Detection and Elimination of Denial-of-Service Attack Using Supervised Machine Learning Considering Heterogeneous Measurements

A

Thesis

Submitted in partial fulfillment of the requirements for the

Degree of

MASTER OF TECHNOLOGY

by

Akesh Kotnana

(224102102)

Under the Supervision of

Dr. Sreenath J G

Department of Electronics and Electrical Engineering

Indian Institute of Technology, Guwahati

May. 2024

Declaration

This is to certify that the thesis entitled "**Detection and Elimination of Denial-of-Service Attack Using Supervised Machine Learning Considering Heterogeneous Measurements**", submitted by me to the Indian Institute of Technology Guwahati, for the award of the degree of M.Tech, is a bonafide work carried out by me under the supervision of **Dr. Sreenath J G**. The content of this thesis, in full or in parts, have not been submitted to any other University or Institute for the award of any degree.

Akesh Kotnana

Department of Electronics and Electrical Engineering,
Indian Institute of Technology Guwahati, Assam.

Certificate

This is to certify that the work contained in this thesis entitled "**Detection and Elimination of Denial-of-Service Attack Using Supervised Machine Learning Considering Heterogeneous Measurements**" is a bonafide work of **Akesh Kotnana** (**Roll No. 224102102**), carried out in the Department of Electronics and Electrical Engineering, Indian Institute of Technology, Guwahati under my supervision and it has not been submitted elsewhere for a degree.

Supervisor: **Dr. Sreenath J G**

Assistant Professor,

May, 2024

Department of Electronics and Electrical Engineering,

Guwahati.

Indian Institute of Technology Guwahati, Assam.

Acknowledgements

First and foremost, I feel it as a great privilege in expressing my deepest and most sincere gratitude to my supervisor **Dr. Sreenath J G** for their excellent guidance throughout my study. Your expertise and mentor ship have shaped my research and academic growth. Your patience and insightful suggestions have motivated me to strive for excellence. I am truly grateful for the knowledge and skills I have gained under your guidance.

I would like to express my gratitude to the faculty members of IIT Guwahati for their valuable insights and encouragement. Their commitment to knowledge and critical thinking has inspired me.

I am deeply thankful to my family for their unwavering love, encouragement, and belief in my abilities. Their support has been my source of strength during challenging times.

To my friends, thank you for your constant support and uplifting spirits. Our discussions and shared laughter have made this journey memorable.

Sincerely

Akesh Kotnana

Abstract

Cyber systems are essential for enhancing power system operation's dependability and efficiency as well as making sure the system stays within safe operating parameters. An adversary can compromise the cyber layer's enabled control and monitoring applications, thereby causing significant harm to the physical system underneath.Distribution system state estimation (DSSE) is a critical task for the reliable and efficient operation of power distribution systems. It involves estimating the voltage and current magnitudes at all nodes in a distribution network using a limited set of measurements. Traditional DSSE methods, such as weighted least squares (WLS), are often inaccurate and computationally expensive, especially for large and complex distribution networks.Machine learning (ML) has emerged as a promising tool for DSSE due to its ability to learn complex relationships from data. In recent years, several ML-based DSSE methods have been proposed, showing significant improvements in accuracy and efficiency compared to traditional methods. This abstract provides an overview of ML-based DSSE methods, focusing on their advantages and challenges. The decision tree model is used for estimating the states of the cyber-physical power system(CPPS). The IEEE 33 bus distribution system is considered for this study. Both static and dynamic state estimation are implemented using one of the supervised machine learning models known as the decision tree model.One of major cyber attack known as DoS attack is discussed,a data driven estimation method for the attack interval is analyzed.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

This chapter introduces basic power system state estimation and what are the different types of conventional estimation techniques we are using. The importance of state estimation is discussed with a brief history of the past events that happened in the power system.

1.1 Background

1.1.1 Power System State Estimation and its significance

A power system, also known as an electrical power system, is a complex network designed to generate, transmit, and distribute electrical energy to meet the demands of consumers. It comprises various components, including power plants that generate electricity, transmission lines to carry the power over long distances, substations for voltage transformation, and distribution networks that deliver electricity to end-users. Distribution systems are generally planned to function in a radial layout, featuring feeders that extend from distribution substations and branch out across the distribution area, resembling a tree-like structure [1]. In the period between 1969 and 1974, Schweppe introduced the weighted least-squares method for addressing static state estimation challenges in power networks. This approach presupposes that a network topology processor has thoroughly analyzed a bus-section/switching-device model, leading to a seamless bus/branch model [2, 3].

Need for state estimation:

Power system operation is overseen by system operators from area control centers. Their primary objective is to maintain the system's normal secure state throughout the day's

changing operating conditions. To achieve this goal, the system conditions must be continuously monitored, the operating state must be identified, and appropriate control actions must be taken [1].

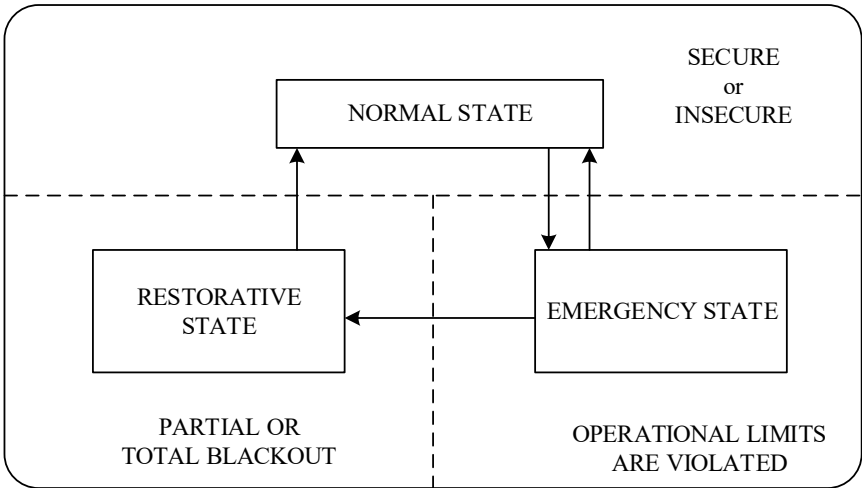


Figure 1.1: Security states of Power system

In the year 2000, attackers took control of 150 sewage pumping stations at the Malucci sewage treatment plant in Australia. This unauthorized access led to the direct discharge of over one million liters of untreated sewage from the storm drains into the natural water system, resulting in significant environmental damage to the local area [4]. Cyber-attacks on power grids have become increasingly common in recent years, with several high-profile incidents causing widespread blackouts and disruptions. In 2015, numerous regional power grids in Ukraine experienced widespread blackouts as a result of cyber-attacks. The following year, the Israel Electric Power Company was compelled to take a significant number of computers offline due to a cyber-attack [5]. In 2020, Venezuela's national grid faced a targeted attack on the 765 trunk line, resulting in blackouts across all eleven states except for the capital, Caracas. [4].

1.1.2 Measurements in power system

The swift progress of information and communication technologies (ICTs) has resulted in the extensive implementation of intelligent instruments and devices within power systems. This evolution is reshaping conventional power systems into cyber-physical power systems (CPPSs), facilitating smooth integration and interaction among physical infrastructure, information sensing and analysis, and cyber-based system operation and control [6].

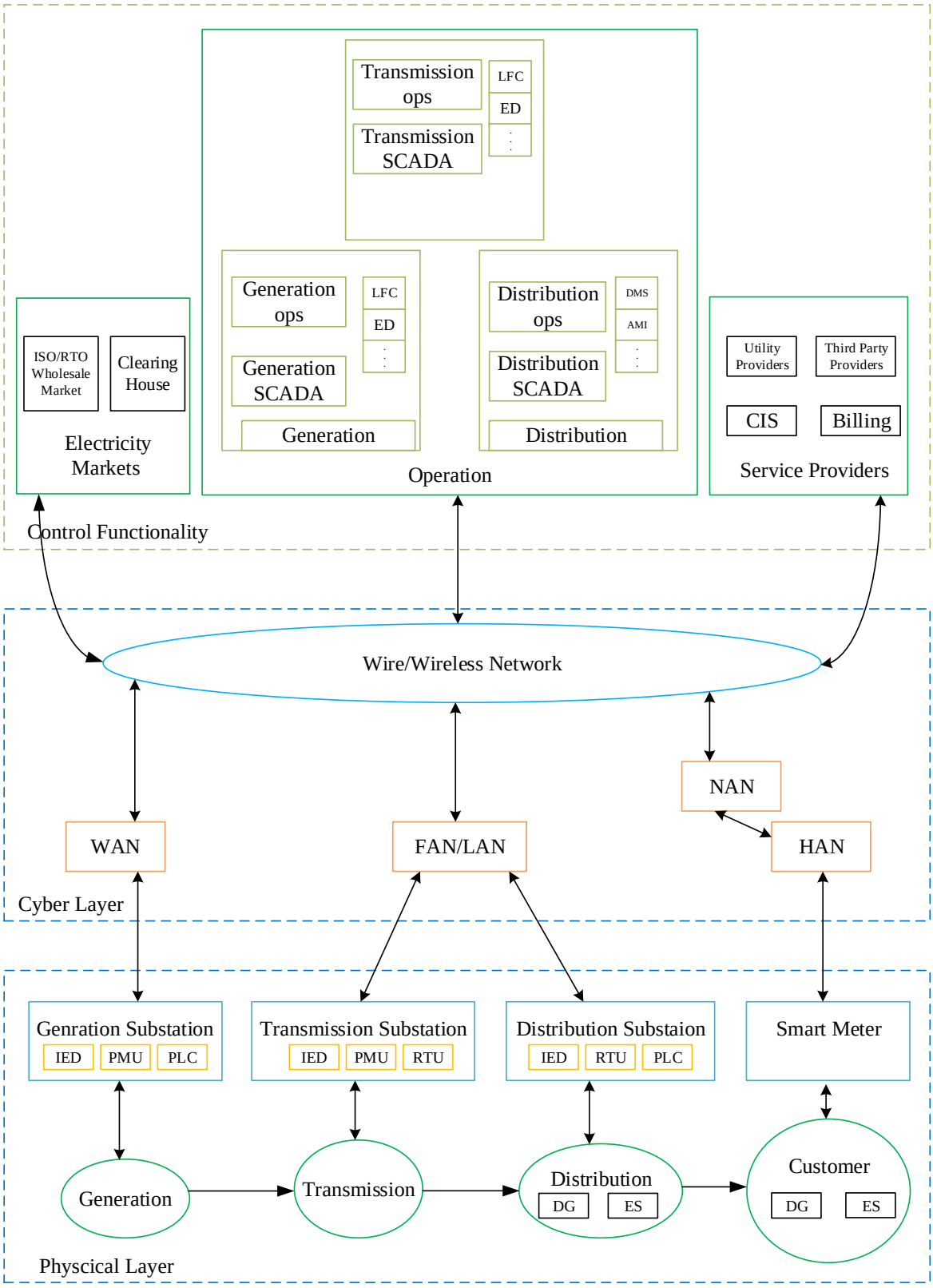


Figure 1.2: Framework of CPPS

Cyber-physical power systems (CPPSs) encompass a dual-layered structure, comprising both a physical layer and a cyber layer. The physical layer comprises tangible infrastructure and assets, including generation substations, transmission substations, distribution substations, and smart meters. On the other hand, the cyber layer encompasses the information and communication systems that underpin the operation and control of the physical layer [4]. The cyber layer plays a pivotal role in gathering data from sensors distributed across the CPPS, processing that data to generate state estimates and control decisions, and then transmitting those control decisions to actuators in the physical layer. The cyber layer also includes analytical tools that support monitoring and control of the energy flow from generators to end users. In Fig 1.2, The operations (ops) of an energy management system (EMS) rely on advanced metering infrastructure (AMI) and customer information systems (CIS) to efficiently manage electricity generation, transmission, and distribution through bulk storage management (BSM) and economic dispatch (ED). Regional transmission organizations (RTOs) and independent system operators (ISOs) utilize wide area networks (WANs), field area networks (FANs), and local area networks (LANs) to maintain load frequency control (LFC) and ensure the reliability of the power grid. Intelligent electronic devices (IEDs), such as phasor measurement units (PMUs) and remote terminal units (RTUs), collect data and communicate with programmable logical controllers (PLCs) to optimize energy storage (ES) and distribution generation (DG).

