Zero-Sequence-Voltage-Based Detection and Localization Schemes for False Data Injection Attacks in Multiphase Power Distribution Systems

by

Chengran Ma

A thesis submitted in partial fulfillment of the requirements for the degree of

Master of Science

in

Communications

Department of Electrical and Computer Engineering
University of Alberta

Abstract

Modern power systems are vulnerable to false data injection attacks (FDIAs) due to the widespread applications of two-way communication networks for system operation and control. Diagnosing such malicious attacks are of great significance for the resilient operations of power systems.

Firstly, to detect the presence of FDIAs, a novel FDIA detection scheme is proposed in this thesis for three-phase distribution systems based on zero-sequence voltage (ZSV). From the voltage and power measurements, the bus voltages are estimated, and then the estimated ZSV is calculated as the sum of the estimated bus voltages on the three phases to represent the degree of unbalance of the distribution system. Via mathematical analysis of the linear distribution system state estimation (DSSE) model, the distribution of the estimated ZSV under the normal condition is derived, based on which a whitening process is adopted on the estimated ZSV to weaken the effect of measurement noises. The $\mathcal{L}_2$-norm of the whitened ZSV vector is then compared with a predefined threshold for the FDIA detection. Moreover, the probability of false alarm of the proposed scheme is derived, which can be utilized to determine the detection threshold for a desired tolerance of false alarm rate. The proposed FDIA detection scheme is validated on several IEEE Test Feeders and simulation results show the effectiveness of the proposed scheme in detecting FDIAs in three-phase distribution systems.

To further specify the locations of FDIAs, a ZSV-based FDIA localization scheme is also proposed in this thesis for three-phase distribution systems. Based on the estimated ZSV of a bus relative to others, the bus under attack is localized. By eliminating the effect of estimation error, an estimation of the injected attack is obtained. With an optimal test to minimize the error rate, the phase under attack can be diagnosed. By analyzing the estimated ZSV values in three steps, the bus localization and phase diagnosis can be achieved. Simulation results verify the effectiveness of the proposed FDIA localization method with high accuracy.

Preface

The material presented in this thesis is based on the original work by Chengran Ma. As detailed in the following, materials from some chapters of this thesis have been submitted as journal articles under the supervision of Prof. Yindi Jing and Prof. Hao Liang.

Chapter 2 includes the results published in the following journal paper:

- C. Ma, H. Liang, and Y. Jing, " A novel ZSV-based detection scheme for FDIAs in multiphase power distribution systems," *IEEE Trans. Smart Grid*, 2022, in press.

Chapter 3 includes the results to be submitted in the following journal paper:

- C. Ma, H. Liang, and Y. Jing, " A ZSV-based localization scheme for FDIAs in multiphase power distribution systems," finalizing and to be submitted to *IEEE Power Eng. Lett.*

Acknowledgements

First, I would like to express my sincere appreciation to my supervisors, Prof. Yindi Jing and Prof. Hao Liang for their patient guidance and continuous support of my M.Sc. study and research. Their immense knowledge, professional supervision, and encouragement helped me so much through my research at the University of Alberta.

In addition, it is a great honor for me to extend my gratitude to all my M.Sc. committee members for reviewing my thesis and providing valuable comments to improve it. I also thank all my colleagues and friends I met at the University of Alberta. Their help and friendship made my experience of M.Sc. Program productive and pleasant.

Finally, I would like to thank my parents for their unconditional love and encouragement throughout my research. I also thank my boyfriend, Mingzhe Wu, for his great support and companionship over the past six years.

Table of Contents

List of Tables

List of Figures

List of Symbols

$\boldsymbol{a}$	Attack vector injected to $\boldsymbol{V}_{mea}$ and $\boldsymbol{I}_{equ}$
$\boldsymbol{A}_S$	Index matrix for power measurements
$\boldsymbol{A}_V$	Index matrix for voltage measurements
$\boldsymbol{a}_{equ}$	Equivalent attack vector injected to $\boldsymbol{V}_{mea}$ and $\boldsymbol{S}_{mea}$
$\boldsymbol{c}$	Estimation deviation vector
$\boldsymbol{e}$	Complex measurement noise vector
$\boldsymbol{e}_I$	Complex current measurement noise vector (virtual)
$\boldsymbol{e}_S$	Complex power measurement noise vector
$\boldsymbol{e}_V$	Complex voltage measurement noise vector
$\boldsymbol{H}$	Matrix of linear measurement functions
$\boldsymbol{h}(\cdot)$	Vector of nonlinear measurement functions
$\boldsymbol{I}$	Actual complex current vector
$\boldsymbol{I}_{equ}$	Equivalent complex current vector
$\boldsymbol{I}_{mea}$	Complex current measurement vector (virtual)
$\boldsymbol{R}$	Covariance matrix of the measurement noise $\boldsymbol{e}$
$\boldsymbol{r}$	Residual vector
$\boldsymbol{r}_a$	Residual vector under attack
$\boldsymbol{R}_S$	Covariance matrices of the conjugate of the power measurement noise $\boldsymbol{e}_S^*$
$\boldsymbol{R}_V$	Covariance matrices of the voltage measurement noise $\boldsymbol{e}_V$
$\boldsymbol{S}$	Actual complex power vector
$\boldsymbol{S}_{mea}$	Complex power measurement vector
$\boldsymbol{U}_n$	The $n \times n$ identity matrix

$\boldsymbol{V}$	Actual complex bus voltage vector
$\boldsymbol{V}_0$	Zero-sequence voltage vector
$\boldsymbol{V}_a/\boldsymbol{V}_b/\boldsymbol{V}_c$	Actual complex bus voltage vector on phase $a/b/c$
$\boldsymbol{V}_p/\boldsymbol{V}_n$	Positive-sequence/negative-sequence voltage vector
$\boldsymbol{V}_{0,ave}$	Vector of the average of actual zero-sequence voltage
$\boldsymbol{V}_{0,proc}$	Processed zero-sequence voltage vector
$\boldsymbol{V}_{mea}$	Complex bus voltage measurement vector
$\boldsymbol{W}$	Transformation matrix for estimated zero-sequence voltage vector
$\boldsymbol{x}$	State variables
$\boldsymbol{x}_a$	State variables under attack
$\boldsymbol{Y}$	Admittance matrix
$\boldsymbol{z}$	Measurement vector
$\boldsymbol{z}_a$	Measurement vector under attack
$\boldsymbol{z}_n$	Measurement vector with no attack
$\Delta\boldsymbol{V}$	Estimation error vector for bus voltages
ϵ	Iteration threshold
$\hat{\boldsymbol{V}}$	Estimated bus voltage vector
$\hat{\boldsymbol{V}}_0$	Estimated zero-sequence voltage vector
$\hat{\boldsymbol{x}}$	Estimated state variables
$\hat{\boldsymbol{x}}_n$	Estimated state variables with no attack
$\hat{\boldsymbol{z}}$	Estimated measurement vector
$\hat{\boldsymbol{z}}_a$	Estimated measurement vector under attack
$\hat{c}$	Estimated injected fault value
$\hat{V}_{0,k,nei}$	Estimated zero-sequence voltage of the neighbor bus of bus k
λ	Bad data detection threshold
$\overline{\hat{V}_0}$	The average of estimated zero-sequence voltage of all buses
$\theta_a/\theta_b/\theta_c$	The angles of c in polar coordinates of three phases
h	Detection threshold
H_0	The hypothesis that the system is not under attack

H_1	The hypothesis that the system is under attack
k	The index of the bus under attack
m	Number of measurement units
m_1	Number of voltage measurement units
m_2	Number of power measurement units
n	Number of state variables
P_D	Detection rate
P_F	False alarm rate
P_L	Localization rate
P_M	Miss rate
P_{FL}	False localization rate
r	Residual value, the $\mathcal{L}_2$-norm of $\boldsymbol{r}$
T	Test statistic of detection scheme
$T_{NoWhiten}$	Test statistic of detection scheme with no whitening process

Abbreviations

BDD Bad Data Detection.

CPS Cyber Physical System.

DSSE Distribution System State Estimation.

EMS Energy Management System.

FDIA False Date Injection Attack.

PMU Phasor Measurement Unit.

RTU Remote Terminal Unit.

SCADA Supervisory Control and Data Acquisition.

WLS Weighted Least Square.

ZSV Zero-Sequence Voltage.

Chapter 1

Introduction

1.1 Background

With increasing penetrations of information and communication technologies, the traditional power system is gradually transitioning towards a future smart grid. The smart grid is a fully automatic electric network that can monitor and control all customers and nodes, enabling a two-way flow of electricity and information between the utility and users, as well as all nodes between them [1]. Facilitated by the highly integrated structure of information and communication technologies, as well as advanced electrical infrastructures, the smart grid possesses numerous advantages over the conventional power grid, such as improved fault monitory and recovery capabilities, increased efficiency and flexibility in the operation and control of power systems, as well as enhanced resiliency and robustness to outer disturbances [2, 3].

As the smart grid is a hybrid of power, information, and communication systems, in today's standards, it is also characterized as a typical cyber-physical system (CPS) [4]. As shown in Fig. 1.1, a CPS usually includes four layers, i.e., physical layer, sensor/actuator layer, network layer, and control layer [5]. The physical layer of a power system includes generation, transmission, and distribution networks, as well as the consumers. The information and data of the physical layer are measured in real-time by remote terminal units (RTUs) including meters and sensors, and then sent to the control layer via the communication network. The control center is usually equipped with the supervisory control and data acquisition (SCADA) system, whose function includes bad data detection (BDD), state estimation, economic dispatch, fault analysis, power flow calculation and optimization, etc. Then, the operation command on the power network is made in the control layer and delivered to the actuators via the communication network to control the physical layer, e.g., operating the power line circuit breaker.

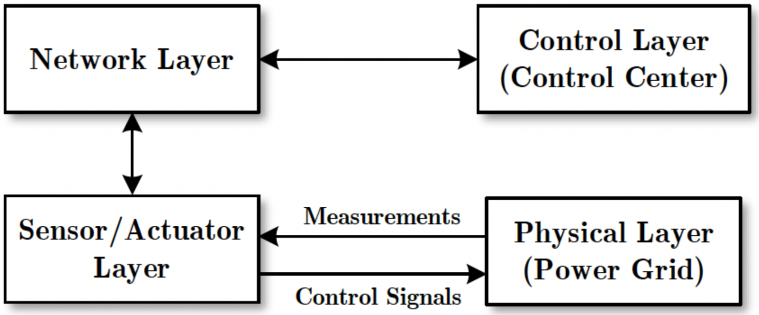

Figure 1.1: General structure of a CPS with multiple layers.

In the smart grid, the cyber system and physical process are tightly coupled. Due to cyber system vulnerabilities of the information and communication networks, cyber-attacks can be easily launched in various ways [6]. The typical types of cyber-attacks include denial of service attack, data injection attack, energy theft, the insertion of malware or worms, etc., all of which can cause significant economic and physical impacts on the CPS [7]. A summary of the major cyber-attacks in energy industry is presented in Table 1.1 [8]. Besides their huge physical and economical impacts, the increasing number of cyber-attacks is also considered as a real threat. According to the report from the U.S. Department of Energy [9], there were about 362 cases of power disturbances caused by the cyber-attacks from 2011 to 2014, where the number of attacks increased from 31 in 2011 to 161 in 2013.

Compared with power transmission systems where fiber optics are widely used for data communications, power distribution systems are more vulnerable to cyber-attacks due to the uses of public networks (e.g., Internet) and/or devices with broad-

Table 1.1: Major Cyber-Attacks in Energy Industry

Year	**Place**	**Attack Type**	**Attack Impact**
1982	Soviet Union	Code Manipulation	Three kilotons TNT equivalent explosion
1999	Bellingham, U.S.	Code Manipulation	A huge fireball that caused people injuries
2003	Oak Harbor, U.S.	Malware Injection	Parameter Display System was OFF for 5 hours
2008	Refahiye, Turkey	False Data Injection	Oil explosion and 300 barrels were leaked
2012	Saudi Arabia & Qatar	Malware Injection	Affected the generation and delivery of energy
2015	Kiev, Ukraine	False Data Injection	Large blackout affecting 225,000 customers

cast channels (e.g., cellular phone or Zigbee). Besides, the large number of customer devices and dispersed measurement units in power distribution systems provide more entry points of cyber-attacks, which exacerbate the difficulty for attack defense. A well-known example of cyber-attack on power distribution system is the Ukraine case in December 2015, as also summarized in Table 1.1. Aimed at affecting the power supply, three power distribution companies were under cyber-attacks, and a malicious remote operation of the circuit breakers was conducted via virtual private network (VPN), affecting approximately 225,000 customers across half of the country for over twelve hours [10].

Among the common types of cyber-attacks, the false data injection attack (FDIA) is considered as the most prominent and detrimental one [11, 12]. In smart grids, the potential targets for FDIAs can be either the physical devices (i.e., physical-based FDIAs) or data transmitted via the communication networks (i.e., communication-based FDIAs), as shown in Fig. 1.2. For physical-based FDIA, by injecting malicious data into the measurement, control, and protection devices that installed amongst the power grid, the attackers can tamper the estimated state variables, then control and disrupt the power system operations. The power system data collected by RTUs can also be modified via the data transmission process by communication-based FDIA through the communication networks.

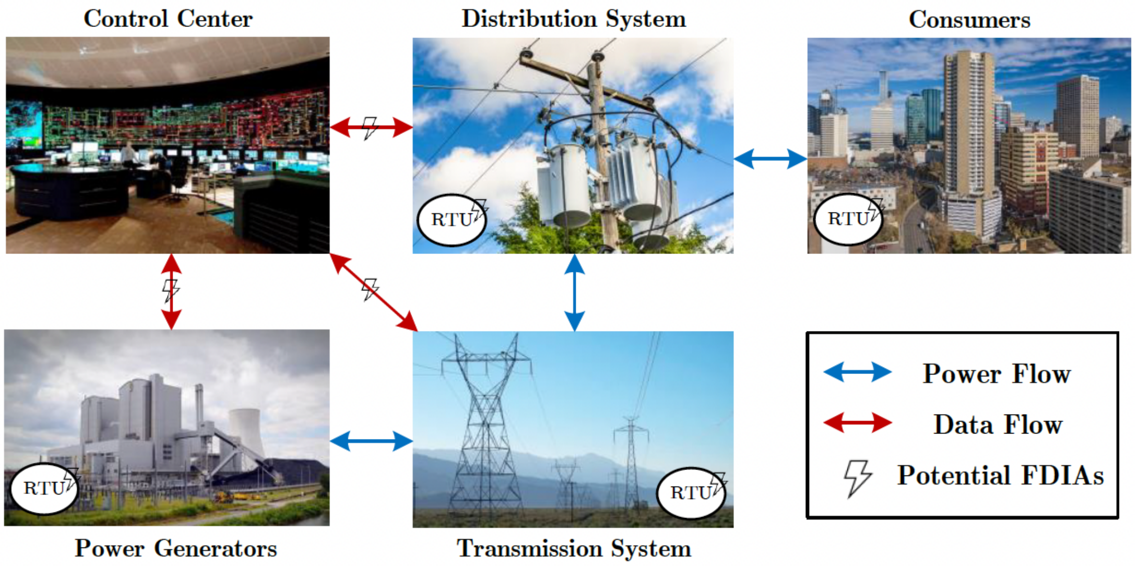

Figure 1.2: Potential targets of FDIAs on power systems.

In order to successfully launch FDIAs on power systems, various studies have been conducted on FDIA constructions. Although the targets of FDIAs include both transmission systems (transmit electric power from generating sites to electrical substations) and distribution systems (distribute electric power from substations to consumers), as shown in Fig. 1.2, their FDIA construction mechanisms are not identical due to their distinct characteristics. At the power transmission system level, *Liu et al.* first introduced the basic concept and construction mechanism of FDIAs that can avoid being detected by the BDD in control center [13]. On this basis, some improved FDIA construction models for power transmission systems have been developed under different considerations [14–18]. For example, the FDIA construction model proposed by *Liu* and *Li* in [14] only needs the local topology information for attack vector designs, instead of the complete topology information as in [13]. Such simplification was achieved by using a mixed integer programming model to reduce the required information. Then, in [18], *Liu* and *Li* extended the FDIA construction model under linear DC state estimation [14] to nonlinear AC state estimation, which is also applicable with incomplete topology information.

On the other hand, the FDIA construction models for power transmission systems cannot be straightforwardly applied to power distribution systems, as they were customized to the unique features of power transmission systems, such as the low x-to-r-ratio in distribution feeders, limited real-time measurement units, unbalanced load distribution, asymmetrical line parameters, and missing phase conditions in certain topologies. To fill this gap, firstly, in [19], a type of cyber-attack was analyzed by *Isozaki et al.* against voltage regulation for power distribution systems. Then, in [19], *Deng et al.* proposed an FDIA model for three-phase balanced distribution systems with limited knowledge of system states. To be more consistent with practical models, in [20] and [21], the linearized and physical-constraint-based nonlinear FDIA construction mechanisms in multiphase unbalanced distribution systems were further investigated.

As the well-designed FDIAs can easily bypass the BDD in the control center, it is of great significance in designing the effective countermeasures for FDIAs to protect the normal operations of power systems. The works in this thesis focus on the design of FDIA detection and localization schemes on multiphase distribution systems.

1.2 General Terms and Definitions

In this section, important terms used in this thesis are defined.

1.2.1 Power System State Estimation

Power system state estimation is a data processing tool performed by the energy management system (EMS) in the control center, for converting meter readings and other available information into an estimate of the state of power systems [22]. By collecting the real-time measurement data generated by the SCADA system and phasor measurement units (PMUs), including the bus voltage, active and reactive power of generators, power line, and load data, as well as the tap positions of transformers or phase shifters, the values of state variables (i.e., the bus voltage amplitudes and phase angles) of the power system can be obtained by state estimators. For most cases, the power system state estimation refers to the static state estimation to consider only the quasi steady-state operating conditions of power systems, while their dynamics such as generator dynamics and load dynamics are usually not taken into account.

1.2.2 Bad Data Detection

Considering the sampling errors of various measurement devices and the potential malicious cyber-attacks, in order to improve the accuracy of state estimation, the BDD technology is usually adopted after obtaining the estimated state variables to determine whether there is bad data in the measurements received by the SCADA. The BDD technology is operated by analyzing the difference between the measurement data and the estimated state variables, then compares it with a predefined threshold to identify the existence of the bad data in measurements and/or determine the locations of the measurement units where the bad data has been injected. After successfully identifying the bad data in the measurement set, the operators can first estimate the bad data value, and then use the estimated value to modify the original state estimation results. However, a well-designed FDIA construction can bypass the BDD.

1.2.3 Zero-Sequence Voltage

In order to analyze the unbalance degree of three-phase distribution systems, the three-phase unbalanced components (voltage or current) can be decomposed into three sequence components, i.e., zero-sequence component, positive-sequence component, and negative-sequence component [23]. Zero-sequence voltage consists of three-phase voltages with equal magnitudes and zero phase displacement. In other words, ZSV is the summation of voltages on three phases. Accordingly, positive-sequence voltage and negative-sequence voltage consist of three-phase voltages with equal magnitudes and 120-degree phase displacements with positive-sequence and negative-sequence, respectively. For perfectly balanced three-phase distribution systems, zero-sequence voltage and negative-sequence voltage are both zero, while the output voltages are only the positive-sequence components. As a result, the zero-sequence component, especially zero-sequence voltage, can well-represent the unbalance degree of distribution systems.

