Dynamic State Estimation for Power Grids with Unconventional Measurements

Liang Hu

Department of Computer Science
Brunel University London

This dissertation is submitted for the degree of
Doctor of Philosophy

May 2016

I would like to dedicate this thesis to my wife, Chunyang.

Declaration

I, Liang Hu, hereby declare that this thesis and the work presented in it is entirely my own. Some of the work has been previously published in journal or conference papers, and this has been mentioned in the thesis. Where I have consulted the work of others, this is always clearly stated.

Liang Hu
May 2016

Acknowledgements

First of all, I wish to express my deepest gratitude to my supervisors, Prof. Zidong Wang and Prof. Xiaohui Liu for their constant support, professional guidance and invaluable encouragement. Prof. Zidong Wang is a great supervisor. Not only did his ideas and insights help to shape my research, but his aesthetic sense and intuition taught me what good research is truly about. The responsible attitude toward work I learned from him will definitely benefit my career greatly. Prof. Xiaohui Liu is very kind and always encourages and helps me whenever and wherever I face difficulties. I have always appreciated his best effort to provide me an excellent environment for doing research.

I am truly grateful to my former supervisor Prof. Huijun Gao in China, who encouraged me to apply for the PhD student position at Brunel University London and have given me continued support over these years.

In addition, I would like to express my gratitude to the following people for useful discussions, suggestions, comments, and supports of my research during the PhD stage: Prof. Hongli Dong, Prof. Jun Hu, Dr. Derui Ding, Lei Zou, Wei Pan, Prof. Jiahu Qin, Dr. Lifeng Ma, Dr. Jie Zhang, Dr. Yong Zhang, Dr. Li Sheng, Dr. Chuanbo Wen, Prof. Chenxiao Cai, Qinyuan Liu, Dr. Miqing Li, Chuang Wang and Weibo Liu.

I would like to thank all my colleagues and friends at the Centre for Intelligent Data Analysis for the pleasant and enjoyable working atmosphere: Dr. Miqing Li, Chuang Wang, Dr. Djibril Kaba, Dr. Valeria Bo, Neda Trifonova, Dr. Izaz Rahman, Mohsina Ferdous, Weibo Liu, Khalid Eltayef, Bashir Dodo, Navid Dorudian, Shakirat Adesola, Ahmed Al-Madi, Dr. Emma Haddi, Dr. Yuanxi Li, Dr. Ali Tarhini. I would also like to thank the Department of Computer Science, Brunel University London for funding my PhD research.

The last but not the least, I owe the most to my family. My parents and grandmother worked hard and supported me unconditionally all the time, which inspired me and kept me move forward. My wife and my son, who never complained of receiving less time and attention from me due to my busy work, brought endless love and happiness to my life. I also wish to acknowledge my parents-in-law for their unselfish love and care.

Abstract

State estimation problem for power systems has long been a fundamental issue that demands a variety of methodologies dependent on the system settings. With recent introduction of advanced devices of phasor measurement units (PMUs) and dedicated communication networks, the infrastructure of power grids has been greatly improved. Coupled with the infrastructure improvements are three emerging issues for the state estimation problems, namely, the coexistence of both traditional and PMU measurements, the incomplete information resulting from delayed, missing and quantized measurements due to communication constraints, and the cyber-attacks on the communication channels.

Three challenging problems are faced when dealing with the three issues in the state estimation program of power grids: 1) how to include the PMU measurements in the state estimator design, 2) how to account for the phenomena of incomplete information occurring in the measurements and design effective state estimators resilient to such phenomena, and 3) how to identify the system vulnerability in state estimation scheme and protect the estimation system against cyber-attacks.

In this thesis, with the aim to solve the above problems, we develop several state estimation algorithms which tackle the issues of mixed measurements and incomplete information, and examine the cyber-security of the dynamic state estimation scheme.

- To improve the estimation performance of power grids including PMU measurements, a hybrid extended Kalman filter and particle swarm optimization algorithm is developed, which has the advantages of being scalable to the numbers of the installed PMUs and being compatible with existing dynamic state estimation software as well.

