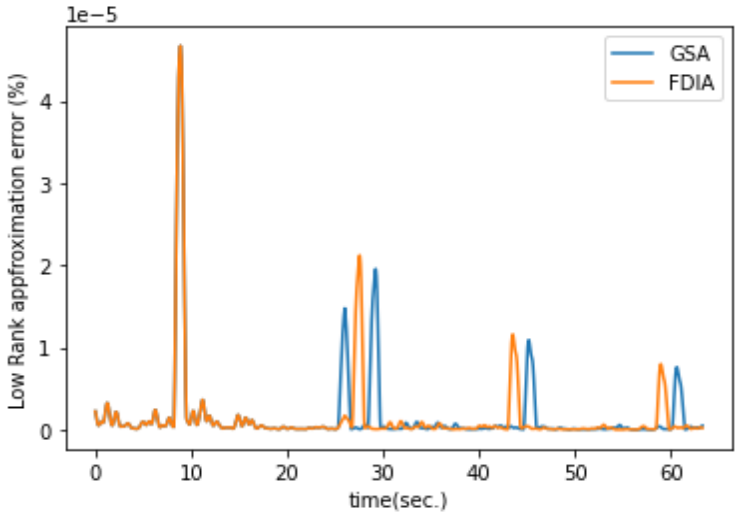

Figure 5.9: Low-rank approximation error for real-world PMU data: unwrapped phase angle Hankel-matrix

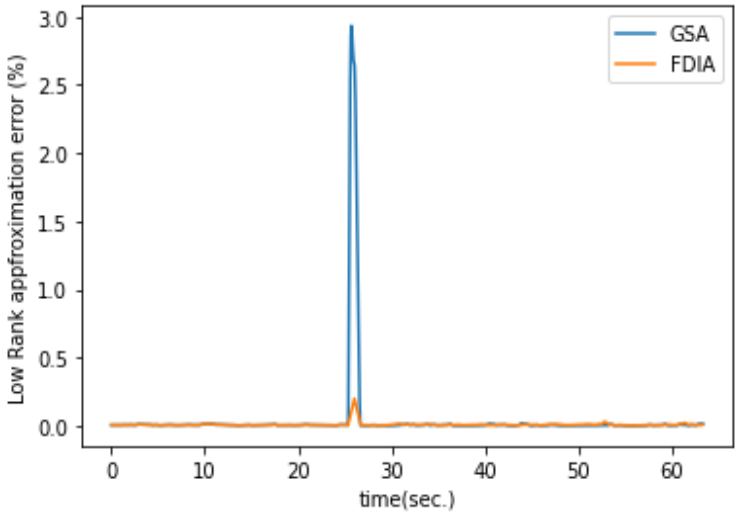

Figure 5.10: Low-rank approximation error for real-world PMU data: phase angle difference Hankel-matrix

Results show the superior performance of enhanced Hankel-matrix algorithm over general Hankel-matrix algorithm in [114] and [117] in detecting GPS-spoofing attack. For very high noisy data, such as real-world PMU data, we get the best result if the Hankel-matrix is

created using phase angle difference of target PMU from a reference trusted PMU.

5.3.3 Computational efficiency enhancement results

As discussed in section 4.5.2, the computational time can be further reduced if we use predetermined low-rank instead of running the low-rank approximation at every iteration of Hankel-matrix algorithm. We simulated Hankel-matrix based model for a steady state portion of measurements received from PNNL. The low-rank needs to be predetermined using PMU measurements under steady-state conditions over a specific time period. Therefore it is critical to identify the low-rank variation for different sets of measurements under different condition such as: time, interconnect, phasor type etc. For each of three interconnects (A, B, and C), we chose 1 hour measurements from three different seasons (May, August, December). We perform low-rank calculation from eqn. 4.3 and 4.4 with dataset from each set of measurements, and run the calculation for phase angle difference, magnitude, and raw phase angle separately. The Hankel-matrix data-window length is $W = 80$, making the full-rank of the Hankel-matrix 40.

Table 5.2: Low-rank for different sets of real-wrold PMU measurements: Interconnect A

Measurement type	Low-rank Month: May	Low-rank Month: August	Low-rank Month: December
Phase angle difference	32-39	34-39	30-38
Magnitude	37-39	36-39	37-38
Raw phase angle	12-40	15-40	14 - 40

Table 5.2-5.4 shows that the phase angle difference Hankel-matrices' low-rank varies between 22 and 35 for interconnect B and interconnect C. Even though the phase angle difference change with time, the low-rank is calculated using normalized measurements, therefore the error remains within a specific range. In contrast, interconnect A has noisier measurements

Table 5.3: Low-rank for different sets of real-wrold PMU measurements: Interconnect B

Measurement type	Low-rank Month: May	Low-rank Month: August	Low-rank Month: December
Phase angle difference	23-33	24-33	22-35
Magnitude	35-39	36-39	36-39
Raw phase angle	15-40	16-40	13 - 40

Table 5.4: Low-rank for different sets of real-world PMU measurements: Interconnect C

Measurement type	Low-rank Month: May	Low-rank Month: August	Low-rank Month: December
Phase angle difference	22-35	27-36	26-35
Magnitude	34-39	35-39	36-38
Raw phase angle	10-40	12-40	9 - 40

therefore its phase angle differences show higher range of low-rank compared to other interconnects The magnitude measurements are typically of larger values (order of 10^3 or more), therefore the magnitude measurements can be approximated with relatively larger low-rank. Tables 5.2 - 5.4 show that the low-rank remain within the higher range of 35-39 for all three interconnects. The raw phase angle, as it varies between 180^o to -180^o, demonstrates very large variation in low-rank approximation too. In our experiment, the low-rank approximation for Hankel-matrices with raw phase angle measurements vary largely between 9 to 40, therefore it is more difficult to predetermine low-rank using raw phase angle measurements. All three interconnects show similar results for raw phase angle measurements. In real-world implementation, we need to predetermine the low-rank for every interconnect and for each measurement type (phase angle difference, raw phase angle, and magnitude). A particular low-rank for a specific measurement type at a certain interconnect does not show seasonal variation.

For the demonstration of the computational burden reduction using predetermined low-rank approximation, we choose the particular dataset from interconnect B to predetermine

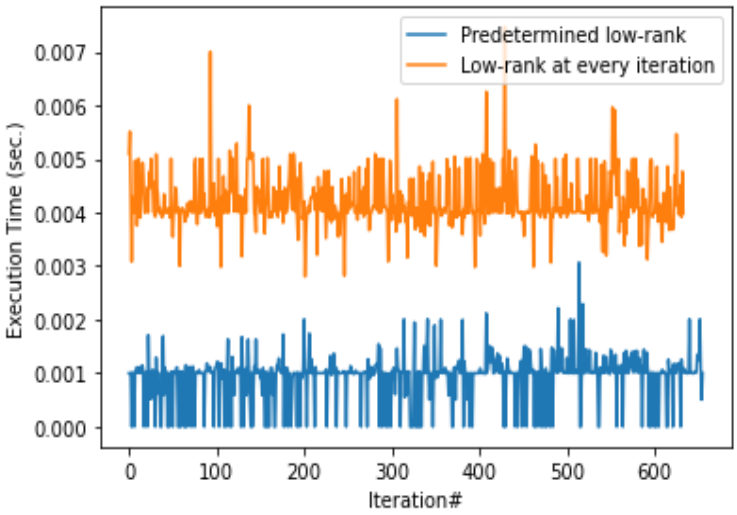

Figure 5.11: Computational time for predetermined low-rank and running low-rank at each iteration

average low-rank span from $2017-08-03\ 04:00:00.000$ and end at UTC $2017-08-03\ 04:05:00.000$. The low-rank approximation varies from 27 to 36 for Hankel-matrix data window length of 80. We chose the minimum low-rank of 27 to test the effectiveness of enhanced Hankel-matrix model. Fig. A.1 depicts the computational time for each iteration of phase angle difference Hankel-matrix, and the time is significantly reduced (with an average value of $\approx 2msec.$ if we use predetermined low-rank of our proposed enhanced model instead of running low-rank approximation as previously done in ref [114] and [117].

5.4 Implementation of Real-time Sequential Event Classification Algorithm

In this section, we analyze the utility of the VT PMU-PDC testbed described in chapter 2 using conventional GPS-spoofing attacks. The testbed used in this work, depicted in Fig. 5.12 and described in chapter 2, contain three parts: the PMU simulator, PDC, and the

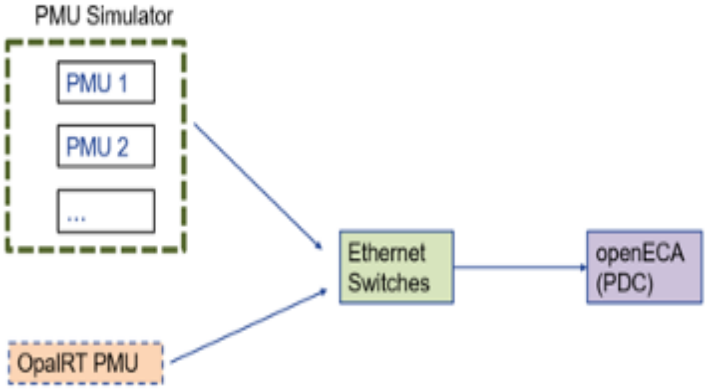

Figure 5.12: Proposed PMU-PDC testbed

communication link. The synchrophaosor data transmission is performed with the *PMU simulator* model developed in [139]. The Phasor Data Concentrator (PDC) is implemented with the *OpenECA* platform [140]. Both the *PMU simulator* and *OpenECA* are open source tools. The *PMU simulator* in the test system provides UTC timestamped PMU data with a sampling interval of 1/60 sec. The simulator transmits its data to *OpenECA* through TCP or UDP communication protocols. *OpenECA* aligns the data from all the PMU channels with the timestamps and is able to communicate with the next layer of cyber system/ system server. The data format during all communication between PMU-PDC-PMU and PDC to SO is in IEEE C37.118.2 protocol [141]. The physical power system is the IEEE 13 node test feeder system [142], simulated in *MATLAB SIMULINK*, with PMUs added at buses 611, 632, 633, 634, 646, 671, 675, 680 and 692 (Fig. 5.13). The physical event is modeled with three separate line to ground faults at each of the lines connecting bus-671 to bus-692, bus-632 to bus-633 and bus-671 to bus-680. For each line, three types of line-to-ground faults are applied, i.e. single line to ground (SLG), double line to ground (DLG), and triple line to ground (TLG) faults. Furthermore, fault impedance during each type of fault is varied from $0.01p.u.$ to $0.1p.u.$, with a step size of $0.01p.u.$. This variations in fault impedance, location, and fault types generate a total $10 \times 3 \times 3 = 90$ number of physical events.

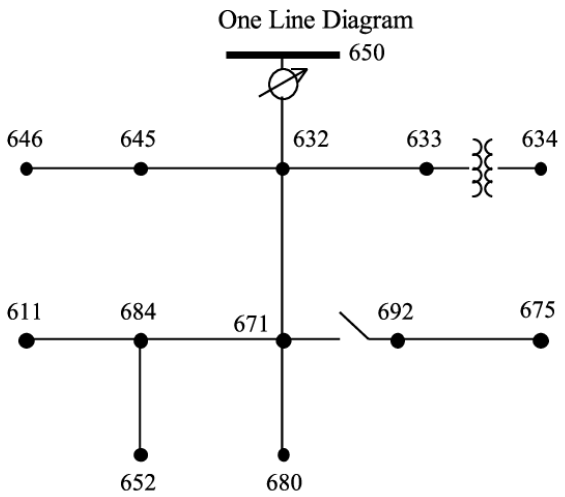

Figure 5.13: IEEE 13 node test feeder

Two types of FDIA are modelled in this work to verify two different parts of the proposed sequential algorithm. The first type is done by adding an attack value a to the voltage magnitude measurements. The goal of the attacker is to avoid getting detected by SO, therefore a should follow a trade-off between small enough to avoid detection and large enough to cause significant impact to the system. To demonstrate the feasibility of our proposed real-time event detection and classification schemes, a variable attack value between 1% to 5% of the peak voltage magnitude measurements are added to the actual measurements. The second type of FDIA will be discussed later at this section.

The simulated PMU data from *PMU simulator* is transmitted at a rate of 60 frame per second to *OpenECA*. The *OpenECA* is enabled with a $TestHarness$ system that runs the user-defined algorithm to perform designated tasks. The algorithm 2 was implemented in the $TestHarness$ system in real time. At each timestamp t_s, the algorithm receives N_s number of measurements from previous N_s times stamps, spanning from the measurement with timestamp $t_s - N_s + 1$ to the measurement with timestamp t_s. A major advantage of the proposed model is it is computationally efficient. The algorithms are executed in python, in

a computer with an Intel Core i5, 1.8 GHz CPU and 8.00 GB RAM. The PMU-PDC testbed runs the $TestHarness$ in real-time, and the $TestHarness$ calls the python script at every 1 millisecond to 100 miliseconds, depending on the data-window length.

Considering the beginning of simulation as timestamp 00:00:00.000, the IEEE 13 bus system as in Fig. 5.13 runs over 50 second for each test case, generating $60 \times 50 = 3000$ measurements. The final timestamp of the measurements received by *OpenECA* from *PMU simulator* is 00:00:49.833. Initially, testbed is simulated for normal condition, i.e. no physical event or cyberattack. This normal condition provides event detection threshold τ^h. For each of 90 physical events represented by different line to ground faults described above, the testbed is simulated over 50 seconds, with the fault applied to the grid at the timestamp 00:00:14.117 and is removed at the timestamp 00:00:28.050. For the first type of FDIA, each of three different attack values are applied to the voltage measurement at the same timestamp 00:00:14.117 for respective simulation of the testbed, the three attack values being 1%, 3%, and 5% of rated peak voltage measurement. The FDIA targeting the voltage measurement is used for the second part of the proposed algorithm, that is identifying event type.

After the cause of event is identified as cyberattack, the proposed model uses phase angle data to distinguish GSA from FDIA as discussed in previous section. GPS-spoofing attack is modeled by shifting the timestamp at the PMU simulator by $\frac{\Delta\theta}{2\pi\times 60}$. The term $\Delta\theta$ represents the deviation in phase angle due to the GSA, as shown in eqn 4.8. As the most significant impact of GPS 1 PPS shift during GSA is reflected by a change in phase angle data, we have added a phase angle deviation $\Delta\theta$ to the actual measurements to demonstrate the effect of GSA. Phase angle deviation larger than 0.57 degrees results in a Total Vector Error (TVE) 1% [134], therefore the attacker must ensure the GPS 1 PPS shift to be small enough to produce an angle shift ($\Delta\theta$) less than 0.57^o. For a particular amount of GPS 1 PPS signal

shift that is equivalent to $\Delta\theta$, the phase angle will be shifted by $\Delta\theta$ the next 1 second. In order to reflect two consecutive GPS 1 PPS shift, first phase angle shift is applied at the timestamp 00:00:14.117, and the next 120 sample data is also shifted by the same degree, until the timestamp, 00:00:16.100.

Our goal is to differentiate GSA from FDIA, therefore a second type of FDIA should come into consideration with attack values applied to the phase angle data only. This second type of FDIA can be used for the third part of proposed algorithm, that is identifying cyberattack type. For the second type of FDIA, three different test cases are created with three different phase angle shifts with the values: 0.1^o, 0.3^o and 0.5^o. Each test cases are applied at the same 00:00:14.117 timestamp as previous faults and cyberattacks.

The combined sequential event detection and classification model is further tested with IEEE 118 bus system [143], simulated in Python-Siemens PSS/E to implement dynamics. We have created 20 separately physical events by applied line-ground faults with four different impedance (0.0005 p.u, 0.005 p.u., 0.05 p.u., and 0.5 p.u.) at five different branches.

The FDIA is simulated by applying an attack values of 1%, 3% and 5% of the peak voltage measurements. The physical events and cyberattacks for IEEE 118 bus systems are analyzed under same computational environment as it is for IEEE 13 node test feeder, and the LG faults and FDIA are applied at the timestamp 00:00:14.117 and are removed at the timestamp 00:00:28.05.

Each of the three parts of algorithm in Table 2 is implemented in the test harness sequentially, the first part, which is the BDD is being executed over times-series moving data-window in real time. If BDD indicates the existence of event, the second part, which is differentiating physical event and cyberattack, is executed for the next time-series moving data-window. When the type of event is identified as cyberattack, the third part is executed over the same

data-window to determine the cyberattack type: FDIA or GSA.

5.4.1 Part I: Event Detection Results

For each test case of physical events and cyberattacks, PMU simulator transmit data to OpenECA at GPS synchronized timestamp t_s, and OpenECA feeds the data into the test harness. The test harness runs the event detection algorithm using the measurement from timestamp t_s along with $T-1$ number of previous voltage and current measurements, constituting a time-window with size T. For a test case scenario under normal condition, i.e. no event, set V_m denotes the set of voltage magnitude measurements over 50 sec, period, and σ denotes the standard deviation. The event threshold τ^h can be determined using the relation as follows:

$$\tau^h = max(V_m) + 3\sigma(V_m) \tag{5.1}$$

At timestamp 00 : 00 : 14.117, a sample physical fault testcase with a TLG fault has been applied near bus 680 of IEEE 13 bus node test feeder. The TLG fault is removed at the timestamp 00 : 00 : 28.0167. The voltage magnitude measurements at bus 80 with random Gaussian noise of mean 0 and standard deviation 1 reflects the change over the fault duration (Fig. 5.14).