The majority of current measurements in power systems are asynchronous conventional measurements obtained from RTUs. These measurements, which include real and reactive power injection and flow measurements, as well as voltage and current magnitude measurements, are collected by the supervisory control and data acquisition (SCADA) system. The collection frequency for these conventional measurements is typically set at intervals of 1 to 5 seconds [7]. Phasor measurement units (PMUs) are essential power system components. They provide synchronized, high-accuracy measurements of voltage and current phasors at strategic locations in the power grid. Subsequently, this information is transmitted to a phasor data concentrator (PDC). The data obtained from PMUs is instrumental in monitoring the electronic power network operations. It plays a crucial role in real-time decision-making and control processes within the power system [8].

1.2 Literature Review

The conventional state estimation in the aspect of cyber security is introduced in this chapter. Different types of stealthy attacks and their effect on residual and power flows have been shown mathematically. The role of the history of machine learning in the power system is discussed in this chapter.

1.2.1 Conventional state estimation

Several state estimation techniques are employed to determine the most accurate representation of the current operating conditions in a power distribution system. These techniques leverage mathematical models, measurements, and algorithms to estimate the states of the system components [4]

Charactesristic	**Conventional Power system**	**CPPS**
Measurement	Electromagnetic meters	Smart meters with bidirectional communication capabilities
Communication	One-way communication between power systems	Bidirectional communication linking power systems and users
Power flow mode	Unidirectional Power flow	Bi-directional power flow
Control	Centralized control	Centralized and distributed control

Table 1.1: Conventional power system versus CPPS

1.2.2 Aspects of Cybersecurity

Cyber-attacks manifest in two primary forms: passive attacks and active attacks. Passive attacks aim to obtain unauthorized access to system data, with attackers monitoring internet traffic data logs to track sources and destinations. Additionally, they may scan internet-connected devices for vulnerabilities [9, 10]. In contrast, active attacks aim to modify data in some way. Following are a few types of active attacks:

1. Modification of the data
2. Identity Spoofing (IP Address Spoofing)
3. Denial-of-Service Attack

4. Man-in-the-Middle Attack (MITM)

The fundamental principle of a false data injection attack is discussed here. For a given topology of the network, parameters of the branch, and data from measurements, denote $\mathbf{z}_{meas}$ as the vector of all the measurements. The connection between $\mathbf{z}_{meas}$ and $\mathbf{h}(\mathbf{x})$, as denoted in Eq 1.1. This formulation characterizes a nonlinear Dynamic System State Estimation (DSSE) model.

$$\mathbf{z}_{meas} = \mathbf{h}(\mathbf{x}) + \mathbf{v} \tag{1.1}$$

Following reasonable assumptions are considered to inject false data into the system:

1) The attacker has the information completely. [11].

2)It is possible to convert any type of nonlinear DSSE into linear DSSE

3) Attacker can transform the $\mathbf{z}_{meas}$(original measurement data) into $\mathbf{z}_{equ}$(equivalent measurement data) in the linear DSSE model. In the linear three-phase DSSE model, a solution expressed in closed form is provided as follows,

$$\hat{\mathbf{x}} = (\mathbf{H}^{\mathrm{T}}\mathbf{R}^{-1}\mathbf{H})^{-1}\mathbf{H}^{\mathrm{T}}\mathbf{R}^{-1}\mathbf{z}_{meas} \tag{1.2}$$

$$\mathbf{z}_{equ} = \mathbf{H}\hat{\mathbf{x}} + \mathbf{v} \tag{1.3}$$

In the given context, $\hat{\mathbf{x}}$ represents the state computed by the conventional DSSE, and $\mathbf{R}$ is a matrix that gives the variance of measurement error. Post-cyber-attack DSSE model upon injection of attack vector $\mathbf{a}$ is given as:

$$\mathbf{z}_{equ} + \mathbf{a} = \mathbf{H}\hat{\mathbf{x}}_a + \mathbf{v} \tag{1.4}$$

where $\hat{\mathbf{x}}_a$ is the state estimated after the cyber-attack by the linear DSSE model. It's important to note that the measurement coefficient matrix $\mathbf{H}$ in the linear DSSE model differs from the measurement function $\mathbf{h}()$ in the original nonlinear DSSE. Following the injection attack, the alignment between measurements and estimated states becomes inconsistent, and this discrepancy is articulated by the Eq 1.4

$$\mathbf{z}_{meas} + \mathbf{a} \neq \mathbf{h}(\hat{\mathbf{x}}_a) + \mathbf{v} \tag{1.5}$$

To ensure the solution $\hat{\mathbf{x}}_a$ is the same as the solution of the model which is the nonlinear DSSE, it is mandatory to discover a constant vector $\Delta\mathbf{z}$ to satisfy Eq.1.5, and the original measurement data is manipulated with $\mathbf{z}_{meas} + \Delta\mathbf{z}$.

$$\mathbf{z}_{meas} + \Delta\mathbf{z} = \mathbf{h}(\hat{\mathbf{x}}_a) + \mathbf{v} \tag{1.6}$$

The residual in Eq 1.5, after injection of $\mathbf{a}$ is given as

$$\begin{aligned} \mathbf{v}^a &= \mathbf{z}_a - \mathbf{H}\hat{\mathbf{x}}_a = \mathbf{z}_{equ} + \mathbf{a} - \mathbf{H}(\hat{\mathbf{x}} + (\mathbf{H}^{\mathrm{T}}\mathbf{R}^{-1}\mathbf{H})^{-1}\mathbf{H}^{\mathrm{T}}\mathbf{R}^{-1}\mathbf{a}) \\ &= \mathbf{z}_{equ} - \mathbf{H}\hat{\mathbf{x}} + \mathbf{a} - \mathbf{H}(\mathbf{H}^{\mathrm{T}}\mathbf{R}^{-1}\mathbf{H})^{-1}\mathbf{H}^{\mathrm{T}}\mathbf{R}^{-1}\mathbf{a} \end{aligned} \tag{1.7}$$

Let $\mathbf{a} = \mathbf{Hd}$, where $\mathbf{d}$ is any arbitrary constant vector.The residual can be reformulated as:

$$\begin{aligned} \mathbf{v}^a &= \mathbf{z}_{equ} - \mathbf{H}\hat{\mathbf{x}} + \mathbf{H}d - \mathbf{H}(\mathbf{H}^{\mathrm{T}}\mathbf{R}^{-1}\mathbf{H})^{-1}(\mathbf{H}^{\mathrm{T}}\mathbf{R}^{-1}\mathbf{H})\mathbf{d} \\ &= \mathbf{z}_{equ} - \mathbf{H}\hat{\mathbf{x}} + \mathbf{Hd} - \mathbf{Hd} = \mathbf{z}_{equ} - \mathbf{H}\hat{\mathbf{x}} = \mathbf{v} \end{aligned} \tag{1.8}$$

Since the residual after the cyber-attack remains unchanged from the pre-attack state, it can be concluded that if the pre-attack residual successfully passed the MNR test, the post-attack residual will also pass the MNR test.

The impact of spoofing on measurements:

A GPS clock within an extensive network serves as a shared time reference for voltage and current measurements captured by PMUs. Each signal is assigned a timestamp by the PMU, enabling synchronized sampling. Receiver time t changes to $t + t_{spf}$ when the hacker attacks the PMU receiver Here, t_{spf} represents the time difference due to the spoofing attack. [12]. The phase angle of the measured signals following the spoofing attack is determined as shown below.

$$\varphi^{\text{atk}} = \theta_{spf} + \varphi \tag{1.9}$$

$$\theta_{spf} = 2\pi f t_{spf} \tag{1.10}$$

The phase angle shift, denoted by θ_{spf}, introduced by the spoofing attack on a measured signal is represented by the difference between the original phase angle, φ, and the post-attack phase angle, φ^{atk}. This shift is directly proportional to the spoofing attack's frequency, f, which is characteristic of the power system.

The cyber-attack has compromised the integrity of phase angles derived from synchro-

phasor measurements, rendering them unreliable for analyzing bus voltages and branch currents. Suppose that a bus is connected to N_b branches. If $v(t) = |v|\sin(\omega t + \theta_V)$ and $i_n(t) = |i_n|\sin(\omega t + \theta_{In})$ are the nth branch current signal and the voltage signal that a PMU has measured before being attacked, respectively, The influence of the spoofing attack on these signals is illustrated as follows:

$$i_n^{\text{atk}}(t) = |i_n^{\text{atk}}|\sin(\omega t + \theta_{In} + \theta_{spf}) = |i_n|\sin(\omega t + \theta_{In} + \theta_{spf}) \tag{1.11}$$

$$v_n^{\text{atk}}(t) = |v_n^{\text{atk}}|\sin(\omega t + \theta_V + \theta_{spf}) = |v|\sin(\omega t + \theta_V + \theta_{spf}) \tag{1.12}$$

When a PMU is subjected to a GPS spoofing attack, only the phase angles of the phasor measurements are altered, while their magnitudes remain unchanged. Since the spoofing attack's impact is consistent across all signals measured by a PMU at a given time, the phase angles of voltage and currents shift uniformly. Consequently, the complex power,S_n, active power,P_n, and reactive power,Q_n, of the nth branch connected to the bus, derived from the corresponding voltage and current signals, remain unaffected by the GPS spoofing attack. As it is stated in, this fact can be shown as follows:

$$S_n = P_n + jQ_n = VI_n^* = |V||I_n|\angle(\theta_V - \theta_{In}) \tag{1.13}$$

$$S_n^{\text{atk}} = P_n^{\text{atk}} + jQ_n^{\text{atk}} = V^{\text{atk}}I_n^{\text{atk}*}|V||I_n|\angle(\theta_V + \theta_{spf} + \theta_{In} + \theta_{spf}) = S_n \tag{1.14}$$

where I_n and V are the phasor forms of $i_n(t)$ and $v(t)$ signals, respectively. Also $I_n^{\text{atk}}(t)$ and V^{atk} are the phasor forms of $i_n^{\text{atk}}(t)$ and v^{atk}signals, respectively. And in turn the total power of the bus that is calculated from $S = \sum_{n=1}^{N_b} v^{\text{atk}}I_n^{\text{atk}*}$ is reliable and GPS spoofing will have no impact on it [12].

1.3 Machine Learning in Power System

In [13], the authors argue that traditional physics-based models are not well-suited for capturing the complex dynamics of power systems, and that machine learning methods can enhance the accuracy and robustness of state estimation. In [14] authors propose a hybrid deep learning (DL) model for power system state estimation and forecasting and argue that DL models can be used to overcome the limitations of traditional state estimation techniques, such as computational inefficiency and suboptimal performance.

In [15] authors propose a bidirectional Long Short-Term Memory (BiLSTM) machine learning method for power system state forecasting. The authors argue that BiLSTM is well-suited for capturing the temporal dependencies in power system data and that it can achieve high accuracy even in the presence of missing data or noise. vulnerabilities of ML-integrated power systems are discussed in [16]. Machine learning (ML) algorithms are gaining more relevance in the power grid domain, despite the ongoing advancements in traditional estimation techniques based on deterministic models are still proposed as more accurate and trustworthy. ML algorithms are anticipated to address gaps in short- to medium-term power grid predictions, providing benefits like computational speed and scalability [17].