1.3 Literature Review

In this section, the existing research works regarding the DSSE, model-based and data-driven FDIA detection methods, as well as the FDIA localization methods are reviewed.

1.3.1 Distribution System State Estimation

Distribution system state estimation (DSSE) is used to obtain the state variables, e.g., bus voltage magnitude and phase angle, using the available measurement data collected at specific points over the distribution systems [24]. Similar to the state estimation design for power transmission systems, most of the DSSE methods are also voltage-based, i.e., the bus voltage magnitudes and phase angle values are used as state variables for DSSE. The forms of the state variables in voltage-based DSSE can be either based on polar form, i.e., magnitude and phase angle, or rectangular form, i.e., real and imaginary parts.

For polar form-based implementations of DSSE, in [25], a DSSE method based on the weighted least square (WLS) was proposed, which included the general measurement functions with a fast convergence speed. However, the Jacobina matrix with this method is both state-dependent and impedance-dependent, and it can be used for radial distribution networks only. In [26], a branch-based DSSE was proposed based on decomposing the whole WLS problem of the system into a series of WLS subproblems, so that each subproblem only relates to a single-branch state estimation. Such simplification can significantly improve the computational efficiency compared with [25]. However, the application scope of this method is still limited to the radial topology. In order to extend the application scope as well as to further reduce the computational burden, in [27], a linearized DSSE method was proposed, which can get rid of the iterative solving process and obtain the solutions directly. Both three-phase unbalanced and single-phase distribution systems are considered in this method, as well as the meshed distribution topology. The limitation of this method is its slightly reduced accuracy, i.e., the small angle difference assumption is made in this method that can degrade its accuracy to some extent.

For rectangular form-based implementations of DSSE, in [28], the rectangular coordinates are introduced to represent the state variables, where the resulted Jacobian matrix can be state-independent which reduces the overall complexity. However, as the current-based measurement functions are used in [28], the power measurements need to be converted into their equivalent currents in each iteration, which increases its complexity in implementation. Besides, the application scope of this method is still limited to radial distribution topology. In [29], a quasi-symmetric impedance matrix is used to formulate the distribution feeder and a matrix reduction technique is used to obtain the state variables. As a result, the computation efficiency can be improved, and the application scope can be extended to both radial and weakly meshed topologies. The major drawback is its complexity in the formulation.

1.3.2 Model-Based Detection Schemes for FDIAs

The existing FDIA detection schemes can be generally classified into model-based detection schemes and data-driven detection schemes, as shown in Fig. 1.3 [8]. For model-based detection schemes, they can be classified into estimation-based and estimation-free methods, depending on whether the state estimation is used in the detection process, including both static state estimation and dynamic state estimation. In this section, the existing model-based FDIA detection schemes are reviewed.

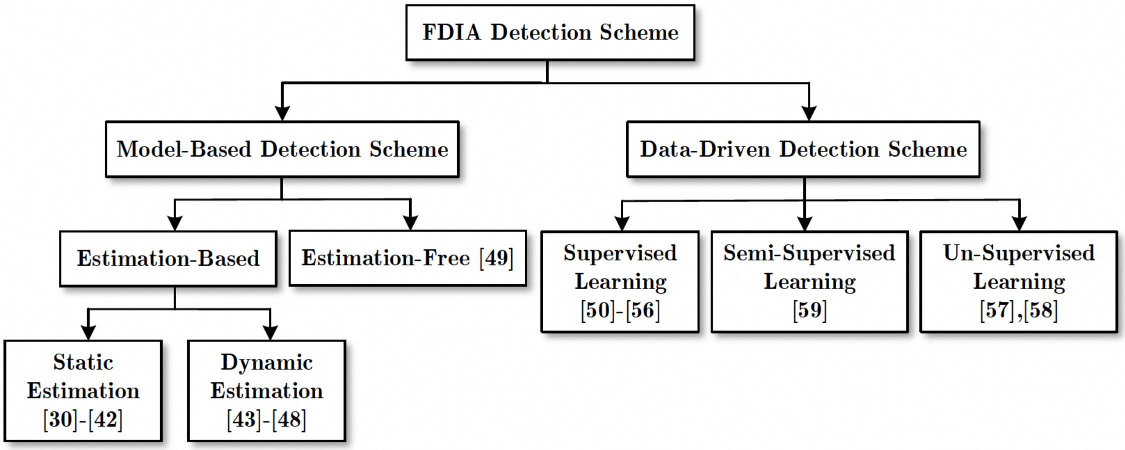
FDIA Detection Scheme
Model-Based Detection Scheme
Data-Driven Detection Scheme
Estimation-Based
Estimation-Free [49]
Supervised Learning [50]-[56]
Semi-Supervised Learning [59]
Un-Supervised Learning [57],[58]
Static Estimation [30]-[42]
Dynamic Estimation [43]-[48]

Figure 1.3: General classification of the existing FDIA detection schemes.

Static power system state estimation is the most widely-used state estimation method, which assumes the quasi steady-state operations of power systems. As discussed previously, the WLS is a main tool for static state estimation. In [30], the WLS with a residual pre-whitening procedure was used to detect in real-time the existence of FDIA that targets on the voltage measurements. In [31], a recursive state estimation method based on WLS was proposed, which combined the historical data and the current measurement data recursively to increase both the detection accuracy and the convergence speed of state estimation. In [32], the WLS was used to detect in real-time the FDIA that targets on the voltage controllers in transmission systems, with the help from the control signals and quantitative node voltage stability index. In [33], a model-based FDIA detection scheme was proposed based on a linearized three-phase interval state estimation (ISE) with WLS, which leverages the information in the state domain. The existence of FDIA in distribution systems is detected when the estimated state variables are out of the boundaries set by the linearized ISE. However, one limitation of this method is that the calculated boundaries are sensitive to noises which may lead to high false alarm rate and low detection rate. Moreover, the data used for calculating the boundaries are obtained from measurements collected in previous operation periods from SCADA which may be outdated. In order to further increase the detection accuracy, some proactive FDIA detection methods have been developed that based on distributed flexible AC transmission system (D-FACTS) devices [34–36]. By changing the system parameters actively, the existence of FDIAs can be reflected by the WLS state estimation results after modifications. The detailed analysis on its feasibility and limitations were presented in [34]. Despite the WLS-based methods, other static state estimation methods have also been adopted for detecting FDIAs, such as the median filtering (MF) [37], Kriging estimator (KE) [38], maximum likelihood estimation (MLS) [39–41], and minimum mean square error estimator (MMSE) [42].

For dynamic power system modeling that considers the transients and dynamic changes, the dynamic state estimation tools are used for FDIA detection, where the Kalman filter (KF) is considered to be the most widely used one [43–45]. Some advanced versions of KF, such as distributed KF (DKF) with reduced computational burden [46] and extended KF (EKF) with nonlinear modeling [47] were also used to detect FDIA in power systems. Despite the KF and its variants, the unknown input observation (UIO) was also used for FDIA detections [48].

On the other hand, some model-based detection methods are only based on the system model and/or parameters without utilizing the state-estimation. For example, in [49], the FDIA detection problem was re-formulated as a matrix separation problem based on both the measurement matrix and the attack matrix. Then the performances of different algorithms in solving this matrix separation formulation for FDIA detection were compared, including augmented lagrange multipliers (ALMs), the low rank matrix factorization (LMaFit), as well as the Go Decomposition (GoDec) approaches. Compared with the estimation-based method, such direct representations based on system parameters (e.g., measurement matrix) are more straightforward, but more complicated in the formulation and implementation process.

1.3.3 Data-Driven Detection Schemes for FDIAs

The data-driven FDIA detection schemes are based on machine learning. Machine learning schemes can be classified into supervised learning, semi-supervised learning, and un-supervised learning, depending on whether the data used for training is labelled and/or unlabelled, where the labelled data means that the data are known to be either malicious or normal.

For supervised machine learning-based methods, in [50], the distributed support vector machine (SVM) was used to detect FDIAs, which was based on the alternating direction method of multipliers and can ensure provable optimality and convergence rate. In [51–54], various artificial neural network (ANN)-based methods were developed, such as feedforward neural network (FNN) [51], recurrent neural network (RNN) [52], deep neural network (DNN) [53], and convolutional neural network (CNN) [54], etc., and each type of neural network has its unique characteristics in FDIA detection. For example, the superiority of CNN in extracting different features of the target makes it popular for pattern recognition, which is also advantageous for FDIA detection. In [55], the decision tree (DT), which is another popular tool in machine learning, was used together with the SVM for FDIA detection. The input data are first processed by DT and then are sent to the SVM classifier to obtain the detection result. Such two-layer implementation can improve the detection accuracy compared with conventional SVM-based methods. In [56], the detection performance of FDIAs in power distribution systems using Bayesian network (BN), SVM, K-nearest neighbour (KNN), DT, and multilayer perceptron were analyzed and compared comprehensively. Overall, although satisfactory detection performance can be achieved with supervised learning-based methods, a large amount of labelled data are needed for model training purposes, which are often unavailable in practice.

For unsupervised machine learning-based methods where the input data are unlabelled, the hidden features of the data are studied and classified by the machine, thus can also be used for detecting FDIAs. In [57], an FDIA detection method by deep belief network (DBN) was proposed, and the comparison results show that it has better performance than the SVM-based methods. In [58], the hidden Markov model (HMM) was used to detect FDIA in advanced metering infrastructure (AMI) in power systems.

The semi-supervised learning has also been adopted for FDIA detection for power distribution systems [59], which only requires a limited set of labelled training data to ensure the detection accuracy. For example, the labelled data only consist of 12.5% of the whole data set used for the modeling and the training purpose.

Compared with model-based FDIA detection schemes, the data-driven methods are free from the system model and parameters. Besides, they usually have fast detection process to enable real-time FDIA detections, and they avoid the issue of the threshold selection needed in many model-based detection methods. However, for data-driven detection methods, extensive training and/or extra memory space are usually required, as well as a large amount of historical data set of the power system for training purposes.

1.3.4 Localization Schemes for False Data Injection Attacks

Although various FDIA detection schemes for power systems have been developed, there are very few attempts on the FDIA localization [60–65]. Accurate localizations of FDIAs can help operators deploy countermeasures quickly and efficiently, reducing the impacts on power systems.

The FDIA localization schemes in [60] and [61] are based on interval observers [60], [61], and those in [62–65] use advanced machine learning tools. The interval observer-based methods with dynamic model of power systems suffer from high complexity in modelling and constructing the customized logical localization judgment matrix, which limits their scalability and implementations in real-world large power systems. For machine learning-based schemes, the first attempt was made in [62], with the help of the CNN as a multilabel classifier as well as the classical BDD unit. In [63], a joint FDIA detection and localization scheme was proposed based on graph neural networks (GNN), which can exploit the inherent graph topology of power systems and the spatial correlations of the measurement data to help detect and localize the FDIAs. In [64], a method by combining SVM and ANN was used to detect and localize FDIAs, which is based on dividing the power systems into several areas and equipping each area with an ANN-based detector. With a distributed state estimation, the state of each local area can be estimated and used as the trained neural network input to detect and localize FDIAs. However, the method in [64] can only find the approximate area of the FDIA, not the accurate location. In [65], an auto-encoder-based generative adversarial network was used for detecting the FDIA, and a pattern match algorithm was used for localizing the FDIA. The implementation of these schemes is also limited by not only their high complexity but also privacy concerns.

1.4 Thesis Motivation and Contribution

According to the discussion above, although there are many research works on detecting and localizing the FDIAs for power systems, the majority of them are focused on power transmission systems, which cannot be straightforwardly extended to distribution systems that are featured by larger scale and less labeled data with lower-level measurement accuracy. The large topology scale of distribution systems, as well as their unbalanced and dynamic nature introduce extra complex and nonlinear relationships in the historical data set, which make the existing FDIA detection and localization methods less effective for power distribution systems. Due to the innate difficulties in detecting FDIAs for power distribution systems, only a handful of studies have been conducted [33], [56], and [59], where their shortcomings and limitations have been discussed in details previously. Moreover, no existing study has focused on designing the FDIA localization scheme for power distribution systems. Therefore, it is of great significance to develop training-data-free, simple-implementation, but effective FDIA detection and localization schemes for power distribution systems, which are the motivations of this work.

The thesis contributions are summarized as follows.

- **ZSV-Based FDIA Detection Scheme for Multiphase Distribution Systems**

We propose a novel detection scheme for FDIAs in multiphase distribution systems based on ZSV. The utilization of ZSV transforms the detection of FDIAs from the measurement domain to the state domain, which can directly detect the stealth FDIAs with high precision. Besides, the estimation error of the approximate linear DSSE is analyzed under the normal condition, based on which a transformation process is proposed to whiten the estimated ZSV vector. This process eliminates the correlation among the entries of the estimated ZSV vector, subsequently weakening the effect of system noises on the detection. Finally, the probability of false alarm is derived for the proposed detection scheme. This result can be used to find the detection threshold for a given level of false alarm rate, which is crucial for practical implementations in utility grids.

- **ZSV-Based FDIA Localization Scheme for Multiphase Distribution Systems**

We propose an FDIA localization scheme based on ZSV for multiphase distribution systems. With the estimated bus voltages derived from DSSE, the estimated ZSV vector is calculated. By comparing the estimated ZSV values, the bus under attack can be localized. Then the information of estimation deviation can be extracted by eliminating the effect of estimation error. Finally, the phase under attack can be diagnosed by analyzing the information of estimation deviation. The proposed FDIA localization scheme is the first in literature that designed for power distribution systems, which can be implemented under all existing DSSE methods with high universality. In addition, the proposed FDIA localization scheme shows very high accuracy in localizing both the bus under attack and phase under attack of the power distribution systems under various testing conditions.

1.5 Thesis Outline

This thesis consists of four chapters which are organized as follows: in Chapter 1, the research background and some key definitions are introduced. Besides, the related works for DSSE, FDIA detection and localization schemes in recent years are reviewed. In addition, the research motivation and contributions are presented. Chapter 2 presents an FDIA detection method for multiphase distribution systems based on ZSV. Both the implementation process and mathematical analysis of the proposed FDIA detection method are presented. The performance of this proposed FDIA detection scheme is evaluated using case studies based on standard IEEE Test Feeders. In Chapter 3, an FDIA localization scheme for multiphase distribution systems based on ZSV is proposed, where both the bus and phase under attack can be accurately localized. The feasibility of the proposed FDIA localization scheme is verified using the standard IEEE Test Feeders under various environments. In Chapter 4, the contributions of this thesis and the future works are summarized.

Chapter 2

ZSV-Based FDIA Detection Scheme for Multiphase Power Distribution Systems

In this chapter, an FDIA detection scheme based on ZSV is proposed for multiphase power distribution systems. By calculating the sum of the estimated bus voltages on the three phases, the estimated ZSV is obtained, which represents the unbalance degree of a three-phase distribution system. Mathematical analysis is conducted on the estimation error of the bus voltages and the distribution of the obtained ZSV vector for the case that the system is not under attack. Based on the analytical results, a whitening process is implemented to eliminate the correlation among the elements of the estimated ZSV vector and reduce the influence of noises. Then the FDIA detection scheme is carried out by comparing the $\mathcal{L}_2$-norm of the processed estimated ZSV vector with a predetermined threshold. The relationship between the false alarm rate and the detection threshold is also derived. Case studies based on IEEE Test Feeders verify the effectiveness of the proposed method.

The remainder of this chapter is organized as follow. In Section 2.1, we introduce the state estimation and FDIA principles for three-phase distribution systems. Section 2.2 presents the FDIA detection scheme based on ZSV for multiphase distribution systems as well as its detailed mathematical analysis. In Section 2.3, the simulation results are provided to validate the effectiveness of the proposed method.

Finally, the summary of this chapter is given in Section 2.4.

2.1 State Estimation and FDIA Principles for Three-Phase Distribution Systems

In this section, the nonlinear DSSE model and a DSSE model with linear approximation of the three-phase distribution system are introduced. Then the principles of FDIAs against DSSE are presented.

2.1.1 Non-Linear DSSE in Distribution Systems

We consider a three-phase distribution system with n nodes and m meters, where $m \geq n$. Denote the vector of state variables as $\boldsymbol{x} \in \mathbb{C}^{3n \times 1}$ and the vector of measurements as $\boldsymbol{z} \in \mathbb{C}^{3m \times 1}$. The following non-linear DSSE model can be used for distribution systems [19]:

$$\boldsymbol{z} = \boldsymbol{h}\left(\boldsymbol{x}\right) + \boldsymbol{e}, \tag{2.1}$$

where $\boldsymbol{h}(\cdot)$ contains the measurement functions involving the system topology and parameters, and $\boldsymbol{e} \in \mathbb{C}^{3m \times 1}$ is the vector of measurement noises. A common assumption on the noises is that $\boldsymbol{e} \sim \mathcal{CN}(\mathbf{0}_{3m}, \boldsymbol{R})$, i.e., the noise vector $\boldsymbol{e}$ follows the complex Gaussian distribution whose mean vector and covariance matrix are $\mathbf{0}_{3m}$ and $\boldsymbol{R}$, respectively; and $\mathbf{0}_{3m}$ denotes the $3m \times 1$ vector of all zero entries.

The WLS estimate of the state vector, denoted as $\hat{\boldsymbol{x}}$, is the solution of the following WLS minimization problem [19]:

$$\hat{\boldsymbol{x}} = \arg\min J(\boldsymbol{x}) = \arg\min \left[\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x})\right]^H \boldsymbol{R}^{-1} \left[\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x})\right], \tag{2.2}$$

where $(\cdot)^H$ denotes the Hermitian (or conjugate transpose). The solution of this optimization problem is given by

$$\frac{\partial J(\boldsymbol{x})}{\partial \boldsymbol{x}} = \boldsymbol{H}^H(\boldsymbol{x})\boldsymbol{R}^{-1} \left[\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x})\right] = 0, \tag{2.3}$$

where $\boldsymbol{H}(\boldsymbol{x}) = \partial \boldsymbol{h}(\boldsymbol{x})/\partial \boldsymbol{x}$ is the Jacobian matrix of the measurement functions $\boldsymbol{h}(\boldsymbol{x})$. The WLS estimate is usually solved iteratively by

$$\hat{\boldsymbol{x}}_{k+1} = \hat{\boldsymbol{x}}_k + \left[\boldsymbol{H}^H(\boldsymbol{x})\boldsymbol{R}^{-1}\boldsymbol{H}(\boldsymbol{x})\right]^{-1}\boldsymbol{H}^H(\boldsymbol{x})\boldsymbol{R}^{-1}[\boldsymbol{z} - \boldsymbol{h}(\boldsymbol{x})], \tag{2.4}$$

where $\hat{\boldsymbol{x}}_k$ is the estimated state vector in the k-th iteration.

2.1.2 Non-Linear FDIA Principles

With the objective of misleading the operators, hackers usually inject malicious data into the meters. The measurement vector under attack $\boldsymbol{z}_a$ can be modeled as

$$\boldsymbol{z}_a = \boldsymbol{z}_n + \boldsymbol{a}, \tag{2.5}$$

where $\boldsymbol{a} \in \mathbb{C}^{3m\times 1}$ denotes the erroneous vector on the three phases which manipulates the measurement vector with no attack $\boldsymbol{z}_n$.