For the data-window length of 100, the estimation residual using Hankel-matrix as described in algorithm in Table 1 remains less than the threshold τ^h before the fault occurrence. However, just after the occurrence of the TLG fault, estimation residual exceeds the τ^h for more than 3 consecutive measurements, as in Fig. 5.15. Therefore, the system operator can

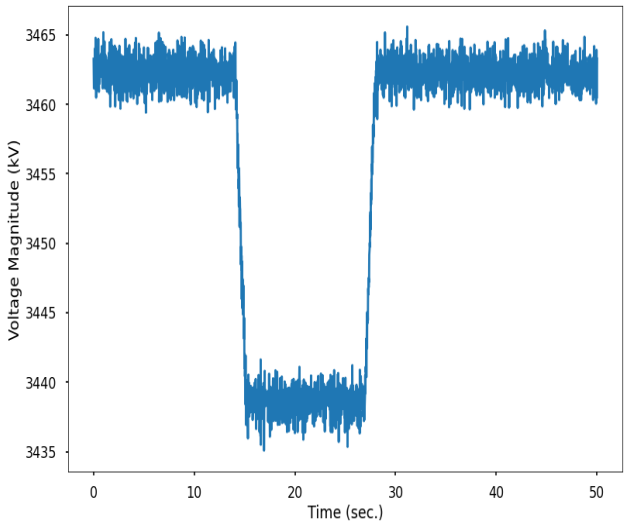

Figure 5.14: Noisy voltage magnitude measurement near bus 80

detect the occurrence of event around timestamp 00 : 00 : 14.117.

The accuracy of Hankel-matrix based event detection method is expected to depend on the data-window length W. Smaller data-window length provides smaller dataset to estimate the next measurement, therefore it can be assumed that event detection accuracy increases with larger data-window length W. To check the dependence of accuracy on the data-window length W, total number of 99 testcases, including 90 physical events and 9 FDIAs are executed in the testbed. The proposed method provides 100% accuracy for data window length larger than 130, as illustrated in fig. 5.16. Smaller window length reduces the event detection accuracy, which confirms the expected relation between data-window length and accuracy.

5.4.2 Part II: Event Classification Results

After the existence of event is detected at timestamp 00:00:14.117, the second part of algorithm 2, which is identification of event type, is executed in the test harness. Theoretically, the low rank approximation error (eqn 4.4) for physical event is expected to change after

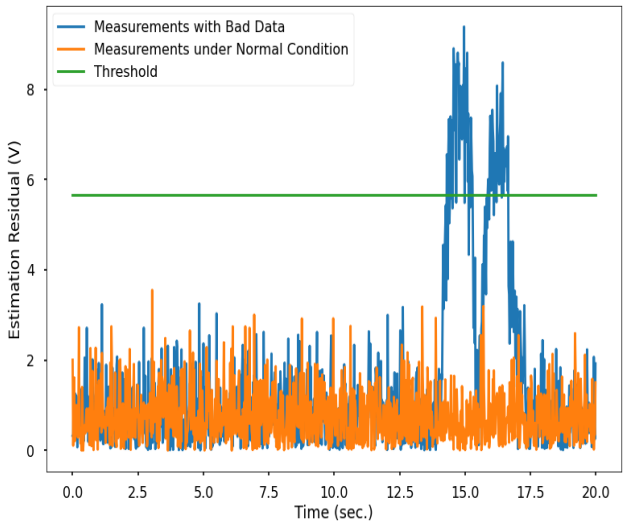

Figure 5.15: Event detection using Hankel Matrix

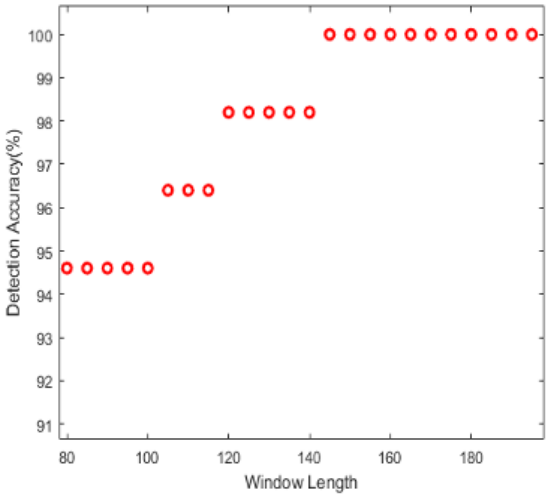

Figure 5.16: Detection accuracy variation with data-window length

random column permutation, whereas for cyberattack the change is expected to be zero. Due to the existence of measurement noise and randomness of column permutation, the change in low rank approximation error before and after random column permutation may not be exactly zero. Therefore a threshold η as described in algorithm in Table 1 must be selected to indicate any significant change in the low rank approximation error. A heuristic value of $\eta = 0.1$ is selected as threshold to distinguish cyberattack and physical event.

We have executed two testcases in the testbed to verity the proposed algorithm: the first being a TLG fault at near bus 692 with fault impedance 0.01 p.u. and the second one being a FDIA with 1% deviation added to voltage magnitude measurements from bus 692, both initiated at the timestamp 00:00:14.117 separately. With a data-window length of 120, the event is detected at first for the timestamp 00:00:14.117, with similar results as shown in Fig. 5.15. When event is detected, the second part of algorithm in Table 2 is executed immediately, with the measurement from timestamp 00:00:14.117 and the previous 119 measurements, constituting total data-window length of 120. For each test case, the algorithm uses multi-PMU Hankel-matrix as depicted in eqn 4.2. Since bus 692 is physically connected with bus 671 and bus 675, the measurement matrix contains three rows, and the number O from algorithm in Table 1 is 3.

Measurements from the timestamp 00:00:14.117, which is the 847^{th} measurement, contain the first instance of event, the random column permutation based method sometimes fail to indicate the correct fault type. The event identification algorithm needs to applied for the next data set, that contains measurements from the timestamp next to 00:00:14.117, which is 00:00:14.133 or the 848^{th} measurements, and the previous 119 measurements. The process has to be repeated for moving data-window over time until the data-window contains enough measurement points to demonstrate significant change in low rank approximation error after random column permutation. For 120 data-window length, low rank approximation error

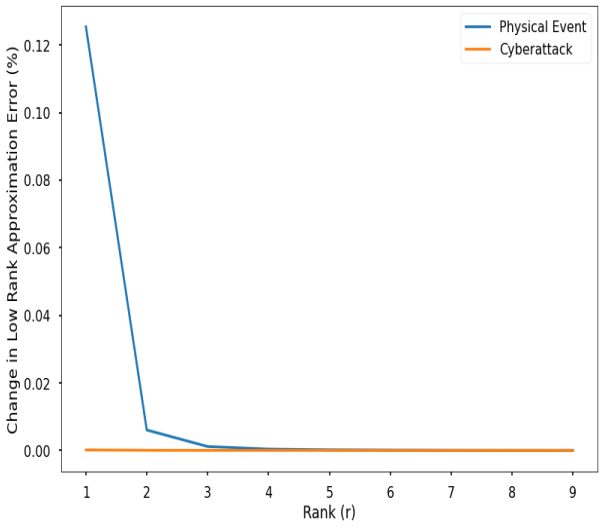

Figure 5.17: Event type identification: differentiating cyberattack from physical event W = 120

after random column permutation shows a change larger than $\eta = 0.1$ for the first time for a data-window starting from 760^{th} measurement and ending at 880^{th} measurement. Fig. 5.17 indicates that the rank-1 approximation error is larger than 0.1 for TLG fault. The change in low rank approximation error before and after random column permutation over the same data-window for the testcase containing FDIA data remains approximately 0, implying a different behavior for cyberattack and physical event.

If the low rank approximation error indicates a change larger than threshold η after random column permutation for the data-window starting from measurements of timestamp $t_s - 2W/3$ to measurements of timestamp $t_s + W/3$, cause of event is identified as physical event, and the corresponding restorative actions need to be taken by the system operation. However, if the event type is identified as cyberattack, the third part of the proposed algorithm is executed using the same data-window that demonstrated the change in low rank approximation error as greater than η.

As mentioned before, data-window needs to contain a minimum number of measurements

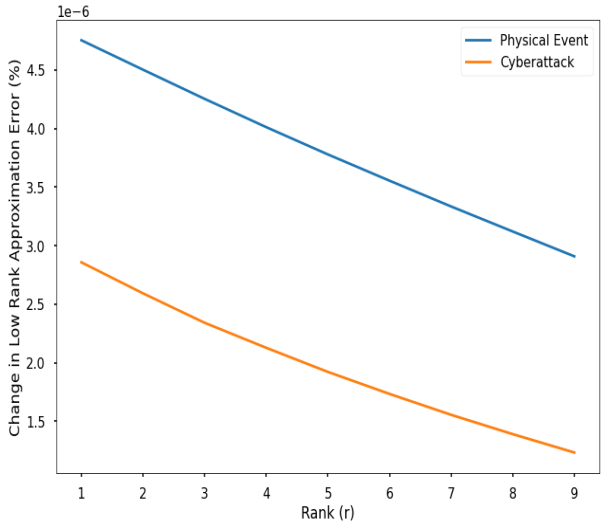

Figure 5.18: event type identification: differentiating cyberattack from physical event with W = 70

to indicate any change in low rank approximation error after random column permutation. algorithm in Table 1 has reported correct event type for $W \geq 73$. For instance, Fig. 5.18 depicts the failure of proposed model in identifying event type correctly when W = 70, since both of physical event and cyberattack display insignificant changes ($<< \eta$) in rank-1 approximation errors.

5.4.3 Part III: Differentiating FDIA from GSA Results

In the next step, the algorithm computes low rank approximation error of unwrapped voltage phase angle measurements. If the gradient of rank-1 approximation error is larger than 0 for three consecutive points, the type of cyberattack can be determined as GPS-spoofing attack, otherwise, it is an FDIA. A testcase is executed with 0.3^o deviation added to voltage angle measurements of bus 692 over two seconds starting at the timestamp 00:00:14.117 to reflect shift in two consecutive GPS 1 PPS signal, thereby imitating GPS-spoofing attack. We have observed positive gradients of low rank approximation error for single channel measurements

for more than 3 consecutive measurements. Another testcase of FDIA is executed with 0.3^o deviation added to voltage angle measurement of bus 692 over data-window length of 120. The result shows no positive gradient of low rank approximation error for the single channel phase angle measurements over same data-window length, confirming the FDIA as the cyberattack type in this testcase.

Smaller length of data-window W may provide insufficient dataset for the Hankel-matrix to demonstrate any significant change in low rank approximation error. For GPS-spoofing attack, after GPS 1 PPS signal is shifted, phase angle measurements for the next 1 sec. are modified, along with the transition points from $+/-\pi$ to $-/+\pi$. As a result, the unwrapped phase angle data exhibit deviation for the next 1 sec., that is until the arrival of another GPS 1 PPS signal. The proposed Hankel-matrix based model relies on the sudden variation or break-point of unwrapped phase angle data at the moment of attack. For the case of a very large number of dataset fed into Hankel-matrix, one break-point in the unwrapped phase angle measurements is not sufficient to display any significant change in low rank approximation error. Therefore a there exists a trade-off between smaller and larger data-window length. Analyzing test-cases with different phase angle shift due to GSA over different data-window length confirms this assumption (Fig. 5.19). Larger phase angle shift (0.5 degree) demonstrates positive gradient in low rank approximation error over larger data-window length. From Fig. 5.19, it can be concluded that data-window length from 80 to 120 works best for distinguishing GSA from FDIA over wide range of phase angle variation.

Even though the proposed model is applied in real-time, there are computational and network constraints. Each part of algorithm in Table 2 requires a fraction of a second to be executed. Data-window length affects the computational time, the larger the data-window, the longer it takes to execute the algorithm. Variations of average computational time of each portion

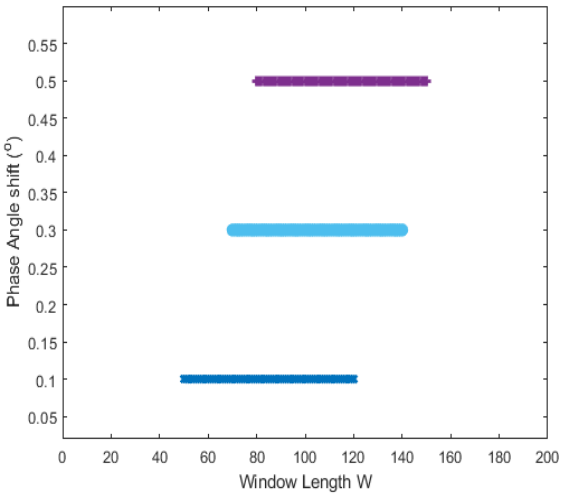

Figure 5.19: Data-window lengths' variations with different GSA for differentiating GSA from FDIA

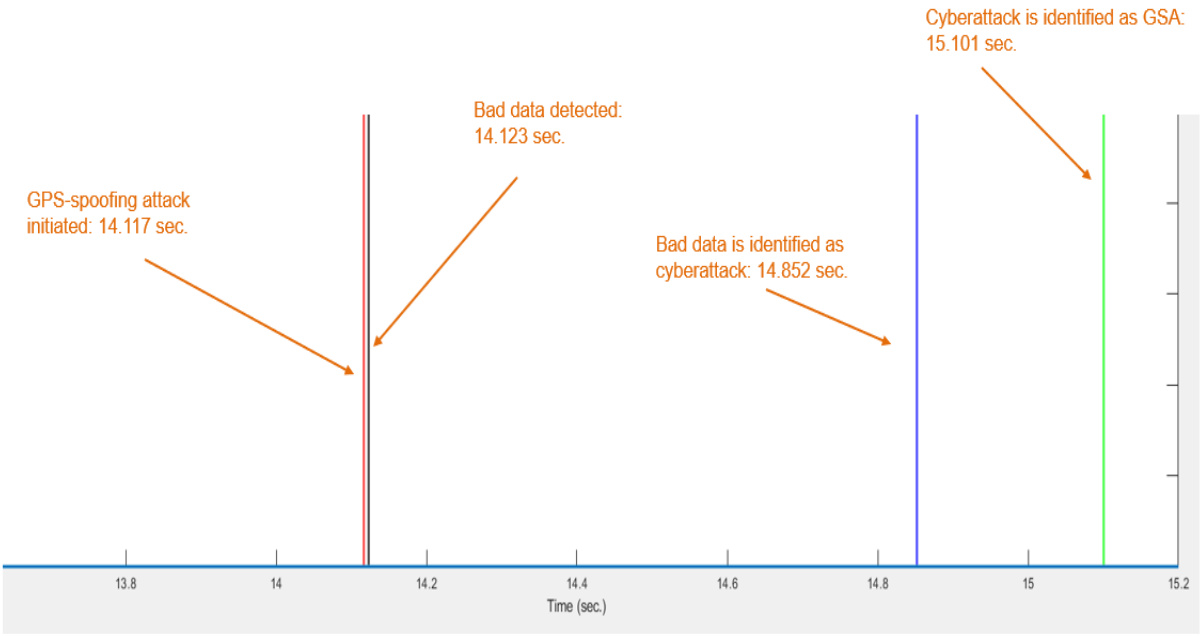

Figure 5.20: Time-series visualization of sequential real-time implementation of algorithm 2 in testbed from fig. 5.12 (IEEE 13 node test feeder)

of the proposed real-time algorithm against data-window length W are tabulated in Table 5.5. Total computational time for data-window length 90 is $\approx 0.91 sec.$, including the time

required to move the time-series data-window to include enough measurements for event type identification in subsection VI-B.

Table 5.5: Computational time vs data-window length

Data-window length W	Event detection	event classification	GPS-spoofing type identification
80	0.006437 sec.	0.085991 sec.	0.228165 sec.
90	0.006327 sec.	0.095918 sec.	0.254029 sec.
120	0.011000 sec.	0.149227 sec.	0.405938 sec.
130	0.016136 sec.	0.176000 sec.	0.498000 sec.

From the above analysis of the impact of data-window length on the effectiveness of each part of the algorithm, data window lengths of 90-100 can be considered as optimum data-window length, since it can indicate the event occurrence, its type and the type of cyberattack in less than 1 sec. The effectiveness of the testbed used to implement the proposed real-time event detection model is visually depicted in Fig. 5.20. event detection model is executed in real-time for moving time series data-window with length 90, using a testcase of GSA with 0.3^o deviation in phase angle measurement. event is initialized at the timestamp 00:00:14.117 sec., and the proposed detection model indicates the occurrence of event after $\approx 0.006 sec.$ of computational time. The next two parts are executed sequentially. event type identification requires 0.55 sec. to include enough measurements to the moving data-window so that it can demonstrate low rank approximation error change after random column permutation. It requires approximately 0.096 sec. to execute the low rank approximation error after random column permutation for data-window length of 90. Immediately after the detection of cyberattack, the third part requires approximately 0.25 sec. to identify GPS-spoofing attack. Considering the network delay of 0.033 sec. in *WIRESHARK* [63], we can correctly identify and locate the GPS-spoofing attack in the cyber-physical system in less than 1 sec.