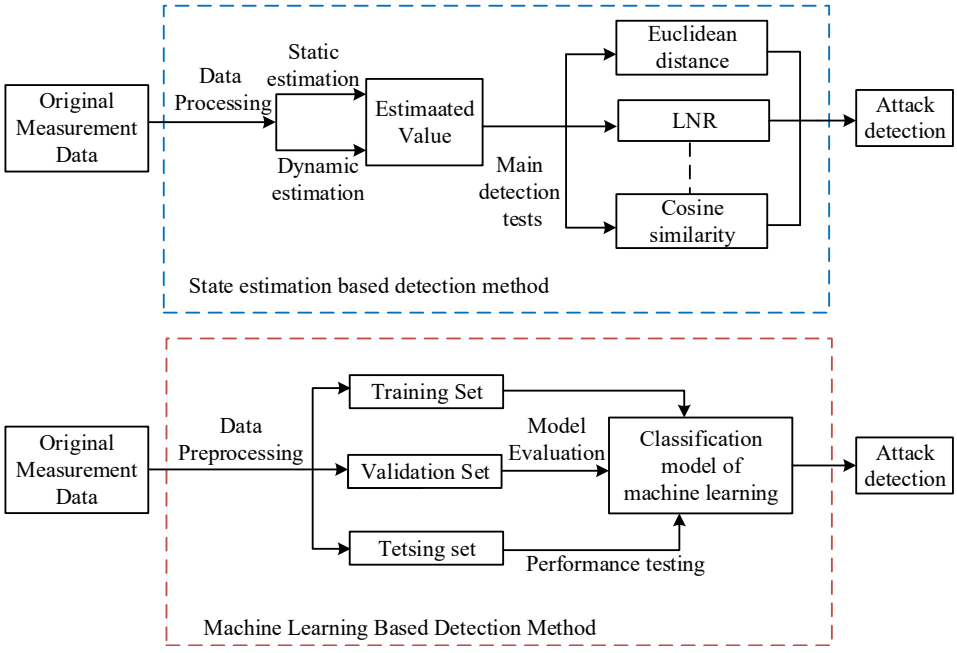


Figure 1.3: State estimation versus machine learning-based detection method

Machine learning-based detection methods offer an alternative approach to state estimation-based methods for identifying cyber-attacks. Unlike state estimation methods, which rely on mathematical models of the physical system, machine learning methods depend entirely on historical data from the system under investigation. Machine learning, an interdisciplinary field involving statistics, artificial intelligence, and computer science, enables knowledge extraction from data. It is versatile, applying to both classification and regression tasks. Regression, which aims to make numerical predictions, has found wide-

Category	Advantage	Disadvantage
Static	1. Low time complexity 2. High implementation	1. Low estimation accuracy 2. Low suitability for large system
	Ex. χ^2 WLSE [18] ,Maximum Normalized Residual [19, 20]	
Dynamic	1. High estimation accuracy 2. Good for nonlinear models	1. High time complexity 2 Easy divergence
	Ex. Kalman Filter(KF) [21],Extended KF,Unscented KF [22, 23]	

Table 1.2: Convnetional State Estimation methods

Category	Advantage	Disadvantage
Supervised	1. No need for system models 2. Known attack detection is fast	1. Labels required for data set 2. The application of new attack detection is not feasible
	Ex. KNN [24], Decision tree(DT)	
Unsupervised	1. No need for system models 2. New attack detection is applicable	1. Large number of training is required.
	Ex. K-means clustering(KMC), Isolation forest(IF)	

Table 1.3: Machine learning based SE methods

spread application in power system load forecasting. Classification, on the other hand, involves dividing predicted values into distinct categories. Cyber-attack detection is a prime example of a classification task. For instance, a machine learning-based classifier trained on historical data can be used to detect anomalous changes in data, potentially signaling cyber-attacks in CPPSs [4].

One of the primary applications of ML in power systems is predictive maintenance. By analyzing historical data on equipment performance and maintenance records, ML algorithms can predict potential failures before they occur, allowing operators to schedule maintenance activities proactively and minimize downtime. This proactive approach not only reduces maintenance costs but also improves the overall reliability of the power grid.In contrast to machine learning-based state estimation, which uses data-driven models and algorithms to identify patterns and relationships straight from data, conventional state estimation is based on mathematical models and optimization strategies derived from the physical principles of the power system.

1.4 Motivation and Problem Formulation

The increasing integration of modern cyberinfrastructure into power systems has made cybersecurity a paramount concern. SCADA systems, has the duty of managing and supervising electricity grids, are vulnerable to attacks targeting data communication infrastructures, control centers, and even remote terminal units (RTUs) [23]. The increasing demand for electricity, which can put a strain on the system To address these challenges, it is essential to have accurate and reliable knowledge of the state of the distribution system. This information can be used to improve system operation, reliability, and efficiency. Historically, SCADA-based approaches face limitations in capturing the swiftly evolving electromechanical dynamics of the system, primarily attributed to their slow sampling rate, typically around 0.25–0.5 Hz [25]. Traditional power system state estimation methods are not well-suited for distribution systems due to several factors, including:

- Distribution systems are typically radial, with few or no redundant paths. This means that a small disturbance can have a cascading effect on the entire system.
- Distribution systems are highly distributed, with millions of nodes and lines. This makes it computationally challenging to perform state estimation on these systems.
- Distribution systems are often subject to high levels of uncertainty due to the variability of DERs and the aging infrastructure.

Machine learning (ML) methods have the potential to overcome these challenges and provide a more accurate and reliable way to perform state estimation in distribution systems. ML methods can be used to learn the complex relationships between the different variables in the distribution system and to use this knowledge to estimate the state of the system even in the presence of uncertainty.

The problem of machine learning-based distribution system state estimation can be formulated as follows:

- Utilize machine learning methods to estimate the system state by leveraging a set of measurements obtained from the distribution system along with known system parameters.
- The system state can be denoted by a vector of variables, including the voltage

and current at each node in the system, while measurements can be represented by another vector of variables, such as the power flow on each line in the system.

- In machine learning-based distribution system state estimation, the objective is to learn a function that correlates measurements to the state of the system. This function can be acquired through diverse machine-learning algorithms, including support vector machines, decision trees, and neural networks.
- Once the function has been learned, it can be used to estimate the state of the system for new measurements. This information can then be used to improve system operation, reliability, and efficiency.

Unsupervised learning is advantageous in detecting zero-day attacks as it doesn't require training on specific attack scenarios. However, it is prone to high false positives. In contrast, supervised learning offers a more targeted approach, enhancing detection confidence. [24]. Based on this, supervised machine-learning methods are used to carry out experiments.

1.5 Thesis Outline

- **Chapter 1: Introduction -** This chapter gives the overview of the conventional and machine learning based state estimation algorithms.Research problems and motivation for the study also presented.
- **Chapter 2: Machine Learning Model Development -** In this chapter , an introduction to machine learning is discussed and implementation of one the supervised machine learning models known as decision tree model is analyzed
- **Chapter 3:Decision Tree with heterogeneous measurements -** In this chapter , data processing for the training and validating the model is discussed and performance of the given model with heterogeneous measurements is analyzed.
- **Chapter 4: DoS Attack on Distribution System -** This chapters gives whole idea of basic implementation of DoS attack with the attack detection technique and data driven estimation method to estimates the states in the attack interval.
- **Chapter 5: Conclusion -** The primary findings of this work, together with the contributions to the field of dynamic state estimation in power systems, are outlined in this chapter. The chapter also discusses the study's shortcomings and potential lines of inquiry for related future research.

Chapter 2

ML model development

Implementation of one of the supervised machine learning models decision tree model is discussed in this chapter. Information about the measurement data process before training the model is discussed.

2.1 Introduction to ML algorithms

In general, machine learning-based techniques are broadly classified into three categories: supervised machine learning, unsupervised machine learning, and semi-supervised machine learning. This section focuses on discussing the algorithms within the supervised and unsupervised machine learning domains.

Supervised Machine Learning:

Supervised machine learning involves training a model on a labeled data set, consisting of input data paired with corresponding output labels. The objective is to learn a mapping function from the input data to the output labels, allowing the model to predict output labels for new, unseen input data.

Supervised machine learning algorithms are frequently employed for classification and regression tasks. Classification tasks entail predicting a discrete output label, like determining whether an email is spam or not spam. In contrast, regression tasks involve predicting a continuous output value, such as estimating the price of a house.

Some common supervised machine learning algorithms include:

- Linear regression: Linear regression is a regression algorithm that predicts a continuous output value from a linear combination of input features.

- Logistic regression: It is a classification algorithm, designed to forecast the likelihood of an event taking place.
- Support vector machines (SVMs): SVMs are a classification algorithm that finds a hyperplane that separates the training data into two classes.

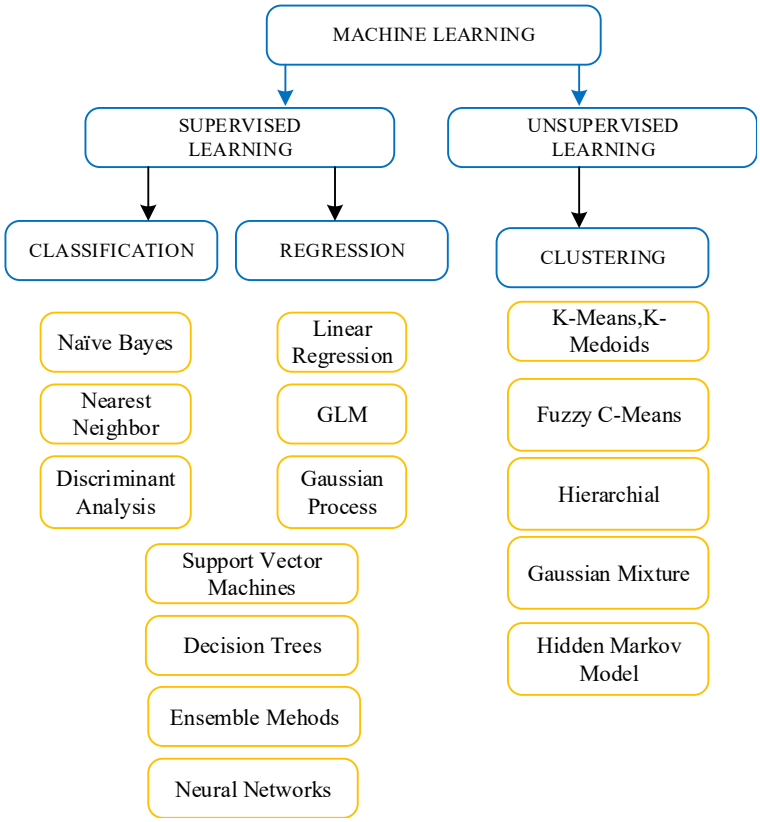


Figure 2.1: Different machine learning techniques

Unsupervised Machine Learning:

When a model is not trained on a labeled data set, it is referred to as unsupervised machine learning. Instead, an unlabeled data set is given to the model, and its job is to find any inherent structures or patterns in the data.

Some common unsupervised machine learning algorithms include:

- K-means clustering: A procedure called K-means clustering divides a data set into a predetermined number of clusters.
- Principal component analysis (PCA): PCA is an algorithm for dimensionality reduction that projects a dataset onto a lower-dimensional subspace.

- Isolation forest: Isolation forest is an anomaly detection algorithm that identifies outliers by isolating them from the rest of the data.

Both supervised and unsupervised machine learning are effective methods for training computers and potent tools in the field. For tasks where we have labeled data, supervised machine learning works well; for jobs without labeled data, unsupervised machine learning works well.

2.2 Decision Tree regression model implementation

2.2.1 System under study

Modeling a real-world distribution system scenario necessitates the incorporation of a radial distribution system. The IEEE 33 bus system serves as an exemplary radial bus system network for implementing the state estimation algorithm. The IEEE 33 bus system comprises a radial network with 33 buses, where the first bus is linked to the substation and acts as a generator bus, while the remaining buses serve as load buses, as depicted in Fig.2.2

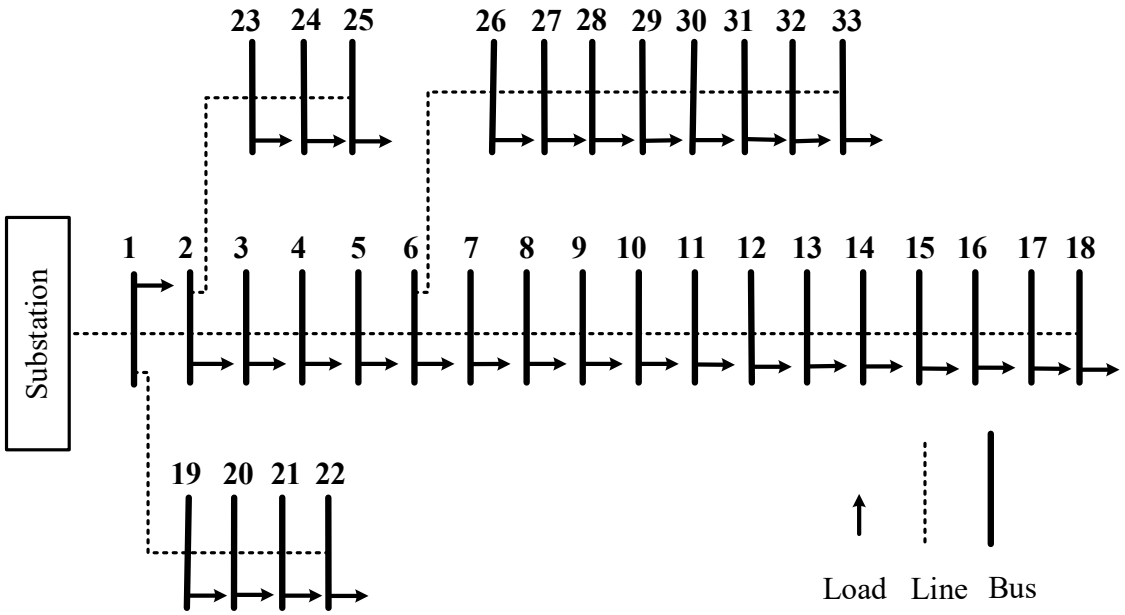


Figure 2.2: IEEE 33 bus system

The IEEE 33 bus system's characteristics closely resemble those of real-world distribution systems, making it a suitable platform for evaluating and validating state estimation techniques. To evaluate the performance of the state estimation algorithm against actual values, one must possess accurate information on all system variables, including bus voltages, line currents, bus-specific load profiles, active and reactive power flows through each line, and power injections at each bus. Load flow analysis, performed using the Forward-Backward sweep method, provides the true and accurate values of these variables for the IEEE 33 bus system. This analysis serves as a benchmark against which the state estimation algorithm's results can be compared and validated.