- **Residual-Based BDD**

A widely used method to detect erroneous data is the residual-based BDD. The residual vector $\boldsymbol{r}$ is the difference between the measurements $\boldsymbol{z}$ and the estimated measurements $\hat{\boldsymbol{z}} \triangleq \boldsymbol{h}(\hat{\boldsymbol{x}})$, i.e.,

$$\boldsymbol{r} = \boldsymbol{z} - \hat{\boldsymbol{z}} = \boldsymbol{z} - \boldsymbol{h}(\hat{\boldsymbol{x}}). \tag{2.6}$$

The residual value r, which is the $\mathcal{L}_2$-norm of $\boldsymbol{r}$, i.e., $r \triangleq \|\boldsymbol{r}\|_2$, is compared with a predefined threshold λ to detect the attack. If $r > \lambda$, the detection result is the existence of an attack, and vice versa. The BDD can detect many malicious injections, however, it does not function for stealthy FDIAs [8].

- **Stealthy FDIA**

Stealthy FDIAs are specifically designed to mislead the operators to obtain a deviated state estimation $\hat{\boldsymbol{x}}_a$, modeled as $\hat{\boldsymbol{x}}_a = \hat{\boldsymbol{x}}_n + \boldsymbol{c}$, where $\hat{\boldsymbol{x}}_n$ is the supposed state estimation when there is no attack and $\boldsymbol{c} \in \mathbb{C}^{3n\times 1}$ denotes the estimation deviation of the three-phase state variables. Particularly, for the general non-linear DSSE model in (2.1), the attack vector $\boldsymbol{a}$ is designed to satisfy

$$\boldsymbol{a} = \boldsymbol{h}(\hat{\boldsymbol{x}}_a) - \boldsymbol{h}(\hat{\boldsymbol{x}}_n). \tag{2.7}$$

With this design, from (2.5), the residual vector under attack can be calculated as

$$\boldsymbol{r}_a = \boldsymbol{z}_a - \hat{\boldsymbol{z}}_a = \boldsymbol{z}_n + \boldsymbol{a} - \boldsymbol{h}(\hat{\boldsymbol{x}}_a) = \boldsymbol{z}_n - \boldsymbol{h}(\hat{\boldsymbol{x}}_n) = \boldsymbol{r}, \tag{2.8}$$

which is the same as the residual vector when the attack does not exist. It can thus bypass BDD.

2.1.3 DSSE and FDIA with Linear Approximation

When practically implementing stealth FDIAs, due to the limitation of attacker's capability and the lack of knowledge of state variables and measurements [66], the linearization of DSSE in distribution systems is necessary. Different approaches have been developed in recent works [24]. For the multiphase unbalanced distribution systems considered in this work, we use the DSSE method with linear approximation in [28].

In this model, the three-phase measurements $\boldsymbol{z}$ consist of voltage measurements $\boldsymbol{V}_{mea}$ and equivalent current measurements $\boldsymbol{I}_{equ}$, which are calculated from the power measurements $\boldsymbol{S}_{mea}$. Here, $\boldsymbol{V}_{mea} \in \mathbb{C}^{3m_1 \times 1}$ is composed of both complex bus voltages and equivalent complex bus voltages; and the total number of voltage measurements is $3m_1$ for all three phases. Also, $\boldsymbol{S}_{mea} \in \mathbb{C}^{3m_2 \times 1}$ is composed of both complex power injections and complex power flows; and the total number of power measurements is $3m_2$ for all three phases. Thus, $m_1 + m_2 = m$. Further, the equivalent complex voltages are obtained from the bus voltage magnitudes combined with the phase angle of the nearest bus equipped with a PMU. The complex bus voltages $\boldsymbol{V}$ in the power distribution system are chosen as the state variables. The notations $\boldsymbol{e}_V \in \mathbb{C}^{3m_1 \times 1}$ and $\boldsymbol{e}_S \in \mathbb{C}^{3m_2 \times 1}$ are used for the vectors of the voltage and power measurement noises, respectivley, where the elements are assumed to follow zero-mean complex Gaussian distributions.

Due to limited resources in some systems, not all nodes are equipped with measurement units. Two indicator matrices are introduced to represent the elements of the state variables that have corresponding measurements. Specifically, the $3m_1 \times 3n$ matrix $\boldsymbol{A}_V$ and the $3m_2 \times 3n$ matrix $\boldsymbol{A}_S$ show the elements of $\boldsymbol{V}$ which have voltage and power measurements, respectively. The elements of $\boldsymbol{A}_V$ and $\boldsymbol{A}_S$ are either 1's or 0's, and there is a single 1 in each row of these two matrices. Take a 5-bus three-phase distribution system as an example. Assuming that the bus voltages are measured in three phases at bus 1 and bus 2, and the power injections are measured in three phases at bus 3, bus 4, and bus 5, then the two indicator matrices are given by

$$\boldsymbol{A}_V = \begin{bmatrix} 10000 \\ 01000 \end{bmatrix} \otimes \boldsymbol{U}_3, \boldsymbol{A}_S = \begin{bmatrix} 00100 \\ 00010 \\ 00001 \end{bmatrix} \otimes \boldsymbol{U}_3, \tag{2.9}$$

where $\boldsymbol{U}_3$ denotes the 3×3 identity matrix and $\otimes$ represents the Kronecker product.

The DSSE model with linear approximation can be written as

$$\boldsymbol{z} \approx \boldsymbol{H}\boldsymbol{V} + \boldsymbol{e}, \tag{2.10}$$

where

$$\boldsymbol{z} \triangleq \begin{bmatrix} \boldsymbol{V}_{mea} \\ \boldsymbol{I}_{equ} \end{bmatrix}, \boldsymbol{H} \triangleq \begin{bmatrix} \boldsymbol{A}_V \\ \boldsymbol{Y}\boldsymbol{A}_S \end{bmatrix}, \boldsymbol{e} \triangleq \begin{bmatrix} \boldsymbol{e}_V \\ \boldsymbol{e}_S^* \end{bmatrix}. \tag{2.11}$$

Here, $\boldsymbol{Y}$ represents the admittance matrix, which is composed of both the complex bus admittance matrix and the complex branch admittance matrix with respect to the power measurements. The notation $(\cdot)^*$ represents the complex conjugate.

For systems without direct current measurements but with power measurements of some nodes, we use $\boldsymbol{I}$ to denote the $3m_2 \times 1$ vector of current values where power measurements are available, given by

$$\boldsymbol{I} = \boldsymbol{Y}\left(\boldsymbol{A}_S\boldsymbol{V}\right). \tag{2.12}$$

Thus the power measurements can be written as

$$\boldsymbol{S}_{mea} = \boldsymbol{S} + \boldsymbol{e}_S = \text{diag}\{\boldsymbol{I}\}^* \boldsymbol{A}_S \boldsymbol{V} + \boldsymbol{e}_S, \tag{2.13}$$

where diag$\{\boldsymbol{I}\}$ is the diagonal matrix whose diagonal entries are elements of the vector $\boldsymbol{I}$. When there is no measurement noises, the true current vector is

$$\boldsymbol{I} = \text{diag}^{-*}\{\boldsymbol{A}_S \boldsymbol{V}\}\boldsymbol{S}^*, \tag{2.14}$$

where $(\cdot)^{-*}$ represents the conjugate of the inverse of a matrix. But when the noises exist, we use the power measurement $\boldsymbol{S}_{mea}$ and the estimated voltages $\hat{\boldsymbol{V}}$ to obtain equivalent current measurements, which is given by

$$\boldsymbol{I}_{equ} = \text{diag}^{-*}\{\boldsymbol{A}_S \hat{\boldsymbol{V}}\}\boldsymbol{S}^*_{mea}, \tag{2.15}$$

where $\hat{\boldsymbol{V}}$ is the bus estimated voltage vector. The equivalent current vector $\boldsymbol{I}_{equ}$ is used as an approximation for the direct current measurements $\boldsymbol{I}_{mea}$ to obtain the approximate linear DSSE model in (2.10). For this DSSE model, the WLS state estimation is known to be

$$\hat{\boldsymbol{V}} = (\boldsymbol{H}^H \boldsymbol{R}^{-1} \boldsymbol{H})^{-1} \boldsymbol{H}^H \boldsymbol{R}^{-1} \boldsymbol{z}. \tag{2.16}$$

If $\boldsymbol{e}_V$ and $\boldsymbol{e}_S$ are independent, then the covariance matrix of noise vector can be presented as

$$\boldsymbol{R} \triangleq \begin{bmatrix} \boldsymbol{R}_V & \boldsymbol{0} \\ \boldsymbol{0} & \boldsymbol{R}_S \end{bmatrix}, \tag{2.17}$$

where $\boldsymbol{R}_V$ and $\boldsymbol{R}_S$ represent the covariance matrices of the noise vectors $\boldsymbol{e}_V$ and $\boldsymbol{e}^*_S$, respectively. Note that since the equivalent complex current is calculated as the conjugate of the ratio of power and voltage in (2.15), the noise vector at the power measurements is the conjugate form $\boldsymbol{e}^*_S$.

To implement the state estimation, the equivalent currents and the voltage estimates are calculated iteratively using (2.15) and (2.16), respectively, until convergence. For the initialization step, a common choice for $\hat{\boldsymbol{V}}$ is the vector of all 1's. A small positive value, denoted as ϵ, is used as the threshold for the termination of the iterations.

In distribution systems, some of the buses may only be equipped with one or two phases. For these buses, the virtual lines can be added to facilitate the implementation of the proposed detection scheme [20]. Specifically, the admittance of the missing phases is assigned with arbitrary values, and the mutual admittance between an existing phase and a missing phase is set to zero. Accordingly, the corresponding power and current measurements on missing phases are set as zero, and the voltage measurements are set as the voltages of the nearest upstream bus equipped with the missing phases. In this way, each bus in the distribution system is virtually equipped with three phases, and the proposed scheme is generalized for systems with missing phases.

For this linear approximate DSSE, by following the conditions in (2.7), a stealthy FDIA needs to be designed to satisfy

$$\boldsymbol{a} = \boldsymbol{H}\boldsymbol{c}, \tag{2.18}$$

so the residual vector $\boldsymbol{r}$ is unchanged under the attack. Since the second part of the measurement function matrix $\boldsymbol{H}$ in (2.11) is constructed based on the equivalent current measurements $\boldsymbol{I}_{equ}$, the corresponding part of the designed stealthy attack $\boldsymbol{a}$ is related to the virtual injections on the equivalent current measurements. In the practice of the attack, $\boldsymbol{a}$ needs to be transformed to $\boldsymbol{a}_{equ}$, which is the attack vector injected into the direct voltage measurements $\boldsymbol{V}_{mea}$ and power measurements $\boldsymbol{S}_{mea}$, such that with the injection of $\boldsymbol{a}_{equ}$ to the voltage and power measurements, the resulting measurement vector $\boldsymbol{z}$ becomes $\boldsymbol{z} + \boldsymbol{a}$. More detailed derivation steps of the transformation can be found in [20].

2.2 FDIA Detection Scheme Based on ZSV

To deal with the challenging FDIA detection problem in distribution systems, we propose to conduct the detection in the state domain. Particularly, the ZSV vector is used, which reflects the unbalance degree of each bus. Furthermore, a whitening process is designed to reduce the influence of measurement noises. In this section, the concept of ZSV is introduced first. Then, the proposed detection scheme is elaborated. Additionally, the estimation error and the false alarm rate of the proposed scheme are analyzed.

2.2.1 ZSV in Three-Phase Distribution Systems

In a three-phase distribution system, the three phase voltages $\boldsymbol{V}_a$, $\boldsymbol{V}_b$ and $\boldsymbol{V}_c$ can be resolved into three sequence components [23]: zero-sequence component $\boldsymbol{V}_0$, positive-sequence component $\boldsymbol{V}_p$, and negative-sequence component $\boldsymbol{V}_n$. The three sequence voltages can be formulated as follows:

$$\begin{bmatrix} \boldsymbol{V}_0 \\ \boldsymbol{V}_p \\ \boldsymbol{V}_n \end{bmatrix} = \frac{1}{3} \begin{bmatrix} 1 & 1 & 1 \\ 1 & a & a^2 \\ 1 & a^2 & a \end{bmatrix} \begin{bmatrix} \boldsymbol{V}_a \\ \boldsymbol{V}_b \\ \boldsymbol{V}_c \end{bmatrix}, \tag{2.19}$$

where $a = e^{j(2\pi/3)}$.

In power transmission systems, the topology is a mesh structure, and each bus is equipped with three phases in good balance [67]. Thus the attacker can inject the FDIAs in a substation on three phases at the same time. The operator can transform the three-phase balanced system into a single-phase system for FDIA detection. However, in power distribution systems, the topology is a radial structure, and each customer is usually connected to a single phase [68]. Thus, the attacker usually injects the attack in a single phase of a bus only. The ZSV vector $\boldsymbol{V}_0$ represents the voltage on the neutral wire of each bus in a distribution system. If the system is perfectly balanced, $\boldsymbol{V}_0$ is a vector with all 0's. In a three-phase unbalanced distribution system, the values of $\boldsymbol{V}_0$ may be non-zero and they reflect the unbalance degree

[69]. In a healthy and normally operating distribution system, the ZSV vector is very close to zero. The estimation deviation $\boldsymbol{c}$ of a stealthy FDIA in distribution systems is usually on the voltage magnitude of one phase of a bus. This injected deviation will cause an apparent change in the unbalance degree of the system. Therefore, we can assume that a sudden and obvious change of ZSV represents the existence of an FDIA. If the attacker injects several FDIAs into multiple phases or multiple buses in the distribution system, the ZSV-based detection scheme can still be applied if the FDIAs cause system unbalanced that affects the ZSV of the buses. There is one special and uncommon case that the FDIAs are injected into one bus on all three phases with the same magnitudes. In this case, the proposed detection scheme is not applicable. Instead, we can equate the model to a single-phase distribution system and implement detection schemes designed for single-phase distribution systems.

The utilization of ZSV transforms the FDIA detection from the measurement domain to the state domain. For the traditional residual-based BDD and many other detection schemes, the values and features of measured data are used for detection. One problem is that the measured data obtained by operators is limited in distribution systems and the attacker can design stealthy FDIAs according to the measurement function $\boldsymbol{H}$. In this case, transforming the detection problem into the state domain is more effective. The ZSV vector can directly reflect abnormal changes of state variables and can be used for FDIA detection in three-phase unbalanced distribution systems.

2.2.2 Proposed FDIA Detection Scheme

The FDIA detection problem is a binary hypothesis testing problem with the following two hypotheses: the system is not under attack (denoted as H_0) and the system is under attack (denoted as H_1). From the linear approximate model in (2.10), the detection problem can be modeled as the following

$$H_0: \quad \boldsymbol{z} \approx \boldsymbol{H}\boldsymbol{V} + \boldsymbol{e}, \tag{2.20}$$

$$H_1 : \quad \boldsymbol{z} \approx \boldsymbol{HV} + \boldsymbol{a} + \boldsymbol{e}, \tag{2.21}$$

where $\boldsymbol{a} \neq \boldsymbol{0}$.

The voltage vector is constructed as

$$\boldsymbol{V} = \left[\boldsymbol{V}_a^T,\ \boldsymbol{V}_b^T,\ \boldsymbol{V}_c^T\right]^T, \tag{2.22}$$

where $\boldsymbol{V}_a, \boldsymbol{V}_b, \boldsymbol{V}_c \in \mathbb{C}^{n\times 1}$ are the voltage vectors of the three phases, and $(\cdot)^T$ denotes the vector/matrix transpose. The state estimation result is denoted as $\hat{\boldsymbol{V}}$ which has the same structure as (2.22), given by

$$\hat{\boldsymbol{V}} = \left[\hat{\boldsymbol{V}}_a^T,\ \hat{\boldsymbol{V}}_b^T,\ \hat{\boldsymbol{V}}_c^T\right]^T. \tag{2.23}$$

The estimated ZSV $\hat{\boldsymbol{V}}_0$, can thus be calculated as

$$\hat{\boldsymbol{V}}_0 = \hat{\boldsymbol{V}}_a + \hat{\boldsymbol{V}}_b + \hat{\boldsymbol{V}}_c = \tilde{\boldsymbol{U}}\hat{\boldsymbol{V}}, \tag{2.24}$$

where

$$\tilde{\boldsymbol{U}} \triangleq [1, 1, 1] \otimes \boldsymbol{U}_n. \tag{2.25}$$

Next, three processing steps are introduced on $\hat{\boldsymbol{V}}_0$ to enhance the detection performance. The first step is to represent it in the real-valued form for subsequent derivations, given by

$$\hat{\boldsymbol{V}}_0^{vec} \triangleq \left[\hat{\boldsymbol{V}}_{0,real}^T, \hat{\boldsymbol{V}}_{0,imag}^T\right]^T, \tag{2.26}$$

where $\hat{\boldsymbol{V}}_{0,real}$ and $\hat{\boldsymbol{V}}_{0,imag}$ are the real and imaginary parts of $\hat{\boldsymbol{V}}_0$, respectively. Notice that

$$\hat{\boldsymbol{V}}_0 = \hat{\boldsymbol{V}}_{0,real} + j\hat{\boldsymbol{V}}_{0,imag} \tag{2.27}$$

is an $n \times 1$ complex-valued vector while $\hat{\boldsymbol{V}}_0^{vec}$ is the $2n \times 1$ real-valued vector equivalent to $\hat{\boldsymbol{V}}_0$. The second processing step is to eliminate the intrinsic non-zero ZSV of the system under the normal condition. In a three-phase unbalanced system, the actual ZSV vector is not exactly zero though close-to-zero. To take this into account in the detection, the intrinsic ZSV is subtracted from the estimated ZSV. Let $\boldsymbol{V}_{0,ave}$

denote the average of the ZSV vector under the normal condition. In practice, an approximation of $\boldsymbol{V}_{0,ave}$ can be obtained from historical measurements. The third process is a linear transformation to reduce the effect of the correlation among the noise components in $\hat{\boldsymbol{V}}_0^{vec}$. For this, a $2n \times 2n$ real-valued transformation matrix $\boldsymbol{W}$ is introduced with the function of noise-whitening. The design of the transformation matrix $\boldsymbol{W}$ will be presented in a subsequent subsection. The processed ZSV vector is thus

$$\boldsymbol{V}_{0,proc} \triangleq \boldsymbol{W}(\hat{\boldsymbol{V}}_0^{vec} - \boldsymbol{V}_{0,ave}^{vec}), \tag{2.28}$$

where $\boldsymbol{V}_{0,ave}^{vec}$ is the real-valued form of $\boldsymbol{V}_{0,ave}$, whose structure is similar to that in (2.26).

The proposed detection scheme is based on the $\mathcal{L}_2$-norm of the processed ZSV. Specifically, the proposed detection rule is

$$\begin{cases} \text{Decision is “no attack” if } \|\boldsymbol{V}_{0,proc}\|_2^2 < h; \\ \text{Decision is “under attack” if } \|\boldsymbol{V}_{0,proc}\|_2^2 \geq h, \end{cases} \tag{2.29}$$

where h is the detection threshold. This decision rule can also be represented as

$$T \triangleq \|\boldsymbol{V}_{0,proc}\|_2^2 = \left\|\boldsymbol{W}(\hat{\boldsymbol{V}}_0^{vec} - \boldsymbol{V}_{0,ave}^{vec})\right\|_2^2 \underset{H_0}{\overset{H_1}{\gtrless}} h, \tag{2.30}$$

where T is the test statistic.