5.4.4 Results with IEEE 118 Bus System

The dynamic simulation by SIEMENS PSS/E with LG faults at 5 different locations, each with 4 different fault impedance show similar result as of those obtained with the IEEE 13 node test feeder. For the LG fault of 0.005 p.u. impedance applied at the branch connecting bus 49 and bus 66, the data anomaly is detected within 0.02 second of timestamp 14.117 sec (Fig. 5.21). The low rank approximation error from Fig. 5.21 is calculated using the estimation of voltage measurement at bus 49, with data-window length of 100.

After detecting the existence of event, the voltage measurements are passed to the event classification step described in section 4.6.2. The event is correctly classified as physical event (Fig. 5.22). The similar steps are applied for cyberattack, formulated by applying FDIA with attack value 0.1% of voltage measurements. Fig. 5.22 shows that the change in low rank approximation error is much larger for physical event than it is for cyberattack. This scenario is expected, since in a larger system like the IEEE 118 bus system, there are more interconnected buses to a particular node. As a result, a random column permutation will destroy the temporal relation among interconnected nodes more severely than it does for smaller system with small number of interconnected nodes. Also, a very short data-window, for example the window length of 40, is enough to detect this change in low rank approximation error.

Table 5.6: Computational time vs data-window length for IEEE 118 bus system

Data-window length W	Event detection	event classification	GPS-spoofing identification
40	0.001999 sec.	0.271844 sec.	0.238516 sec.
80	0.006996 sec.	0.468730 sec.	0.224139 sec.
100	0.013992 sec.	0.623647 sec.	0.415231 sec.
120	0.020988 sec.	0.845527 sec.	0.504000 sec.

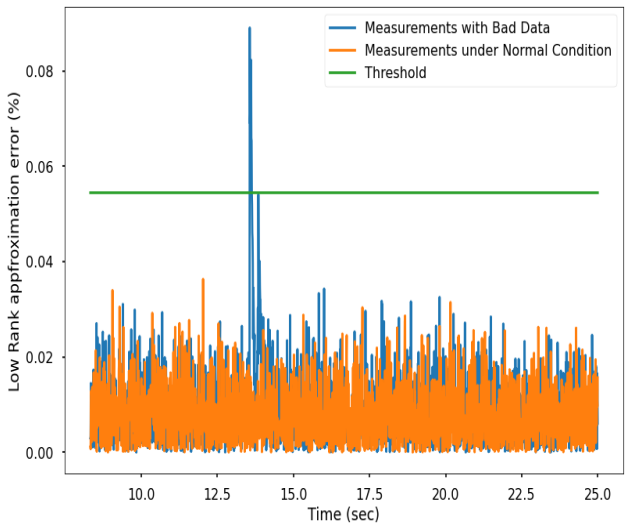

Figure 5.21: Event detection using Hankel-matrix for IEEE 118 bus system

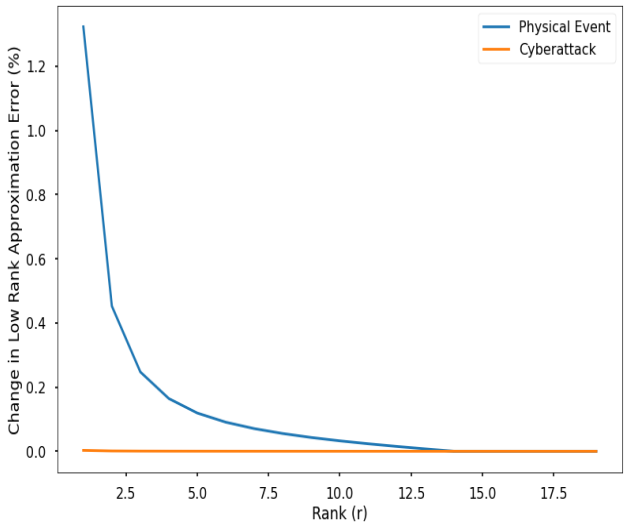

Figure 5.22: Event type identification: differentiating cyberattack from physical event with W = 40

The computational time for sequential detection and classification with varying data-window length is illustrated in Table 5.6. The additional computational time in IEEE 118 bus system comes from the multiple channel Hankel-matrix from eqn 4.2, the larger system with more interconnected nodes leads to a larger multiple channel Hankel-matrix. Including the communication delay between PMUs and PDCs, the total event detection and classification time with data-window length of 90 is approximately 2.9519 sec. However, with smaller data window of length 40, total event detection and classification time is approximately 1.8323 sec, less than 2 seconds.

5.5 Test of Enhanced Hankel-matrix Model on Stealthy Incremental GPS-Spoofing Attack

So far we analyzed our enhanced Hankel-matrix algorithm and tested its feasibility in identifying conventional GPS-spoofing attack. In this section we check the feasibility of our enhanced Hankel-matrix algorithm to detect the stealthy incremental GPS-spoofing attack proposed in chapter 3. Moreover, we test the impact of proposed attack model in power flow calculation, followed by undetectability analysis of such attack model against conventional detection algorithms. The proposed stealthy incremental attack has been tested on IEEE 24 bus reliability test system (appendix A.1). The physical power system is simulated in PSS/E.

The attack vector a corresponds to the voltage phase angle. The attacker calculates the phase angle deviation required to instigate undetectable attack described in section 3.4.1, and then creates the corresponding time shift by spoofing the GPS 1 PPS signal. The relation between the time shift t_d and corresponding specific angle variation $\Delta\theta$ can be written as:

$$\Delta\theta = 2\pi f_0 t_d \tag{5.2}$$

The optimization criterion described in eqn 3.17 is solved using MATLAB **Yalmip** tool box. For each time instance, the phase angle shift required to satisfy all the constraint in eqn 3.17 is computed by using the **Yalmip** solver. The attack vector a represents the required phase angle shift $\Delta\theta$ to incur successful attack. The attack vector **a**, which is calculated with optimization equation, is added to the phase angle and power measurements extracted from PSS/E simulation results.

The attacker solves the optimization algorithm of eqn. 3.17 at each 1 PPS signal to estimate the deviation a_i and a_j required to initiate proposed relentless GPS-spoofing attack, over a very long time period T which coincides with the peak load hour. Since the deviation at each 1 PPS signal is very small, the attacker needs to start spoofing the GPS signal long time ahead of T, during off-peak hour.

To evaluate the undetectability of the proposed phase angle shift caused by GPS-spoofing attack, we have utilized the aforementioned event detection methods: conventional WLSE residual test, Deviation based Kalman Filtering based residual test (DKF) and Hankel-matrix based estimation residual test. The residuals between the actual measurement and estimation using each method are tested with a predetermined threshold. The threshold is determined using Largest Normalized Residual test [144]. The predetermined threshold β is chosen as 3 [144]. Finally, we test the effectiveness of the gradient-change in low-rank approximation error among neighboring node-PMUs, as discussed in subsection 5.5.3.

For IEEE 24 bus RTS used for this work, load (L_1) at bus 13 is increased incrementally by 50% of L_1 at 5 sec., at 9 sec., and at 13 sec. In this way, a dynamic load varying condition is considered which behaves similarly as off-peak and peak-hour of real-world load variation.

Here 13 sec. to 15 sec. time period is considered as peak-hour. The attacker instigate a small shift in GPS 1 PPS over time period T, such that the perceived power flow through the branch 13-23, which is calculated from DC power flow using the shifted phase angle measurements at each end of the branch , increases. The target is to make a significant impact on the calculated power flow during the peak load after 13 sec. At this time, the calculated power flow through the branch 13-23, perceived by SO, will cross the critical MVA limit of the branch, even though the actual MVA is within the limit. The MVA rating of the line 13-23 of IEEE 24 bus RTS is 500 MVA [93].

Since the attacker instigates small incremental deviation in phase angle over time, it requires a long time for power flow to become large enough to cross MVA limit. As a result, attacker starts the attack at much earlier time of the peak-hour. In our simulation, the attacker starts the GSA at the 2 seconds mark.

The effectiveness of the proposed attack and defense model is evaluated in two steps. First, we have checked the impact of the relentless GPS-spoofing attack on power flow measurements. After that, the undetectability of the attack model is tested against conventional event detection methods as well as the proposed gradient change of low rank approximation error model proposed in section IV.

5.5.1 Impact on Power Flow Calculations

At first, starting at 2 seconds mark, the proposed optimization algorithm for each time instance is executed and the corresponding optimal attack vector $a_{op} = \theta_0$, which is the phase angle shift required to achieve the target of misleading the power flow calculation, is determined. In the rest of the chapter, the term attack vector and phase angle shift are used interchangeably. Time-shifts (as in eqn. 5.2) are applied to the GPS 1 PPS signal of the

corresponding PMUs located at the bus 23, simulated by adding corresponding optimized attack value a to the voltage phase angle measurements of bus 23 and bus 13 ($i = 23$ and $j = 13$). The power flow through the branch connecting the buses 13 and 23 is calculated using DC power flow equation. Since there is a presence of time shift in the GPS 1 PPS into the corresponding PMUs at the both ends of the branch connecting buses 13 and 23, the perceived power flow through the branch will be different from the actual value.

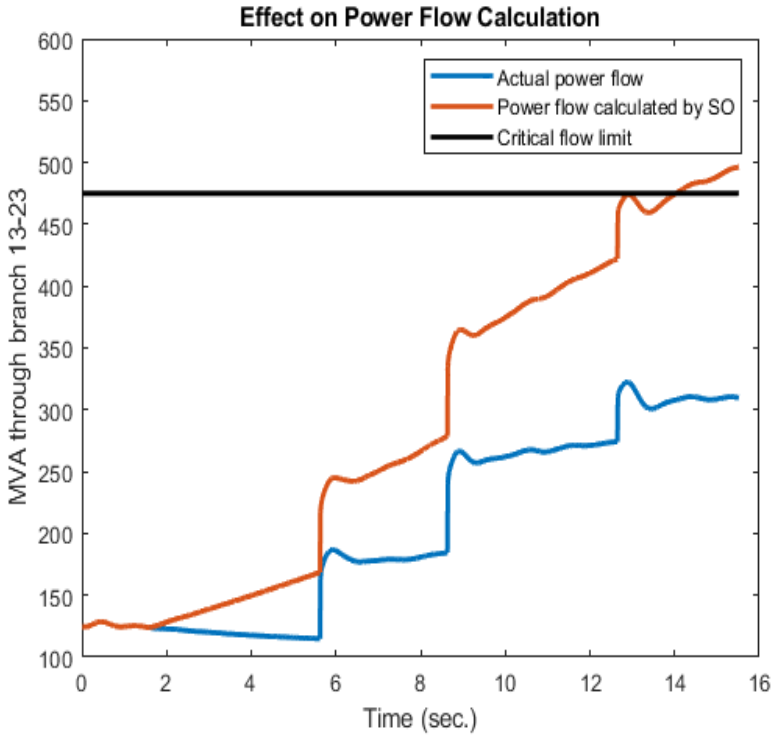

Figure 5.23: Power flow calculation between bus 13 and bus 23 for a_{op} over T time period

Fig. 5.23 demonstrates the results obtained from applying GPS-spoofing attack using proposed attack model. From fig. 5.23, we can observe that the perceived power flow calculated using the shifted phase angle measurement is higher than the actual power flow through the branch 13-23. for each time instance after initiating attack at 2 seconds. When the power flow through the branch increases, the calculated power flow is also increased by a small amount, keeping the calculated power flow within the line flow limit. After 14 sec-

onds, when the maximum power flows through the branch at peak hour, the calculated MVA exceeds the critical line flow limit, which is 95% of 500 MVA. Therefore the control center detects that critical MVA limit has been exceeded, and will be forced to take contingency actions despite the actual flow is within the limit, and the branch 13-23 will be tripped.

From fig. 5.23, we can conclude that the attacker can successfully initiate gradual change in power flow calculation by initiating an incremental GPS-spoofing attack over a long time, and the attacker can make the perceived flow calculation by SO exceed the flow limit for a particular branch, forcing the SO react against a false alarm of critical flow limit breach.

5.5.2 Undetectability Analysis

To check the undetectability of proposed attack scheme, normalized estimated residuals at each timestamp is calculated using WLSE and DKF methods separately. The state variable, X, is a 24×1 matrix comprised of voltage phase angles, and the Jacobian matrix, H, is 38×24 bus admittance matrix. The current measurement variable, Z, is a 38×1 matrix representing the current flow through the 38 branches of IEEE 24 bus RTS. Fig. 5.24 and 5.25 demonstrate the normalized estimation residuals obtained using WLSE and DKF methods, respectively. The normalized estimation residuals $\frac{||r||_2}{||\Omega||_2}$ at each timestamp is observed. From the results, it is evident that the largest normalized residual is less than threshold $\beta = 3$ for both WLSE and DKF methods.

Results from fig. 5.24 and 5.25 confirm the undetectability of the proposed attack model using two of most commonly used robust detection techniques: WLSE and DKF.

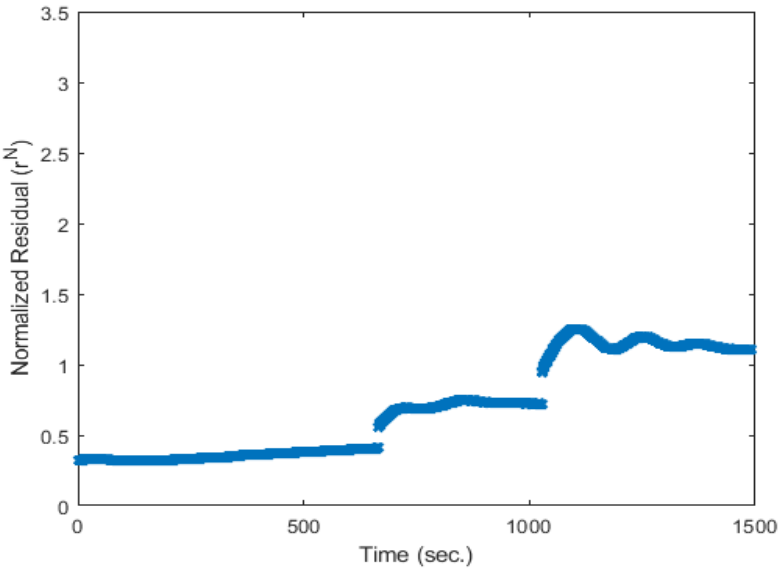

Figure 5.24: Normalized WLSE residuals between the observed and expected current measurements through the branch between bus 13 and 23

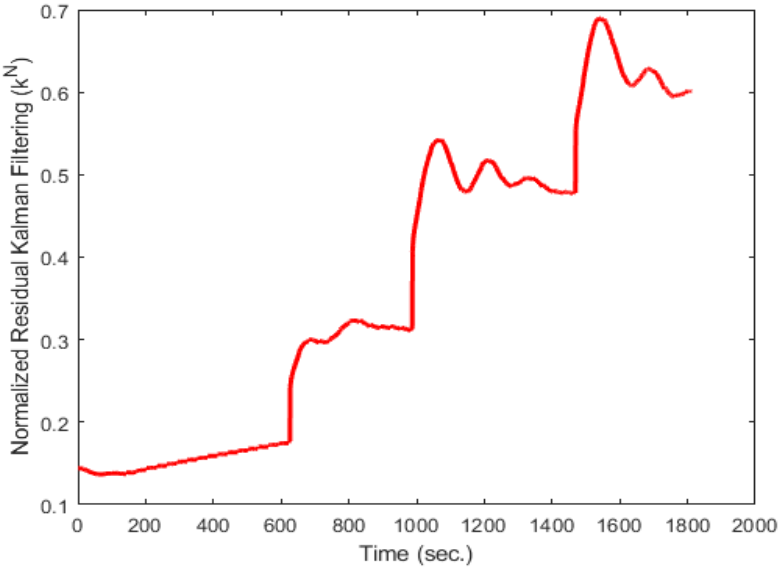

Figure 5.25: Normalized DKF residuals between the observed and expected current measurements through the branch between bus 13 and 23

5.5.3 Performance of Enhanced Hankel-matrix Algorithm

Hankel-matrix based detection model proposed in [90] detects distortion in unwrapped phase angle measurements to determine the possibility of GPS-spoofing attack. To analyze the effectiveness of Hankel-matrix model, we have extracted unwrapped phase angle measurements for normal condition (without 15 sec. time period), and then again with gradual GPS-spoofing attack condition (over same time period). Estimation errors are computed using Low rank approximation over moving time window of varying lengths $W = 80$, $W = 100$ and $W = 120$.