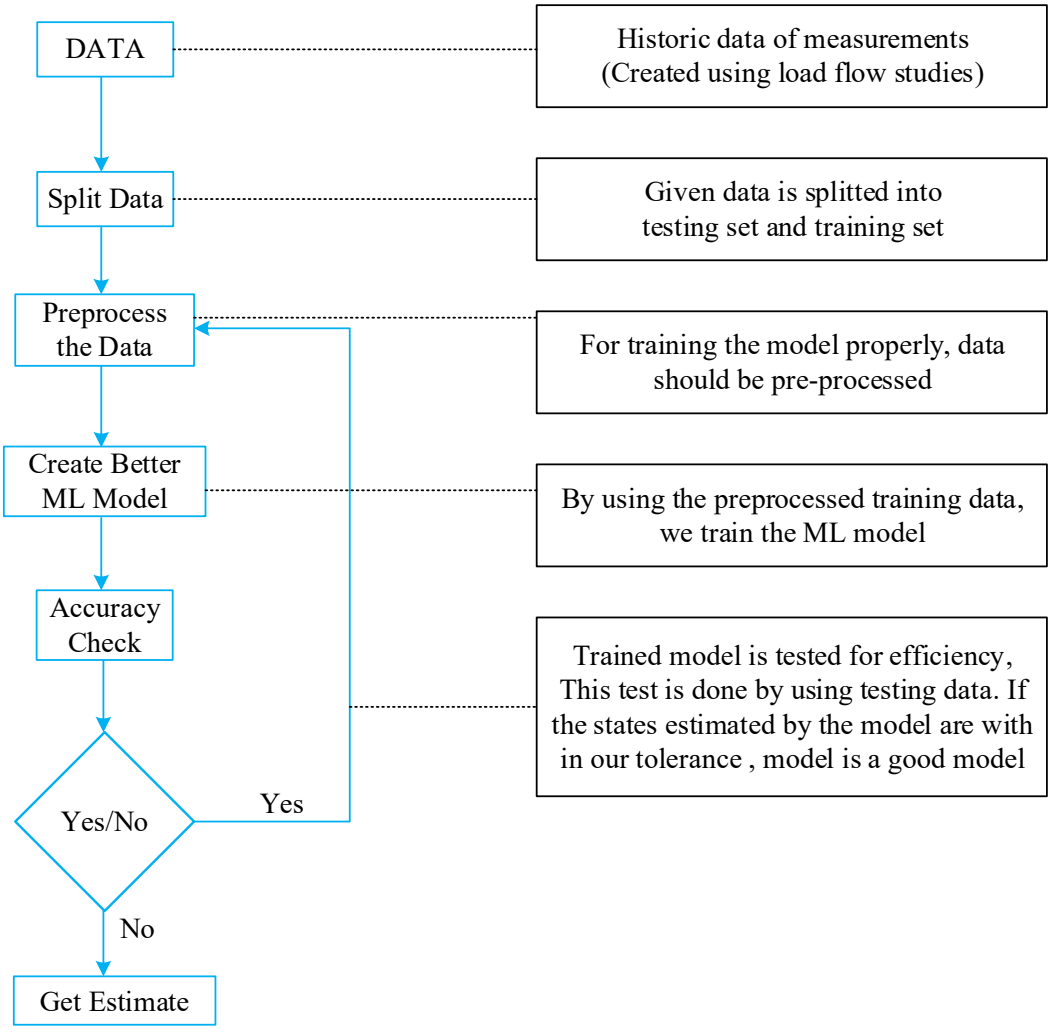


Figure 2.3: Model flowchart

In general, in any distribution load flow studies, Bus 1 is typically regarded as the reference bus in systems with N buses, hence its phase angle is fixed to 0 degrees. The state vector x

includes the following expression for its $(2N-1)$ elements, which include N bus voltage magnitudes and $(N-1)$ phase angles. In our case, 33 bus voltages and 32 bus phase angles need to be estimated.

$$\mathbf{x}^T = [\delta_2 \quad \delta_3 \quad \dots \quad \delta_N \quad V_1 \quad V_2 \quad \dots \quad V_N] \tag{2.1}$$

As we already discussed in previous chapters, the measurements that we have considered are μPMU measurements, RTU measurements, and SM measurements.

- The measured values provided by the μPMU are voltage phasors and current phasors.

$$\mathbf{z}_{\text{PMU}} = [\mathbf{z}_v \quad \mathbf{z}_a \quad \mathbf{z}_{iRe} \quad \mathbf{z}_{iIm}] \tag{2.2}$$

- The measured values provided by the RTU are voltage magnitude, power flow, and power injection.

$$\mathbf{z}_{\text{RTU}} = [\mathbf{z}_v \quad \mathbf{z}_{Pf} \quad \mathbf{z}_{Qf} \quad \mathbf{z}_{Pinj} \quad \mathbf{z}_{Qinj}] \tag{2.3}$$

- The measured values provided by the SM are active and reactive power flows.

$$\mathbf{z}_{\text{SM}} = [\mathbf{z}_{Pf} \quad \mathbf{z}_{Qf}] \tag{2.4}$$

2.2.2 Data Processing

In power systems, data processing plays a pivotal role in the efficacy of decision tree models. Before training, raw data collected from various sensors across the grid undergoes meticulous to ensure accuracy and reliability. This preprocessing involves steps such as handling missing values, removing outliers, and normalizing data to maintain consistency. Once prepared, the data is then split into training and testing sets, facilitating model training and evaluation. As shown in Fig 2.3, the measurement data from all the meters should be used for training as well as testing the model.

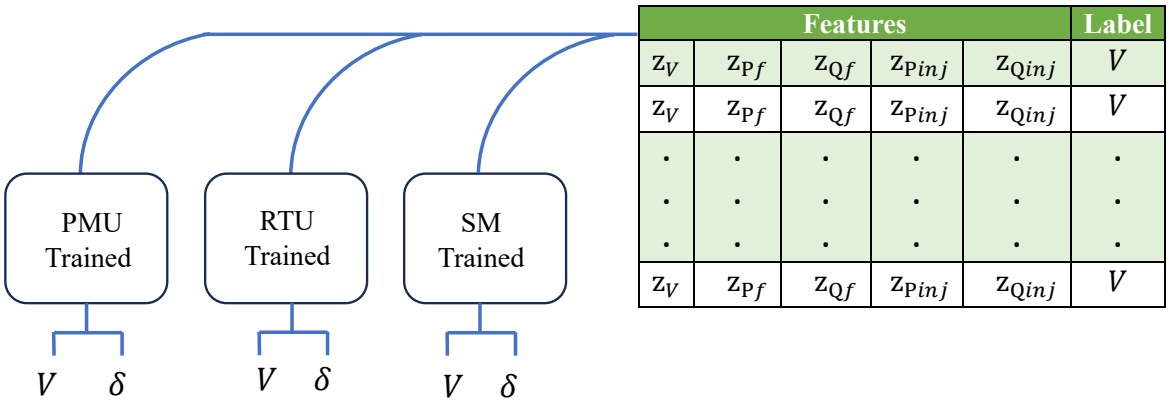
Case 1: Static state estimation:

In the case of static state estimation, we have to estimate the voltages and phase angles at all(33 buses) for a given instant for producing the data, the given data (load active and reactive power)is changed from 80% to 110% (of original data)with an increment of 0.1%.

At every variation, voltage magnitudes and phase angles at each bus are taken. Hence, 301 sets of data are obtained with each set containing 33 voltage magnitudes and 33 respective angles. This data is split into training and testing data with a split ratio of 0.8 by using the data splitting module.

Case 2: Dynamic state estimation:

In dynamic state estimation, voltage and phase angles at a single bus are estimated for different hours with dynamic changes in load. For this case, data is produced by changing original data from 50% to 150% with an increment of 0.1% which results in data of 1001 rows. The Data Split module uses the split ratio of 0.8 for dividing the original data into training and testing. Hence 80% of the data used for training the model and 20% data is used for testing the model.



Features					Label
z_V	z_{Pf}	z_{Qf}	z_{Pinj}	z_{Qinj}	V
z_V	z_{Pf}	z_{Qf}	z_{Pinj}	z_{Qinj}	V
.	.	.	.	.	.
.	.	.	.	.	.
.	.	.	.	.	.
z_V	z_{Pf}	z_{Qf}	z_{Pinj}	z_{Qinj}	V

Figure 2.4: Model Feature Training

In Fig.2.4 only RTU features are shown, but each of the model are trained with their respective features in training phase. Each individual model generates their own voltage and load angles , these data will be further sent to global estimator to get final estimates which is discussed in next chapter.

Chapter 3

Decision Tree with heterogeneous Meters

By using one of the supervised machine learning models DT model, both static and dynamic state estimation for the IEEE 33 bus distribution system has been implemented and the results are discussed in this chapter.

3.1 Static State Estimation Using DT model

In static state estimation of the IEEE 33 bus system, voltages at every bus in the system are estimated using the DT model. As one can observe from Fig 3.1, the DT model is estimating the voltage magnitudes with good accuracy.