2.2.3 Mathematical Analysis of the Three-Phase DSSE

For the design of the transformation matrix $\boldsymbol{W}$ and the performance analysis of the proposed detection scheme, the distribution of $\hat{\boldsymbol{V}}_0$ needs to be derived, and from (2.24), this requires studies of the state estimation $\hat{\boldsymbol{V}}$. For linear system models with Gaussian noises and the WLS estimation in (2.16), the distribution of $\hat{\boldsymbol{V}}$ can be obtained straightforwardly. However, for the linear approximate DSSE, the state estimation is obtained by iteratively using (2.15) and (2.16). The mathematical analysis on the estimation vector is significantly more challenging, and there has not been any result in the literature. In this subsection, the analysis of the state estimate $\hat{\boldsymbol{V}}$

under H_0 is conducted. The results are crucial for the design of $\boldsymbol{W}$ and the derivation of the false alarm rate.

By using (2.12) and (2.13) in (2.15), the equivalent current vector can be written as

$$\begin{aligned}\boldsymbol{I}_{equ} &= \text{diag}^{-*}\{\boldsymbol{A}_S\hat{\boldsymbol{V}}\}\left(\text{diag}\{\boldsymbol{A}_S\boldsymbol{V}\}\boldsymbol{I}^* + \boldsymbol{e}_S\right)^* \\ &= \text{diag}^{-*}\{\boldsymbol{A}_S\hat{\boldsymbol{V}}\}\text{diag}^*\{\boldsymbol{A}_S\boldsymbol{V}\}\boldsymbol{Y}(\boldsymbol{A}_S\boldsymbol{V}) + \text{diag}^{-*}\{\boldsymbol{A}_S\hat{\boldsymbol{V}}\}\boldsymbol{e}_S^*. \qquad (2.31)\end{aligned}$$

Then the equivalent measurement vector defined in (2.11) can be rewritten as

$$\begin{aligned}\boldsymbol{z} &= \begin{bmatrix}\boldsymbol{V}_{mea}\\ \boldsymbol{I}_{equ}\end{bmatrix} = \begin{bmatrix}\boldsymbol{A}_V\boldsymbol{V} + \boldsymbol{e}_V\\ \text{diag}^{-*}\{\boldsymbol{A}_S\hat{\boldsymbol{V}}\}\boldsymbol{S}_{mea}^*\end{bmatrix} = \begin{bmatrix}\boldsymbol{A}_V\boldsymbol{V} + \boldsymbol{e}_V\\ \text{diag}^{-*}\{\boldsymbol{A}_S\hat{\boldsymbol{V}}\}\left[\text{diag}\{\boldsymbol{I}\}\boldsymbol{A}_S^*\boldsymbol{V}^* + \boldsymbol{e}_S^{-*}\right]\end{bmatrix} \\ &= \begin{bmatrix}\boldsymbol{A}_V\boldsymbol{V} + \boldsymbol{e}_V\\ \text{diag}^{-*}\{\boldsymbol{A}_S\hat{\boldsymbol{V}}\}\text{diag}^*\{\boldsymbol{A}_S\boldsymbol{V}\}\boldsymbol{Y}\boldsymbol{A}_S\boldsymbol{V} + \text{diag}^{-*}\{\boldsymbol{A}_S\hat{\boldsymbol{V}}\}\boldsymbol{e}_S^*\end{bmatrix} \\ &= \begin{bmatrix}\boldsymbol{A}_V\\ \text{diag}^{-*}\{\boldsymbol{A}_S\hat{\boldsymbol{V}}\}\text{diag}^*\{\boldsymbol{A}_S\boldsymbol{V}\}\boldsymbol{Y}\boldsymbol{A}_S\end{bmatrix}\boldsymbol{V} + \begin{bmatrix}\boldsymbol{1} & \boldsymbol{0}\\ \boldsymbol{0} & \text{diag}^{-*}\{\boldsymbol{A}_S\hat{\boldsymbol{V}}\}\end{bmatrix}\begin{bmatrix}\boldsymbol{e}_V\\ \boldsymbol{e}_S^*\end{bmatrix} \\ &= \boldsymbol{H}\boldsymbol{V} + \begin{bmatrix}\boldsymbol{1} & \boldsymbol{0}\\ \boldsymbol{0} & \text{diag}^{-*}\{\boldsymbol{A}_S\hat{\boldsymbol{V}}\}\end{bmatrix}\boldsymbol{e} + \begin{bmatrix}\boldsymbol{0}\\ (\text{diag}^{-*}\{\boldsymbol{A}_S\hat{\boldsymbol{V}}\}\text{diag}^*\{\boldsymbol{A}_S\boldsymbol{V}\} - \boldsymbol{1})\boldsymbol{Y}\boldsymbol{A}_S\end{bmatrix}\boldsymbol{V}, \quad (2.32)\end{aligned}$$

where $\boldsymbol{H}$ and $\boldsymbol{e}$ are also defined in (2.11). To help the presentation, we define

$$\boldsymbol{A} \triangleq (\boldsymbol{H}^H\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^H\boldsymbol{R}^{-1}. \qquad (2.33)$$

By using (2.32) in (2.16), the state estimation can be presented as

$$\begin{aligned}\hat{\boldsymbol{V}} &= (\boldsymbol{H}^H\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^H\boldsymbol{R}^{-1}\boldsymbol{z} = \boldsymbol{A}\boldsymbol{z} \\ &= \boldsymbol{A}\left(\boldsymbol{H}\boldsymbol{V} + \begin{bmatrix}\boldsymbol{1} & \boldsymbol{0}\\ \boldsymbol{0} & \text{diag}^{-*}\{\boldsymbol{A}_S\hat{\boldsymbol{V}}\}\end{bmatrix}\boldsymbol{e} + \begin{bmatrix}\boldsymbol{0}\\ \left(\text{diag}^{-*}\{\boldsymbol{A}_S\hat{\boldsymbol{V}}\}\text{diag}^*\{\boldsymbol{A}_S\boldsymbol{V}\} - \boldsymbol{1}\right)\boldsymbol{Y}\boldsymbol{A}_S\end{bmatrix}\boldsymbol{V}\right) \\ &= \boldsymbol{V} + \boldsymbol{A}\begin{bmatrix}\boldsymbol{1} & \boldsymbol{0}\\ \boldsymbol{0} & \text{diag}^{-*}\{\boldsymbol{A}_S\hat{\boldsymbol{V}}\}\end{bmatrix}\boldsymbol{e} + \boldsymbol{A}\begin{bmatrix}\boldsymbol{0}\\ \left(\text{diag}^{-*}\{\boldsymbol{A}_S\hat{\boldsymbol{V}}\}\text{diag}^*\{\boldsymbol{A}_S\boldsymbol{V}\} - \boldsymbol{1}\right)\boldsymbol{Y}\boldsymbol{A}_S\end{bmatrix}\boldsymbol{V}. (2.34)\end{aligned}$$

It provides an expression of the estimated vector $\hat{\boldsymbol{V}}$ for the iterative estimation scheme in terms of the parameters of the power grids, such as voltages, impendence, and noises. However, the expression in (2.34) is recursive and implicit as the state estimation $\hat{\boldsymbol{V}}$ appears on both sides of the equality. Further analysis is needed to understand the distribution of $\hat{\boldsymbol{V}}$. Define the estimation error as the difference between the true values and the estimated values, given by,

$$\Delta \boldsymbol{V} \triangleq \boldsymbol{V} - \hat{\boldsymbol{V}}, \tag{2.35}$$

and let

$$\Delta \boldsymbol{V}^{vec} = \left[\Delta \boldsymbol{V}_{real}^{T}, \Delta \boldsymbol{V}_{imag}^{T}\right]^{T}, \tag{2.36}$$

which is the real-valued equivalent representation of $\Delta \boldsymbol{V}$.

Theorem 1 *Define*

$$\boldsymbol{E}_1 \triangleq \boldsymbol{A} \begin{bmatrix} \mathbf{1} & \mathbf{0} \\ \mathbf{0} & \operatorname{diag}^{-*}\{\boldsymbol{A}_S \hat{\boldsymbol{V}}\} \end{bmatrix}, \tag{2.37}$$

$$\boldsymbol{E}_2 \triangleq \boldsymbol{A} \begin{bmatrix} \mathbf{0} \\ \operatorname{diag}^{-*}\{\boldsymbol{A}_S \hat{\boldsymbol{V}}\}\operatorname{diag}\{\boldsymbol{Y}\boldsymbol{A}_S \hat{\boldsymbol{V}}\}\boldsymbol{A}_S^{*} \end{bmatrix}, \tag{2.38}$$

$$\boldsymbol{E} \triangleq \begin{bmatrix} \mathbf{1} + \boldsymbol{E}_{2,real} & \boldsymbol{E}_{2,imag} \\ \boldsymbol{E}_{2,imag} & \mathbf{1} - \boldsymbol{E}_{2,real} \end{bmatrix}^{-1} \begin{bmatrix} \boldsymbol{E}_{1,real} & -\boldsymbol{E}_{1,imag} \\ \boldsymbol{E}_{1,imag} & \boldsymbol{E}_{1,real} \end{bmatrix}, \tag{2.39}$$

where $\boldsymbol{E}_{1,real}$, $\boldsymbol{E}_{2,real}$ and $\boldsymbol{E}_{1,imag}$, $\boldsymbol{E}_{2,imag}$ are the real and imaginary parts of matrices $\boldsymbol{E}_1$ and $\boldsymbol{E}_2$, respectively. Further, define

$$\boldsymbol{R}^{rec} \triangleq \begin{bmatrix} \boldsymbol{R}_{real} & -\boldsymbol{R}_{imag} \\ \boldsymbol{R}_{imag} & \boldsymbol{R}_{real} \end{bmatrix}, \tag{2.40}$$

with $\boldsymbol{R}_{real}$ and $\boldsymbol{R}_{imag}$ being the real and imaginary parts of $\boldsymbol{R}$, respectively. With the approximate DSSE model (2.10) and the state estimation in (2.16), when the system is not under attack, the estimation error in the real-valued format $\Delta \boldsymbol{V}^{vec}$ can be approximated as a zero-mean Gaussian vector whose covariance matrix is $\boldsymbol{E}\boldsymbol{R}^{vec}\boldsymbol{E}^{T}$. That is, $\Delta \boldsymbol{V}^{vec} \sim \mathcal{N}(\mathbf{0}, \boldsymbol{E}\boldsymbol{R}^{vec}\boldsymbol{E}^{T})$.

Proof. For the $(2,1)$-block of the matrix in the last term in (2.32), by using (2.35) to replace $\boldsymbol{V}$ with $\hat{\boldsymbol{V}} + \Delta \boldsymbol{V}$, we have

$$\left(\operatorname{diag}^{-*}\{\boldsymbol{A}_S \hat{\boldsymbol{V}}\}\operatorname{diag}^{*}\{\boldsymbol{A}_S \boldsymbol{V}\} - \mathbf{1}\right)\boldsymbol{Y}\boldsymbol{A}_S \boldsymbol{V}$$

$$\begin{aligned}&= \left(\text{diag}^{-*}\{\boldsymbol{A}_S\hat{\boldsymbol{V}}\}\text{diag}^{*}\{\boldsymbol{A}_S(\hat{\boldsymbol{V}}+\Delta\boldsymbol{V})\} - \boldsymbol{1}\right)\boldsymbol{Y}\boldsymbol{A}_S\left(\hat{\boldsymbol{V}}+\Delta\boldsymbol{V}\right)\\ &= \left(\text{diag}^{-*}\{\boldsymbol{A}_S\hat{\boldsymbol{V}}\}\text{diag}^{*}\{\boldsymbol{A}_S\hat{\boldsymbol{V}}\} + \text{diag}^{-*}\{\boldsymbol{A}_S\hat{\boldsymbol{V}}\}\text{diag}^{*}\{\boldsymbol{A}_S\Delta\boldsymbol{V}\} - \boldsymbol{1}\right)\boldsymbol{Y}\boldsymbol{A}_S\left(\hat{\boldsymbol{V}}+\Delta\boldsymbol{V}\right)\\ &= \text{diag}^{-*}\{\boldsymbol{A}_S\hat{\boldsymbol{V}}\}\text{diag}^{*}\{\boldsymbol{A}_S\Delta\boldsymbol{V}\}\boldsymbol{Y}\boldsymbol{A}_S\left(\hat{\boldsymbol{V}}+\Delta\boldsymbol{V}\right). \qquad (2.41)\end{aligned}$$

When the power system is under normal condition without attack, the effect of the noises is small compared to the actual voltage values or estimated values, i.e., $\Delta\boldsymbol{V} \ll \boldsymbol{V}$ or $\Delta\boldsymbol{V} \ll \hat{\boldsymbol{V}}$. Thus, by ignoring the $\Delta\boldsymbol{V}$ at the end of (2.41), we have the following approximation:

$$\begin{aligned}&(\text{diag}^{-*}\{\boldsymbol{A}_S\hat{\boldsymbol{V}}\}\text{diag}^{*}\{\boldsymbol{A}_S\boldsymbol{V}\} - \boldsymbol{1})\boldsymbol{Y}\boldsymbol{A}_S\boldsymbol{V}\\ \approx\ &\text{diag}^{-*}\{\boldsymbol{A}_S\hat{\boldsymbol{V}}\}\text{diag}^{*}\{\boldsymbol{A}_S\Delta\boldsymbol{V}\}\boldsymbol{Y}\boldsymbol{A}_S\hat{\boldsymbol{V}}\\ =\ &\text{diag}^{-*}\{\boldsymbol{A}_S\hat{\boldsymbol{V}}\}\text{diag}\{\boldsymbol{A}_S^{*}\Delta\boldsymbol{V}^{*}\}\boldsymbol{Y}\boldsymbol{A}_S\hat{\boldsymbol{V}}\\ =\ &\text{diag}^{-*}\{\boldsymbol{A}_S\hat{\boldsymbol{V}}\}\text{diag}\{\boldsymbol{Y}\boldsymbol{A}_S\hat{\boldsymbol{V}}\}\boldsymbol{A}_S^{*}\Delta\boldsymbol{V}^{*}. \qquad (2.42)\end{aligned}$$

Then, by using (2.42) in (2.34), the following approximation can be obtained on the state estimation and the estimation error:

$$\hat{\boldsymbol{V}} \approx \boldsymbol{V} + \boldsymbol{E}_1\boldsymbol{e} + \boldsymbol{E}_2\Delta\boldsymbol{V}^{*}, \qquad (2.43)$$

which is equivalent to

$$-\Delta\boldsymbol{V} \approx \boldsymbol{E}_1\boldsymbol{e} + \boldsymbol{E}_2\Delta\boldsymbol{V}^{*}. \qquad (2.44)$$

Both $\Delta\boldsymbol{V}$ and its conjugate $\Delta\boldsymbol{V}^{*}$ appear in (2.44) and they cannot be straightforwardly combined in the complex form. To further obtain the distribution of $\Delta\boldsymbol{V}$, the vectors and matrices in (2.44) are converted into their equivalent real-valued forms. With the following equalities,

$$\begin{aligned}\Delta\boldsymbol{V}\ &= \Delta\boldsymbol{V}_{real} + j\Delta\boldsymbol{V}_{imag},\\ \Delta\boldsymbol{V}^{*} &= \Delta\boldsymbol{V}_{real} - j\Delta\boldsymbol{V}_{imag},\end{aligned} \qquad (2.45)$$

(2.44) can be rewritten in rectangular forms as

$$\begin{aligned}-\Delta\boldsymbol{V}_{real} &\approx \boldsymbol{E}_{1,real}\boldsymbol{e}_{real} - \boldsymbol{E}_{1,imag}\boldsymbol{e}_{imag} + \boldsymbol{E}_{2,real}\Delta\boldsymbol{V}_{real} + \boldsymbol{E}_{2,imag}\Delta\boldsymbol{V}_{imag},\\ -\Delta\boldsymbol{V}_{imag} &\approx \boldsymbol{E}_{1,imag}\boldsymbol{e}_{real} + \boldsymbol{E}_{1,real}\boldsymbol{e}_{imag} + \boldsymbol{E}_{2,imag}\Delta\boldsymbol{V}_{real} - \boldsymbol{E}_{2,real}\Delta\boldsymbol{V}_{imag}.\end{aligned} \qquad (2.46)$$

From (2.46), we can obtain

$$\begin{aligned} -\begin{bmatrix} \Delta\boldsymbol{V}_{real} \\ \Delta\boldsymbol{V}_{imag} \end{bmatrix} &\approx \begin{bmatrix} \boldsymbol{E}_{1,real} & -\boldsymbol{E}_{1,imag} \\ \boldsymbol{E}_{1,imag} & \boldsymbol{E}_{1,real} \end{bmatrix} \begin{bmatrix} \boldsymbol{e}_{real} \\ \boldsymbol{e}_{imag} \end{bmatrix} + \begin{bmatrix} \boldsymbol{E}_{2,real} & -\boldsymbol{E}_{2,imag} \\ \boldsymbol{E}_{2,imag} & \boldsymbol{E}_{2,real} \end{bmatrix} \begin{bmatrix} \Delta\boldsymbol{V}_{real} \\ -\Delta\boldsymbol{V}_{imag} \end{bmatrix} \\ &= \begin{bmatrix} \boldsymbol{E}_{1,real} & -\boldsymbol{E}_{1,imag} \\ \boldsymbol{E}_{1,imag} & \boldsymbol{E}_{1,real} \end{bmatrix} \begin{bmatrix} \boldsymbol{e}_{real} \\ \boldsymbol{e}_{imag} \end{bmatrix} + \begin{bmatrix} \boldsymbol{E}_{2,real} & \boldsymbol{E}_{2,imag} \\ \boldsymbol{E}_{2,imag} & -\boldsymbol{E}_{2,real} \end{bmatrix} \begin{bmatrix} \Delta\boldsymbol{V}_{real} \\ \Delta\boldsymbol{V}_{imag} \end{bmatrix} \end{aligned} \tag{2.47}$$

The estimation error in the real-valued form can be derived from (2.47) as

$$\Delta\boldsymbol{V}^{vec} \approx -\boldsymbol{E}\boldsymbol{e}^{vec}, \tag{2.48}$$

where

$$\boldsymbol{e}^{vec} = \left[\boldsymbol{e}_{real}^T, \boldsymbol{e}_{imag}^T\right]^T \tag{2.49}$$

is the real-valued form of the noise vector $\boldsymbol{e}$, and it is a Gaussian vector following $\mathcal{N}(\mathbf{0}, \boldsymbol{R}^{vec})$. From (2.48), it can be seen that $\Delta\boldsymbol{V}^{vec}$ is also a zero-mean Gaussian vector whose variance is $\boldsymbol{E}\boldsymbol{R}^{vec}\boldsymbol{E}^T$, i.e., $\Delta\boldsymbol{V}^{vec} \sim \mathcal{N}(\mathbf{0}, \boldsymbol{E}\boldsymbol{R}^{vec}\boldsymbol{E}^T)$. Therefore, the theorem is proved. ■