- Two kinds of network-induced phenomena, which leads to incomplete information of measurements, are considered. Specifically, the phenomenon of missing measurements is assumed to occur randomly and the missing probability is governed by a random variable, and the quantized nonlinear measurement model of power systems is presented where the quantization is assumed to be of logarithmic type. Then, the impact of the incomplete information on the overall estimation performance is taken into account when designing the estimator. Specifically, a modified extended Kalman

filter is developed which is insensitive to the missing measurements in terms of acceptable probability, and a recursive filter is designed for the system with quantized measurements such that an upper bound of the estimation error is guaranteed and also minimized by appropriately designing the filter gain.

- With the aim to reduce or eliminate the occurrence of the above-mentioned network-induced phenomena, we propose an event-based state estimation scheme with which communication transmission from the meters to the control centre can be greatly reduced. To ensure the estimation performance, we design the estimator gains by solving constrained optimization problems such that the estimation error covariances are guaranteed to be always less than a finite upper bound.

- We examine the cyber-security of the dynamic state estimation system in power grids where the adversary is able to inject false data into the communication channels between PMUs and the control centre. The condition under which the attacks cause unbounded estimation errors is found. Furthermore, for system that is vulnerable to cyber-attacks, we propose a system protection scheme through which only a few (rather than all) communication channels require protection against false data injection attacks.

Table of contents

List of figures

List of tables

Nomenclature

Symbols

$\mathbb{N}$	the set of all nonnegative integers
$\mathbb{R}$	the set of all real numbers
$\mathbb{C}$	the set of all complex numbers
$\mathbb{R}^+$	the set of all nonnegative real numbers
$\mathbb{R}^n$	the n-dimensional Euclidean space
$\mathbb{R}^{n\times m}$ $(\mathbb{C}^{n\times m})$	the $n \times m$ real (complex) matrices
$\mathbb{S}^n_+$	the set of $n \times n$ positive semi-definite matrices
I	the identity matrix of compatible dimension
0	the zero matrix of compatible dimension
I_m (0_m)	the m-dimensional vector with all elements equal to 1 (0)
$*$	the ellipsis for terms induced by symmetry, in symmetric block matrices
$\mathrm{diag}_N\{*\}$	$\mathrm{diag}\{\underbrace{*,\cdots,*}_{N}\}$
$\mathrm{diag}_N\{A_i\}$	$\mathrm{diag}\{A_1,A_2,\cdots,A_N\}$
$\mathrm{vec}_N\{x_i\}$	$\begin{bmatrix} x_1 & x_2 & \cdots & x_N \end{bmatrix}$
$A \circ B$	the the Hadamard product of two matrices A and B
A^T	the transpose of the matrix A
A^{-1}	the inverse of the matrix A

A^+ the Moore-Penrose pseudo inverse of the matrix A

$\mathrm{tr}(A)$ the trace of the matrix A

$\det(A)$ the determinant of the matrix A

$\mathrm{Rk}(A)$ the rank of the matrix A

$\rho(A)$ the spectral radius of the matrix A

$\sigma_{\max}(A)$ the maximum singular value of a matrix A

$\lambda_{\min}(A)$ the smallest eigenvalue of a square matrix A

$\lambda_{\max}(A)$ the largest eigenvalue of a square matrix A

$\mathbb{E}\{x\}$ the expectation of the stochastic variable x with respect to the given probability measure probability

$\mathrm{Re}(\alpha)$ the real part of α, where $\alpha \in \mathbb{C}$

$\mathrm{Prob}(\cdot)$ the occurrence probability of the event "$\cdot$"

$X > 0$ ($X \geq 0$) X is positive definite (semi-definite)

$X \geq Y$ ($X > Y$) $X - Y$ is positive semi-definite (semi-definite)

$\{x(k)\}$ an infinite sequence $x(1), x(2), \cdots, x(k), \cdots$

I_m^s the s-th column of $m \times m$-dimensional identity matrix I_m, e.g, $I_m^s = [\underbrace{\overbrace{0,\ldots,0}^{s-1},1,0,\ldots,0}_{m}]^T$

Acronyms / Abbreviations

ADC analog-to-digital

AMSE average mean square error

DDSE distributed dynamic state estimation

DOS denial-of-service

DSE dynamic state estimation

DSSE distributed static state estimation

EKF	extended Kalman filter
EMS	energy management system
FDI	false data injection
LQG	linear quadratic Gaussian
LTI	linear time-invariant
MMSE	minimum mean square error
MMSE	mean square error
PDC	phasor data concentrator
PMU	phasor measurement unit
PSO	particle swarm optimization
PSSE	power system state estimation
RTU	remote terminal unit
SCADA	supervisory control and data acquisition
SE	state estimation
SOD	send-on-delta
SSE	static state estimation
UKF	uncented Kalman filter
WLS	weighted least square