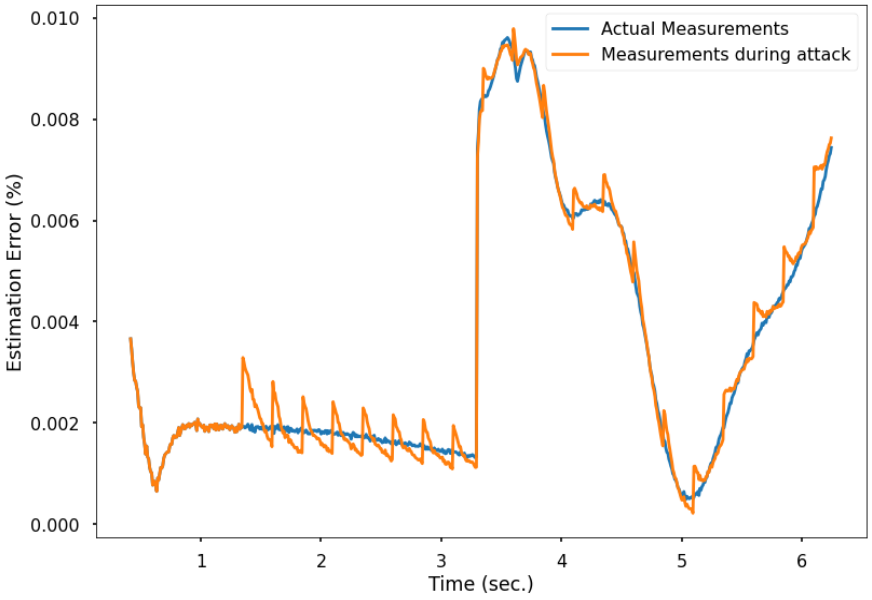

Figure 5.26: Estimation error of Hankel-matrix under normal and attack conditions over moving time window, W = 80

All three cases of different time-window lengths W, the attack condition demonstrates spikes in estimation error using low-rank approximation of Hankel-matrix. However, similar spike can be observed for phase angle deviations due to load changes too. Therefore, the spikes in fig. 5.26 to 5.28 are not conclusive evidence of GPS-spoofing attack.

Practically, the model [90] is not sufficient to identify small relentless GPS-spoofing attack

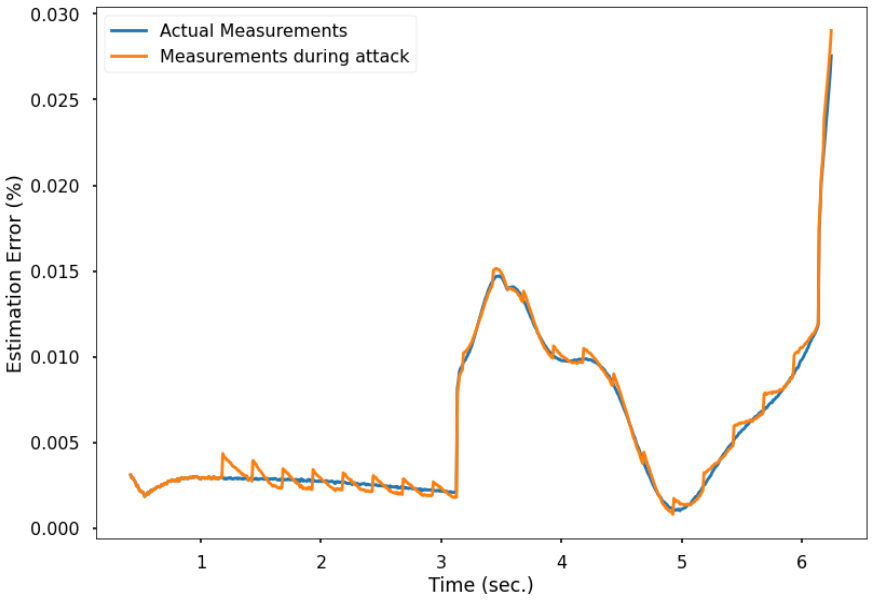

Figure 5.27: Estimation error of Hankel-matrix under normal and attack conditions over moving time window, W = 100

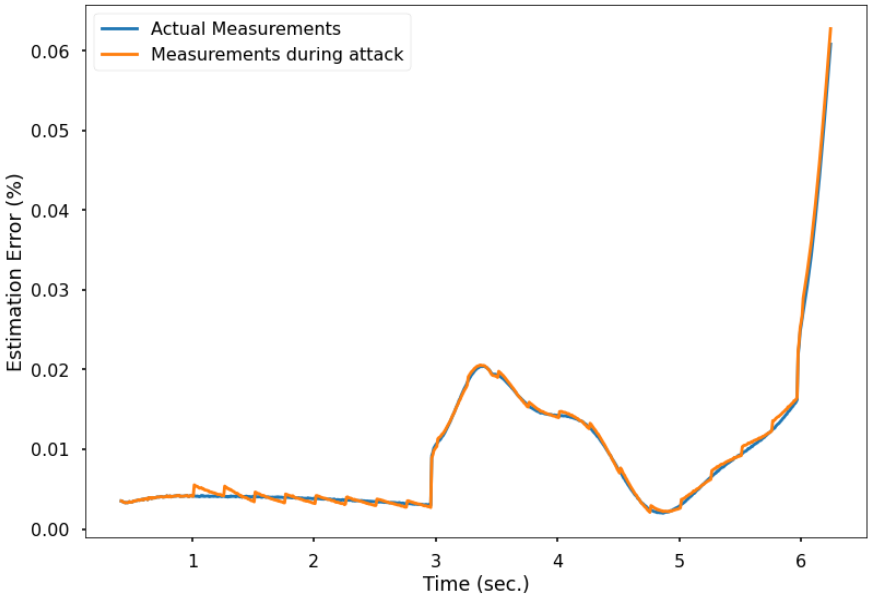

Figure 5.28: Estimation error of Hankel-matrix under normal and attack conditions over moving time window, W =120

discussed in previous section. For conclusive detection of such attack, we have exploited the spatial relation among the affected node and its topologically neighboring nodes. The

gradient change of low-rank approximation error of a single node is not enough evidence that the measurements from that node are under attacked since similar low-rank approximation error can be observed during load changes.

For any load variation driven angle deviation of a particular node, it is expected that such angle-variation will be propagated to the neighboring location of the grid. Therefore, the affected node should show similar gradient change, either positive or negative, as the neighboring nodes in low-rank approximation error of unwrapped phase angle measurements. For GPS-spoofing attack targeting a particular node, the gradient change in low-rank approximation error for that particular node is opposite to the gradient change in low-rank approximation error of neighboring or topologically connected nodes. We can analytically express the relation between the change of gradient in low-rank approximation error among node i and all other M nodes that are physically connected to i as below:

$$\frac{Gr_i}{|Gr_i|} \neq \frac{Gr_M}{|Gr_M|} \tag{5.3}$$

$$Gr_k = \frac{\Delta L_k}{\Delta t} \tag{5.4}$$

Where L_k = Unwrapped voltage/current phase angle measurements of node k.

5.5.4 Effectiveness of Differential Gradient Hankel-Matrix Algorithm

As discussed in subsection 5.5.3, the comparison of change in gradient of low-rank approximation error among neighboring PMUs can indicate small deviation in phase angle mea-

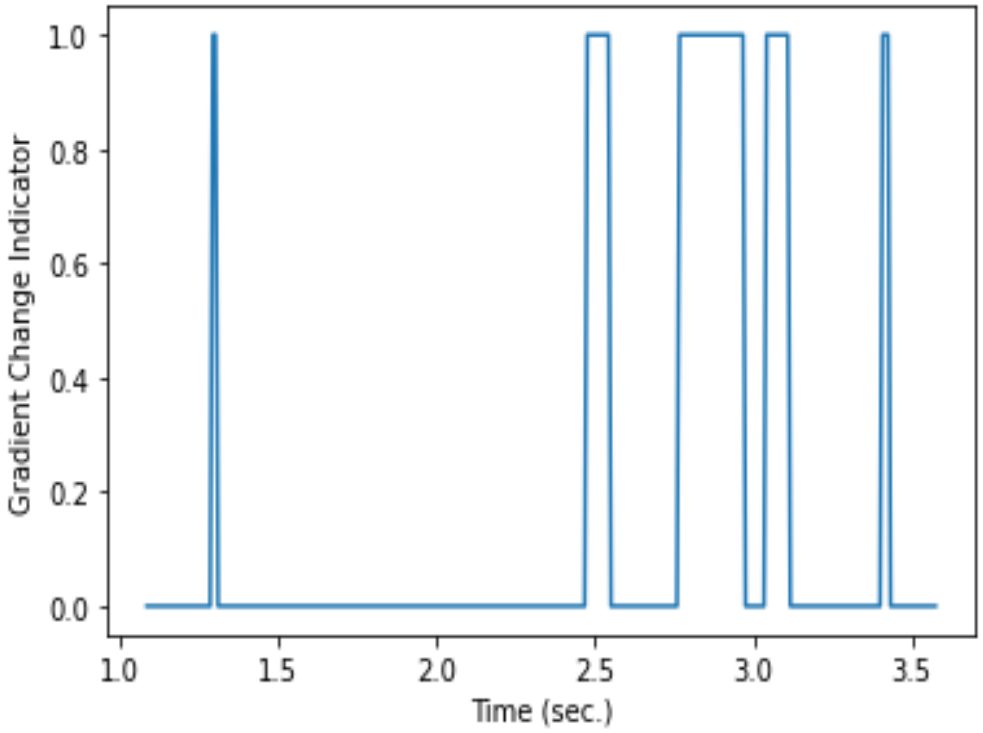

Figure 5.29: Change in gradient of low-rank approximation error between Bus 13 and 23

surements of a particular PMU measurements, implying a possible GPS-spoofing attack.

The change in gradient of low-rank approximation error between two buses is demonstrated with a Boolean expression. The value 1 signifies a change in gradient of low-rank approximation error between two buses, and the value 0 signifies unchanged condition. Fig. 5.29 shows that, the gradient changes frequently after 2 sec. among the low-rank approximation errors of Hankel-matrices of bus 13 and 23, using unwrapped phase angle measurements. Similar changes are observed among bus 23 and 12, and bus 23 and 11, separately. However, gradients of low-rank approximation errors of Hankel-matrices using unwrapped phase angle measurements does not demonstrate any change among bus 13 and 12 (fig. 5.30). The results imply the effectiveness of differential gradient Hankel-matrix model in the detection of proposed gradual undetectable GPS-spoofing attack.

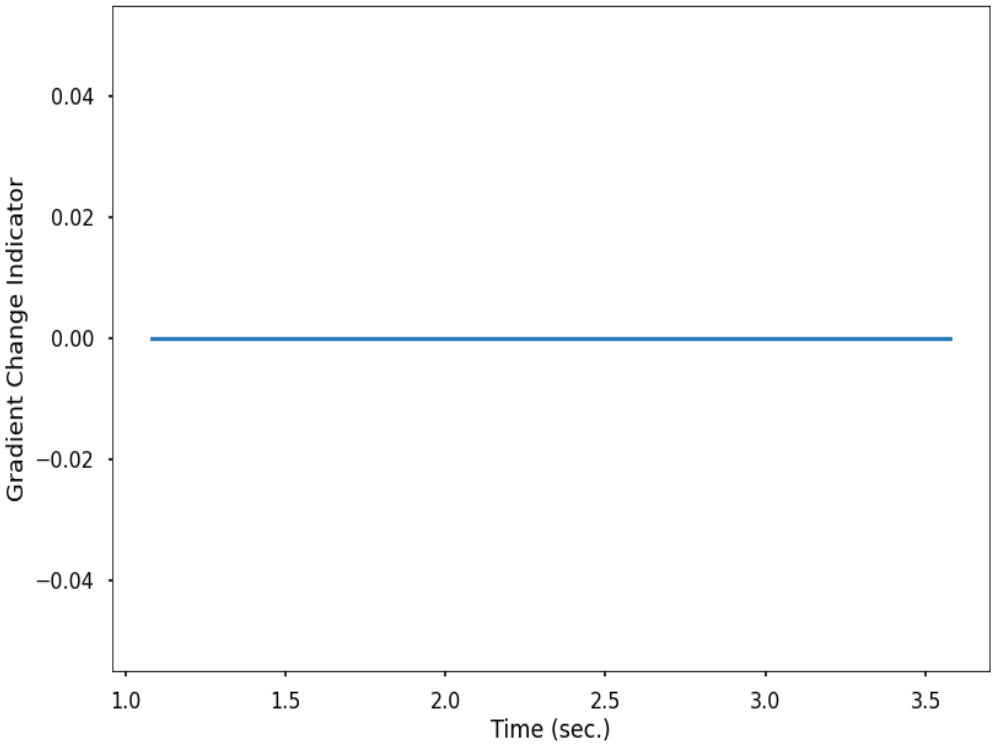

Figure 5.30: Change in gradient of low-rank approximation error between Bus 13 and 12

5.6 Detection of GPS-Spoofing Driven Forced Oscillation Attack

In this section, we analyze the GPS-spoofing driven FO attack model described in chapter 3. At first we model the proposed attack using periodic spoofing of time reference, followed by applying enhanced Hankel-matrix using both the phase angle difference and unwrapped phase angle measurements.

To model the proposed spoofing driven FO attack, we have considered IEEE 13 node test feeder as depicted in fig. 5.13. The power system model is simulated in Simulink, and the voltage and current measurements are extracted over 1 min. Phasor measurements are calculated using the non-recursive synchrophasor algorithm described in eqn. 3.26, where the periodic shift in 1 PPS time reference (t_s) signal due to GPS spoofing attack is reflected by angle deviation in eqn. 3.27. The angle deviation must be less than 0.57 to comply with IEEE C37.118.2 [32], therefore the attacker must keep the shift in 1 PPS signal in the order of 10^{-6}. In our work, we have created a periodic shift of $t_s = 25 \times 10^{-6}$. The attack is initiated at 2 seconds of the simulation, and the corresponding angle variation is applied to synchrophasor algorithm for the voltage and current measurements at bus 692. Periodic zero, positive, zero, and negative angle deviations, which correspond to the respective time shift t_s, are applied in same order a total 1 min. time window. The angle deviations complete a full cycle in 4 sec., as discussed in section 3.5.

Using the phasor measurements obtained from synchrophasor algorithm with corresponding periodic phase angle variation, the power spectral density of the voltage waveform is calculated in the frequency domain. From fig. 5.31, we can observe the additional oscillations at frequencies less than 1Hz, nominal frequency being 60Hz. Fig 5.32 demonstrate the occurrence of FO at 0.2596Hz and 0.778Hz, which are resonant with inter area mode frequencies

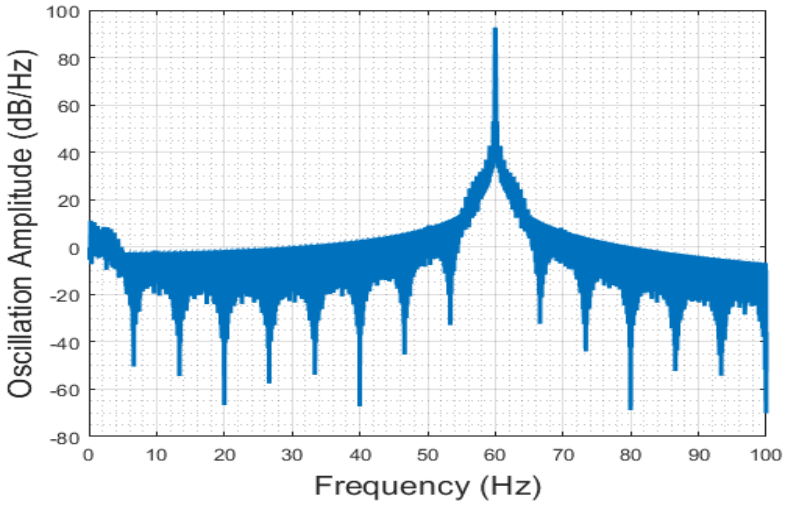

Figure 5.31: Power spectral density over frequency domain

of 25Hz and 0.77Hz as mentioned in ref [84]. The system operator, after analyzing the power spectral density of PMU voltage measurements at bus 692, will consider this as forced oscillations occurring at approximately 0.25Hz, 0.778Hz and beyond.

Results from fig. 5.32 indicates that the attacker can mimic a FO in the PMU measurements by carefully crafting periodic GPS-spoofing attack, which will make the system operator consider a possible FO event caused by periodic physical faults. The attacker can create the FO using GPS-spoofing at different locations of grid, using the similar periodic shift in 1 PPS signal. If the attack is initiated at different timestamps at different locations, the system operator will consider the FO to be propagated over a large area, and will perform unwanted restorative action against wide area FO event, even though the FO is caused by the GPS-spoofing, not by any physical fault.