2.2.4 Transformation Matrix Design and False Alarm Rate Analysis

Define

$$\tilde{\boldsymbol{U}}^{vec} \triangleq \begin{bmatrix} \tilde{\boldsymbol{U}}_{real} & -\tilde{\boldsymbol{U}}_{imag} \\ \tilde{\boldsymbol{U}}_{imag} & \tilde{\boldsymbol{U}}_{real} \end{bmatrix} = \boldsymbol{U}_2 \otimes \tilde{\boldsymbol{U}}. \tag{2.50}$$

By using (2.35) and (2.24) in (2.28), we have

$$\begin{aligned} \boldsymbol{V}_{0,proc} &= \boldsymbol{W}(\hat{\boldsymbol{V}}_0^{vec} - \boldsymbol{V}_{0,ave}^{vec}) \\ &= \boldsymbol{W}\left[\tilde{\boldsymbol{U}}^{vec}(\boldsymbol{V}^{vec} - \Delta\boldsymbol{V}^{vec}) - \boldsymbol{V}_{0,ave}^{vec}\right] \\ &= -\boldsymbol{W}\tilde{\boldsymbol{U}}^{rec}\Delta\boldsymbol{V}^{rec} + \left(\boldsymbol{W}\tilde{\boldsymbol{U}}^{rec}\boldsymbol{V}^{rec} - \boldsymbol{W}\boldsymbol{V}_{0,ave}^{rec}\right) \\ &\approx -\boldsymbol{W}\tilde{\boldsymbol{U}}^{vec}\Delta\boldsymbol{V}^{vec} \\ &\approx \boldsymbol{W}\tilde{\boldsymbol{U}}^{vec}\boldsymbol{E}\boldsymbol{e}^{vec}, \end{aligned} \tag{2.51}$$

where the last two steps are due to (2.48) and

$$\boldsymbol{V}_{0,ave} \approx \tilde{\boldsymbol{U}}\boldsymbol{V} \Leftrightarrow \boldsymbol{V}_{0,ave}^{vec} \approx \tilde{\boldsymbol{U}}^{vec}\boldsymbol{V}^{vec}. \tag{2.52}$$

For detection problems with Gaussian noises, whitening is known to be an important step of many optimal detectors. It is used in this work for the design of the transformation matrix $\boldsymbol{W}$, where the goal is to transform the test vector $\boldsymbol{V}_{0,proc}$ to a white Gaussian vector with the identity matrix as the covariance matrix. In this way, the correlation among the estimation error components can be removed. Notice that $\boldsymbol{V}_{0,proc}$ is zero-mean. Thus, for whitening, the condition on the transformation matrix $\boldsymbol{W}$ is

$$\mathbb{E}\left[\boldsymbol{V}_{0,proc}\boldsymbol{V}_{0,proc}^{T}\right] = \boldsymbol{U}, \tag{2.53}$$

which is equivalent to

$$\begin{aligned} &\mathbb{E}\left[\boldsymbol{W}\tilde{\boldsymbol{U}}^{vec}\boldsymbol{E}\boldsymbol{e}^{vec}(\boldsymbol{W}\tilde{\boldsymbol{U}}^{vec}\boldsymbol{E}\boldsymbol{e}^{vec})^{T}\right] \\ =& \boldsymbol{W}\tilde{\boldsymbol{U}}^{vec}\boldsymbol{E}\,\mathbb{E}\left[\boldsymbol{e}^{vec}\boldsymbol{e}^{vecT}\right]\boldsymbol{E}^{T}\tilde{\boldsymbol{U}}^{vecT}\boldsymbol{W}^{T} \\ =& \boldsymbol{W}\tilde{\boldsymbol{U}}^{vec}\boldsymbol{E}\boldsymbol{R}^{vec}\boldsymbol{E}^{T}\tilde{\boldsymbol{U}}^{vecT}\boldsymbol{W}^{T} = \boldsymbol{U}. \end{aligned} \tag{2.54}$$

Therefore, the following design is proposed:

$$\boldsymbol{W} = \left(\tilde{\boldsymbol{U}}^{vec}\boldsymbol{E}\boldsymbol{R}^{vec}\boldsymbol{E}^{T}\tilde{\boldsymbol{U}}^{vecT}\right)^{-\frac{1}{2}}. \tag{2.55}$$

With this design, we have $\boldsymbol{V}_{0,proc} \sim \mathcal{N}(\boldsymbol{0}, \boldsymbol{U})$. And thus the statistic T under H_0, which is the square of $\mathcal{L}_2$-norm of $\boldsymbol{V}_{0,proc}$, follows the centralized Chi-squared distribution with degree $2n$, e.g., $T|H_0 \sim \chi^2(2n)$ [70].

The false alarm rate P_F is the probability that the detection result is under attack when the system is not under attack. The P_F for the detection rule in (2.30) can be calculated as

$$P_F = \mathbb{P}(T \geq h|H_0) = \frac{1}{\Gamma(n)}\Gamma\left(n, \frac{h}{2}\right), \tag{2.56}$$

where $\Gamma(n)$ is the gamma function and

$$\Gamma(n, x) \triangleq \int_{x}^{\infty} x^{n-1}e^{-x}dx \tag{2.57}$$

is the upper incomplete gamma function.

The result in (2.56) provides a tractable analytical formula for the false alarm rate of the proposed detection scheme. It only depends on the detection threshold h and the number of system states n, as a result of the whitening transformation on the estimated ZSV. To determine the threshold value has been a challenging problem in many practical detection systems. A widely used method is to find the threshold based on a tolerance level of the false alarm rate. This usually requires a good amount of historical data or extensive trials, and the process needs to be repeated when the system parameters change or the desired P_F level changes. Our derived result in (2.56) can be used to analytically and straightforwardly set the threshold value h according to the desired level on the false alarm rate and the number of the buses in the topology. For example, in a three-phase distribution system with 35 buses, i.e., $n = 35$, if the desired level of false alarm rate is $P_F = 1\%$, the detection threshold can then be calculated as $h = 45.42$; if the desired level of false alarm rate is $P_F = 0.1\%$, the detection threshold can then be calculated as $h = 39.05$.

2.2.5 Detection Algorithm and Discussions

The proposed FDIA detection method based on DSSE and ZSV is summarized in Algorithm 1.

The proposed detection scheme is general and can be implemented for any DSSE methods in three-phase distribution systems. We can use the estimated bus voltages resulted from any DSSE method to calculate the estimated ZSV. The estimated ZSV vector can reflect the unbalance degree, which has abnormal change under FDIAs. However, the transformation matrix should be adjusted according to the DSSE method based on the distribution of the estimation error $\Delta \boldsymbol{V}$. Particularly, if the DSSE method is based on a linear model with no approximation and the system state is chosen as bus voltages, the corresponding analysis, including the derivation of the distribution of estimation error $\Delta \boldsymbol{V}$ and the design of the transformation matrix, can be significantly simplified. On the other hand, if the DSSE method is non-linear

Algorithm 1 Proposed detection scheme based on DSSE and ZSV.

```
1: Initialize $\hat{\boldsymbol{V}}$ and $\epsilon$. Let $Flag = 1$.
2: while $Flag == 1$ do
3:     Calculate the equivalent current vector $\boldsymbol{I}_{equ}$ using (2.15).
4:     Update the state estimate using (2.16) and name it $\hat{\boldsymbol{V}}_{new}$.
5:     if $\|\hat{\boldsymbol{V}}_{new} - \hat{\boldsymbol{V}}\|_{\infty} > \epsilon$ then
6:         $\hat{\boldsymbol{V}} = \hat{\boldsymbol{V}}_{new}$.
7:     else
8:         $Flag = 0$.
9: return $\hat{\boldsymbol{V}}$.                                  ▷ The state estimate $\hat{\boldsymbol{V}}$.
10: Calculate $\boldsymbol{E}_1, \boldsymbol{E}_2$, and $\boldsymbol{E}$ using (2.37), (2.38), and (2.39), respectively.
11: Calculate $\boldsymbol{W}$ using (2.55).
12: Calculate $\boldsymbol{V}_{0,proc}$ using (2.28).
13: Calculate $T$ and compare with a predetermined detection threshold $h$ as in (2.30).
                                                                 ▷ The detection result.
```

and complicated, the corresponding mathematical analysis can be more challenging. The proposed scheme only needs real-time measurement data for fault detection. The load profile, which characterizes the variation in electrical load versus time, does not influence the performance of the proposed detection scheme.

The overall complexity order of the proposed scheme is $O(m^3t)$, where t is the number of iterations in the DSSE. Particularly, the complexity order of the DSSE (Steps 1-9 of Algorithm 1) and the remaining part (Steps 10-13 of Algorithm 1) is $O(m^3t)$ and $O(m^3)$, respectively. In comparison, the traditional ISE-based detection scheme [33], which also operates from the state domain, has the same overall complexity order since it also needs the DSSE, and the complexity order of the part other than the DSSE is also $O(m^3)$.

2.3 Case Study

To evaluate the performance of the proposed FDIA detection scheme for three-phase distribution systems, the IEEE 37 Bus Test Feeder as well as the IEEE 123 Bus Test Feeder are used in the case studies, whose topologies and the branches with missing phases are shown in Fig. 2.1 and Fig. 2.2, respectively [71]. The slack bus is selected as bus 701 in IEEE 37 Bus Test Feeder and bus 149 in IEEE 123 Bus Test Feeder. For the IEEE 123 Bus Test Feeder, some switches are usually closed on the branches, such as branches 13-152, 18-135, 60-160, 97-197. For simplicity, each pair of buses connected by these branches is combined in Fig. 2.2.

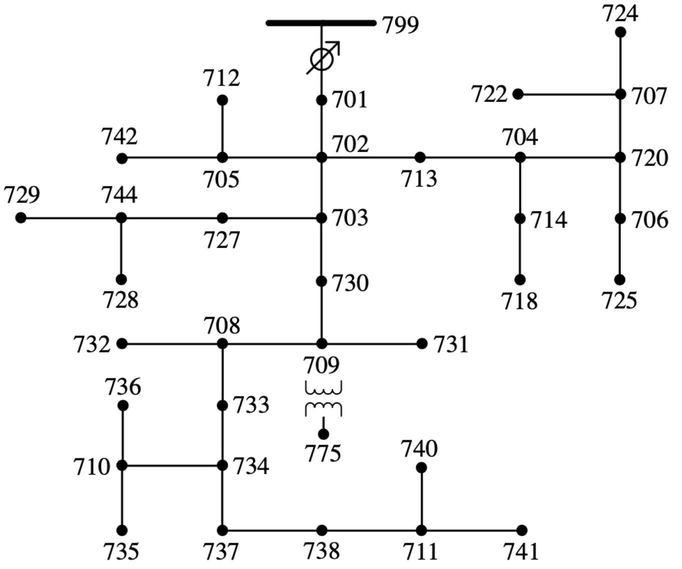

Figure 2.1: The distribution system topology of IEEE 37 Bus Test Feeder.

To understand the performance with different numbers of measurements, two cases of direct measurement arrangements are considered: the case of Least Measurements and the case of Half Measurements. Since most distribution systems in practice are equipped with a small number of measurements units for the voltages due to the cost consideration, the Least Measurements setting is used to simulate such application environment. On the other hand, with the emerging of smart grid technologies, more real-time voltage measurement units are expected to be available in future distribution systems. Therefore, the Half Measurements setting is also considered to test and show the performance for the proposed detection scheme for such systems. The Least Measurements contain the power injection measurements on each node, one power flow measurement on the main branch, one bus voltage injection measurement on the top node, and one equivalent bus voltage injection measurement on the terminal node.

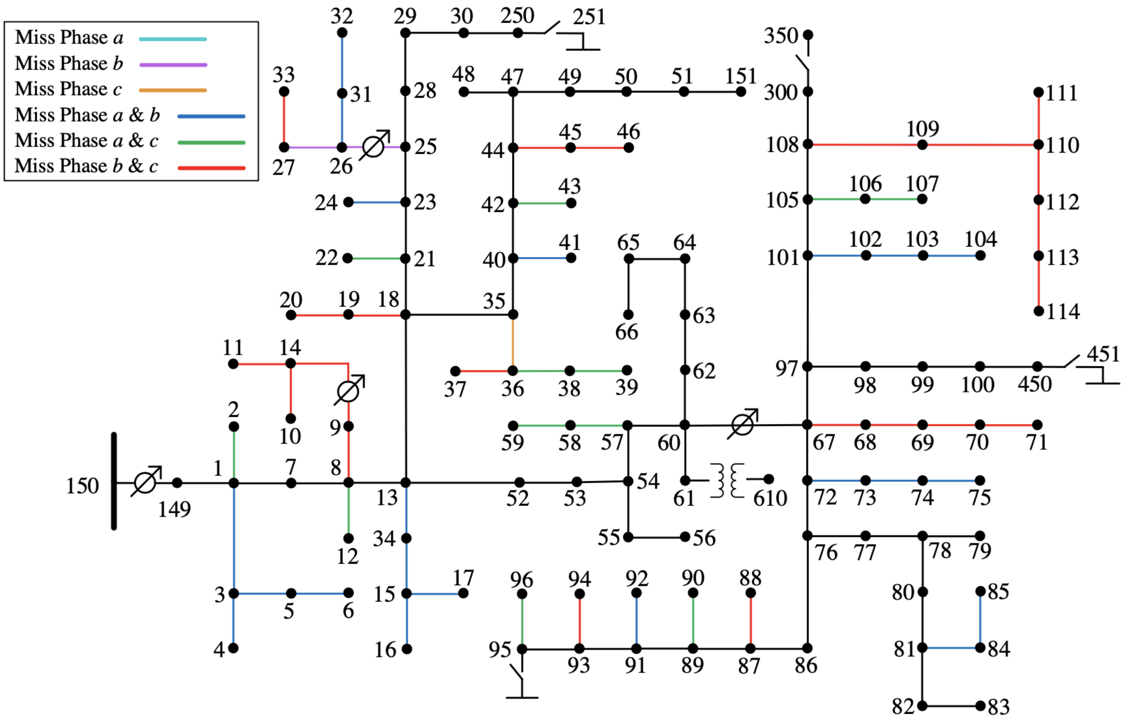

Figure 2.2: The distribution system topology of IEEE 123 Bus Test Feeder.

The Half Measurements contain the power injection measurements on each node, power flow measurements on the main branches, bus voltage injection measurements on the intersection nodes, and equivalent bus voltage injection measurements on the terminal nodes. The locations of the measurements for IEEE 37 Bus and IEEE 123 Bus test feeders are shown in Table 2.1 and Table 2.2, respectively.

Table 2.1: The Measurement Arrangement of IEEE 37 Bus Test Feeder

	Least Mea.	Half Mea.
Equivalent Bus Voltage Injections	740	712, 742, 722, 724, 718, 725, 729, 728, 731, 732, 735, 736, 740, 741
Bus Voltage Injections	701	701, 702, 703, 727, 713, 704, 720, 730, 709, 708, 733, 734, 737, 738, 711
Power Injections	All Buses	All Buses
Power Flows	701-702	701-702, 702-703, 703-730, 730-709, 709-708, 702-713

Pseudo measurements based on historical data are also used, whose noise variance

Table 2.2: The Measurement Arrangement of IEEE 123 Bus Test Feeder

	Least Mea.	Half Mea.
Equivalent Bus Voltage Injections	114	2, 4, 6, 10, 11, 12, 16, 17, 20, 22, 24, 32, 33, 37, 39, 41, 43, 46, 48, 51, 56, 59, 66, 71, 75, 79, 83, 85, 88, 90, 92, 94, 96, 104, 107, 111, 114, 250, 300, 450
Bus Voltage Injections	149	1, 7, 8, 13, 18, 21, 23, 25, 26, 40, 42, 44, 47, 52, 53, 54, 57, 60, 67, 72, 76, 77, 78, 86, 97, 101, 105, 108, 149
Power Injections	All Buses	All Buses
Power Flows	149-1	149-1, 1-7, 7-8, 8-13, 13-18, 152-52, 18-21, 18-135, 35-40, 40-42, 42-44, 44-47, 21-23, 23-25, 25-26, 52-53, 53-54, 54-57, 57-60, 160-67, 67-72, 67-97, 72-76, 76-77, 77-78, 76-86, 197-101, 101-105, 105-108

is assumed to be 20 or 60 times that of direct measurements [72]. The two cases of pseudo measurements are referred to as Pseudo Measurements (20) and Pseudo Measurements (60). For the FDIA event, one entry of the estimation deviation $\boldsymbol{c}$ is randomly chosen and set as 5% [73], which can cause damage in distribution systems. All measurement values, DSSE, and detection are simulated in MATLAB. The threshold for the DSSE iteration is set to be $\epsilon = 1 \times 10^{-6}$.

2.3.1 Results on the Detection Performance

A common method to show the performance of a binary detector is the receiver operating characteristic (ROC) curve [74], which is the correspondence between the detection rate P_D and the false alarm rate P_F. In simulation, the detection rate P_D is the ratio of the number of detected attacks to the number of attack events. However, since the detection rates simulated in many case studies are very closed to one, the P_D v.s. P_F curves of different cases are very close to each other, thus it is difficult to make insightful observations from the plots. Therefore, we replace the detection rate P_D with the miss rate P_M (where $P_M = 1 - P_D$) and use the logarithmic scale for clear presentation.

In simulation, the miss rate P_M is the ratio of the number of attack events that are not detected to the number of attack events. There is an intrinsic trade-off between P_M and P_F, i.e., by adjusting the detection threshold, one can improve the P_M-performance by sacrificing the P_F-performance and vice versa. 10^6 events are generated where half of them are under attack. For each under-attack event, the location of FDIA is randomly chosen as one phase of a bus in the distribution system. Four cases of measurements are simulated: 1) Least Measurements, 2) Least Measurements and Pseudo Measurements (20), 3) Least Measurements and Pseudo Measurements (60), and 4) Half Measurements.

The P_M v.s. P_F curves are shown in Fig. 2.3 and Fig. 2.4 for the IEEE 37 Bus Test Feeder and IEEE 123 Bus Test Feeder, respectively. The variance of noises at all measurement units are assumed to be 0.1, that is, $\boldsymbol{R} = 0.1\boldsymbol{U}$, which is a large noise setting in practice [75]. The figures show that the detection accuracy with Half Measurements is obviously better than that with Least Measurements. This is because more direct measurements improve the detection performance. Among the three cases with Least Measurements, the one with the addition of Pseudo Measurements (20) has the best performance. The figures also show that the addition of Pseudo Measurements (60) to Least Measurements can improve the detection performance even with a high noise variance. The use of Pseudo Measurements (20) can further improve the performance due to its lower variance in the noise. With Least and Pseudo Measurements (20), for IEEE 37 Bus Test Feeder, at the false alarm rate of 1%, the proposed FDIA detection scheme can achieve 2% of miss rate, which is equivalent to 98% of correct detection rate; for IEEE 123 Bus Test Feeder, even for a very low false alarm rate of 0.1%, the proposed detection scheme can achieve 0.2% of miss rate, which is equivalent to 99.8% correct detection rate.

The cases with different noise variances are also simulated, where five noise levels are considered: $\sigma^2 = 0.01, 0.03, 0.05, 0.08, 0.1$; and $\boldsymbol{R} = \sigma^2\boldsymbol{U}$. The curves of P_M v.s.