Chapter 1

Introduction

1.1 Motivation

The power grid, which is regarded as one of the greatest engineering achievements in the 20th century, has been undergoing important changes since the beginning of the 21st century [49]. Due to the low-carbon requirement, more and more renewable distributed generations such as photovoltaic (PV) generators and wind farms are incorporated in the power grids and, therefore, the nowadays power grids have inevitably become complex large-scale dynamic networks demanding sophisticated analysis and control tools. To monitor and control such networks in an efficient and flexible way, the supervisory control and data acquisition (SCADA) system, as the information technology (IT) infrastructure in power grids, has been enhanced by the development in sensor and network technologies. Specifically, the advanced phasor measurement units (PMUs) and the communication networks have truly been the enabling technologies in SCADA systems. A typical system structure of power grids is depicted in Fig. 1.1.

Synchronized PMU is an advanced meter developed in 1980s, which is capable of directly measuring both voltage/current magnitudes and phase angles. In addition, PMUs sample at a much higher frequency compared to conventional remote terminal units (RTUs), and all PMUs are synchronized by the GPS universal clock. When a sufficient number of PMUs are deployed in the power grid, all system states are observable and can be easily calculated from the linear PMU measurement equation. However, for economic reasons, it is not affordable to replace all the conventional RTUs with PMUs in the foreseeable future. As a result, it is a challenge to make the most of the mixed (PMU and RTU) measurements to better monitor and control the power grid.

While PMUs provide accurate and timely system measurements for the power grid, the communication network does play an important role to deliver the measurements from the

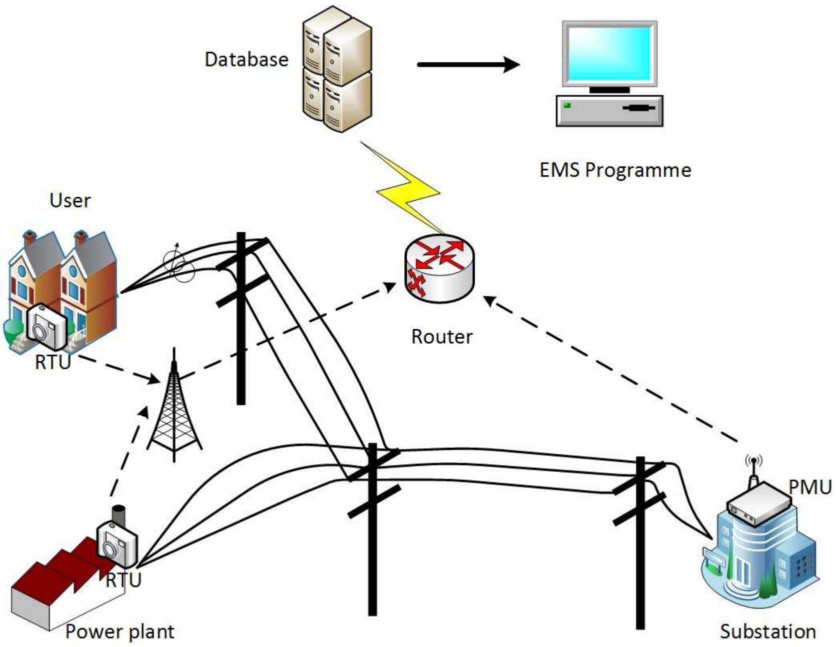


Fig. 1.1 A typical system structure of power grids

meters to the control centre. Depending on the transmission distance and communication capability, a variety of communication technologies have been used in the SCADA systems that include, but are not limited to, power line, wired network and wireless network [54, 49]. Power lines, though mainly used for power transmissions, can transmit information using the signal modulation techniques. Typically, the data transmission via power lines is limited in the area between two transformers as no signal can propagate through the transformers. Wired networks connected through telephone line and/or optical fibre can provide reliable communication in long distance, but great investments are needed for deploying such networks in the geographically wide-spanned power grids. Compared with the wired network, the wireless one has the benefits of low installation and maintenance cost, but wireless signals are generally susceptible to external disturbances and noises that could deteriorate the signal quality.