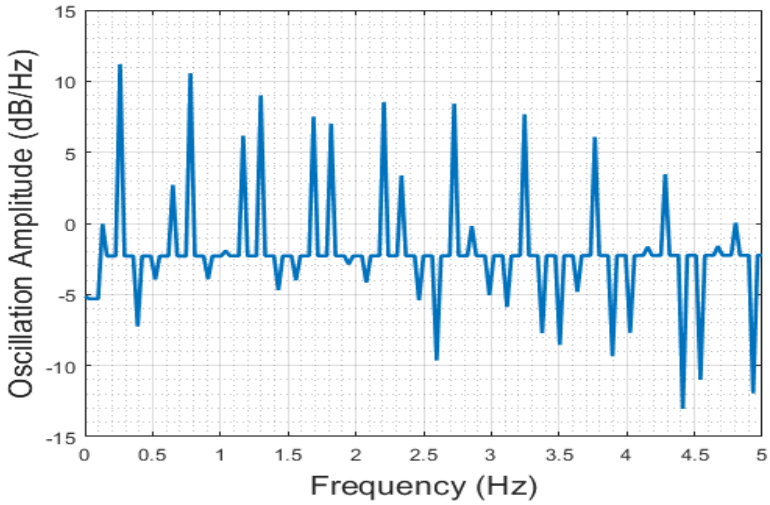

Figure 5.32: FO oscillations at $\approx 0.25Hz$, and $\approx 0.77Hz$

5.6.1 Performance of Enhanced Hankel-matrix Algorithm

We created multiple GPS-spoofing driven forced oscillation in separate simulations using IEEE 13 node test feeder by applying different periodic shifts t_s on the phasor measurements of bus 692, in each separate simulation run. In our enhanced Hankel-matrix algorithm and sequential event classification, the phasor measurements must pass two steps to detect GPS-spoofing as the cause of low frequency oscillation in the PMU measurements. First we need to identify if the data anomaly in phasor measurement is due to cyberattack, not physical fault. The second step is detecting GPS-spoofing and differentiating it from FDIA using phase-angle-only Hankel-matrix. For the first step, we perform random column permutation of the Hankel-matrix and calculate the change in low-rank approximation error, as described in chapter 4. The multi-PMU Hankel-matrix is created at each timestamp using the phasor measurements of neighboring PMUs of bus 692. The low-rank approximation errors do not show any significant change after 2 seconds of simulation time. This behavior signifies that the low rank approximation errors do not indicate any temporal correlation in the measurements among neighboring PMUs. Observing this behavior, we can conclude that

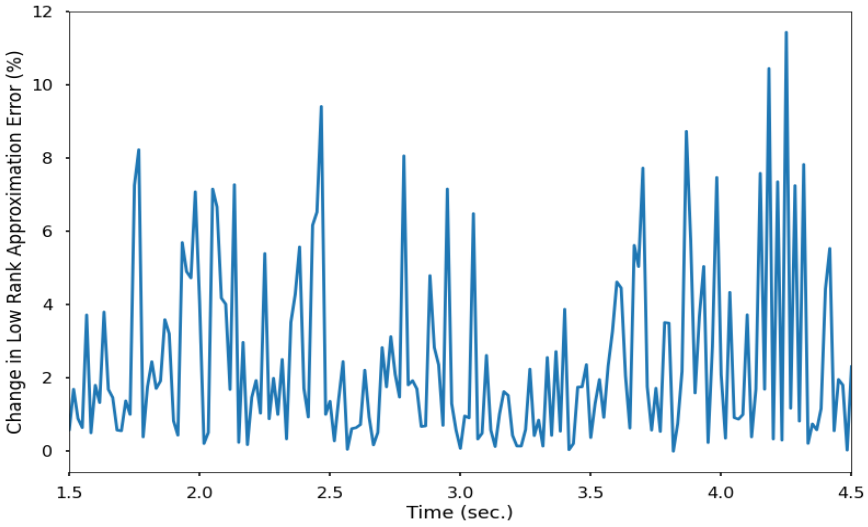

Figure 5.33: Change in low rank approximation error before and after random column permutation of multi-PMU Hankel-matrix under GPS-spoofing driven FO attack

the oscillation in measurement of bus 692 is due to cyberattack, not physical fault.

The second step is to observe low-rank approximation error using phase-angle-only PMU Hankel-matrix. We computed the low-rank approximation errors of Hankel-matrix using unwrapped phase angle measurement of bus 692 for different t_s. We also calculated the low-rank approximation error of Hankel-matrix using phase angle difference between bus 692 and bus 675 (reference PMU measurements).

Fig. 5.34, 5.35 and 5.36 illustrate the gradient of low-rank approximation error for the GPS-spoofing driven FO attack. The periodic time reference shift is $0.7ms$. For such small time shift, the unwrapped phase angle measurement based Hankel-matrix algorithm fails to identify the occurrence of spoofing at 2 sec, whereas it can detect the spoofing with periodic time reference shift of $2.1ms$, as depicted in fig. 5.35. On the other hand, the phase angle difference based Hankel-matrix can successfully identify the spoofing starting after 2 sec.

The smaller periodic shift demonstrates higher chance of going undetected by enhanced Hankel-matrix algorithm. Table 5.7 summarizes the minimum periodic time-shift required

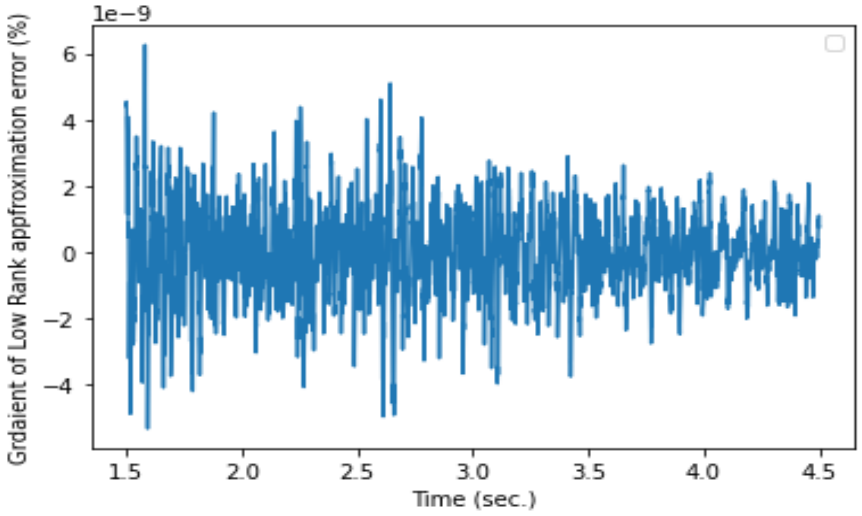

Figure 5.34: Enhanced Hankel-matrix performance using unwrapped phase angle measurement of bus 692, periodic time reference shift $10ms$

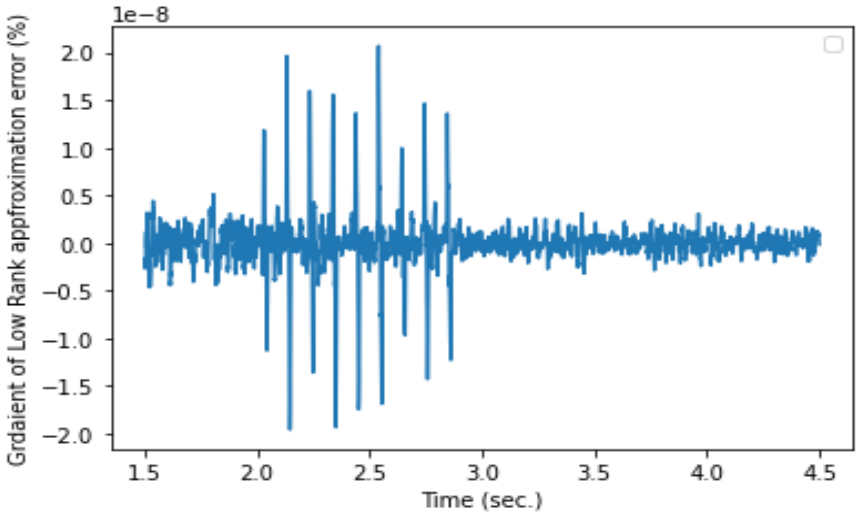

Figure 5.35: Enhanced Hankel-matrix performance using unwrapped phase angle measurement of bus 692, periodic time reference shift $30ms$

Table 5.7: Minimum periodic time shift for spoofing detection

Hankel-matrix input data	Minimum time shift (milliseconds)
Unwrapped Phase Angle Measurements	1.4
$\Delta\theta$ between bus 692 and reference bus 675	0.35

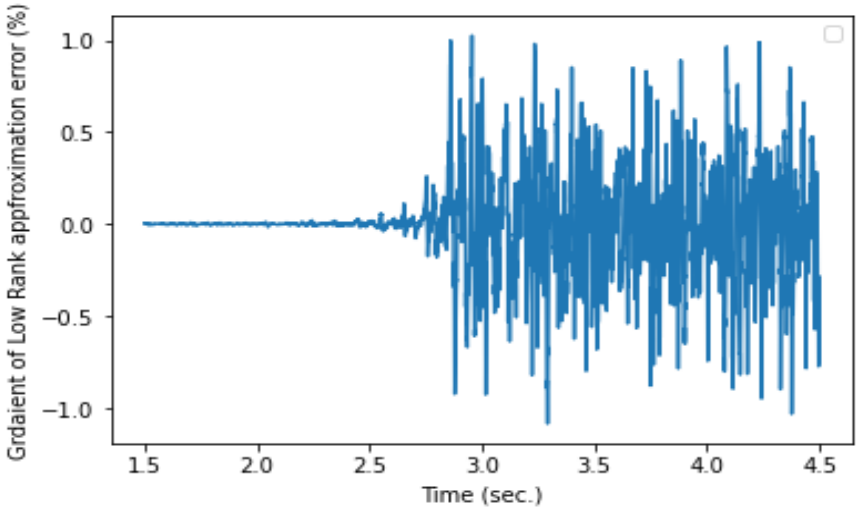

Figure 5.36: Enhanced Hankel-matrix performance using phase angle difference of bus 692 and bus 675, periodic time reference shift $10ms$

for the attack getting detected.

The enhanced Hankel-matrix, combined with sequential event classification algorithm, can detect the GPS-spoofing attack as the cause of FO in the PMU measurements.

GPS-spoofing attacks affects the phase angles of both voltage and current measurements of the same PMU. We exploit this fact and show that power flow calculation using PMU measurements provide simpler and computationally efficient way to detect GPS-spoofing driven FO attack. We explain the details in section 5.6.2.

5.6.2 Detection of FO using Power Flow Calculation

For the case of an actual FO event, if the voltage/current measurements from a PMU at bus k are found to contain forced oscillation components with low frequencies, and are resonant with inter area modes, f_h, the voltage at bus k can be expressed as $V_k = V_{mk}cos(2\pi f_0 t+\theta_{vk})+ V_{mhk}cos(2\pi f_h t+\theta_{vhk}) = V_{0k}+V_{fk}$. The current measurement provided by the same PMU that

corresponds to the current flow from bus k to bus j can be expressed as $I_{kj} = I_{mkj}cos(2\pi f_0 t + \theta_{ikj}) + I_{mhkj}cos(2\pi f_h t + \theta_{ihkj}) = I_{0kj} + I_{fkj}$. Here V_{0n} and I_{0n} refer to fundamental components of voltage and currents respectively at bus n, and V_{fn} and I_{fn} respectively refer to the FO components with frequency f. For each bus, V_m and I_m, respectively, are PMU voltage and current magnitudes, whereas θ_v and θ_i, respectively, are PMU voltage and current phase angle measurements. Suffix of each term in voltage and current equations reflects corresponding bus number. The real power flow between bus k and bus j, calculated with voltage and current measurements at bus k, can be written as:

$$\begin{aligned} P_{kj} &= V_k \times I_{kj}^* = (V_{0k} + V_{fk}) \times (I_{0kj}^* + I_{fkj}^*) \\ &= |V_{mk}||I_{mkj}|cos(\theta_{vk} - \theta_{ikj}) + P_f \end{aligned} \tag{5.5}$$

In eqn. 5.5, the power flow between two buses contain the power flow for fundamental components of voltage and current, plus an additional oscillation term P_f that is the sum of multiplication of FO and fundamental components of voltage and current. Therefore, the power flow will fluctuate with additional oscillations when there exist additional oscillatory components in the signal during an FO event.

Under the GPS-spoofing attack, there is no V_{fk} and I_{fkj} oscillatory terms in the voltage and current signal respectively. However the synchrophasor algorithm described in eqn. 3.27 will cause a deviation of $\Delta\theta_{vk}$ in the voltage phase angle for bus k and $\Delta\theta_{ikj}$ in the current phase angle. There will be small spikes in the voltage and current magnitudes, V_{mk} and I_{mkj} respectively, due to the shift in samples during the shift in time reference. The power flow equation will not contain P_f oscillatory term since there is no oscillatory term in the original signal V_k and I_{kj}, nevertheless for the angle deviation and the spikes in the magnitude, the

new power flow equation becomes.

$$P_k = ||V_{mk}||I_{mkj}|cos(\theta_{vk} + \Delta\theta_{vk} - \theta_{ikj} - \Delta\theta_{ikj}) \tag{5.6}$$

As a single PMU provides voltage measurement at bus k and the current measurement I_{kj} flowing out of bus k, spoofing of GPS signal for the PMU will create same shift in time reference for both voltage and current measurements. Thus, the phase angle deviation in both voltage and current will be equal ($\Delta\theta_{vk} = \Delta\theta_{ikj}$). This phenomenon will cause the $\Delta\theta$ terms in eqn. 5.6 cancel each other, resulting in no significant change in the power flow equation, except for the spikes in magnitudes. The spikes in V_{mk} and I_{mkj} terms will cause small spikes in the power flow equation, however unlike actual FO, there will be no sustained oscillation in the power flow. This contrast in the behavior of power flow graphs can help the system operator identify spoofing driven FO attack and distinguish it from actual FO event due to any fault in physical system. Once the system operator identifies the occurrence of FO using the PMU voltage and current measurements of a specific bus, it needs to look at the power flow from that specific bus using both voltage and current phasor measurements. If the power flow shows additional oscillation from the initial occurrence moment of FO, it is actual FO event due to physical fault in the system. On the other hand, if power flow does not show any additional oscillation, except small spikes at regular interval, the FO is due to spoofing of PMU time synchronization.

To figure out that the additional oscillation in the PMU measurement is caused by GPS-spoofing and not due to an actual FO event, the system operator needs to look at the power flow using voltage and current measurements from a PMU. We have observed the power flow using the voltage measurements at bus 692 and the current measurements from bus 692 to 675 (fig. 5.13). The actual FO event is modelled by injecting low frequency oscillatory

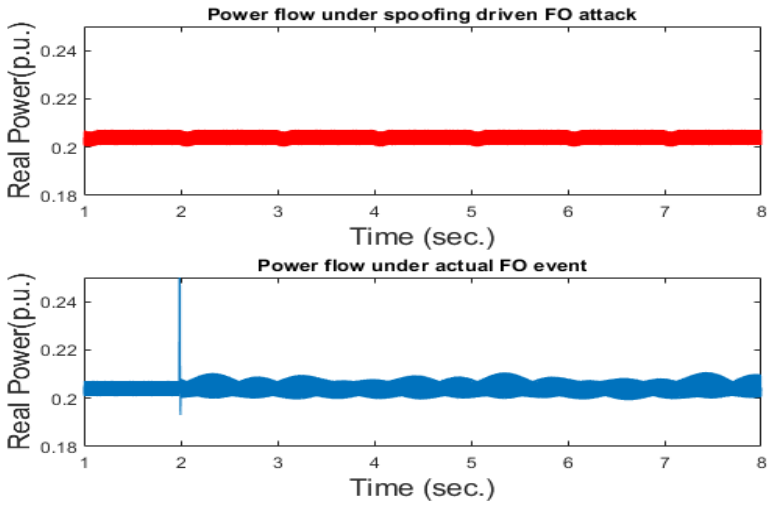

Figure 5.37: Power flow calculation using voltage and current measurements at bus 692

signals with frequencies: $0.25Hz$, $0.64Hz$, $0.778Hz$, and $1.17Hz$ to the measurements from bus 692. The FOs are added to original signal from 2 sec, and simulation setup for both power grid and synchrophasor calculation are same as it is for the aforementioned GPS-spoofing attack. The per unit power flow calculations under both conditions: spoofing driven FO attack and actual FO event can be visualized in fig. 5.37.

Fig 5.37 demonstrates that an actual FO event due to physical periodic faults in the system shows additional oscillations in the power flow calculation using PMUs of affected buses, starting from 2 sec. In contrast, a GPS-spoofing driven FO attack does not show any additional oscillation in the power flow, rather it shows small spikes at regular interval. These contradictory behaviors can help system operator differentiate spoofing driven FO attack from an actual FO event due to physical faults.