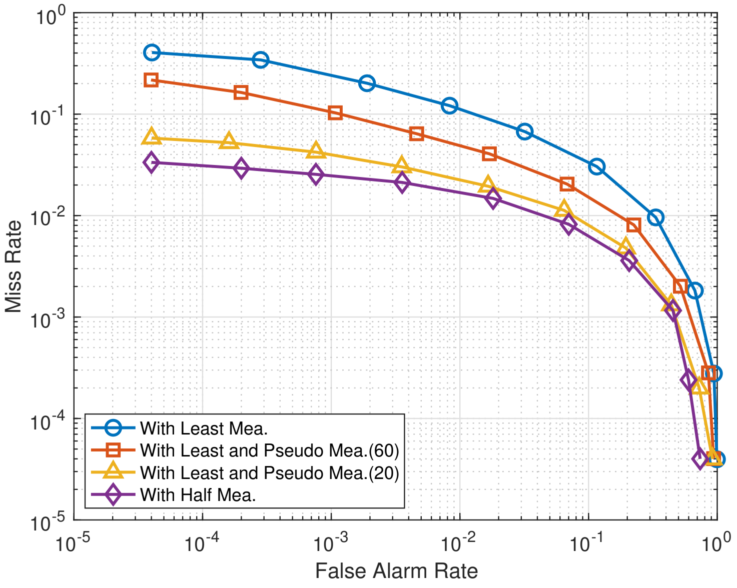

Figure 2.3: P_M v.s. P_F with different measurements of IEEE 37 Bus Test Feeder.

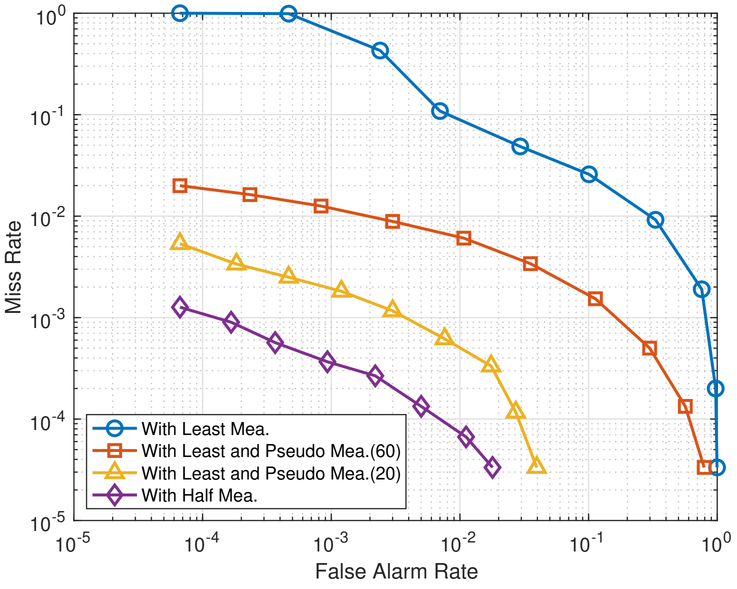

Figure 2.4: P_M v.s. P_F with different measurements of IEEE 123 Bus Test Feeder.

P_F of the proposed detection scheme with Least Measurements for IEEE 37 Bus Test Feeder and IEEE 123 Bus Test Feeder are shown in Fig. 2.5 and Fig. 2.6, respectively. From these figures, it can be seen that as the noise variance decreases, the detection performance improves. With the noise variance of $\sigma^2 = 0.05$, for IEEE 37 Bus Test

Feeder, at the false alarm rate of 1%, the proposed FDIA detection scheme can achieve 1% of miss rate, which is 99% of correct detection rate; for IEEE 123 Bus Test Feeder, even for the very low false alarm rate of 0.5%, the proposed FDIA detection scheme can achieve 0.6% of miss rate, which is 99.4% of correct detection rate. For the case where $\sigma^2 = 0.01$, the proposed scheme achieves the perfect performance where $P_M = 0$ and $P_F = 0$. Since the logarithmic scale is used in the figure, the P_M v.s. P_F curve of this case cannot be shown.

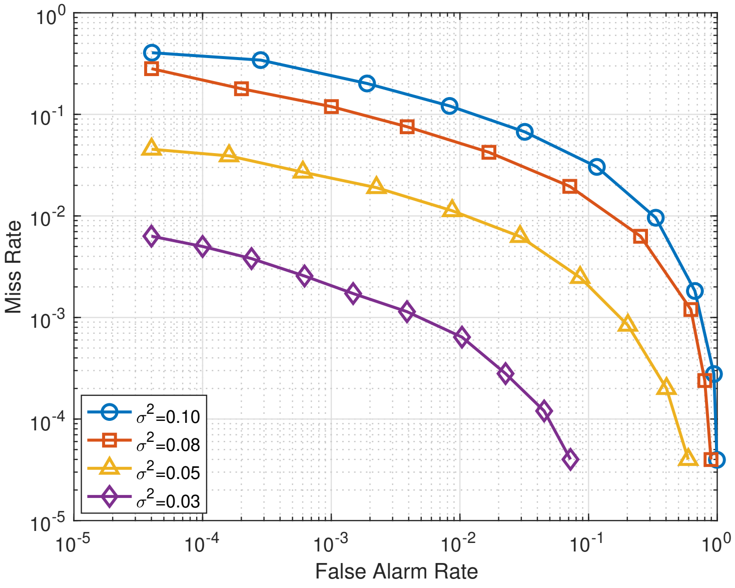

Figure 2.5: P_M v.s. P_F with different noise variance of IEEE 37 Bus Test Feeder.

2.3.2 Comparison with Existing Approach

In this subsection, the proposed detection scheme is compared with the detection scheme using ISE [33]. Similar to our proposed ZSV-based detection scheme, the ISE-based detection scheme also operates from the state domain, which offers a direct comparison of the detection performance. The same as the proposed method, the ISE detection scheme is model-based and targets at unbalanced distribution systems to detect the FDIA from the state domain. When $P_F = 1\%$, the comparison results of P_D of IEEE 123 Bus Test Feeder are summarized in Table 2.3. Here, we set $\boldsymbol{R} = 0.1\boldsymbol{U}$.

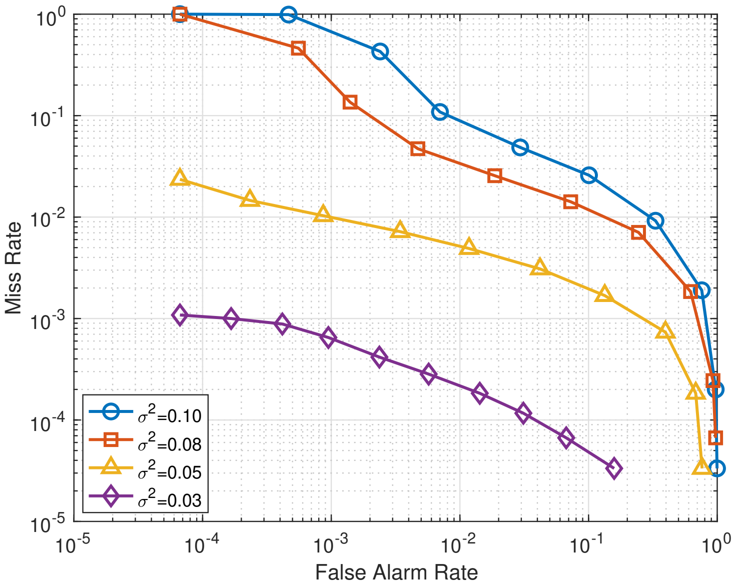

Figure 2.6: P_M v.s. P_F with different noise variance of IEEE 123 Bus Test Feeder.

Compared with the ISE-based detection scheme, the proposed scheme has obvious advantage in the detection rate for all four cases of measurements. One reason is that, in the ISE-based scheme, the lower and upper boundaries on each individual state are sensitive to the noises, and the deviation in bounds is likely to cause a false alarm or a miss of detection. Moreover, the proposed scheme enlarges the intrinsic unbalance degree of buses when the system is under attack, and uses $\mathcal{L}_2$-norm of the transformed ZSV, which is a more effective feature in measuring the system status. Further comparisons of the ZSV-based and the ISE-based detection schemes for the case of $\sigma^2 = 0.1$ and Least and Pseudo Measurements (20) are conducted, i.e., in Fig. 2.7, the test statistic values of the proposed scheme for 100 no-attack events and 100 under-attack events are shown; in Fig. 2.8, the state variables of one of the no-attack event are shown; and in Fig. 2.9, the state variables of one of the under attack event are shown. Fig. 2.7 shows the test statistic value T of two hundred events: the first half are no-attack events corresponding to H_0 and the other half are under-attack events corresponding to H_1. With an appropriately selected threshold, the attacks can be successfully detected with no false alarm. Two representative events, one for

Table 2.3: P_D Comparison between ISE-Based Detection Scheme and ZSV-Based Detection Scheme at $P_F = 1\%$

Detection Rate	ISE-Based	ZSV-Based
Least Mea.	72.84%	91.15%
Least and Pseudo Mea.(60)	85.91%	99.38%
Least and Pseudo Mea.(20)	92.65%	99.95%
Half Mea.	95.43%	99.9933%

no-attack and one for under-attack, are further studied for the ISE-based detection scheme. Fig. 2.8 shows the estimated states of all buses and the detection boundaries for the H_0 event. It can be seen that the estimates of Bus 60 exceeds its upper boundary, which results in a false alarm. The H_1 event is an attack injected into Bus 60 and Fig. 2.9 shows the state estimates of all buses and their boundaries. With a 5% estimation deviation, the estimated states has a peak on Bus 60, but the value does not exceed the bounds calculated by ISE, which leads to a miss of detection. While the noises in these two events affect the calculations of the bounds for the ISE-based scheme, the proposed ZSV-based scheme can effectively conquer the influence of noise for better performance.

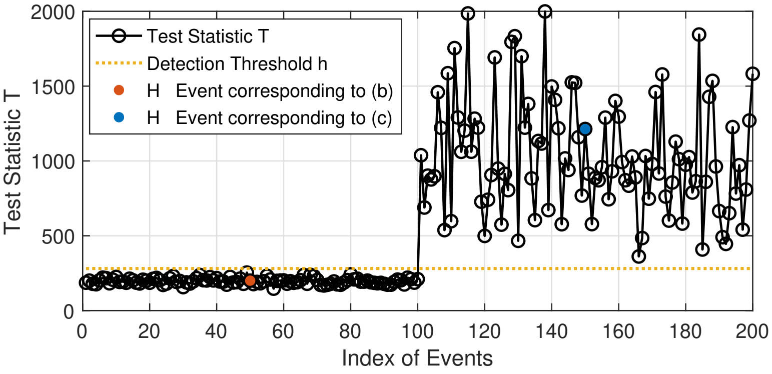

Figure 2.7: Test statistic values of the ZSV-based detection scheme for 200 events.

As to the computation load of the proposed detection scheme, the simulation time in MATLAB in detecting an event is 279.43 ms for the IEEE 37 Bus Test Feeder and

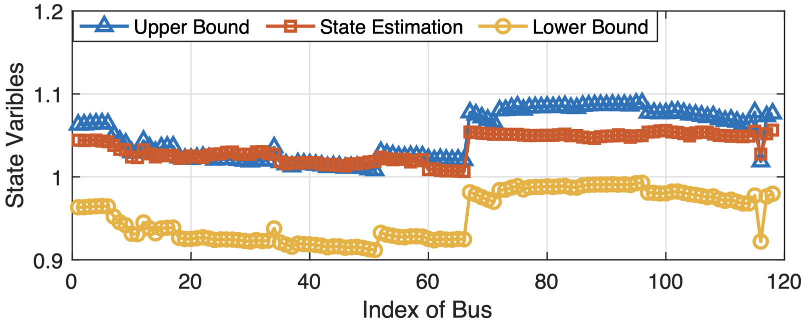

Figure 2.8: State variables of the ISE-based detection scheme for one H_0 event.

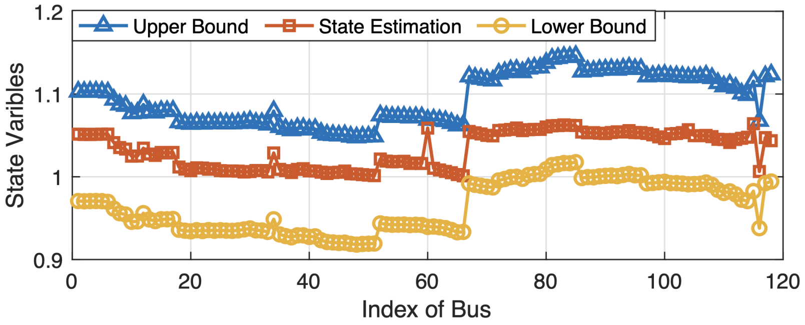

Figure 2.9: State variables of the ISE-based detection scheme for one H_1 event.

3857.12 ms for the IEEE 123 Bus Test Feeder, respectively, for Least and Pseudo Measurements (20). In comparison, the simulation time of the ISE-based detection scheme is 201.96 ms and 4488.76 ms, respectively, for the same setting. The computation load of our proposed scheme is slightly higher than that of the ISE-based detection scheme. Yet, it scales well as the system dimension increases, similar to that of the ISE-based detection scheme, which conforms with our analytical results in Chapter 2.2.3.

2.3.3 Effect of the Whitening Process

A whitening transformation matrix $\boldsymbol{W}$ is designed in (2.55) and is applied to the estimated ZSV as shown in (2.28). This transformation eliminates the correlation among the noise components in the estimated ZSV under the normal condition. It is important for the performance improvement of the proposed detection scheme and the derivation of the false alarm rate. In this subsection, the effect of the whitening process is investigated. The detection scheme without the transformation on the test variables can be represented as follows:

$$T_{NoWhiten} \triangleq \left\| \hat{\boldsymbol{V}}_0^{vec} - \boldsymbol{V}_{0,ave}^{vec} \right\|^2 \underset{H_0}{\overset{H_1}{\gtrless}} h. \tag{2.58}$$

The P_M v.s. P_F curves of the ZSV-based schemes with and without the transformation for IEEE 123 Bus Test Feeder are shown in Fig. 2.10. The two considered measurement cases are Least and Pseudo Measurements (20) and Least and Pseudo Measurements (60), where the noise variance is $\boldsymbol{R} = 0.1\boldsymbol{U}$. It can be seen from the figure that the two measurement cases have the same performance, although the quality of pseudo measurements is different. The (0.5, 0.5) point, which represents the performance of a naive random guess, is on the curves. This observation indicates that the performance without the transformation is very low, and the whitening process can significantly improve the detection performance. The performance of the proposed detection scheme with whitening improves when the quality of pseudo measurements improves from 60 times to 20 times the noise variance.

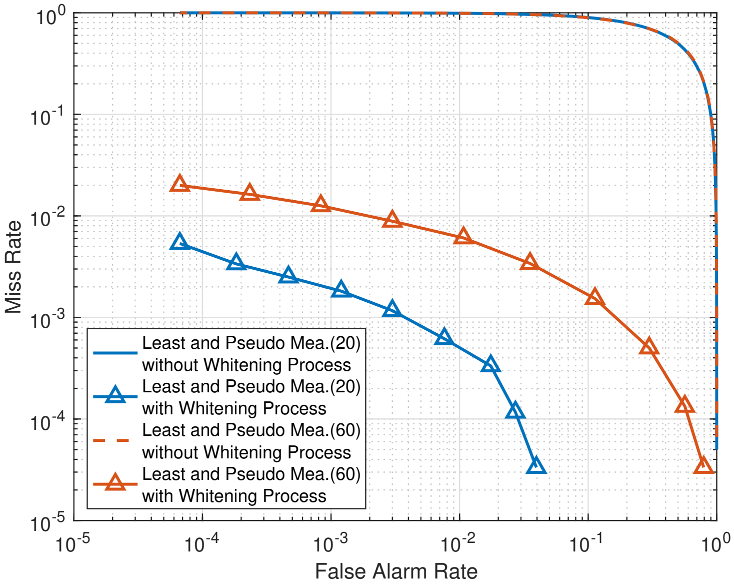

Figure 2.10: P_M v.s. P_F with and without whitening of IEEE 123 Bus Test Feeder.

2.3.4 Results on the False Alarm Rate

In order to verify the accuracy of the derived results in (2.56), simulation results on the false alarm rate for different threshold values are shown in Fig. 2.11 and Fig. 2.12 for IEEE 37 Bus Test Feeder and IEEE 123 Bus Test Feeder, respectively. Four cases are considered: 1) analytical results using (2.56), 2) simulation results with Half Measurements where $\boldsymbol{R} = 0.01\boldsymbol{U}$, 3) simulation results with Least and Pseudo Measurements (20) where $\boldsymbol{R} = 0.005\boldsymbol{U}$, and 4) simulation results with Least and Pseudo Measurements (20) where $\boldsymbol{R} = 0.01\boldsymbol{U}$. It can be seen from Fig. 2.11 and Fig. 2.12 that the simulation results for Case 2 and Case 3 have tight match with the analytical results. For the case of Least and Pseudo Measurements (20) with $\boldsymbol{R} = 0.01\boldsymbol{U}$, where the direct measurements are of lower quality due to the higher noise variance, there is a small gap between the simulation result and the analytical result. The gap comes from the approximation in (2.42), which is tight when $\Delta\boldsymbol{V} \ll \boldsymbol{V}$ or $\Delta\boldsymbol{V} \ll \hat{\boldsymbol{V}}$, i.e., the estimation error is small compared with the value of the state vector. Higher noise variance leads to higher estimation error. As a result, the analytical result on P_F derived in (2.56) is slightly higher than that of the simulated one, which shows that the use of the analytical formula to set the threshold can guarantee the P_F level for this case.

2.3.5 Effect of the Intrinsic ZSV Subtraction

In (2.28), the intrinsic ZSV is subtracted from the estimated ZSV in order to eliminate the impact of three-phase system unbalance. In this simulation, the effect of the subtraction of the intrinsic ZSV is studied. In Fig. 2.13, the P_M v.s. P_F curves for the proposed scheme with average ZSV subtraction and the scheme without average ZSV subtraction are shown for IEEE 123 Bus Test Feeder. The two considered measurement cases are Least and Pseudo Measurements (20) and Least and Pseudo Measurements (60), where $\boldsymbol{R} = 0.1\boldsymbol{U}$. The figure shows that subtracting the intrinsic ZSV can improve the performance. On the other hand, even without the subtraction

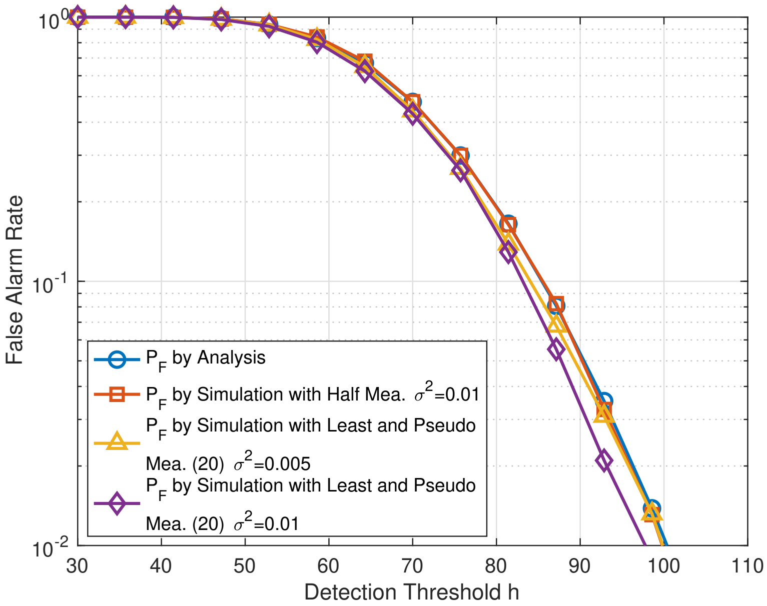

Figure 2.11: P_F v.s. h of IEEE 37 Bus Test Feeder.