Though the deployment of the communication networks has greatly improved the efficiency and reliability of the SCADA system, the bandwidth-constrained communication networks still remain as the bottleneck when a huge amount of measurement data are transmitted over a long distance. In such a case, the networked-induced phenomena (e.g. transmission delays, data asynchronization, quantization and packet losses) may occur. For instance, it has been reported that, in the Bonneville Power Administration system, the transmission of PMU packets using modems has high latency (60–100 ms) and relatively high dropout rates, and the latency using fibre optic digital communication is approximate 30 ms [163]. A direct consequence of network-induced phenomena is that only incomplete information of the measurements can be received by the control centre. On the other hand, the pervasive usage of communication networks makes the power grid vulnerable to cyber-attacks. Since the power grid is a closely coupled cyber-physical system, the attacks on the communication networks can mislead the system operations and subsequently affect the physical dynamics of the power grid.

A seemingly natural idea to handle the emerging network-induced issues of mixed measurements, incomplete information and cyber-attacks is to widely deploy PMUs and develop reliable, secure and low-latency communication network infrastructures in the SCADA systems. This idea is, unfortunately, not physically feasible in the near future simply because of technological and financial constraints. As such, it is practically significant and theoretically important to develop new algorithms and update existing energy management software (EMS) so as to tackle the network-induced limitations. Among the programs in the EMS software package, In particular, we focus on the power system state estimation (PSSE) in the thesis. The PSSE program serves to monitor the state of power grids and enables EMS to perform other control and optimization tasks such as bad data detection and power flow optimization.

Traditional state estimation methods used in the control centres have been designed to deal with the conventional RTU measurements alone. Compared with the RTUs, the PMUs provide more accurate measurements with a much higher sampling rate. Due to the differences between these two kinds of measurements, the traditional state estimators cannot be directly used to deal with the PMU measurements. As such, much research effort has been devoted to the development of new yet effective estimation algorithms that are suitable for mixed RTU and PMU measurements. Moreover, the incomplete information occurring in the measurements is usually ignored in the traditional state estimator and, as such, there is no guarantee that the estimation performance is as good as expected in the presence of network-induced phenomena such as packet dropouts and communication delays. To this end, there is a rather urgent need to develop new state estimators that are robust against incomplete information yet efficient in handling mixed RTU/PMU measurements. Two issues that we would have to face are the characterization of the incomplete information and the examination of the impact from incomplete information on the overall estimation performance for power grids.

As to the cyber-security issue of the state estimation system in power grids, the false data injection (FDI) attacks have been paid special attention in the past few years. Through designing the attack data deliberately, the attacker can modify the measurements and subsequently the state estimate of the power grid via bypassing the bad data detection scheme in power grids. As such, it is important yet challenging to identify the system vulnerability in the existing state estimation schemes and develop effective attack detection methods as well as system protection mechanisms. It should be pointed out that, since the power system dynamics is closely related with the behaviours in communication networks, the cyber-security issue in power systems cannot be solved using only classical system and control approaches or existing information security methods [150]. For instance, reliance on communication networks increases the possibility of intentional cyber-attacks against physical plants, and this problem cannot be solved by simply using classical control design approaches. On the other hand, information security methods (e.g. authentication, access control, message integrity) do not explicitly exploit the system dynamics of the underlying physical process, and are therefore inapplicable since system dynamics is often the target for cyber-attacks. As such, it is important yet challenging to identify the system vulnerability in the existing state estimation schemes and to develop effective attack detection methods and system protection mechanisms.

1.2 Contribution

The main contributions of the thesis are listed as follows.

- A new dynamic state estimation scheme is proposed to improve the estimation performance of power system including PMU measurements. 1) Such a scheme has the advantages of being scalable to the numbers of the installed PMUs and of being compatible with existing DSE software. 2) Practical issues of missing measurements in communication network are investigated thoroughly and a modified EKF algorithm is developed which is insensitive to the measurement unreliability in terms of acceptable probability. 3) Extensive comparative experiments have been implemented based on different missing rates of the RTU measurements and it is confirmed that our proposed estimation algorithm provides better performance than the traditional EKF in the presence of the missing measurements.

- An explicit model for power system with quantized nonlinear measurement is proposed that is closer to the engineering practice. Based on the proposed model, a recursive estimation algorithm is developed for the system with consideration of both the nonlinear measurements and quantization effects. It is to be noted that the developed recursive algorithm is computational efficient and suitable for on-line application in power systems.