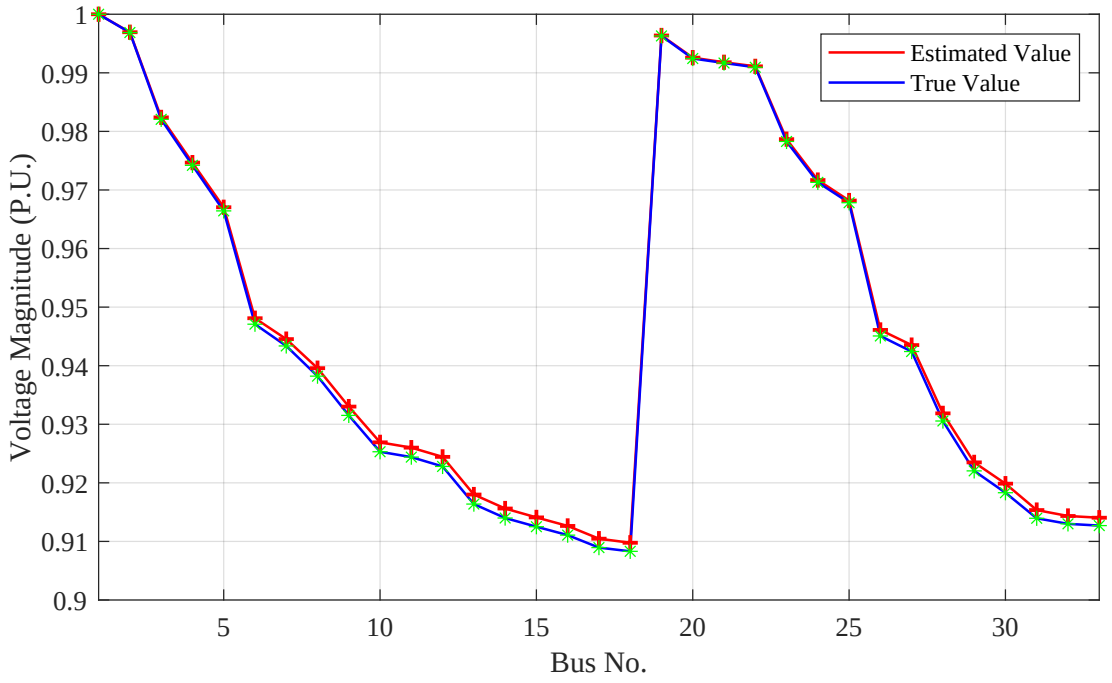


Figure 3.1: Voltage Magnitude estimation by DT model

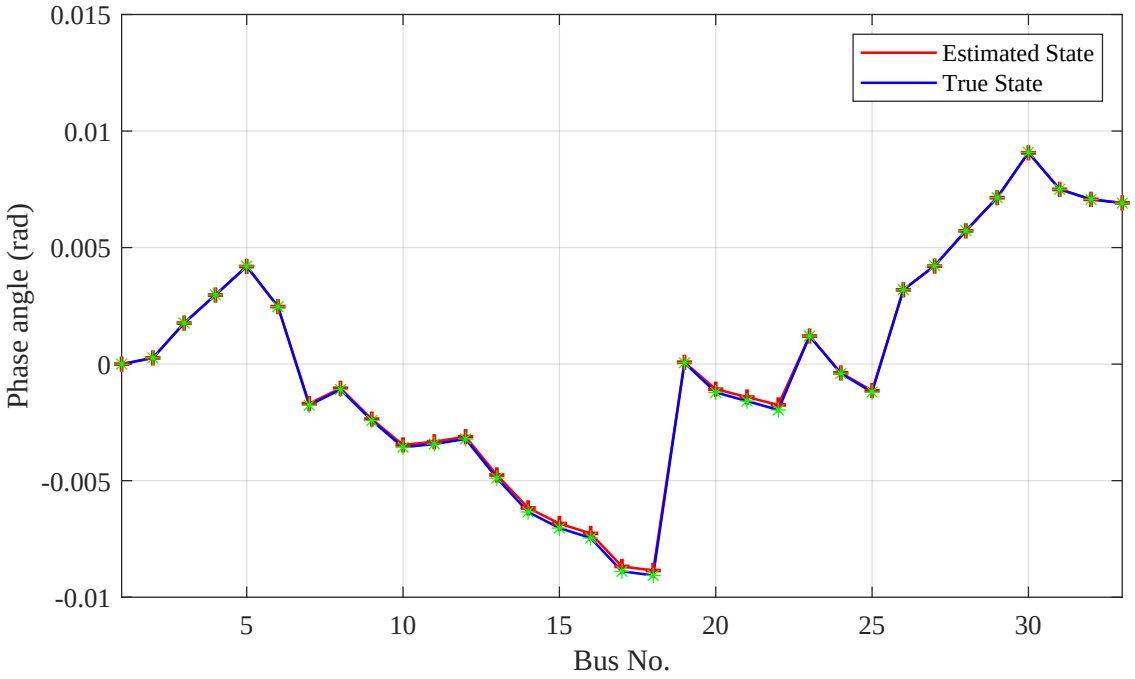


Figure 3.2: Phase Angle estimation by DT model

In the static distribution system state estimation(DSSE) all the power flows in turn states of the system are fixed values for a given instant, hence it is called static state estimation. Phase angles estimated by the DT model are shown in Fig 3.2. The angles estimated for the initial buses are estimated with good accuracy, but one can observe that some bus's angles are not in the acceptable range of tolerance, this might happened because of the testing data. Improving the training data, and properly pre-processing the data will give us a better model always.

3.2 Dynamic Estimation Using DT model

3.2.1 DT model with μPMU measurements

In this case, μPMU measurements(Voltage and current phasors) are used for training and testing the model. Dynamic voltages estimated DT model which is trained by using μPMU is shown in Fig.3.3 and the dynamic angle estimated by the DT model is shown in Fig.3.4.The root mean square error(RMSE) for voltgae and angle estimation is 1.07×10^{-3} and 2.84×10^{-4} respectively.

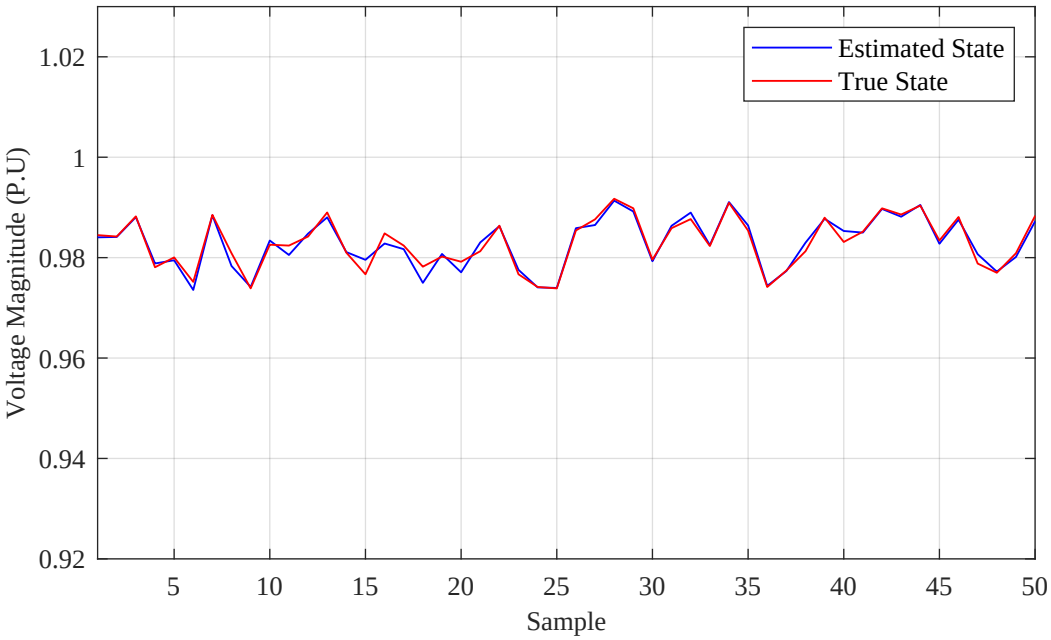


Figure 3.3: Dynamic voltage estimation by μPMU trained DT model

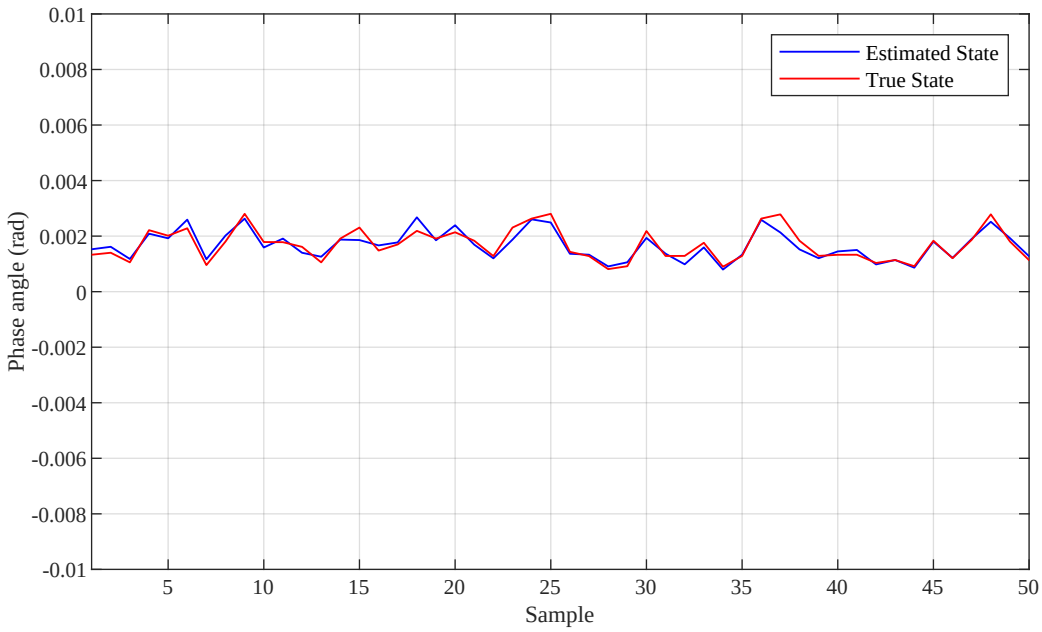


Figure 3.4: Dynamic angle estimation by μPMU trained DT model

3.2.2 DT model with RTU measurements

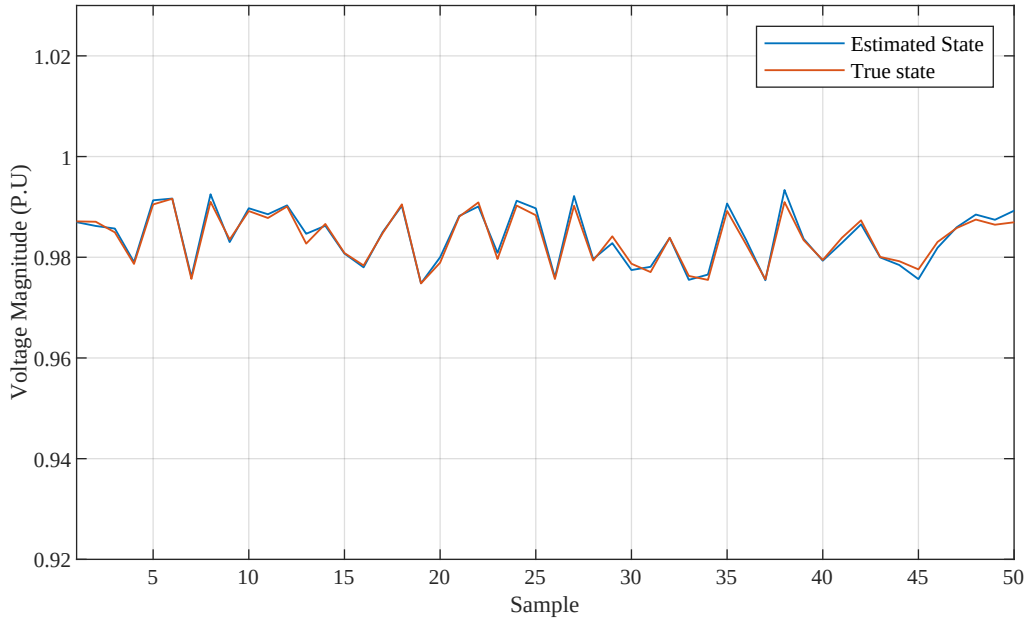


Figure 3.5: Dynamic voltage estimation by RTU trained DT model

In the case of RTU trained DT model, RTU measurements are used for training and testing the model. Voltage and angles estimated by the DT model trained by RTU measurements (voltage magnitude, power flow, and power injection) are shown in Fig.3.5 and Fig.3.6 with a RMS error of 2.87×10^{-4} and 2.37×10^{-4} respectively.Here, in all dynamic estimation cases, bus number 4 is considered and it is an arbitrary selection.

By amalgamating information from diverse sensors spread throughout the grid ranging from voltage and current sensors to temperature gauges and phasor measurement units (PMUs)—decision tree regression enables operators to gain a nuanced understanding of grid dynamics. Through this method, operators can predict vital parameters like power consumption, voltage levels, and equipment health status with remarkable accuracy. Leveraging historical data and real-time sensor readings, these models decipher complex patterns and distill them into actionable insights. Such predictive capabilities empower operators to proactively address potential faults, optimize energy distribution, and enhance overall grid reliability.