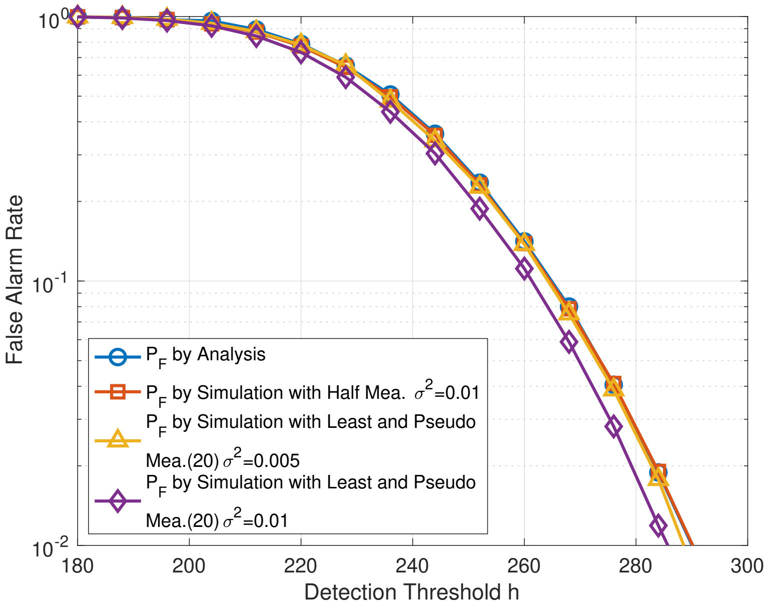

Figure 2.12: P_F v.s. h of IEEE 123 Bus Test Feeder.

of the intrinsic ZSV, the detection scheme still works well for the case with high-quality measurements. For systems where historical data are not available to obtain the average ZSV or systems with highly dynamic ZSV, the scheme without average

ZSV subtraction can be applied.

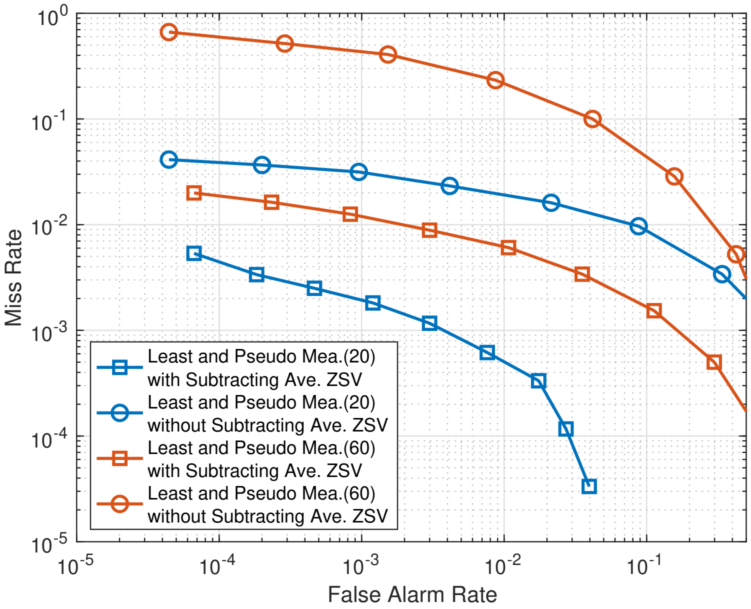

Figure 2.13: P_M v.s. P_F with and without subtracting intrinsic ZSV of IEEE 123 Bus Test Feeder.

2.4 Summary

In this chapter, an FDIA detection scheme based on ZSV is proposed for three-phase unbalanced distribution systems.

In this scheme, the estimation of ZSV is obtained from the DSSE with linear approximation. Then, the estimated ZSV is processed by subtracting the intrinsic ZSV average value and a whitening transformation matrix. By comparing the $\mathcal{L}_2$-norm of the processed estimated ZSV vector with a predefined threshold, the existence of FDIA can be detected. Besides, the distribution of the state estimation is analyzed, based on which the whitening transformation matrix is designed and the false alarm rate is derived in a simple analytical form. Various case studies on standard IEEE Test Feeders show that the proposed method can detect the presence of FDIAs with high accuracy and low false alarm rate. In addition, simulation results validate the analytical result on false alarm rate and demonstrate the significance of the designed processes on the estimated ZSV, including the whitening transformation and the intrinsic-ZSV subtraction.

Chapter 3

ZSV-Based FDIA Localization Scheme for Multiphase Power Distribution Systems

In this chapter, an FDIA localization scheme based on ZSV is proposed for multiphase distribution systems. Based on the estimated ZSV value of a bus relative to that of others, the bus under attack is localized first. Then by eliminating the effect of estimation error from the estimated ZSV, the estimated injected fault is obtained. Finally, by minimizing the error rate with an optimal test, the phase under attack can be diagnosed. With these three steps to analyze the estimated ZSV vector, the bus localization and phase diagnosis can be achieved. Some simulation results are provided to verify the proposed FDIA localization scheme with high accuracy.

The remainder of this chapter is organized as follow. In Section 3.1, we introduce the three steps of the FDIA localization scheme. In Section 3.2, the simulation results are presented to validate the performance of the proposed scheme. Section 3.3 summarizes this chapter.

3.1 FDIA Localization Scheme

In this section, the proposed FDIA localization scheme for the three-phase distribution systems is presented. The localization method is based on the assumption that the existence of an FDIA has been successfully detected using existing FDIA detection schemes, e.g., the detection method in Chapter 2. Our goal is to localize which bus and which phase is under attack using measurement signals. The cases of miss detection and false alarm are not considered.

As mentioned in Chapter 2.2.1, the ZSV vector symbolizes the unbalance degree of three-phase distribution systems. For healthy systems without any attack, the unbalance degree of all buses is usually similar. Since the attacker usually only injects the estimation deviation into a single phase of a bus, the system unbalance degree of the bus with a fault injection in one of the phases is increased when an FDIA exists. Thus, we can use the estimated ZSV for FDIA localization. By calculating the estimated ZSV vector as (2.24), we can design the FDIA localization scheme in three steps which are presented in the following subsections.

3.1.1 Localization of the Bus Under Attack

The first step is to localize the bus under attack. As explained above, an FDIA causes a change in the unbalance degree of the bus under attack. Thus, we propose to locate the bus under attack by finding the bus whose estimated ZSV value has the largest difference from the average of the estimated ZSV of all buses. The average estimated ZSV value of all n buses is calculated as

$$\overline{\hat{V}}_0 = \frac{1}{n}\sum_{i=1}^{n} \hat{V}_{0,i}, \tag{3.1}$$

where $\hat{V}_{0,i}$ is the ith element of $\hat{\boldsymbol{V}}_0$, representing the ZSV of the ith bus. The bus whose estimated ZSV value has the largest difference from $\overline{\hat{V}}_0$ is determined as the bus under attack, whose index, denoted as $\hat{k}$, follows

$$\hat{k} = \arg\max_{i} \left| \hat{V}_{0,i} - \overline{\hat{V}}_0 \right|. \tag{3.2}$$

Denote the index of the bus under attack as k. For the ideal noiseless case where the voltage estimation is precise, we have

$$\hat{V}_{0,i} = \begin{cases} V_{0,i}, & \text{if } i \neq k; \\ V_{0,k} + c, & \text{if } i = k, \end{cases} \tag{3.3}$$

where c is the ZSV value of the injected fault. As all values of $V_{0,i}$'s are approximately the same, in this case,

$$\overline{V}_0 = \frac{1}{n}\sum_{i=1}^{n} V_{0,i} \approx V_{0,i}, \text{for } i \neq k. \tag{3.4}$$

And

$$\overline{\hat{V}}_0 = \frac{1}{n}\sum_{i=1}^{n} \hat{V}_{0,i} \approx \overline{V}_0 + \frac{c}{n}. \tag{3.5}$$

Thus

$$\left|\hat{V}_{0,i} - \overline{\hat{V}}_0\right| \approx \begin{cases} \left|V_{0,i} - \overline{V}_0 - \frac{c}{n}\right| \approx \frac{1}{n}c, & \text{if } i \neq k; \\ \left|V_{0,k} + c - \overline{V}_0 - \frac{c}{n}\right| \approx \frac{n-1}{n}c, & \text{if } i = k. \end{cases} \tag{3.6}$$

Since $n > 2$, by using the proposed bus localization in (3.2), we have $\hat{k} = k$. Thus the bus under attack can be correctly localized. In practical applications, the voltage estimation is subject to error due to measurement noises. When the estimation error is small compared to the amplitude of the injected fault, the proposed bus localization scheme is expected to work well.

3.1.2 Estimation of the ZSV Value of the Injected Fault

The second step is to obtain an estimation on the ZSV value of the injected fault. Recall that $\hat{k}$ is the bus localization result. The estimated ZSV value of the injected fault, denoted as $\hat{c}$, is obtained as

$$\hat{c} = \hat{V}_{0,\hat{k}} - \hat{V}_{0,\hat{k},nei}, \tag{3.7}$$

where $\hat{V}_{0,\hat{k},nei}$ is the estimated ZSV of the neighbor bus of bus $\hat{k}$. The estimated fault ZSV value in (3.7) is obtained by subtracting $\hat{V}_{0,\hat{k},nei}$ from the estimated ZSV of the bus under attack $\hat{V}_{0,\hat{k}}$.

For the ideal case of no measurement noises in the system, we have $\hat{k} = k$ and thus

$$\hat{c} = c + V_{0,k} - V_{0,k,nei} \approx c, \tag{3.8}$$

where the second step is by using (3.3) and the last step is because the values of $V_{0,i}$'s are approximately the same for all i. Here, we particularly choose the nearest upstream neighbor since such node is usually the one with the closest unbalance degree to the bus under attack. For the practical case with voltage estimation error, similar to the previous step, the proposed estimation is expected to have high quality when the estimation error is small.

3.1.3 Diagnosis of the Phase Under Attack

The third step of the localization scheme is to diagnose the phase under attack, which is given by

$$\hat{\omega} = \begin{cases} a, \text{if } \arg(\hat{c}) \in \left(-\frac{\pi}{3}, \frac{\pi}{3}\right]; \\ b, \text{if } \arg(\hat{c}) \in \left(-\pi, -\frac{\pi}{3}\right]; \\ c, \text{if } \arg(\hat{c}) \in \left(\frac{\pi}{3}, \pi\right]. \end{cases} \tag{3.9}$$

When there is no noise or estimation error, the angles of ZSV voltage deviation caused by an attack injected in the three phases in polar coordinates are $\theta_a = 0$, $\theta_b = -2\pi/3$ and $\theta_c = 2\pi/3$, respectively. The proposed phase diagnosis in (3.9) is to find the phase whose corresponding polar coordinates is the closest to that of the estimated ZSV value of the injected fault.

In practical applications, the estimated injected fault vector $\hat{c}$ is subject to estimation error. One common way is to model the estimation error defined as

$$\Delta c = c - \hat{c}, \tag{3.10}$$

as a zero-mean Gaussian distribution. It has been shown that under the zero-mean Gaussian error model and equal priori, the proposed test in (3.9) is the optimal test that minimizes the error rate. The proposed localization scheme is summarized in Algorithm 2.

3.2 Case Study

To evaluate the performance of the proposed FDIA localization method in three-phase distribution systems, the IEEE 37 Bus Test Feeder and the IEEE 123 Bus Test

Algorithm 2 Proposed FDIA Localization Scheme Based on ZSV.

```
Calculate the estimated voltages $\hat{\boldsymbol{V}}_a$, $\hat{\boldsymbol{V}}_b$, and $\hat{\boldsymbol{V}}_c$ and then the estimated ZSV $\hat{\boldsymbol{V}}_0$.
Calculate an average of the estimated ZSV $\overline{\hat{V_0}}$ using (3.1), and localize the bus under attack using (3.2).
Calculate the estimated ZSV value of the injected fault using (3.7).
Diagnose the phase under attack using (3.9).
                                                    ▷ The localization result of FDIA.
```

Feeder [71] are used in the case studies. A DSSE method with linear approximation proposed by *Zhuang et al.* in [20] is also utilized in the case studies, which is explained in Subsection 2.1.3 in details. The virtual lines are still added to deal with the missing phase problem, so that the diagnosis of the phase under attack can still be implemented on the buses equipped with one or two phases.

There are two cases of direct measurement arrangements of IEEE 37 Bus Test Feeder and IEEE 123 Bus Test Feeder, which are introduced in Table 2.1 and Table 2.2, respectively. Pseudo measurements based on historical data are also used, whose noise variance is assumed to be 20 or 60 times that of direct measurements. Also, 10^6 events are generated where each event is under attack, and the location of the FDIA is randomly chosen as one phase of a bus. The magnitude of the attack is set as 5%. Eight levels of noise variances are considered: 0.005, 0.006, 0.008, 0.01, 0.015, 0.02, 0.025, and 0.03, which are equivalent to 23.0dB, 22.2dB, 21.0dB, 20dB, 18.2dB, 17.0dB, 16.0dB, and 15.2dB, respectively. All measurement values, DSSE, and localization are simulated in MATLAB.

The localization rate P_L is the ratio of the number of attack events that are correctly localized to the number of attack events. It equals to the product of the probability of correctly localizing the bus under attack and the probability of correctly diagnosing the phase under attack. With some further simulations, we find that there are always some special buses in the topology. For each wrong localization, the localization result corresponds to one of these special buses, i.e., they have a higher possibility of being wrongly localized. Take the IEEE 37 and IEEE 123 Bus Test Feeder as examples. For the IEEE 37 Bus Test Feeder, the set of indices of special buses is $\mathcal{Q}_{37} = \{736, 740, 741, 722, 724, 725\}$; for the IEEE 123 Bus Test Feeder, the set of indices of special buses is $\mathcal{Q}_{123} = \{6, 36, 37, 39, 46, 50, 51, 66, 84, 85, 94, 96, 114, 250\}$. For the probability of correctly diagnosing the phase under attack, with some further simulations, we find out that the probability can even achieve 1 with the same settings in the case studies. This is because a wrong phase diagnosis occurs when the polar angle of $\hat{c}$ shifts by $\pi/3$ from that of c, which is an almost impossible event.

Since the localization rates simulated in many case studies are very closed to one, the localization rate P_L is replaced with the false localization rate P_{FL} in the figures (where $P_L = 1 - P_{FL}$) and the logarithmic scale is used for clear presentation. In simulation, the false localization rate P_{FL} is the ratio of the number of attack events that are wrongly localized to the number of attack events. The relationship between P_{FL} and the noise variance with four different measurement cases for the IEEE 37 Bus Test Feeder and IEEE 123 Bus Test Feeder is shown in Fig. 3.1 and Fig. 3.2, respectively.

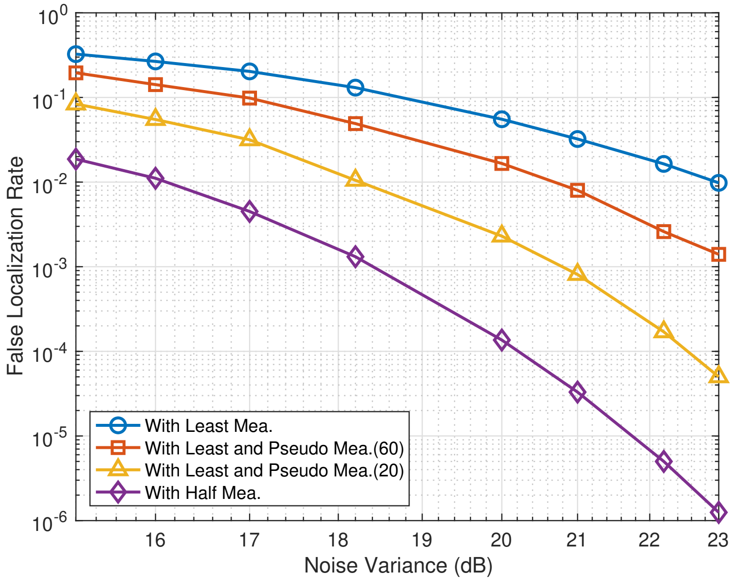

Figure 3.1: P_{FL} v.s. noise variance of IEEE 37 Bus Test Feeder.

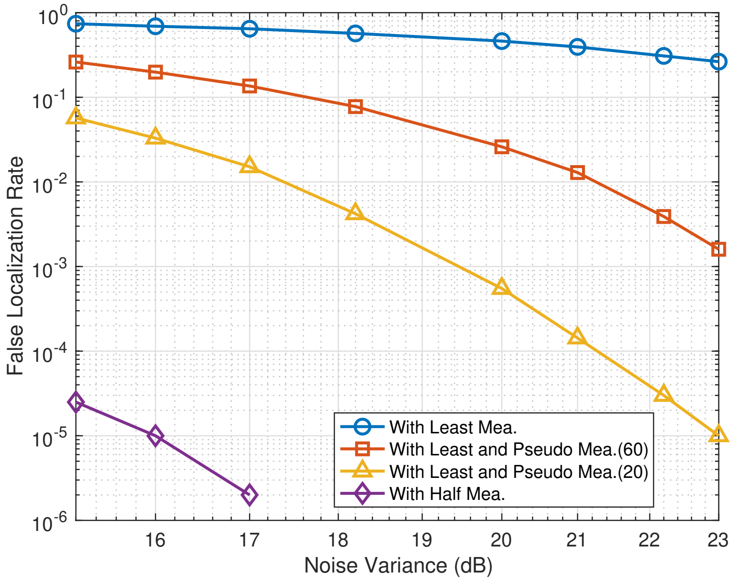

Figure 3.2: P_{FL} v.s. noise variance of IEEE 123 Bus Test Feeder.

Moreover, the values of P_L for the two feeders are shown in Table 3.1 and Table 3.2, respectively.

Table 3.1: P_L v.s. Noise Variance of IEEE 37 Bus Test Feeder

Noise Variance (dB)	Least Mea.			Half Mea.
	Without Pseudo Mea.	With 60% Pseudo Mea.	With 20% Pseudo Mea.	
23.0	0.9902	0.9986	0.99995	0.99999875
22.2	0.9836	0.9974	0.99983	0.999995
21.0	0.9677	0.9920	0.99919	0.999967
20	0.9447	0.9834	0.9977	0.999864
18.2	0.8693	0.9509	0.9895	0.998687
17.0	0.7967	0.9016	0.9684	0.9955
16.0	0.7333	0.8581	0.9451	0.9889
15.2	0.6747	0.8046	0.9163	0.9813

The figures and tables show that as the noise variance decreases or the quality of measurements increases, the localization accuracy improves. With Least and Pseudo

Table 3.2: P_L v.s. Noise Variance of IEEE 123 Bus Test Feeder

Noise Variance (dB)	Least Mea.			Half Mea.
	Without Pseudo Mea.	With 60% Pseudo Mea.	With 20% Pseudo Mea.	
23.0	0.7363	0.9984	0.99999	1
22.2	0.6918	0.9961	0.99997	1
21.0	0.6062	0.9871	0.999857	1
20	0.5385	0.9740	0.99945	1
18.2	0.4316	0.9224	0.9958	1
17.0	0.3545	0.8640	0.9849	0.999998
16.0	0.3092	0.8017	0.9671	0.99999
15.2	0.2602	0.7391	0.9430	0.999975

Measurements (20) and 20dB noise variance, for the IEEE 37 Bus Test Feeder, the proposed FDIA localization scheme can achieve 99.77% of localization rate; for the IEEE 123 Bus Test Feeder, the proposed FDIA localization scheme can achieve 99.945% of localization rate.