- A joint input and state estimator is proposed for the power grid with unknown input based on a novel event-based transmission scheme. The communication burden is lessen in such a scheme where less measurement data are transmitted to the control centre than in the traditional time-based scheme. On the other hand, the joint input/state estimates are guaranteed to be precise within a known confidence interval even though only partial measurements at the event-triggered instants are accessible by the proposed estimator.

- As to the cyber-security issue in the state estimation problem for power grids: 1) new security criteria are proposed for state estimation systems under FDI attacks and, in the case that all communication channels are compromised by the adversary, our criteria are shown to be necessary and sufficient that improve the existing ones; 2) an effective protection scheme is proposed for the system which is insecure under FDIAs; and 3) the developed criteria are applied to security analysis and system protection in the state estimation program of power grids.

1.3 Publication

The following papers report the research results in this thesis:

- **L. Hu**, Z. Wang, I. Rahman and X. Liu, A constrained optimization approach to dynamic state estimation for power systems including PMU and missing measurements, *IEEE Transactions on Control Systems Technology*, 2015, in press. DOI: 10.1109/ TCST.2015.2445852. (Resulting from Chapter 3)

- **L. Hu**, Z. Wang and X. Liu, Dynamic state estimation of power systems with quantization effects: a recursive filter approach, *IEEE Transactions on Neural Networks and Learning Systems*, 2015, in press. DOI: 10.1109/TNNLS.2014.2381853. (Resulting from Chapter 4)

- **L. Hu**, Z. Wang and X. Liu, Event-triggered input and state estimation for linear discrete-time systems, under review (submitted to *International Journal of Control*). (Resulting from Chapter 5)

- **L. Hu**, Z. Wang and X. Liu, State estimation under false data injection attacks: security analysis and attack detection, under review (submitted to *IEEE Transactions on Automatic Control*). (Resulting from Chapter 6)

- **L. Hu**, Z. Wang and X. Liu, A Survey on state estimation of power grids with unconventional measurements, under review (submitted to *IEEE Transactions on Smart Grid*). (Resulting from Chapter 2)
- Z. Wang, **L. Hu**, I. Rahman and X. Liu, A constrained optimization approach to dynamic state estimation for power systems including PMU measurements, International Conference on Automation and Computing (ICAC), 2013, IEEE press. (Resulting from Chapter 3)

1.4 Thesis Structure

This thesis is organised into 7 Chapters (including the present chapter). The contents of the remaining chapters are outlined as follows.

In Chapter 2, we review some recent advances on the state estimation problems for power systems where new measurement devices and communication networks are introduced. Three types of new issues (i.e., mixed measurements, incomplete information and FDI attacks) have been paid particular attentions. This chapter begin with the background knowledge on the topic of power system state estimation. Following that, the state estimation problem with the above mentioned three issues are discussed one by one. We analyse the motivation for each issue, present their impact on the estimation performance and provide overviews on the corresponding research results. Specifically, 1). the research works on mixed measurements are categorized into three frameworks, namely, the dynamic state estimation framework, the static state estimation framework and the hardware-enhanced framework; 2). the methods for dealing with the incomplete information are classified into two types, one is to make the state estimator resilient to incomplete information through improving traditional estimation algorithms, and the other is to eliminate the occurrences of incomplete information by adopting the new decentralized estimation structure; and 3). we summarize the research work on state estimation with FDI attacks from three aspects, namely, system vulnerability, attack detection and system protection.

Starting by the motivation of the work, in Chapter 3 we propose a hybrid filter algorithm to deal with the state estimation problem for power systems by taking into account the impact from the PMUs. Our aim is to include PMU measurements when designing the dynamic state estimators for power systems with traditional measurements. Also, as data dropouts inevitably occur in the transmission channels of traditional measurements from the meters to the control centre, the missing measurement phenomenon is also tackled in the state estimator design. In the framework of extended Kalman filter (EKF) algorithm, the PMU measurements are treated as inequality constraints on the states with the aid of the statistical criterion, and then the addressed state estimation problem becomes a constrained optimization one based on the probability-maximization method. The resulting constrained optimization problem is then solved by using the particle swarm optimization (PSO) algorithm together with the penalty function approach. The proposed algorithm is applied to estimate the states of the power systems with both traditional and PMU measurements in the presence of probabilistic data missing phenomenon. Extensive simulations are carried out on the IEEE 14-bus test system and it is shown that the proposed algorithm gives much improved estimation performances over the traditional EKF method.