5.7 Detection of PDC Data-Drop Attack

We implemented the PDC data-drop attack in our enhanced VT testbed by creating an early arrival in the measurements coming from PMU simulator, and a small delay in the measurements coming from OpalRT. As the PMU simulator measurements arrives early, it forces OpenECA to start the wait-period timer earlier than usual time, therefore causing the delayed measurements from OpalRT getting dropped. The early arrival is formulated using the method described in section 3.6. We used a sample real-world PMU measurements from PNNL (described in section 5.3.2) to send from PMU simulator to OpenECA. The early arrival in the measurement is formulated at 2 second of simulation time.

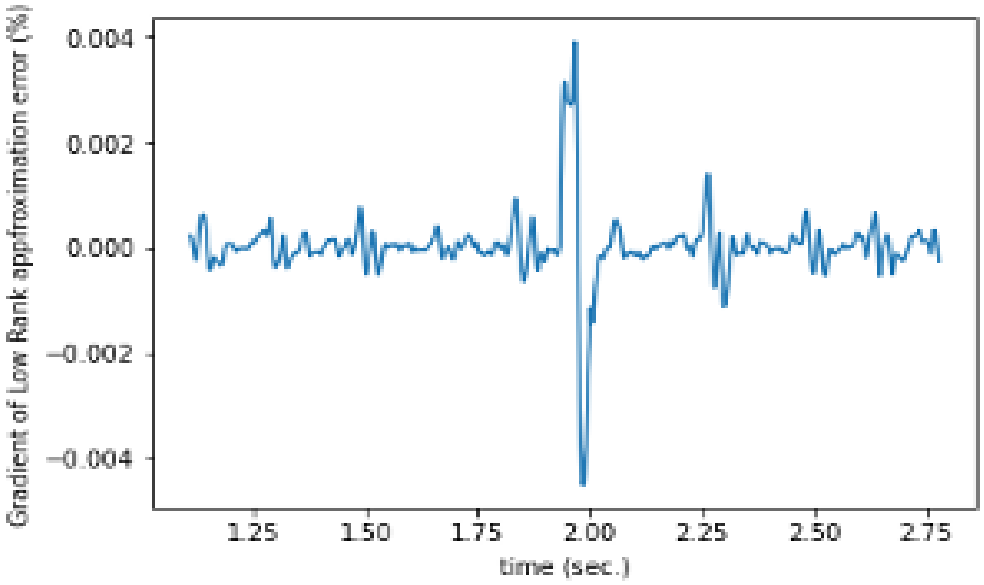

Figure 5.38: Detection of early arrival using stead-state real-world PMU data

We compute the low-rank approximation error at each timestamp for PMU early arrival case. To generate early arrival, we used PNNL steady state data at first. The result, as illustrated in fig 5.38, shows that the gradient of low rank approximation error has significant deviation at 2 second, indicating possible data manipulation.

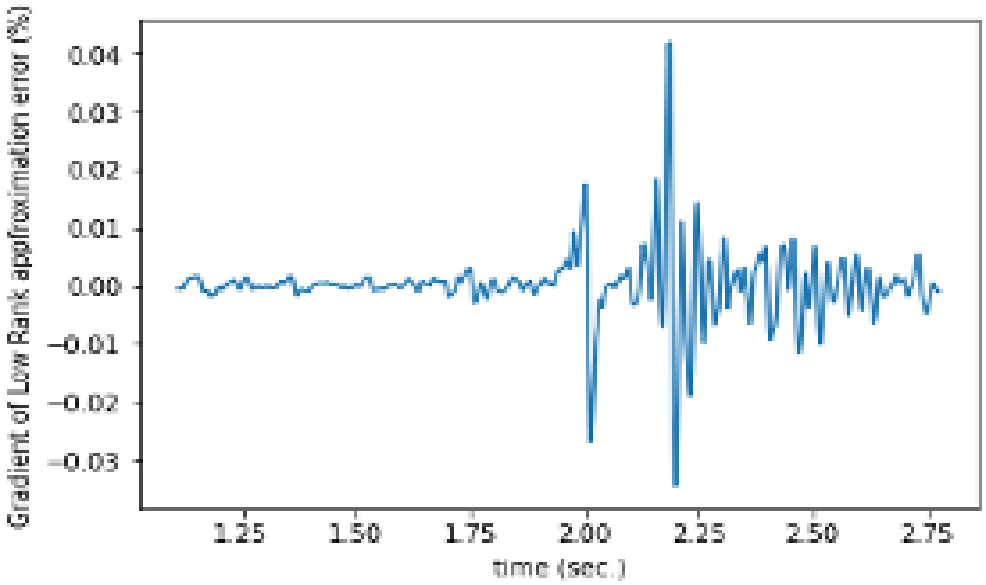

Figure 5.39: Power flow calculation Detection of early arrival using stead-state real-world PMU data

On the other hand, even though the fault-data from PNNL shows spikes in gradient of low rank approximation error, there exists spikes caused by system events. So it is difficult to identify data manipulation if the attacker targets fault-data to create PMU early arrival.

Chapter 6

Conclusions

6.1 Main Contributions

The main contributions of this dissertation in the field of cybersecurity of time-synchronized devices are:

- we developed a PMU-PDC testbed to analyze the cybersecurity of time-synchronized devices. The testbed incorporates real-time implementation of cyberattack detection algorithms, as well as enables user-designed FDIA and GPS-spoofing attack in laboratory setting;
- we design and implement, in our testbed, three sophisticated GPS-spoofing attacks against the time synchronized devices that bypass existing detection techniques;
- we enhance the existing Hankel-matrix algorithm for event detection and GPS-spoofing detection. In addition, we develop a sequential event detection and classification algorithm.
- we use our sophisticated GPS spoofing attacks and demonstrate that our enhanced algorithm is capable of detecting sophisticated GPS-spoofing attacks. Also, our enhanced algorithm can differentiate physical faults from cyberattacks and FDIA attacks from GPS-spoofing attacks with high accuracy.

6.2 Summary

In recent times we have witnessed a widespread integration of time synchronized devices such as PMUs into smart grid. PMUs operates similarly as IEDs, with an addition functionality of time synchronization that allows the measurement of angle differences among devices distributed throughout the system . Like other IEDs, PMUs are prone to conventional cyberattacks. However, PMUs have additional vulnerability, which is the attack against its time-synchronization. In this dissertation, we focus on the cyberattacks targeting the time synchronization of time synchronized devices, particularly PMUs and PDCs.

To study the cyberattacks against time synchronization, such as GPS-spoofing, we need a laboratory testbed capable of emulating time-synchronization attacks. In chapter 2, we present an enhanced PMU-PDC testbed that we developed to provide similar functionality of a real-world PMU-PDC infrastructure. We improved the existing Virginia Tech PMU testbed to simulate the attacks on time-synchronization of PMU. We incorporated OpenECA as a PDC for the testbed and use it to implement real-time algorithms for the detection of data anomalies such as GPS-spoofing attack, physical faults, FDIA etc. The testbed sends system states and quality flags to the control center. The developed testbed can be reproduced in laboratory settings with a very low cost.

After developing the testbed to test attacks on time-synchronization, in chapter 3 we propose three novel cyberattacks exploiting different vulnerabilities of the time-synchronization in time-synchronized devices. The first attack is stealthy incremental GPS-spoofing attack that bypasses conventional event detection techniques and incur damage to the system by manipulating phase angles resulting in changes of the power calculation. The second attack is GPS-spoofing driven Forced Oscillation (FO). The attacker can add oscillation, close to the system resonant frequency, in the PMU's voltage/ current measurements by creating

periodic shifts in GPS 1 PPS time reference. Currently these oscillations are detected using time synchronized devices. The system operator, by observing power spectral density, detects the occurrence of near-resonant frequency oscillation using time-synchronized measurements from PMU. The detection of such oscillations may lead the SO to take unnecessary restorative actions that may result in damage to the grid.

The third kind of attack targets the time-synchronization of PDCs. Due to their real-time operation, PDCs wait for a specific time-period for PMU data to arrive, discarding any data that arrives late and classifies that as a communication delay. By manipulating a string from a PMU to make it arrive earlier an attacker, the attacker forces the PDC to start the wait-counter earlier than normal. Consequently, the wait-period ends earlier than normal. As a second step, the attacker targets a second PMU and creates a small delay in the communication channel of second PMU data. Since the PDC wait-time ends earlier during the attack scenario, even a small delay of second PMU data arrival cause its data discarded by PDC. In this coordinated PDC data-drop attack, the delay of second PMU measurements is small enough to be detected by conventional delay attack detection methods. With this type of attacks the attacker may force the PDC to discard critical data for the detection of cyber-attacks in the system.

There are numerous detection algorithms for GPS-spoofing attack, one of which is Hankel-matrix algorithm. Hankel-matrix algorithm provides superior performance over other event detection algorithms due to its ability to exploit low-rank property and temporal/ spatial correlation among PMU measurements. General Hankel-matrix algorithm can detect conventional GPS-spoofing attacks. In chapter 4, we present our enhancements to the general Hankel-matrix algorithm to detect our proposed coordinated GPS-spoofing attacks in chapter 3. Instead of using full phasor measurements or raw phase angle measurements in general Hankel-matrix algorithm, our enhanced Hankel-matrix algorithm uses unwrapped phase an-

gle measurements and phase angle difference to detect GPS-spoofing attack and differentiate it from FDIA. We also enhance the numerical efficiency of Hankel-matrix algorithm by using phase angle difference and using predetermined low-rank instead of running low-rank approximation at each iteration of event detection. We also develop a sequential event detection and classification algorithm. We propose a multi-PMU Hankel-matrix to classify data anomaly among physical fault and cyberattack, and we use our enhanced phase-angle-only Hankel-matrix to differentiate GPS-spoofing and FIDA.

In chapter 5, we implement enhanced phase-angle-only Hankel-matrix to detect GPS-spoofing attacks and differentiate them from FDIA. The algorithm is verified using both simulation result and real-world PMU measurement provided by PNNL. The results confirm the enhanced Hankel-matrices' ability to identify GPS-spoofing attack conclusively, as well as the reduction in computational burden by approximately 2 milliseconds. This analysis is followed by real-time implementation of sequential event detection and classification algorithm using the testbed described in chapter 2. Using numerical simulation, it can be concluded that the sequential algorithm can detect GPS-spoofing attack within 1 second with properly tuned Hankel-matrix window. Simulation results using both IEEE 13 bus system and IEEE 118 bus system confirm the feasibility of sequential algorithm.

The detectability of stealthy incremental GPS-spoofing attack proposed in chapter 3 is tested using conventional event detection methods such as WLS, and Kalman Filtering. Both WLS and Kalman Filtering state estimations fail to detect proposed attack. The enhanced phase angle only Hankel-matrix show the possible occurrence of incremental GPS-spoofing attack, however, the spoofing attack can be conclusively determined using relative change in gradient of low-rank approximation error of neighboring PMU measurements.

The enhanced algorithm can also detect GPS-spoofing driven FO attack. The phase angle difference Hankel-matrix demonstrates superior performance over unwrapped phase angle

Hankel-matrix algorithm. The power flow calculation using a single PMU's voltage and current measurements can also indicate GPS-spoofing driven FO attack and can differentiate the attack from actual FO caused by physical fault.

6.3 Future Works

Even though we provided an extensive study on the attacks on time-synchronization, there exists some important future research scopes. First of all, the testbed in chapter 2 can be further improved using a real GPS-spoofer device. The PDC portion of the testbed, which is the OpenECA, can be engineered to incorporate a higher number of nodes of the grid. Currently the OpenECA can include a maximum of 144 measurement channels.

The GPS-spoofing driven FO attack in chapter 3 can be expanded to wide area FO by propagating the periodic GPS-spoofing over large area of the grid. Detection of such wide area FO using random column permutation of Hankel-matrix will pose additional challenge to the SO since the wide area attack will add some extent of temporal relation among neighboring PMU measurements. Furthermore, the effect of Phase-Locked-Loop (PLL), used in more advanced PMUs, needs to be investigated on such attacks.

In addition, an accurate detection method for coordinated PDC data-drop attack need to be developed. The smaller delay of second PMU data causes the coordinated data-drop attack go undetected by just observing data arrival time. The future research work can focus on developing an algorithm that can detect both early arrival and delayed arrival using the PMU measurements directly.

Part of our dissertation focuses on creating sophisticated cyberattacks against time-synchronization. For example, the stealthy incremental GPS-spoofing attack requires detailed information re-

garding the grid parameters, and the PDC data-drop attack scenario requires the detailed information about PDC wait-period and manufacturer's details which increases the cost for attacker. A more detailed analysis regarding the cost of attackers to implement such sophisticated attacks is a potential future research scope.

Appendices

Appendix A

A.1 IEEE 24 Bus System

The IEEE 24-bus system was developed by IEEE reliability subcommittee in 1979. In our work, the stealthy GPS-spoofing attacker targets the power flow measurement of between bus 13 and 23, by performing slow incremental attack on the time-reference of bus 13.

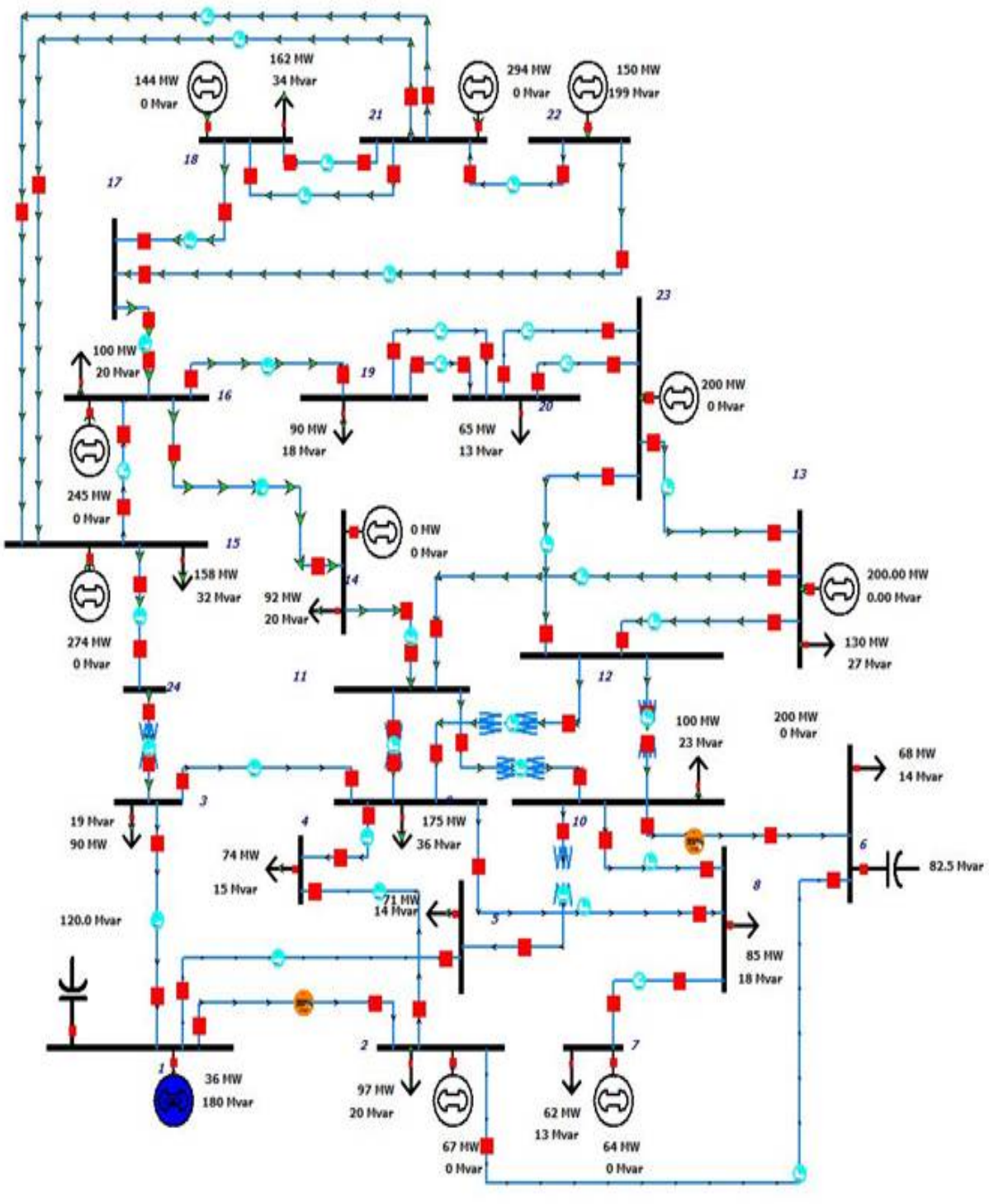

Figure A.1: IEEE 24 Bus System [145]

Bibliography

[1] D. Ton and M. Smith, "The U.S. Department of Energy's Microgrid Initiative." The Electricity Journal, 2012, online: https://www.energy.gov/sites/prod/files/2016/06/f32/The

[2] F. Nejabatkhah, Y. W. Li and H. Tian, "Power Quality Control of Smart Hybrid AC/DC Microgrids: An Overview," in IEEE Access, vol. 7, pp. 52295-52318, 2019, doi: 10.1109/ACCESS.2019.2912376.