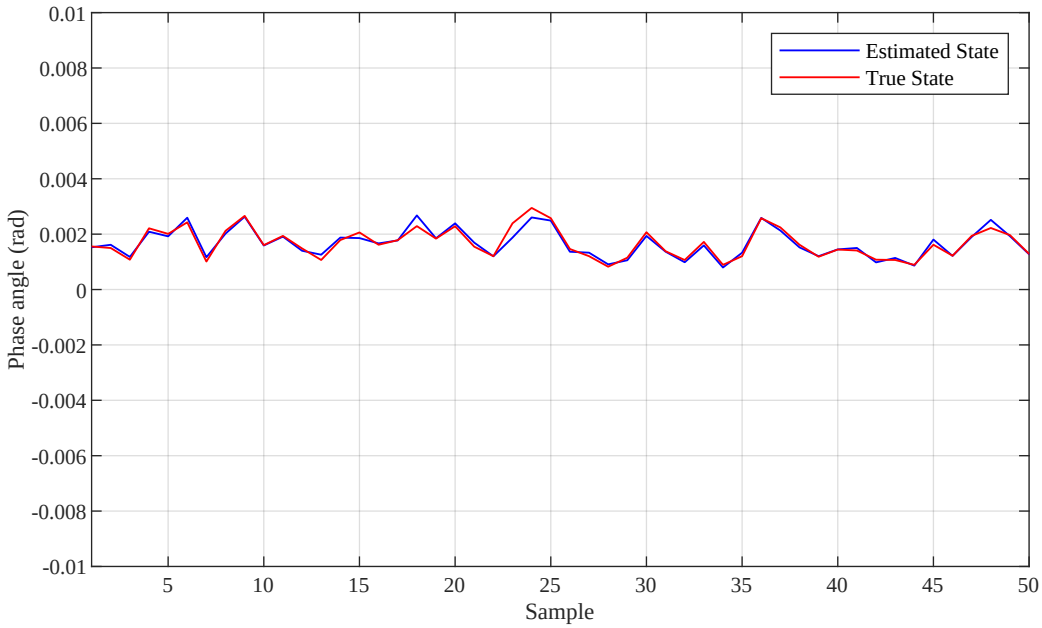


Figure 3.6: Dynamic angle estimation by RTU trained DT model

3.2.3 DT model with SM measurements

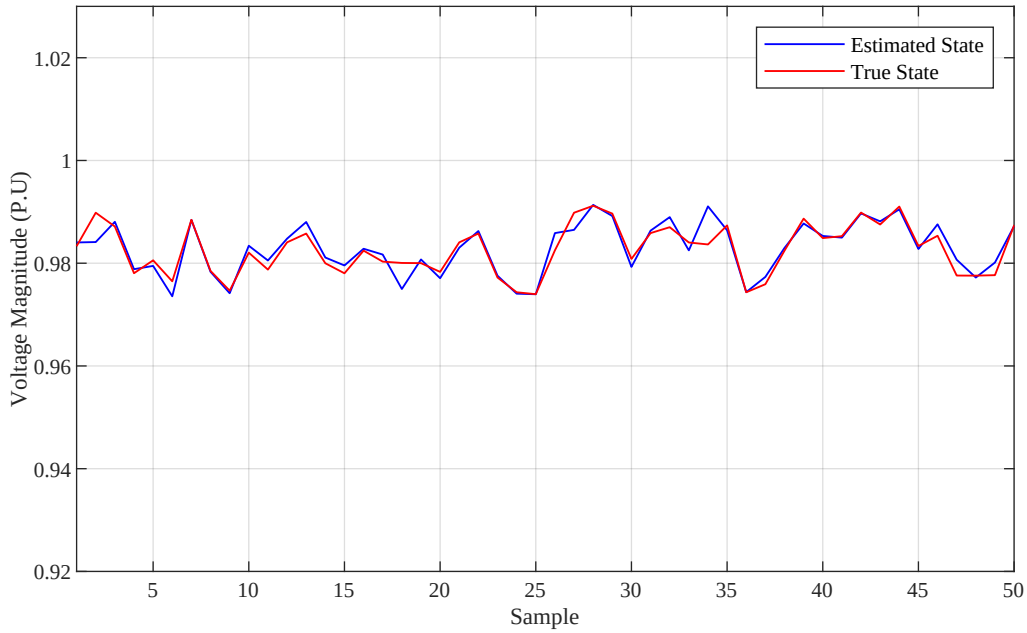


Figure 3.7: Dynamic voltage estimation by SM trained DT model

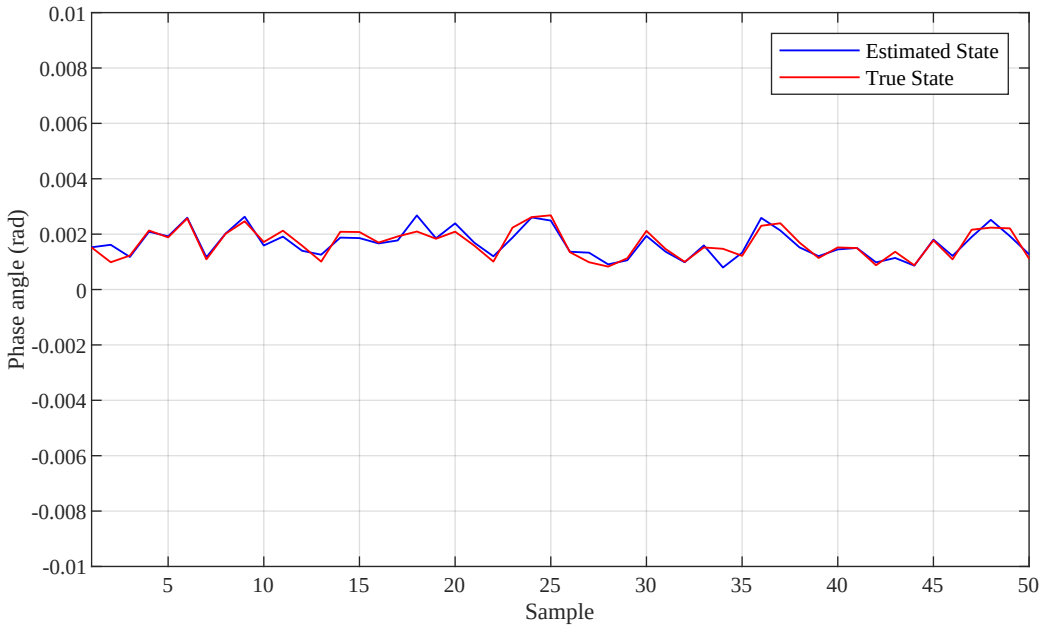


Figure 3.8: Dynamic angle estimation by SM trained DT model

Fig.3.7 shows voltages estimated by the DT model which is trained by using smart meter measurements and Fig.3.8 shows the estimated angles. RMS error for voltage estimation and angle estimation is 4.09×10^{-4} and 2.46×10^{-4} respectively.

Summary of the results(RMS error) can be tabulated as below:

Case		**Voltage (p.u)**	**Angle**
static		3.08×10^{-3}	6.45×10^{-4}
Dynamic	μPMU	1.07×10^{-3}	2.84×10^{-4}
	RTU	2.87×10^{-4}	2.37×10^{-4}
	SM	4.09×10^{-4}	2.46×10^{-4}

Table 3.1: RMS error with DT model

3.3 Multiple Sensor Data Fusion

In the above discussions we have seen how the model performs with the measurements coming from single type of meter. But this may not be the case in practical distribution system. There will be usage of all kinds of meters as mentioned above, Hence all the information coming from different meters should be fused together to obtain a final estimate of a specific electrical attribute.Sensor fusion involves the integration of data from multiple sensors to obtain a more comprehensive and accurate representation of the system.

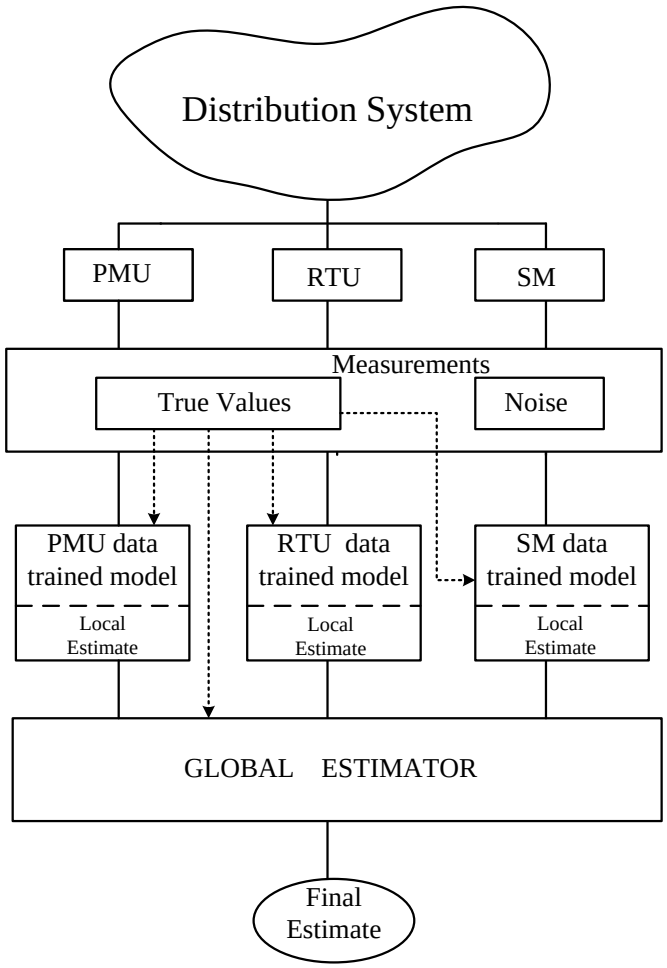


Figure 3.9: Information Fusion Flow Chart

In the context of power systems, this entails combining data from various sensors, including voltage and current sensors, temperature sensors, phasor measurement units (PMUs), synchrophasors, and other relevant devices. By leveraging the information provided by these sensors, sensor fusion enables power system operators to gain deeper insights into

grid conditions and make more informed decisions in real-time. One of the key benefits of sensor fusion in power systems is its ability to improve situational awareness.

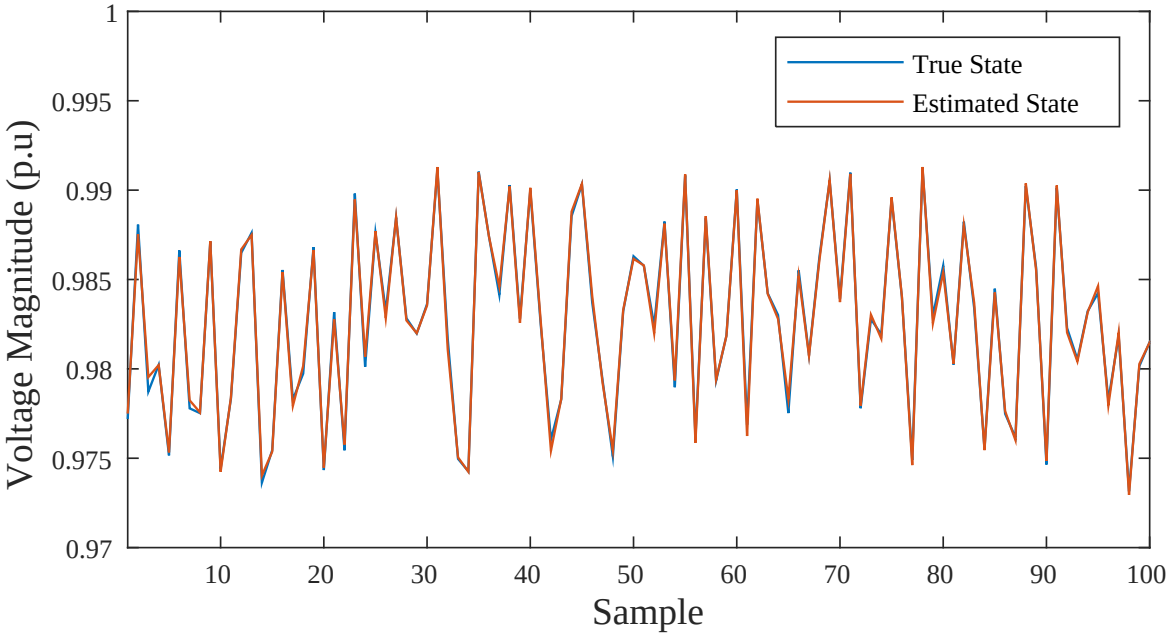


Figure 3.10: Final estimated voltage magnitude after fusion

Input data for the local estimators can be obtained from all the different types of meters in physical layer of the distribution system and these estimates from local estimators sent for information fusion. Fig 3.10 and Fig 3.11 shows final estimated voltages and phase angles after global estimation respectively.

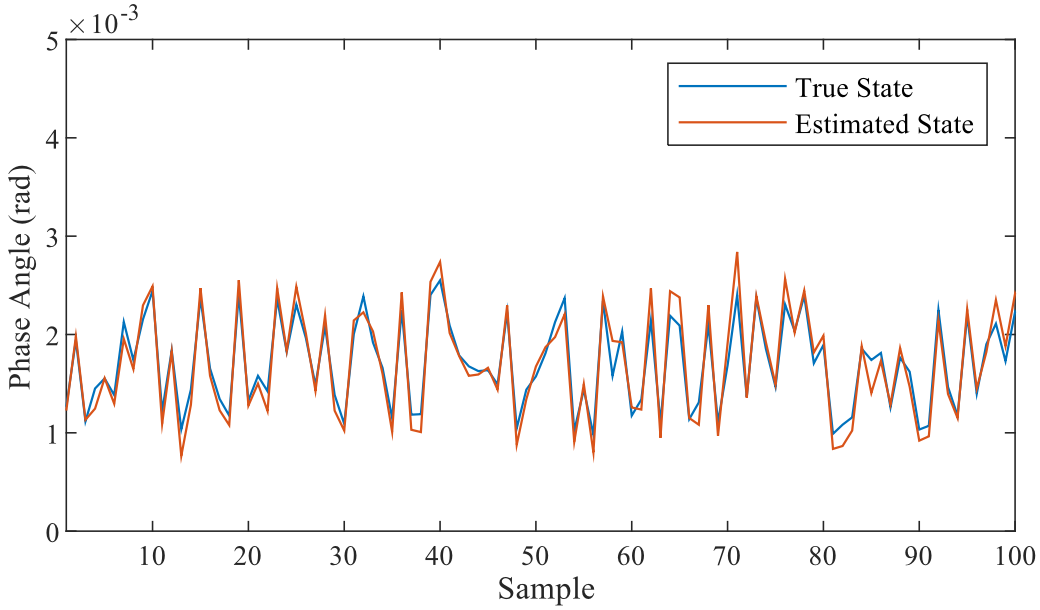


Figure 3.11: Final estimated phase angle after fusion

3.3.1 R-squared (R^2) score

In a regression model, the percentage of the dependent variable's variation that can be predicted from the independent variables is expressed statistically as the R-squared (R^2) score, sometimes referred to as the coefficient of determination. It is frequently employed to assess regression models' performance.