Chapter 4 begin with the measurement model in which the RTUs and the PMUs are subject to quantizations described by a logarithmic quantizer. Then a recursive filter algorithm is developed to deal with the state estimation problem for power systems with quantized nonlinear measurements. Attention is focused on the design of a recursive filter such that, in the simultaneous presence of nonlinear measurements and quantization effects, an upper bound for the estimation error covariance is guaranteed and subsequently minimized. Instead of using the traditional approximation methods in nonlinear estimation that simply ignore the linearisation errors, we treat both the linearisation and quantization errors as norm-bounded uncertainties in the algorithm development so as to improve the performance of the estimator. For the power system with such kind of introduced uncertainties, a filter is designed in the framework of robust recursive estimation, and the developed filter algorithm is tested on the IEEE benchmark power system to demonstrate its effectiveness.

In Chapter 5, We try to design a new state estimation method to handle the networked-induced incomplete information, and find that the event-based estimation could be a promising approach to maintaining the estimation performance under limited communication resources. In the event-based strategy, a sensor is triggered to send the measurement data only if some events occur, thereby consuming less communication bandwidth than the sensor in the time-based one. Considering the unknown input (such as abrupt changes in energy supply and consumption) in power grids, we design an event-based recursive input and state estimator such that the estimation error covariances have guaranteed upper bounds at all times. To this end, the event indicator variable is introduced to reflect the triggering information and reduce the conservatism in the analysis of estimation performance. Moreover, upper bounds of the estimation error covariances are obtained recursively and then reduced by choosing proper scalar parameters and estimator gains according to a given procedure.

In Chapter 6, we consider the security issues in state estimation of power grids, where the adversary can inject false data into the communication channels between sensors and a remote estimator. For the case that the adversary can compromise all communication channels, a necessary and sufficient condition is derived under which the estimation error caused by the attacks is unbounded all the time. For the case that the adversary can only compromise a part of the communication channels, a sufficient condition ensuring the security is derived as well. Moreover, a criterion on protecting a sufficient number of channels such that the estimation error is kept bounded under FDI attacks has been proposed. A simulation example is proposed as well to demonstrate the usefulness of the developed results and algorithms.

In Chapter 7, we summarise the work presented in this thesis and discuss several directions of future research.

Chapter 2

Background

In this chapter, we aim to review the development of state estimation for power grids from a new horizon, namely, the unconventional measurements. The examples of unconventional measurements include, but are not limited to, mixed measurements, delayed measurements, missing measurements and measurements tampered with by FDI attacks. We endeavour to capture all important results despite the rapid growth of the literature. Due to the rapid growth of the literature, we cannot review all but the most relevant to our study. This chapter is organised as follows. In Section 2.1, the measurement model is introduced and typical estimation methods used for the problem of power system state estimation (PSSE) are discussed. The results on PSSE with mixed measurements are reviewed in Section 2.2. Section 2.3 provides a thorough summary of the research works on state estimation for power grids with three kinds of incomplete information: delayed, asynchronous and missing measurements. Finally relevant literature on the cyber-security issue of PSSE is included in Section 2.4.

2.1 Preliminaries on Power System State Estimation

The PSSE program has been a key module in the EMS of power grids. As the core of the PSSE program, the state estimator processes the measurement data and generates the state estimate of the entire power grid that will be needed in other system monitoring, control and planning tasks such as bad data detection and optimal power flow. As application-specific software, the operation of PSSE program relies on the communication backbone in power grids, i.e., the SCADA system. The SCADA system collects measurements from RTUs and then sends them to the control centres. Fig. 2.1 shows the relation of the PSSE module with the EMS/SCADA system.