[3] M. Glinkowski et al., ''Data center power system harmonics: An overview of effects on data center efficiency and reliability,'' Green Grid Assoc., 2014.

[4] C.-L. Su, J.-T. Yu, H.-M. Chin, and C.-L. Kuo, ''Evaluation of power-quality field measurements of an electric bus charging station using remote monitoring systems,'' in Proc. 10th Int. Conf. Compat., Power Electron. Power Eng. (CPE-POWERENG), Bydgoszcz, Poland, Jun./Jul. 2016, pp. 58–63.

[5] Q. Li, S. Tao, X. Xiao, and J. Wen, ''Monitoring and analysis of power quality in electric vehicle charging stations,'' in Proc. 1st Int. Future Energy Electron. Conf. (IFEEC), Tainan, Taiwan, Nov. 2013, pp. 277–282.

[6] S. M. M. Gazafrudi, A. T. Langerudy, E. F. Fuchs, and K. Al-Haddad, ''Power quality issues in railway electrification: A comprehensive perspective,'' IEEE Trans. Ind. Electron., vol. 62, no. 5, pp. 3081–3090, May 2015.

[7] K. Pham, R. S. Thomas, and W. Stinger, Jr, "Operational and safety considerations for light rail DC traction electrification system design," in Proc. Transp. Res. Circular E-CO58: 9th Nat. Light Rail Transit Conf., 2003, pp. 650–668.

[8] Y. Pan, P. Silveira, M. Steurer, T. Baldwin, and P. Ribeiro, “A fault location approach for high-impedance grounded DC shipboard power distribution systems,” in Proc. IEEE Power Energy Soc. Gen. Meet.—Convers. Del. Elect. Energy 21st Century, 2008, pp. 1–6.

[9] X. Wang et al., “Grounding fault location in DC railway system,” in Proc. 22nd Int. CIRED, Jun. 2013, pp. 1–4.

[10] C. Dong et al., “High-resistance grounding fault detection and location in DC railway system,” in Proc. 11th Int. Conf. Develop. Power Syst. Protection, 2012, pp. 1–5.

[11] J. -D. Park, ”Ground Fault Detection and Location for Ungrounded DC Traction Power Systems,” in IEEE Transactions on Vehicular Technology, vol. 64, no. 12, pp. 5667-5676, Dec. 2015, doi: 10.1109/TVT.2015.2388785.

[12] S. Sahoo, S. Mishra, S. Jha, and B. Singh, “A cooperative adaptive droop based energy management and optimal voltage regulation scheme for dc microgrids,” IEEE Trans. Ind. Electron., vol. 67, no. 4, pp. 2894–2904, Apr. 2020.

[13] Queiroz C, Mahmood A, Tari Z. SCADASim – a framework for building SCADA simulations. IEEE Transactions on Smart Grid 2011; 2(4):589–597.

[14] A. Vasilakis, I. Zafeiratou, D. T. Lagos, and N. D. Hatziargyriou, “The evolution of research in microgrids control,” IEEE Open Access J. Power Energy, vol. 7, pp. 331–343, Oct. 2020.

[15] S. Mousavian, J. Valenzuela and J. Wang, ”A Probabilistic Risk Mitigation Model for Cyber-Attacks to PMU Networks,” in IEEE Transactions on Power Systems, vol. 30, no. 1, pp. 156-165, Jan. 2015, doi: 10.1109/TPWRS.2014.2320230.

[16] C. K. Veitch, J. M. Henry, B. T. Richardson, and D. H. Hart, “Microgrid cyber se-

curity reference architecture," Sandia Nat. Lab., Albuquerque, NM, USA, Tech. Rep. SAND2013-5472, 2013.

[17] S. Sahoo, J. C. H. Peng, A. Devakumar, S. Mishra, and T. Dragicevic, "On detection of false data in cooperative dc microgrids—A discordant element approach," IEEE Trans. Ind. Electron., vol. 67, no. 8, pp. 6562–6571, Aug. 2020.

[18] J. De La Ree, V. Centeno, J. S. Thorp, and A. G. Phadke, "Synchronized phasor measurement applications in power systems," IEEE Transactions on Smart Grid, vol. 1, no. 1, pp. 20–27, 2010.

[19] V. Terzija, G. Valverde, D. Cai, P. Regulski, V. Madani, J. Fitch, S. Skok, M. M. Begovic, and A. Phadke, "Wide-area monitoring, protection, and control of future electric power networks," Proceedings of the IEEE, vol. 99, no. 1, pp. 80–93, 2011.

[20] M. Kezunovic, S. Meliopoulos, V. Venkatasubramanian, and V. Vittal, "Application of Time-Synchronized Measurements in Power System Transmission Networks," 2014.

[21] G. B. Giannakis, V. Kekatos, N. Gatsis, S. J. Kim, H. Zhu, and B. F. Wollenberg, "Monitoring and optimization for power grids: A signal processing perspective," IEEE Signal Processing Magazine, vol. 30, no. 5, pp. 107–128, 2013.

[22] Phadke, A.G., Thorp, J.S.: Synchronized phasor measurements and their applications, vol. 1. Springer, New York (2008)

[23] IEEE Power and Energy Society, "IEEE Std C37.118.2-2011 (Revision of IEEE Std C37.118-2005) - IEEE Standard for Synchrophasor Data Transfer for Power Systems.," IEEE Standards, 2011.

[24] C. Tu, X. He, Z. Shuai, and F. Jiang, "Big data issues in smart grid – A review," Renewable and Sustainable Energy Reviews, vol. 79, pp. 1099–1107, 11 2017.

[25] W. Li, L. Vanfretti, and J. H. Chow, "Pseudo-Dynamic Network Modeling for PMU-Based State Estimation of Hybrid AC/DC Grids," IEEE Access, vol. 6, pp. 4006–4016, 11 2017.

[26] Z. Shuai, W. Huang, C. Shen, J. Ge, and Z. J. Shen, "Characteristics and Restraining Method of Fast Transient Inrush Fault Currents in Synchronverters," IEEE Transactions on Industrial Electronics, vol. 64, pp. 7487–7497, 9 2017.

[27] M. N. Aman, K. Javed, B. Sikdar, and K. C. Chua, "Detecting data tampering attacks in synchrophasor networks using time hopping," IEEE PES Innovative Smart Grid Technologies Conference Europe, 7 2016.

[28] O. Vukovic and G. Dan, "Security of fully distributed power system state estimation: Detection and mitigation of data integrity attacks," IEEE Journal on Selected Areas in Communications, vol. 32, no. 7, pp. 1500– 1508, 2014.

[29] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using kalman filter," IEEE Transactions on Control of Network Systems, vol. 1, no. 4, pp. 370–379, 2014.

[30] S. Mousavian, J. Valenzuela, and J. Wang, "A Probabilistic risk mitigation model for cyber-attacks to PMU networks," IEEE Transactions on Power Systems, vol. 30, no. 1, pp. 156–165, 2015.

[31] C. Tu, X. He, X. Liu, and P. Li, "Cyber-attacks in PMU-based power network and countermeasures," IEEE Access, vol. 6, pp. 65594–65603, 2018.

[32] https://www.loc.gov/everyday-mysteries/item/what-is-gps-how-does-it-work/.

[33] A. J. Kerns, K. D. Wesson, and T. E. Humphreys, "A blueprint for civil gps navi-

gation message authentication," in 2014 IEEE/ION Position, Location and Navigation Symposium - PLANS 2014, pp. 262–269, 2014.

[34] A. Grant, P. Williams, N. Ward, and S. Basker, "Gps jamming and the impact on maritime navigation," Journal of Navigation, vol. 62, no. 2, p. 173–187, 2009.

[35] B. Pardhasaradhi, P. Srihari, and P. Aparna, "Navigation in gps spoofed environment using m-best positioning algorithm and data association," IEEE Access, vol. 9, pp. 51536–51549, 2021.

[36] P. Bethi, S. Pathipati, and A. P, "Stealthy gps spoofing: Spoofer systems, spoofing techniques and strategies," in 2020 IEEE 17th India Council International Conference (INDICON), pp. 1–7, 2020.

[37] X. Wei and B. Sikdar, "Impact of gps time spoofing attacks on cyber physical systems," in 2019 IEEE International Conference on Industrial Technology (ICIT), pp. 1155–1160, 2019.

[38] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, "Evaluation of the vulnerability of phasor measurement units to gps spoofing attacks," International Journal of Critical Infrastructure Protection, vol. 5, no. 3, pp. 146–153, 2012.

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

[40] L. D. Scott, "Anti-spoofing and authenticated signal architectures for civil navigation systems," 2003.

[41] O. Pozzobon, L. Canzian, M. Danieletto, and A. D. Chiara, "Antispoofing and open gnss signal authentication with signal authentication sequences," in 2010 5th ESA Workshop

on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), pp. 1–6, 2010.

[42] 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 Transactions on Smart Grid, vol. 6, no. 6, pp. 2659–2668, 2015.

[43] X. Wei, M. N. Aman, and B. Sikdar, "Exploiting correlation among gps signals to detect gps spoofing in power grids," IEEE Transactions on Industry Applications, vol. 58, no. 1, pp. 697–708, 2022.

[44] E. Shereen, M. Delcourt, S. Barreto, G. Dan, J.-Y. Le Boudec, and ´ M. Paolone, "Feasibility of time-synchronization attacks against pmubased state estimation," IEEE Transactions on Instrumentation and Measurement, vol. 69, no. 6, pp. 3412–3427, 2020

[45] R. Ma, S. Basumallik, S. Eftekharnejad, and F. Kong, "Recovery-based model predictive control for cascade mitigation under cyber-physical attacks," 2020 IEEE Texas Power and Energy Conference, TPEC 2020, 2020.

[46] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," IEEE Transactions on Smart Grid, vol. 5, pp. 612–621, 3 2014.

[47] P. Gao, M. Wang, J. H. Chow, S. G. Ghiocel, B. Fardanesh, G. Stefopoulos, and M. P. Razanousky, "Identification of successive 'Unobservable' cyber data attacks in power systems through matrix decomposition," IEEE Transactions on Signal Processing, vol. 64, no. 21, pp. 5557– 5570, 2016.

[48] T. T. Kim and H. V. Poor, "Attacks on Power Grids," IEEE Transactions on Smart Grid, vol. 2, no. 2, pp. 326–333, 2011.

[49] Y. Hao, M. Wang, J. H. Chow, E. Farantatos and M. Patel, "Modelless Data Quality Improvement of Streaming Synchrophasor Measurements by Exploiting the Low-Rank Hankel Structure," in IEEE Transactions on Power Systems, vol. 33, no. 6, pp. 6966-6977, Nov. 2018, doi: 10.1109/TPWRS.2018.2850708.

[50] H. Zhong, D. Du, C. Li, and X. Li, "A novel sparse false data injection attack method in smart grids with incomplete power network information," Complexity, vol. 2018, p. 1–16, 2018.

[51] Z. Zhao, Y. Huang, Z. Zhen, and Y. Li, "Data-driven false data injection attack design and detection in cyber-physical systems," IEEE Transactions on Cybernetics, vol. 51, no. 12, pp. 6179–6187, 2021.

[52] M. Wang, P. Gao, S. G. Ghiocel, J. H. Chow, B. Fardanesh, G. Stefopoulos, and M. P. Razanousky, "Identification of "unobservable" cyber data attacks on power grids," in 2014 IEEE International Conference on Smart Grid Communications (SmartGridComm), pp. 830–835, 2014.

[53] Y. Li and Y. Wang, "False Data Injection Attacks with Incomplete Network Topology Information in Smart Grid," IEEE Access, vol. 7, pp. 3656–3664, 2019.

[54] X. Liu and Z. Li, "False data attacks against ac state estimation with incomplete network information," IEEE Transactions on Smart Grid, vol. 8, no. 5, pp. 2239–2248, 2017.

[55] https://www.naspi.org/sites/default/files/202203/20220330_naspi_webinar_caiso.pdf

[56] Das, Shuvangkar and Vu, Tuyen. (2022). Scalable Cyber-Physical Testbed for Cybersecurity Evaluation of Synchrophasors in Power Systems. 10.48550/arXiv.2207.12610.

[57] Cui, H., Li, F. and Tomsovic, K. (2020), Cyber-physical system testbed for power system monitoring and wide-area control verification. IET Energy Syst. Integr., 2: 32-39. https://doi.org/10.1049/iet-esi.2019.0084

[58] Astha Chawla, Mohd. Asim Aftab, S.M. Suhail Hussain, B.K. Panigrahi, Taha Selim Ustun, Cyber–physical testbed for Wide Area Measurement System employing IEC 61850 and IEEE C37.118 based communication, Energy Reports, Volume 8, Supplement 10, 2022, Pages 570-578, ISSN 2352-4847, https://doi.org/10.1016/j.egyr.2022.05.207.

[59] Stifter, M.; Cordova, J.; Kazmi, J.; Arghandeh, R. Real-Time Simulation and Hardware-in-the-Loop Testbed for Distribution Synchrophasor Applications. Energies 2018, 11, 876. https://doi.org/10.3390/en11040876

[60] P. Kersey, " Applications of PMUsimulator in PDC Testing", Master Thesis, Virginia Tech, April 27th, 2012.

[61] https://www.opal-rt.com/

[62] https://www.gridprotectionalliance.org/

[63] https://www.wireshark.org/

[64] Khan, I., and Centeno, V. (2023). Undetectable gps-spoofing attack on time series phasor measurement unit data. arXiv: 2206.12440 [eess.SY]. Retrieved from: https://arxiv.org/abs/2206.12440

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

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

[67] X. Jiang, J. Zhang, B. J. Harding, J. J. Makela, and A. D. Dom´ınguez- Garc´ıa, "Spoofing GPS receiver clock offset of phasor measurement units," IEEE Transactions on Power Systems, vol. 28, no. 3, pp. 3253– 3262, 2013.

[68] I. Akkaya, E. A. Lee, and P. Derler, "Model-based evaluation of GPS spoofing attacks on power grid sensors," 2013 Workshop on Modeling and Simulation of Cyber-Physical Energy Systems, MSCPES 2013, 2013.

[69] O. Vukovic and G. Dan, "Security of fully distributed power system state estimation: Detection and mitigation of data integrity attacks," IEEE Journal on Selected Areas in Communications, vol. 32, no. 7, pp. 1500– 1508, 2014.

[70] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious Data Attacks on Smart Grid State Estimation: Attack Strategies and Countermeasures," pp. 220–225, 11 2010.

[71] LiuYao, NingPeng, and R. K., "False data injection attacks against state estimation in electric power grids," ACM Transactions on Information and System Security (TISSEC), vol. 14, p. 33, 6 2011.

[72] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systems-attacks, impacts, and defense: A survey," IEEE Transactions on Industrial Informatics, vol. 13, pp. 411–423, 4 2017.

[73] S. Barreto, M. Pignati, G. D´an, J. Y. Le Boudec, and M. Paolone, "Un- detectable Timing-Attack on Linear State-Estimation by Using Rank-1 Approximation," IEEE Transactions on Smart Grid, vol. 9, pp. 3530– 3542, 7 2018.

[74] G. B. Huang, Q. Y. Zhu, and C. K. Siew, "Extreme learning machine: Theory and applications," Neurocomputing, vol. 70, pp. 489–501, 12 2006.

[75] L. Zhu et al., "A Comprehensive Method to Mitigate Forced Oscillations in Large Interconnected Power Grids," in IEEE Access, vol. 9, pp. 22503-22515, 2021, doi: 10.1109/ACCESS.2021.3056123.,

[76] S. A. N. Sarmadi, V. Venkatasubramanian, and A. Salazar, ''Analysis of November 29, 2005 western American oscillation event,'' IEEE Trans. Power Syst., vol. 31, no. 6, pp. 5210–5211, Nov. 2016.

[77] J. Seppänen, M. Lehtonen, M. Kuivaniemi and L. Haarla, "Forced Oscillation and Inter-Area Mode Resonance-Effect of the Location of the Oscillation Source," 2022 IEEE Power and Energy Society General Meeting (PESGM), Denver, CO, USA, 2022, pp. 1-5, doi: 10.1109/PESGM48719.2022.9917223.,

[78] X. Zhao, Y. Xue and X. -P. Zhang, "Isolation and Suppression of Forced Oscillations Through Wind Farms Under Grid Following and Grid Forming Control," in IEEE Access, vol. 9, pp. 76446-76460, 2021, doi: 10.1109/ACCESS.2021.3082166.

[79] B. C. Lesieutre, Y. Abdennadher and S. Roy, "Model-Enhanced Localization of Forced Oscillation Using PMU Data," 2022 58th Annual Allerton Conference on Communication, Control, and Computing (Allerton), Monticello, IL, USA, 2022, pp. 1-8, doi: 10.1109/Allerton49937.2022.9929378.

[80] T. Huang, N. M. Freris, P. R. Kumar and L. Xie, "Localization of forced oscillations in the power grid under resonance conditions," 2018 52nd Annual Conference on Information Sciences and Systems (CISS), Princeton, NJ, USA, 2018, pp. 1-5, doi: 10.1109/CISS.2018.8362302.