Usually, the R-squared (R^2) score falls between 0 and 1. When the regression model receives a score of 1, it means that the dependent variable is perfectly predicted; when the score is zero, it means that the model is no more effective at explaining the variance in the dependent variable than it is at predicting the dependent variable's mean.
The formula to calculate the R-squared score is given by:

$$R^2 = 1 - \frac{SS_{res}}{SS_{tot}}$$

In simpler terms, SS_{res} is the sum of the squared differences between the actual target values and the predicted values, while SS_{tot} is the sum of the squared differences between the actual target values and the mean of the target values. The R-squared (R^2) score for the final estimates are given below :

For Voltage Magnitude: 0.9812

For Phase Angle: 0.9692

For the final estimated values, kalman filter gave RMS error 1.02×10^{-3} for voltage and 8.43×10^{-4} for phase angle where as decision tree gave 3.43×10^{-4} for and 2.43×10^{-4} for voltage and phase angle respectively.

Chapter 4

DoS Attack on Distribution System

It is a cyberattack in which the attacker tries to prevent authorized users from using network resources by temporarily or permanently blocking the services of a device connected to the Internet. Early in the 1980s, the computer science community made the discovery of the DoS attack. The immediate result is that there is no real-time data available for control feedback, which increases the risk of industrial cyber–physical systems (ICPSs) instability or even crashes. An attacker who uses a denial-of-service attack aims to compromise a host's or server's administration. It accomplishes this by being flooded with massive volumes of pointless traffic or requests for external communication.DoS refers to the ongoing transmission of falsified packets over a communication network channel by an attacker, which prevents normal information flow and communication. In this instance, $\mathbf{z}_k$ will lose if the attackers are successful in blocking the communication route. The corresponding model is usually described as:

$$\mathbf{z}_k^a = \rho_k \mathbf{z}_k \tag{4.1}$$

where $\rho_k = \text{diag}(\rho_k(1), \rho_k(2).....\rho_k(n))$ is a diagonal matrix with elements 0 or 1, i.e.,$\rho_k(i) = 1$ represents that the corresponding measurements are successfully transmitted,otherwise $\rho_k(i) = 0$

4.1 DoS Attack Model

Here, the distribution system has been modeled as the sets of buses, branches and their interconnections.Consider a N bus system where N is the total number of buses. Let,$\mathcal{T}$ represents the set of all the buses. Therefore $|\mathcal{T}| = N$, where, $|.|$ indicates the cardinality

of the set. We consider all of the buses to have any one of the measurement meters. As a result, the PMUs gather and forward to the control center all of the bus voltage phasor readings at an appropriate sampling rate. With today's smart grids, this assumption might not hold true because PMUs are typically positioned optimally to save costs and increase observability.

By considering DoS attacks on the cyber layer of the power grid result in unavailability of the data (time series of measured parameters) from a set of the meters those are under attack. Let, $\mathcal{A} \subset \mathcal{T}$ be the set of buses, which their connected meters are attacked by attackers, and $|\mathcal{A}| = Z$. Let, $x_k(t)$ denotes any electrical attribute (e.g., voltage or phase angels) from a meter at time t, where, $k \in \mathcal{T}$. By considering occurs at time t_a, this attack is modeled by assuming unavailability of $x_i(t)$ for $t > t_a$.

4.2 Impact of Dos Attack on Distribution System

Beyond the immediate impact on service availability, DoS attacks can inflict substantial financial losses on utilities and customers alike, encompassing expenses for equipment repair, service restoration, and compensation for downtime.

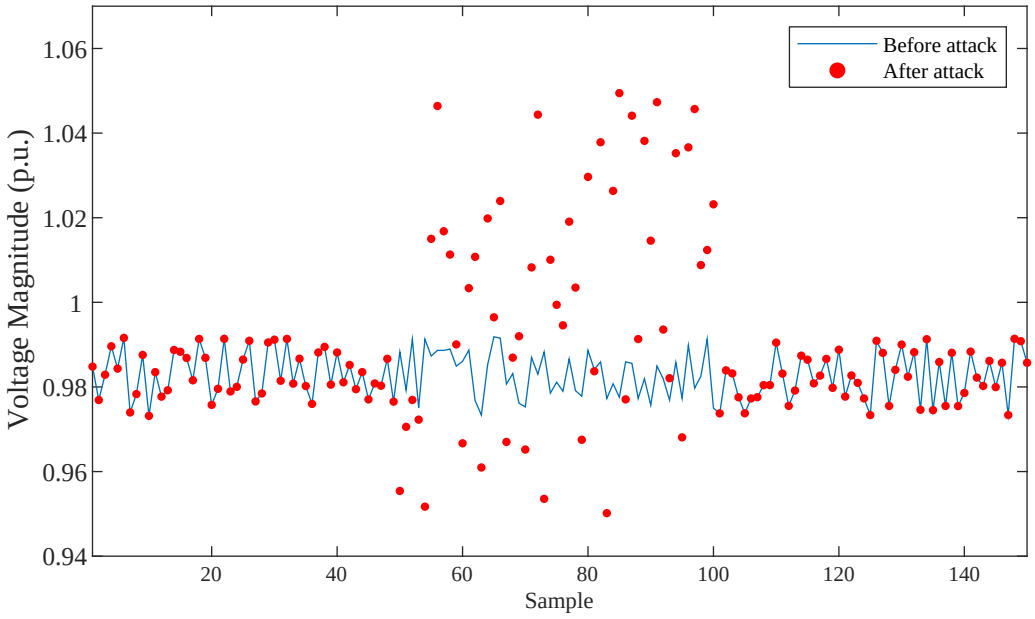


Figure 4.1: Impact on voltage magnitude of Bus No 19

In Fig.4.1, we can see that estimated voltage magnitudes before the attack and after the attack. Here, bus 19 is considered as target for attacker and one can observe that voltage magnitude is totally deviated from the actual values when the meters at that bus hit by Dos attack. Similarly, in Fig4.2, impact of Dos attack on phase angle of the targeted bus is shown.

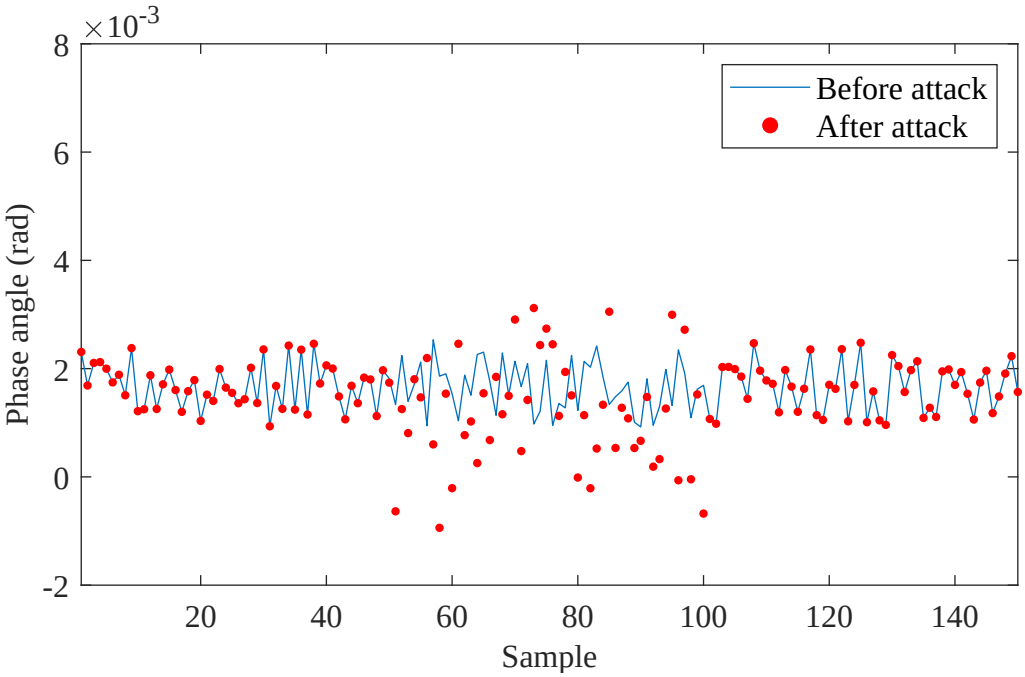


Figure 4.2: Impact on phase angle of Bus No 19

These attacks can jeopardize public safety, disrupt critical infrastructure, and tarnish the reputation of utilities, eroding customer trust. As distribution systems become increasingly interconnected and reliant on digital technologies, the threat posed by DoS attacks underscores the pressing need for robust cybersecurity measures and proactive risk mitigation strategies to safeguard the resilience and integrity of the power grid.

4.3 Detection, Elimination of Dos Attack

4.3.1 Detection of Dos Attack

Detection mechanisms typically involve monitoring network traffic and system behavior for anomalies indicative of an attack. Advanced anomaly detection algorithms, such as

machine learning-based approaches, can identify unusual patterns in data flow or communication traffic that deviate from normal operation. Additionally, techniques like intrusion detection systems (IDS) and signature-based detection methods can flag known attack patterns or malicious activities. Cyber attack detection strategies mainly classified into model based and machine learning based detection methods. Model based detection methods need mathematical model of physical system where as machine learning based methods does not need the same, it totally work depends on historical data under of the system under test.Machine learning can be used for regression problems and classification problems as we discussed in chapter 2. Regression has been widely used power system load forecasting. Cyber-attack detection is a typical classification task. For instance, we can develop a machine learning-based classifier with historical data to identify prospective cyberattacks in CPPSs by detecting odd changes in the data. Rapid detection of DoS attacks enables prompt mitigation measures, such as rerouting traffic, deploying firewalls, or implementing access controls, to minimize the impact on power system operations and ensure continuous service delivery.

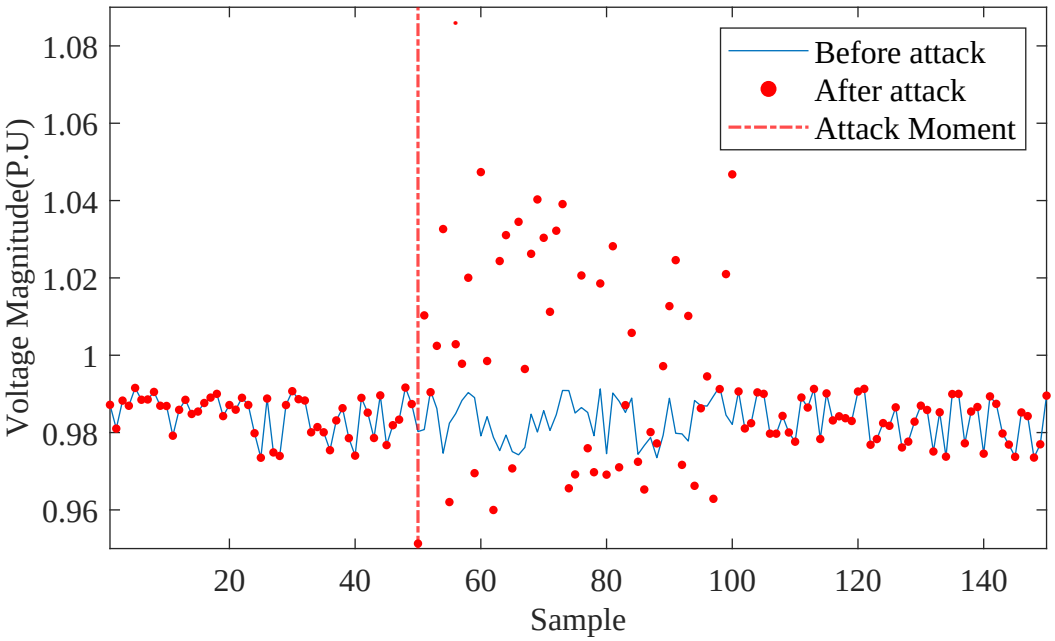


Figure 4.3: Detection of Dos Attack

One of the major outcome of this attack which can be used for detection algorithm is number of inputs to the estimation algorithm get reduced . This reduced number of

inputs is the anomaly or abnormal change . This change can be used for detecting the Dos attack specifically.In Fig 4.3 , one can observe that large deviation in the estimated states of voltage magnitude which might cause false control signal in power grid