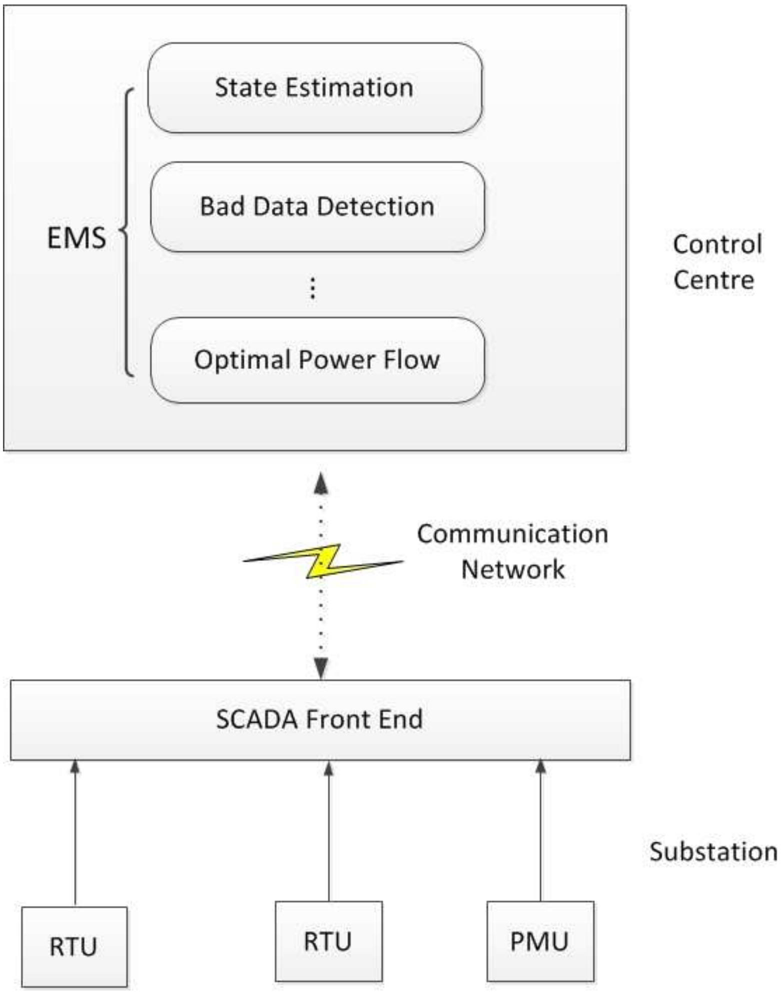


Fig. 2.1 The PSSE module in an EMS/SCADA system

In the following, we first briefly introduce the measurement model, then summarize two different kinds of state estimation schemes widely used in the control centres, and finally describe the bad data detection module in the EMS.

2.1.1 Measurement Model

Two basic elements in power grids are the bus and the line. A bus (line), also called as a node (branch) in some literature, stands for a generator or a load substation (a transmission or distribution line connected two buses). Let us first introduce the basic two-buses π model so as to build the measurement model for a complex large-scale power grid.

In Fig. 2.2, two buses (s and t) are connected by one line, where $Y_{st} := g_{st} + jb_{st}$ is the series admittance of the line connecting buses s and t, and $Y_{st}^0 := g_{st}^0 + jb_{st}^0$ is the half shunt admittance of the line connecting bus s and t. Based on Kirchoff's laws, the following equation is obtained:

$$\overrightarrow{I}_{st} = (g_{st} + jb_{st})(\overrightarrow{V}_s - \overrightarrow{V}_t) + (g_{st}^0 + jb_{st}^0)\overrightarrow{V}_s \tag{2.1}$$

where $\overrightarrow{V}_s$ is the complex voltage at bus s and $\overrightarrow{I}_{st}$ is the current flowing from bus s to t. Using the π model, similar equations can be derived for complex power grids with more than two nodes.

Electrical quantities (e.g. bus voltage, line current and power flow) are all complex-valued in alternative current (AC) power grids, and hence can be represented in either the polar or the rectangular coordinates equivalently. For simplicity, we introduce power grids in the rectangular coordinate as default in this chapter. For a power grid, the voltages at all buses are usually chosen as the system states. In an N-bus network, the state vector has the form $x = \left[x_{r,1}, x_{r,2}, \cdots, x_{r,N}, x_{i,1}, x_{i,2}, \cdots, x_{i,N}\right]^T$, where $x_{r,l}$ and $x_{i,l}$ represent the real and imaginary voltage of the lth bus, respectively. In practice, the system states usually cannot be directly measured. Instead, they need to be estimated using possibly noisy and incomplete measurements.

At present, both traditional instruments and new instrument of PMU have been installed in power grids. Due to their inherently distinct characteristics, the traditional instrument and PMUs are able to measure different electrical quantities in power grids, see the following two subsections for more details.