[81] F. Ghorbaniparvar and H. Sangrody, "PMU application for locating the source of forced oscillations in smart grids," 2018 IEEE Power and Energy Conference at Illinois (PECI), Champaign, IL, USA, 2018, pp. 1-5, doi: 10.1109/PECI.2018.8334996.

[82] A. Canafe, Y. Liu, L. Yang and H. Livani, "DCCA Enhanced Forced Oscillation Frequency Detection Using Real-world PMU Data," 2022 IEEE Texas Power and Energy Conference (TPEC), College Station, TX, USA, 2022, pp. 1-6, doi: 10.1109/TPEC54980.2022.9750846.

[83] https://www.naspi.org/sites/default/files/2022-03/20220330_naspi_webinar_caiso.pdf

[84] https://www.wecc.org/Reliability/WECC%20JSIS%20Modes%20of%20Inter-Area%20Oscillations-2013-12-REV1.1.pdf

[85] E. Shereen, M. Delcourt, S. Barreto, G. D´an, J.-Y. Le Boudec, and M. Paolone, "Feasibility of time-synchronization attacks against pmu- based state estimation," IEEE Transactions on Instrumentation and Measurement, vol. 69, no. 6, pp. 3412–3427, 2020.

[86] S. Mousavian, J. Valenzuela, and J. Wang, "A Probabilistic risk mitiga- tion model for cyber-attacks to PMU networks," IEEE Transactions on Power Systems, vol. 30, no. 1, pp. 156–165, 2015.

[87] D. Mukherjee, "Data-driven false data injection attack: A low-rank approach," IEEE Transactions on Smart Grid, pp. 1–1, 2022.

[88] K. Manandhar, X. Cao, F. Hu, and Y. Liu, "Detection of faults and attacks including false data injection attack in smart grid using kalman filter," IEEE Transactions on Control of Network Systems, vol. 1, no. 4, pp. 370–379, 2014.

[89] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data- injection attacks against power system state estimation: Modeling and countermeasures," Parallel and Distributed Systems, IEEE Transactions on, vol. 25, pp. 717–729, 03 2014.

[90] C. Pei, Y. Xiao, W. Liang, and X. Han, "A deviation-based detection method against false data injection attacks in smart grid," IEEE Access, vol. 9, pp. 15499–15509, 2021.

[91] "IEEE Guide for Phasor Data Concentrator Requirements for Power System Protection, Control, andMonitoring," in IEEE Std C37.244-2013 , vol., no., pp.1-65, 10 May 2013, doi: 10.1109/IEEESTD.2013.6514039.

[92] I. Khan and V. Centeno, "Detecting GPS-spoofing Attack on PMU Data with Phase Angle Unwrapping Technique and Low-Rank Approximation of Hankel Matrix," 2022 IEEE Power and Energy Society General Meeting (PESGM), 2022, pp. 1-5, doi: 10.1109/PESGM48719.2022.9916859.

[93] I. Khan and V. Centeno, "real-time detection of pmu bad data and sequential bad data classifications in cyber-physical testbed," IEEE Access, vol. 11, pp. 71235–71249, 2023.

[94] M. Conti, N. Dragoni, and V. Lesyk, "A survey of man in the middle attacks," IEEE Commun. Surv. Tut., vol. 18, no. 3, pp. 2027–2051, Jul.–Sep. 2016.

[95] S. Sahoo, T. Dragičević and F. Blaabjerg, "Multilayer Resilience Paradigm Against Cyber Attacks in DC Microgrids," in IEEE Transactions on Power Electronics, vol. 36, no. 3, pp. 2522-2532, March 2021, doi: 10.1109/TPEL.2020.3014258.

[96] J. Zhao, L. Mili, and M. Wang, ''A generalized false data injection attacks against power system nonlinear state estimator and countermeasures,'' IEEE Trans. Power Syst., vol. 33, no. 5, pp. 4867–4877, May 2018.

[97] J. Kim, L. Tong, and R. J. Thomas, ‘‘Subspace methods for data attack on state estimation: A data driven approach,’’ IEEE Trans. Signal Process., vol. 63, no. 5, pp. 1102–1114, May 2014.

[98] J. Hao, R. J. Piechocki, D. Kaleshi, W. H. Chin and Z. Fan, ”Sparse Malicious False Data Injection Attacks and Defense Mechanisms in Smart Grids,” in IEEE Transactions on Industrial Informatics, vol. 11, no. 5, pp. 1-12, Oct. 2015, doi: 10.1109/TII.2015.2475695.

[99] 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 Transactions on Smart Grid, vol. 6, no. 6, pp. 2659–2668, Nov 2015.

[100] Z. Zhang, S. Gong, A. Dimitrovski, and H. Li, “Time synchronization attack in smart grid: Impact and analysis,” IEEE Transactions on Smart Grid, vol. 4, no. 1, pp. 87–98, March 2013.

[101] B. Pardhasaradhi, P. Srihari, and P. Aparna, “Navigation in gps spoofed environment using m-best positioning algorithm and data association,” IEEE Access, vol. 9, pp. 51536–51549, 2021.

[102] D. P. Shepard, T. E. Humphreys, and A. A. Fansler, “Evaluation of the vulnerability of Phasor Measurement Units to gps spoofing attacks,” International Journal of Critical Infrastructure Protection, vol. 5, no. 3, pp. 146–153, 2012.

[103] Konstantinou, Charalambos; Sazos, Marios; Musleh, Ahmed S.; Keliris, Anastasis; Al-Durra, Ahmed; Maniatakos, Michail: ’GPS spoofing effect on phase angle monitoring and control in a real-time digital simulator-based hardware-in-the-loop environment’, IET Cyber-Physical Systems: Theory and Applications, 2017, 2, (4), p. 180-187, DOI: 10.1049/iet-cps.2017.0033

[104] M. M. Rana, L. Li, and S. W. Su, "Cyber attack protection and control of microgrids," IEEE/CAA J. Automatica Sinica, vol. 5, no. 2, pp. 602–609, Mar. 2018.

[105] D. Jin et al., "Toward a cyber resilient and secure microgrid using software-defined networking," IEEE Trans. Smart Grid, vol. 8, no. 5, pp. 2494–2504, Sep. 2017.

[106] Y. Li, P. Zhang, L. Zhang, and B. Wang, "Active synchronous detection of deception attacks in microgrid control systems," IEEE Trans. Smart Grid, vol. 8, no. 1, pp. 373–375, Jan. 2017.

[107] G. Intriago and Y. Zhang, "Online Dictionary Learning Based Fault and Cyber Attack Detection for Power Systems," 2021 IEEE Power and Energy Society General Meeting (PESGM), 2021, pp. 1-5, doi: 10.1109/PESGM46819.2021.9637891.

[108] Y. Zhao, X. Jia, D. An and Q. Yang, "LSTM-Based False Data Injection Attack Detection in Smart Grids," 2020 35th Youth Academic Annual Conference of Chinese Association of Automation (YAC), Zhanjiang, China, 2020, pp. 638-644, doi: 10.1109/YAC51587.2020.9337674.

[109] B. D. Barros, N. K. D. Venkategowda and S. Werner, "Quickest Detection of Stochastic False Data Injection Attacks with Unknown Parameters," 2021 IEEE Statistical Signal Processing Workshop (SSP), Rio de Janeiro, Brazil, 2021, pp. 426-430, doi: 10.1109/SSP49050.2021.9513837.

[110] F. Ünal, A. Almalaq, S. Ekici and P. Glauner, "Big Data-Driven Detection of False Data Injection Attacks in Smart Meters," in IEEE Access, vol. 9, pp. 144313-144326, 2021, doi: 10.1109/ACCESS.2021.3122009.

[111] S. Mohammadi, F. Eliassen, Y. Zhang and H. -A. Jacobsen, "Detecting False Data Injection Attacks in Peer to Peer Energy Trading Using machine learning," in IEEE

Transactions on Dependable and Secure Computing, vol. 19, no. 5, pp. 3417-3431, 1 Sept.-Oct. 2022, doi: 10.1109/TDSC.2021.3096213.

[112] D. Huang, X. Shi and W. -A. Zhang, "False Data Injection Attack Detection for Industrial Control Systems Based on Both Time- and Frequency-Domain Analysis of Sensor Data," in IEEE Internet of Things Journal, vol. 8, no. 1, pp. 585-595, 1 Jan.1, 2021, doi: 10.1109/JIOT.2020.3007155.

[113] J. J. Q. Yu, Y. Hou and V. O. K. Li, "Online False Data Injection Attack Detection With Wavelet Transform and Deep Neural Networks," in IEEE Transactions on Industrial Informatics, vol. 14, no. 7, pp. 3271-3280, July 2018, doi: 10.1109/TII.2018.2825243.

[114] Y. Hao,M.Wang, J. H. Chow, E. Farantatos, andM. Patel, "Model-less data quality improvement of streaming synchrophasor measurements by exploiting the low-rank Hankel structure," IEEE Trans. Power Syst., vol. 33, no. 6, pp. 6966–6977, Nov. 2018.

[115] Y. Hao, M. Wang, J. H. Chow, E. Farantatos and M. Patel, "Modelless Data Quality Improvement of Streaming Synchrophasor Measurements by Exploiting the Low-Rank Hankel Structure," in IEEE Transactions on Power Systems, vol. 33, no. 6, pp. 6966-6977, Nov. 2018, doi: 10.1109/TPWRS.2018.2850708.

[116] S. Zhang and M. Wang, "Correction of Corrupted Columns Through Fast Robust Hankel Matrix Completion," in IEEE Transactions on Signal Processing, vol. 67, no. 10, pp. 2580-2594, 15 May15, 2019, doi: 10.1109/TSP.2019.2904021.

[117] M. Yi, M. Wang, T. Hong and D. Zhao, "Bayesian High-Rank Hankel Matrix Completion for Nonlinear Synchrophasor Data Recovery," in IEEE Transactions on Power Systems, vol. 39, no. 1, pp. 2198-2208, Jan. 2024, doi: 10.1109/TPWRS.2023.3254909.

[118] M. Yi, M. Wang, E. Farantatos, and T. Barik. "Bayesian robust hankel matrix completion with uncertainty modeling for synchrophasor data recovery". SIGENERGY Energy Inform. Rev. 2, 1 (February 2022), 1–19. https://doi.org/10.1145/3527579.3527580

[119] A. Mohammad Saber, A. Youssef, D. Svetinovic, H. H. Zeineldin and E. F. El-Saadany, "Anomaly-Based Detection of Cyberattacks on Line Current Differential Relays," in IEEE Transactions on Smart Grid, vol. 13, no. 6, pp. 4787-4800, Nov. 2022, doi: 10.1109/TSG.2022.3185764.

[120] S. Siamak, M. Dehghani and M. Mohammadi, "Dynamic GPS Spoofing Attack Detection, Localization, and Measurement Correction Exploiting PMU and SCADA," in IEEE Systems Journal, vol. 15, no. 2, pp. 2531-2540, June 2021, doi: 10.1109/JSYST.2020.3001016.

[121] S. Barreto, M. Pignati, G. Dán, J. -Y. Le Boudec and M. Paolone, "Undetec Table Timing-Attack on Linear State-Estimation by Using Rank-1 Approximation," in IEEE Transactions on Smart Grid, vol. 9, no. 4, pp. 3530-3542, July 2018, doi: 10.1109/TSG.2016.2634124.

[122] M. Mardani, G. Mateos, and G. Giannakis, "Recovery of low-rank plus compressed sparse matrices with application to unveiling traffic anomalies," IEEE Trans. Inf. Theory, vol. 59, no. 8, pp. 5186–5205, Aug. 2013

[123] R. Otazo, E. Candès, and D. K. Sodickson, "Low-rank plus sparse matrix decomposition for accelerated dynamic MRI with separation of background and dynamic components," Magn. Reson. Medicine, vol. 73, no. 3, pp. 1125–1136, 2015.

[124] J. Wright, A. Ganesh, S. Rao, Y. Peng, and Y. Ma, "Robust principal component analysis: Exact recovery of corrupted low-rank matrices via convex optimization," in Proc. Adv. Neural Inf. Process. Syst., 2009, pp. 2080– 2088.

[125] M. Liao, D. Shi, Z. Yu, Z. Yi, Z. Wang, and Y. Xiang, "An alternating direction method of multipliers based approach for PMU data recovery," IEEE Trans. Smart Grid, vol. 10, no. 4, pp. 4554–4565, Jul. 2019.

[126] C. Genes, I. Esnaola, S. M. Perlaza, L. F. Ochoa, and D. Coca, "Robust recovery of missing data in electricity distribution systems," IEEE Trans. Smart Grid, vol. 10, no. 4, pp. 4057–4067, Jul. 2019.

[127] S. Zhang, Y. Hao, M. Wang, and J. H. Chow, "Multi channel missing data recovery by exploiting the low-rank hankel structures," in Proc. Int. Workshop Comput. Adv. Multi-Sensor Adapt. Process., 2017, pp. 1–5

[128] Al-Homidan, S. Hankel matrix transforms and operators. J Inequal Appl 2012, 92 (2012). https://doi.org/10.1186/1029-242X-2012-92

[129] Ahmad, E., Ozel, C., and Koyuncu, S. (2024). Topology of hankel matrices and applications. Journal of Geometry and Physics, 199, 105150. https://doi.org/10.1016/j.geomphys.2024.105150

[130] M. Fazel, T. K. Pong, D. Sun, and P. Tseng, "Hankel matrix rank minimization with applications to system identification and realization," SIAM J. Matrix Anal. Appl., vol. 34, no. 3, pp. 946–977, 2013.

[131] S. Zhang and M. Wang, "Correction of corrupted columns through fast robust Hankel matrix completion," IEEE Trans. Signal Process., vol. 67, no. 10, pp. 2580–2594, May 2019.

[132] S. Zhang, Y. Hao, M. Wang, and J. H. Chow, "Multichannel Hankel matrix completion through nonconvex optimization," IEEE J. Sel. Topics Signal Process., vol. 12, no. 4, pp. 617–632, Aug. 2018.

[133] J. -F. Cai, T. Wang, and K. Wei, “Fast and provable algorithms for spectrally sparse signal reconstruction via low-rank Hankel matrix completion,” Appl. Comput. Harmon. Anal., vol. 46, no. 1, pp. 94–121, 201

[134] R. Deng, G. Xiao, R. Lu, H. Liang and A. V. Vasilakos, ”False Data Injection on State Estimation in Power Systems—Attacks, Impacts, and Defense: A Survey,” in IEEE Transactions on Industrial Informatics, vol. 13, no. 2, pp. 411-423, April 2017, doi: 10.1109/TII.2016.2614396.

[135] K. Manandhar, X. Cao, F. Hu and Y. Liu, ”Detection of Faults and Attacks Including False Data Injection Attack in Smart Grid Using Kalman Filter,” in IEEE Transactions on Control of Network Systems, vol. 1, no. 4, pp. 370-379, Dec. 2014, doi: 10.1109/TCNS.2014.2357531.

[136] C. Pei, Y. Xiao, W. Liang and X. Han, ”A Deviation-Based Detection Method Against False Data Injection Attacks in Smart Grid,” in IEEE Access, vol. 9, pp. 15499-15509, 2021, doi: 10.1109/ACCESS.2021.3051155.

[137] G. M. De Mijolla, S. Konstantinopoulos, P. Gao, J. H. Chow and M. Wang, ”An Evaluation of Algorithms for Synchrophasor Missing Data Recovery,” 2018 Power Systems Computation Conference (PSCC), 2018, pp. 1-6, doi: 10.23919/PSCC.2018.8442776.

[138] A. Xue et al., ”Correction of Time-varying PMU Phase Angle Deviation with Unknown Transmission Line Parameters,” in CSEE Journal of Power and Energy Systems, vol. 9, no. 1, pp. 315-325, January 2023, doi: 10.17775/CSEEJPES.2021.07280.

[139] https://iitbpdc.sourceforge.net/

[140] https://github.com/GridProtectionAlliance/OpenECA

[141] "IEEE Standard for Synchrophasor Data Transfer for Power Systems," in IEEE Std C37.118.2-2011 (Revision of IEEE Std C37.118-2005) , vol., no., pp.1-53, 28 Dec. 2011, doi: 10.1109/IEEESTD.2011.6111222

[142] https://cmte.ieee.org/pes-testfeeders/resources/

[143] https://electricgrids.engr.tamu.edu/electric-grid-test-cases/ieee-118-bus-system

[144] C. Grigg, P. Wong, P. Albrecht, R. Allan, M. Bhavaraju, R. Billinton, Q. Chen, C. Fong, S. Haddad, S. Kuruganty, W. Li, R. Mukerji, D. Patton, N. Rau, D. Reppen, A. Schneider, M. Shahidehpour, and C. Singh, "The ieee reliability test system-1996. a report prepared by the reliability test system task force of the application of probability methods subcommittee," IEEE Transactions on Power Systems, vol. 14, no. 3, pp. 1010–1020, 1999.

[145] https://icseg.iti.illinois.edu/ieee-24-bus-system/ieee-24-bus/