3.3 Summary

Considering the unbalanced nature of multiphase power distribution systems, an FDIA localization scheme based on ZSV is proposed in this chapter. Based on the estimated ZSV of a bus relative to others, the bus under attack is localized, and the injected attack value is estimated by eliminating the estimation error. With an optimal phase test, the phase under attack is diagnosed with the minimum error. The feasibility of the proposed scheme is verified using the IEEE 37 and 123 Bus Test Feeders. It is shown by simulation results that the proposed scheme can achieve successful FDIA localization under various environments with high accuracy.

Chapter 4

Conclusion and Future Work

In this thesis, we investigate the FDIA detection and localization schemes for multiphase power distribution systems. To detect the presence of stealthy FDIAs, we proposed a ZSV-based FDIA detection scheme. In this scheme, a ZSV estimation is obtained from the DSSE with linear approximation. The estimated ZSV is then processed by subtracting the intrinsic ZSV average value and a whitening transformation matrix. The existence of FDIA is detected by comparing the $\mathcal{L}_2$-norm of the processed estimated ZSV vector with a predefined threshold. The distribution of the state estimation is analyzed, based on which the whitening transformation matrix is designed and the false alarm rate is derived in a simple analytical form. Extensive case studies on both IEEE 37 Bus Test Feeder and IEEE 123 Bus Test Feeder show that the proposed method is capable of accurately detecting FDIAs with low false alarm rate. The comparison with the existing ISE-based detection scheme is also conducted to further demonstrate the superiority of the proposed method. Further, simulation results validate the analytical results on false alarm rate and demonstrate the importance of the designed processes on the estimated ZSV, including the whitening transformation and the intrinsic-ZSV subtraction.

To further specify the location of stealthy FDIAs in multiphase power distribution systems, we proposed a ZSV-based FDIA localization scheme. In this scheme, based on the estimated ZSV value of a bus relative to others, the bus under attack can be localized. The injected fault value on the bus under attack is then estimated by eliminating the estimation error. After localizing the bus under attack, with an optimal phase test, the phase under attack can then be diagnosed with the minimum error. The feasibility of the proposed FDIA localization scheme is verified using the IEEE 37 Bus Test Feeder and IEEE 123 Bus Test Feeder, where the results show that the proposed method can achieve high localization rates under various measurement and noise settings.

In the following, we list several possible future research directions based on the work in this thesis:

- For the proposed detection scheme in Chapter 2, the corresponding mathematical models can be extended for different DSSE methods. Specifically, in Chapter 2, the linearized DSSE method in [28] and its related linearized FDIA model in [20] are used as the foundations for the proposed FDIA detection scheme. The future work can focus on the extended applications of the proposed scheme under nonlinear DSSE methods and FDIA models for distribution systems [21]. The mathematical analysis, e.g., (2.31)-(2.56), needs to be re-conducted to incorporate the nonlinear DSSE, and the Algorithm 1 needs to be updated accordingly for FDIA detection.

- The proposed attack detection and localization schemes in this thesis are designed specifically for FDIAs. In a real-world CPS, there exist other types of cyber-attacks that can also result in significant consequences on the normal operations of power systems, such as denial of service attacks, load altering attacks, energy theft, etc. The future work can focus on the extended applications of the proposed ZSV-based detection and localization schemes on different types of cyber-attacks in CPS, e.g., modeling the energy theft for multiphase distribution systems as the FDIAs in [19, 20, 28], and updating the proposed detection and localization schemes accordingly.

Bibliography

[1] S. Galli, A. Scaglione, and Z. Wang, “For the grid and through the grid: The role of power line communications in the smart grid,” *Proceedings of the IEEE*, vol. 99, no. 6, pp. 998–1027, Jun. 2011.

[2] H. Farhangi, “The path of the smart grid,” *IEEE Power and Energy Magazine*, vol. 8, no. 1, pp. 18–28, Jan.-Feb. 2010.

[3] X. Fang, S. Misra, G. Xue, and D. Yang, “Smart grid — the new and improved power grid: A survey,” *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 944–980, 2012.

[4] X. Yu and Y. Xue, “Smart grids: A cyber–physical systems perspective,” *Proceedings of the IEEE*, vol. 104, no. 5, pp. 1058–1070, May 2016.

[5] T. Nguyen, S. Wang, M. Alhazmi, M. Nazemi, A. Estebsari, and P. Dehghanian, “Electric power grid resilience to cyber adversaries: State of the art,” *IEEE Access*, vol. 8, pp. 87 592–87 608, May 2020.

[6] S. Sridhar, A. Hahn, and M. Govindarasu, “Cyber–physical system security for the electric power grid,” *Proceedings of the IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

[7] H. Zhang, B. Liu, and H. Wu, “Smart grid cyber-physical attack and defense: A review,” *IEEE Access*, vol. 9, pp. 29 641–29 659, Feb. 2021.

[8] A. S. Musleh, G. Chen, and Z. Y. Dong, “A survey on the detection algorithms for false data injection attacks in smart grids,” *IEEE Transactions on Smart Grid*, vol. 11, no. 3, pp. 2218–2234, May 2020.

[9] S. Toppa. “The national power grid is under almost continuous attack, report says.” (Mar. 2015), [Online]. Available: https://bit.ly/1FH246I.

[10] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, “The 2015 ukraine blackout: Implications for false data injection attacks,” *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[11] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, “A review of false data injection attacks against modern power systems,” *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630–1638, Jul. 2017.

[12] 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, no. 2, pp. 411–423, Apr. 2017.

[13] Y. Liu, P. Ning, and M. K. Reiter, “False data injection attacks against state estimation in electric power grids,” *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, May 2011.

[14] X. Liu and Z. Li, “Local topology attacks in smart grids,” *IEEE Transactions on Smart Grid*, vol. 8, no. 6, pp. 2617–2626, Nov. 2017.

[15] M. A. Rahman and H. Mohsenian-Rad, “False data injection attacks against nonlinear state estimation in smart power grids,” in *2013 IEEE Power & Energy Society General Meeting*, Jul. 2013, pp. 1–5.

[16] G. Hug and J. A. Giampapa, “Vulnerability assessment of ac state estimation with respect to false data injection cyber-attacks,” *IEEE Transactions on Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.

[17] J. Liang, O. Kosut, and L. Sankar, “Cyber attacks on ac state estimation: Unobservability and physical consequences,” in *2014 IEEE PES General Meeting - Conference & Exposition*, Jul. 2014, pp. 1–5.

[18] 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, Sep. 2017.

[19] R. Deng, P. Zhuang, and H. Liang, “False data injection attacks against state estimation in power distribution systems,” *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2871–2881, May 2019.

[20] P. Zhuang, R. Deng, and H. Liang, “False data injection attacks against state estimation in multiphase and unbalanced smart distribution systems,” *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6000–6013, Nov. 2019.

[21] N. N. Tran, H. R. Pota, Q. N. Tran, and J. Hu, “Designing constraint-based false data-injection attacks against the unbalanced distribution smart grids,” *IEEE Internet of Things Journal*, vol. 8, no. 11, Jun. 2021.

[22] A. Primadianto and C.-N. Lu, “A review on distribution system state estimation,” *IEEE Transactions on Power Systems*, vol. 32, no. 5, pp. 3875–3883, Sep. 2017.

[23] J. D. D. Glover and M. S. Sarma, *Power System Analysis and Design*, 3rd. USA: Brooks/Cole Publishing Co., 2001, ISBN: 0534953670.

[24] K. Dehghanpour, Z. Wang, J. Wang, Y. Yuan, and F. Bu, “A survey on state estimation techniques and challenges in smart distribution systems,” *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2312–2322, Mar. 2019.

[25] M. Baran and A. Kelley, “State estimation for real-time monitoring of distribution systems,” *IEEE Transactions on Power Systems*, vol. 9, no. 3, pp. 1601–1609, Aug. 1994.

[26] Y. Deng, Y. He, and B. Zhang, “A branch-estimation-based state estimation method for radial distribution systems,” *IEEE Transactions on Power Delivery*, vol. 17, no. 4, pp. 1057–1062, Oct. 2002.

[27] D. A. Haughton and G. T. Heydt, “A linear state estimation formulation for smart distribution systems,” *IEEE Transactions on Power Systems*, vol. 28, no. 2, pp. 1187–1195, May 2013.

[28] C. Lu, J. Teng, and W.-H. Liu, “Distribution system state estimation,” *IEEE Transactions on Power Systems*, vol. 10, no. 1, pp. 229–240, Feb. 1995.

[29] P. M. De Oliveira-De Jesus and A. A. Rojas Quintana, “Distribution system state estimation model using a reduced quasi-symmetric impedance matrix,” *IEEE Transactions on Power Systems*, vol. 30, no. 6, pp. 2856–2866, Nov. 2015.

[30] P. Jokar, N. Arianpoo, and V. C. M. Leung, “Electricity theft detection in ami using customers’ consumption patterns,” *IEEE Transactions on Smart Grid*, vol. 7, no. 1, pp. 216–226, Jan. 2016.

[31] J. G. Sreenath, A. Meghwani, S. Chakrabarti, K. Rajawat, and S. C. Srivastava, “A recursive state estimation approach to mitigate false data injection attacks in power systems,” in *2017 IEEE Power & Energy Society General Meeting*, 2017, pp. 1–5.

[32] R. Xu, R. Wang, Z. Guan, L. Wu, J. Wu, and X. Du, “Achieving efficient detection against false data injection attacks in smart grid,” *IEEE Access*, vol. 5, 2017.

[33] 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, Jul. 2020.

[34] B. Li, G. Xiao, R. Lu, R. Deng, and H. Bao, “On feasibility and limitations of detecting false data injection attacks on power grid state estimation using d-facts devices,” *IEEE Transactions on Industrial Informatics*, vol. 16, no. 2, pp. 854–864, Feb. 2020.

[35] C. Liu, J. Wu, C. Long, and D. Kundur, “Reactance perturbation for detecting and identifying fdi attacks in power system state estimation,” *IEEE Journal of Selected Topics in Signal Processing*, vol. 12, no. 4, pp. 763–776, Aug. 2018.

[36] B. Li, R. Lu, G. Xiao, Z. Su, and A. Ghorbani, “Pama: A proactive approach to mitigate false data injection attacks in smart grids,” in *2018 IEEE Global Communications Conference (GLOBECOM)*, 2018, pp. 1–6.

[37] I. Lukicheva, D. Pozo, and A. Kulikov, “Cyberattack detection in intelligent grids using non-linear filtering,” in *2018 IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe)*, 2018, pp. 1–6.

[38] M. G. Kallitsis, S. Bhattacharya, S. Stoev, and G. Michailidis, “Adaptive statistical detection of false data injection attacks in smart grids,” in *2016 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, 2016, pp. 826–830.

[39] R. Moslemi, A. Mesbahi, and J. M. Velni, “A fast, decentralized covariance selection-based approach to detect cyber attacks in smart grids,” *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4930–4941, Sep. 2018.

[40] Y. Chen, S. Huang, F. Liu, Z. Wang, and X. Sun, “Evaluation of reinforcement learning-based false data injection attack to automatic voltage control,” *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2158–2169, Mar. 2019.

[41] B. Tang, J. Yan, S. Kay, and H. He, “Detection of false data injection attacks in smart grid under colored gaussian noise,” in *2016 IEEE Conference on Communications and Network Security (CNS)*, 2016, pp. 172–179.

[42] I. Akingeneye and J. Wu, “Low latency detection of sparse false data injections in smart grids,” *IEEE Access*, vol. 6, pp. 58 564–58 573, 2018.

[43] M. N. Kurt, Y. Yılmaz, and X. Wang, “Real-time detection of hybrid and stealthy cyber-attacks in smart grid,” *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 2, pp. 498–513, Feb. 2019.

[44] 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, Dec. 2014.

[45] D. B. Rawat and C. Bajracharya, “Detection of false data injection attacks in smart grid communication systems,” *IEEE Signal Processing Letters*, vol. 22, no. 10, pp. 1652–1656, Oct. 2015.

[46] M. N. Kurt, Y. Yılmaz, and X. Wang, “Distributed quickest detection of cyber-attacks in smart grid,” *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 2015–2030, Aug. 2018.

[47] H. Karimipour and V. Dinavahi, “Robust massively parallel dynamic state estimation of power systems against cyber-attack,” *IEEE Access*, vol. 6, pp. 2984–2995, 2018.

[48] Y. Li, J. Li, X. Luo, X. Wang, and X. Guan, “Cyber attack detection and isolation for smart grids via unknown input observer,” in *2018 37th Chinese Control Conference (CCC)*, 2018, pp. 6207–6212.

[49] B. Li, T. Ding, C. Huang, J. Zhao, Y. Yang, and Y. Chen, “Detecting false data injection attacks against power system state estimation with fast go-decomposition approach,” *IEEE Transactions on Industrial Informatics*, vol. 15, no. 5, pp. 2892–2904, May 2019.

[50] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, “Detecting stealthy false data injection using machine learning in smart grid,” *IEEE Systems Journal*, vol. 11, no. 3, pp. 1644–1652, Sep. 2017.

[51] E. M. Ferragut, J. Laska, M. M. Olama, and O. Ozmen, “Real-time cyber-physical false data attack detection in smart grids using neural networks,” in *2017 International Conference on Computational Science and Computational Intelligence (CSCI)*, 2017, pp. 1–6.

[52] S. Binna, S. R. Kuppannagari, D. Engel, and V. K. Prasanna, “Subset level detection of false data injection attacks in smart grids,” in *2018 IEEE Conference on Technologies for Sustainability (SusTech)*, 2018, pp. 1–7.

[53] K Vimalkumar and N Radhika, “A big data framework for intrusion detection in smart grids using apache spark,” in *2017 International Conference on Advances in Computing, Communications and Informatics (ICACCI)*, 2017, pp. 198–204.

[54] 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.

[55] A. Jindal, A. Dua, K. Kaur, M. Singh, N. Kumar, and S. Mishra, “Decision tree and svm-based data analytics for theft detection in smart grid,” *IEEE Transactions on Industrial Informatics*, vol. 12, no. 3, pp. 1005–1016, Jun. 2016.

[56] M. T. Mostafa Mohammadpourfard Yang Weng, “Benchmark of machine learning algorithms on capturing future distribution network anomalies,” *IET Generation, Transmission & Distribution*, vol. 13, no. 8, pp. 1441–1455, Apr. 2019.

[57] L. Wei, D. Gao, and C. Luo, “False data injection attacks detection with deep belief networks in smart grid,” in *2018 Chinese Automation Congress (CAC)*, 2018, pp. 2621–2625.

[58] S. Ntalampiras, “Fault diagnosis for smart grids in pragmatic conditions,” *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 1964–1971, May 2018.

[59] Y. Zhang, J. Wang, and B. Chen, “Detecting false data injection attacks in smart grids: A semi-supervised deep learning approach,” *IEEE Transactions on Smart Grid*, vol. 12, no. 1, pp. 623–634, Jan. 2021.

[60] X. Wang, X. Luo, M. Zhang, Z. Jiang, and X. Guan, “Detection and isolation of false data injection attacks in smart grid via unknown input interval observer,” *IEEE Internet of Things Journal*, vol. 7, no. 4, pp. 3214–3229, Apr. 2020.

[61] X. Luo, Y. Li, X. Wang, and X. Guan, “Interval observer-based detection and localization against false data injection attack in smart grids,” *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 657–671, Jan. 2021.

[62] S. Wang, S. Bi, and Y.-J. A. Zhang, “Locational detection of the false data injection attack in a smart grid: A multilabel classification approach,” *IEEE Internet of Things Journal*, vol. 7, no. 9, pp. 8218–8227, Sep. 2020.

[63] O. Boyaci, M. R. Narimani, K. R. Davis, M. Ismail, T. J. Overbye, and E. Serpedin, “Joint detection and localization of stealth false data injection attacks in smart grids using graph neural networks,” *IEEE Transactions on Smart Grid*, vol. 13, no. 1, pp. 807–819, Jan. 2022.

[64] J. Shi, S. Liu, B. Chen, and L. Yu, “Distributed data-driven intrusion detection for sparse stealthy fdi attacks in smart grids,” *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 68, no. 3, pp. 993–997, Mar. 2021.

[65] X. Huang, Z. Qin, M. Xie, H. Liu, and L. Meng, "Defense of massive false data injection attack via sparse attack points considering uncertain topological changes," *Journal of Modern Power Systems and Clean Energy*, pp. 1–11, 2021.

[66] M. Du, G. Pierrou, X. Wang, and M. Kassouf, "Targeted false data injection attacks against ac state estimation without network parameters," *IEEE Transactions on Smart Grid*, vol. 12, no. 6, pp. 5349–5361, Nov. 2021.

[67] R. Xiao, Y. Xiang, L. Wang, and K. Xie, "Power system reliability evaluation incorporating dynamic thermal rating and network topology optimization," *IEEE Transactions on Power Systems*, vol. 33, no. 6, pp. 6000–6012, Nov. 2018.

[68] O. Pereira, J. Quirós-Tortós, and G. Valverde, "Phase rebalancing of distribution circuits dominated by single-phase loads," *IEEE Transactions on Power Systems*, vol. 36, no. 6, pp. 5333–5344, Nov. 2021.

[69] M. Sun, S. Demirtas, and Z. Sahinoglu, "Joint voltage and phase unbalance detector for three phase power systems," *IEEE Signal Processing Letters*, vol. 20, no. 1, pp. 11–14, Jan. 2013.

[70] D. Horgan and C. C. Murphy, "On the convergence of the chi square and noncentral chi square distributions to the normal distribution," *IEEE Communications Letters*, vol. 17, no. 12, pp. 2233–2236, Dec. 2013.

[71] "Ieee test feeder specifications." (2017), [Online]. Available: http://sites.ieee.org/pes-testfeeders/resources.

[72] R. Singh, B. Pal, and R. Vinter, "Measurement placement in distribution system state estimation," in *2009 IEEE Power & Energy Society General Meeting*, 2009, pp. 1–1.

[73] Y. Isozaki *et al.*, "Detection of cyber attacks against voltage control in distribution power grids with pvs," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 1824–1835, Jul. 2016.

[74] T. Kanungo and R. Haralick, "Receiver operating characteristic curves and optimal bayesian operating points," in *Proceedings., International Conference on Image Processing*, vol. 3, 1995, 256–259 vol.3.

[75] "Smart meters and smart meter systems: A metering industry perspective." (March 2011), [Online]. Available: https://aeic.org/smartmetersfinal032511/.