4.3.2 Elimination of Dos Attack

DoS attack is not a stealthy attack. Often, it can be easily detected. As the main aim of the attacker is unavailability of data,there must be an alternative estimation method to calculate the state estimates. When the system suffers from an attack, as shown Fig 4.3 , control centers loose data of original estimated values of states, which results in wrong or inappropriate control signal. Hence it is of utmost important to restore the information of actual estimates for proper functioning of CPPSs. Here, a state estimation method with a goal to estimate the state of the components, which their measurement meters under attack, from the rest of the components by the rest of meters.We assume that states of electrical attributes $x_i(t)$,where $i \in \mathcal{T} \setminus \mathcal{A}$ are available as a time series. We denote the unobservable states for $t > t_a$ due to DoS attack by $y_j(t)$, where $j \in \mathcal{A}$.
We define the relation between the known and unknown states as follows :

$$\dot{y_j}(t) = \sum_{i=1}^{N-Z} c_{ji}\dot{x_i}(t) \tag{4.2}$$

For Z DoS attacks on Z buses , equation 4.2 will result in a system of equations as follows:

$$\underline{\dot{y}}(t) = C\underline{\dot{x}}(t) \tag{4.3}$$

Here $\underline{\dot{y}}(t)$ and $\underline{\dot{x}}(t)$ denotes vectors with time derivatives of the time series corresponding to observable (known) and unobservable (unknown) states respectively.
The bus-to-bus correlation of the states between the buses that are being attacked by a DoS attack and the buses that are not is contained in the matrix *C*. Every component of *C* is expressed as

$$c_{ji} = e^{kr_{ji}} \tag{4.4}$$

where r_{ji} is the correlation coefficient between $y_j(t)$ and $x_i(t)$ for the last t_c moments before the DoS attack:

$$r_{ji} = \int_{t_a - t_c}^{t_a} x_i(t)y_j(t)dt \tag{4.5}$$

For the discrete-time realization of the continuous-time time series, the derivative of a time series at t, can be considered as the backward difference system:$\dot{g}(t) = g(t) - g(t-1)$,where, g_t is the sampled value of the time series g at time t, and g_{t-1} is the previous sampled value. According to this notion, the Eq.4.2 can be written in the following form:

$$\underline{y}_t - \underline{y}_{t-1} = C(\underline{x}_t - \underline{x}_{t-1}) \tag{4.6}$$

$$\underline{y}_t = \underline{y}_{t-1} + C(\underline{x}_t - \underline{x}_{t-1}), t > t_a \tag{4.7}$$

Here, the weighted sum of the time derivatives of the remaining parameters has been used to estimate the time derivative of a state variable during a denial-of-service attack. The weights originate from the relationships between the attacked state and any state that is not within the attack zone.

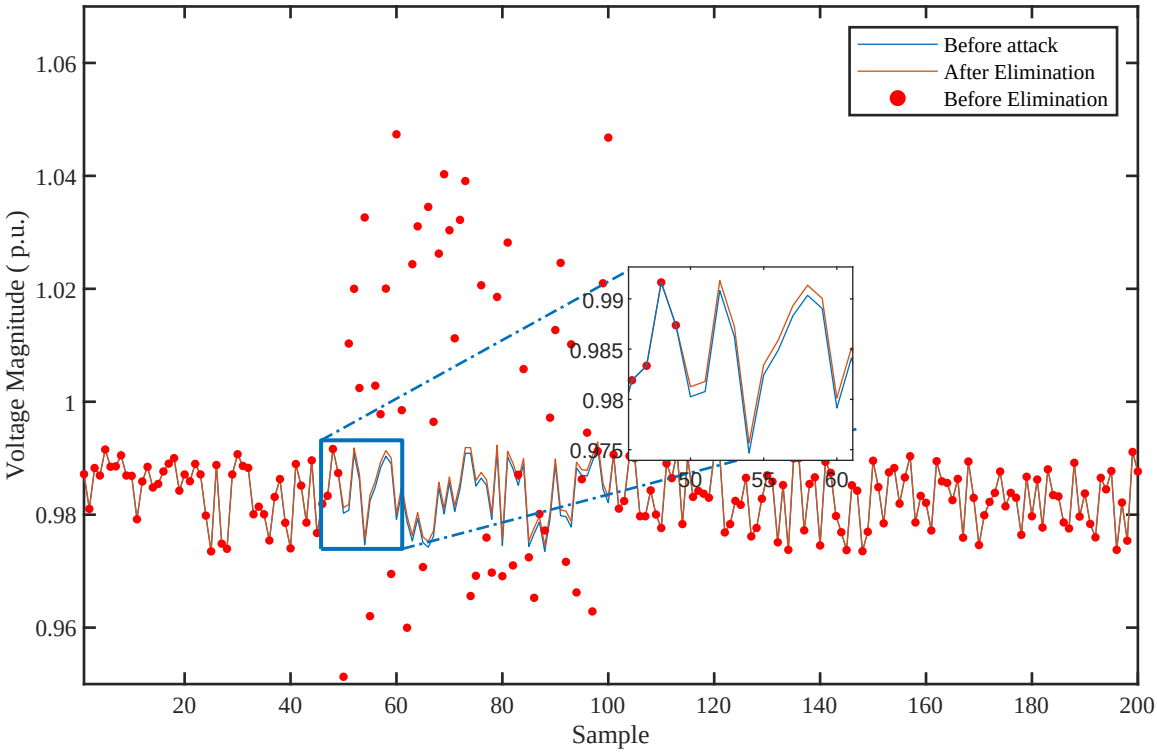


Figure 4.4: Data driven estimation under attack interval

In Fig 4.4, DoS attack is assumed to be present for long time also estimated states before attack and after attack is shown .Instead of estimating the state directly, we first estimated the time derivative of the state because we saw that, despite the states' large

variations in actual values, there were strong connections between numerous states in the way those patterns changed over time.

The choice of parameter k in Eq.4.4 also effects the estimation accuracy of this algorithm.Exact calculation of k requires more expertise on the field of power system such as topology of the network etc. After multiple simulations, it has been determined that selecting k between 1 to 7 results in better accuracy the given data driven estimation. This estimation algorithm is simple to implement and we can see that it is dynamically estimating the states with good accuracy.

Chapter 5

Conclusion

This report discuss the basic idea of state estimation in power system bu using machine learning algorithms . A global ML based algorithm is implemented for information fusion from the three different sensors namely SM,PMU,RTUs.Large data sets are generated for training and validating the models by using MATLAB.Furthermore,the report also discuss one of the frequent security vulnerability −DoS attack on distribution system. Impact of DoS attack is illustrated and a data driven estimation method is shown to estimates the states of the system in the attack interval .

5.1 Future Scope

This work assumes that topology of the system remain unchanged, which in real time scenario not holds true. Hence the model to be implemented to work on topology changes. Dimensional reduction by using principal component analysis can be done for faster execution of proposed algorithm. Data sets generated for the training model are produced by computer software rather than taking from original historic data. For better accuracy in real time case, it is better to train and validate with actual historic data obtained from power system data centers.Unsupervised machine learning can be studied for detection of new type of attacks.

Bibliography

[1] A. Abur and A. G. Exposito, *Power system state estimation: theory and implementation*. CRC press, 2004.

[2] A. Monticelli, *State estimation in electric power systems: a generalized approach*. Springer Science & Business Media, 2012.

[3] F. C. Schweppe and J. Wildes, "Power system static-state estimation, part i, ii & iii," *IEEE Transactions on Power Apparatus and Systems*, vol. 89, no. 1, pp. 120–125, 1970.

[4] D. Du, M. Zhu, X. Li, M. Fei, S. Bu, L. Wu, and K. Li, "A review on cybersecurity analysis, attack detection, and attack defense methods in cyber-physical power systems," *Journal of Modern Power Systems and Clean Energy*, 2022.

[5] H. Long, Z. Wu, C. Fang, W. Gu, X. Wei, and H. Zhan, "Cyber-attack detection strategy based on distribution system state estimation," *Journal of Modern Power Systems and Clean Energy*, vol. 8, no. 4, pp. 669–678, 2020.

[6] R. He, H. Xie, J. Deng, T. Feng, L. L. Lai, and M. Shahidehpour, "Reliability modeling and assessment of cyber space in cyber-physical power systems," *IEEE Transactions on Smart Grid*, vol. 11, no. 5, pp. 3763–3773, 2020.

[7] J. Sreenath, S. Chakrabarti, and A. Sharma, "Implementation of rauch-tung-striebel smoother for power system dynamic state estimation in the presence of pmu measurements," in *2015 IEEE Innovative Smart Grid Technologies-Asia (ISGT ASIA)*. IEEE, 2015, pp. 1–6.

[8] X. Zhong, A. Ahmadi, R. Brooks, G. K. Venayagamoorthy, L. Yu, and Y. Fu, "Side channel analysis of multiple pmu data in electric power systems," in *2015 Clemson University Power Systems Conference (PSC)*. IEEE, 2015, pp. 1–6.

[9] A. C. S. Hettiarachchige-Don, A. K. Manoharan, L. G. Pedaprolu, and V. Aravinthan, "Assessment of system reliability in presence of cyber attack risk on pmu data," in *2018 IEEE International Conference on Information and Automation For Sustainability (ICIAFS)*. IEEE, 2018, pp. 1–5.

[10] M. A. Hasnat and M. Rahnamay-Naeini, "A data-driven dynamic state estimation for smart grids under dos attack using state correlations," in *2019 North American Power Symposium (NAPS)*. IEEE, 2019, pp. 1–6.

[11] H. Long, Z. Wu, C. Fang, W. Gu, X. Wei, and H. Zhan, "Cyber-attack detection strategy based on distribution system state estimation," *Journal of Modern Power Systems and Clean Energy*, vol. 8, no. 4, pp. 669–678, 2020.

[12] S. Siamak, M. Dehghani, and M. Mohammadi, "Dynamic gps spoofing attack detection, localization, and measurement correction exploiting pmu and scada," *IEEE Systems Journal*, vol. 15, no. 2, pp. 2531–2540, 2020.

[13] L. Wang, Q. Zhou, and S. Jin, "Physics-guided deep learning for power system state estimation," *Journal of Modern Power Systems and Clean Energy*, vol. 8, no. 4, pp. 607–615, 2020.

[14] R. Yarlagadda, V. Kosana, and K. Teeparthi, "Power system state estimation and forecasting using cnn based hybrid deep learning models," in *2021 IEEE International Conference on Technology, Research, and Innovation for Betterment of Society (TRIBES)*. IEEE, 2021, pp. 1–6.

[15] S. Singh, A. K. Thakur, and S. P. Singh, "A new machine learning based approach for power system state forecasting," in *2022 IEEE Global Conference on Computing, Power and Communication Technologies (GlobConPT)*. IEEE, 2022, pp. 1–6.

[16] Y. Chen, Y. Tan, and D. Deka, "Is machine learning in power systems vulnerable?" in *2018 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*. IEEE, 2018, pp. 1–6.

[17] S. M. Miraftabzadeh, F. Foiadelli, M. Longo, and M. Pasetti, "A survey of machine learning applications for power system analytics," in *2019 IEEE International Con-*

ference on Environment and Electrical Engineering and 2019 IEEE Industrial and Commercial Power Systems Europe (EEEIC/I&CPS Europe). IEEE, 2019, pp. 1–5.

[18] 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, 2017.

[19] S. V. S. Chauhan and G. X. Gao, "Synchrophasor data under gps spoofing: Attack detection and mitigation using residuals," *IEEE Transactions on Smart Grid*, vol. 12, no. 4, pp. 3415–3424, 2021.

[20] H. C. Kherala and K. P. Badgujar, "Review on injection of false data attack into power system state estimation," in *2018 2nd International Conference on Trends in Electronics and Informatics (ICOEI)*. IEEE, 2018, pp. 1222–1226.

[21] M. H. Basiri, J. G. Thistle, J. W. Simpson-Porco, and S. Fischmeister, "Kalman filter based secure state estimation and individual attacked sensor detection in cyber-physical systems," in *2019 American Control Conference (ACC)*. IEEE, 2019, pp. 3841–3848.

[22] M. Rashed, J. Kamruzzaman, I. Gondal, and S. Islam, "False data detection in a clustered smart grid using unscented kalman filter," *IEEE Access*, vol. 10, pp. 78 548–78 556, 2022.

[23] N. Živković and A. T. Sarić, "Detection of false data injection attacks using unscented kalman filter," *Journal of Modern Power Systems and Clean Energy*, vol. 6, pp. 847–859, 2018.

[24] D. Wang, X. Wang, Y. Zhang, and L. Jin, "Detection of power grid disturbances and cyber-attacks based on machine learning," *Journal of information security and applications*, vol. 46, pp. 42–52, 2019.

[25] G. Tian, Q. Zhou, R. Birari, J. Qi, and Z. Qu, "A hybrid-learning algorithm for online dynamic state estimation in multimachine power systems," *IEEE transactions on neural networks and learning systems*, vol. 31, no. 12, pp. 5497–5508, 2020.