Traditional Measurements

The readings of traditional meters in power grids are collected via RTUs, and then sent to the control centre through communication networks in the SCADA system. Typically, the bus

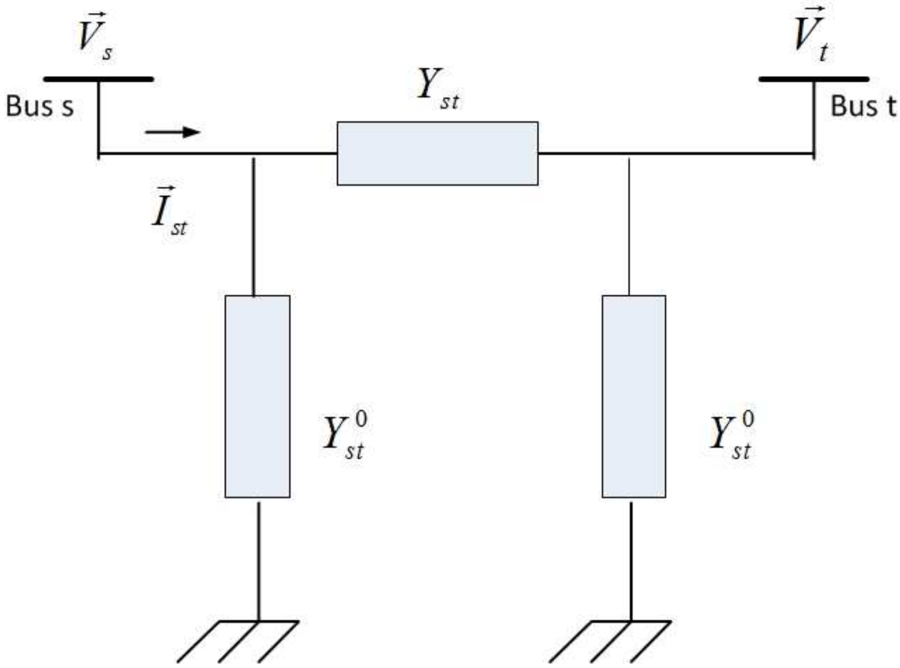


Fig. 2.2 The π model

voltage magnitude, the real and reactive bus power injections, and the real and reactive line power flows are measured. Based on the π model and (2.1), all measurement equations can be represented as follows (for the purpose of simplicity, the time instant k is omitted):

$$\begin{aligned}
V_s &= \sqrt{x_{r,s}^2 + x_{i,s}^2} \\
P_s &= x_{r,s} \sum_{j=1}^{N} (G_{sj} x_{r,j} - B_{sj} x_{i,j}) + x_{i,s} \sum_{j=1}^{N} (G_{sj} x_{i,j} + B_{sj} x_{r,j}) \\
Q_s &= x_{i,s} \sum_{j=1}^{N} (G_{sj} x_{r,j} - B_{sj} x_{i,j}) - x_{r,s} \sum_{j=1}^{N} (G_{sj} x_{i,j} + B_{sj} x_{r,j}) \\
P_{st} &= (x_{r,s}^2 + x_{i,s}^2)(g_{st}^0 + g_{st}) - x_{r,s} x_{r,t} g_{st} - x_{i,s} x_{i,t} g_{st} - x_{i,s} x_{r,t} b_{st} + x_{r,s} x_{i,t} b_{st} \\
Q_{st} &= -(x_{r,s}^2 + x_{i,s}^2)(b_{st}^0 + b_{st}) - x_{i,s} x_{r,t} g_{st} + x_{r,s} x_{i,t} g_{st} + x_{r,s} x_{r,t} b_{st} + x_{i,s} x_{i,t} b_{st}
\end{aligned} \tag{2.2}$$

where V_s, P_s, Q_s, P_{st} and Q_{st} are the voltage magnitude, the real and reactive bus power injections at bus s, and the real and reactive line power flows from bus s to t, respectively.

With consideration of the measurement noise, the traditional measurement can be written in the following compact form:

$$y_1(k) = h\big(x(k)\big) + v_1(k) \tag{2.3}$$

where $y_1(k)$ is the traditional measurement vector, $x(k)$ is the system state and $v_1(k)$ is a zero-mean Gaussian noise. Note that the mapping function $h(x)$ is nonlinear in general.

PMU Measurements

Compared with traditional measuring meters, PMUs can measure the system with a much higher frequency. Typically, the sampling rate of PMUs is 30 measurements every second while that of traditional meters is only once every several seconds. Moreover, all PMU measurements are synchronized and time-stamped by the global position systems (GPS). As PMUs are able to provide more accurate and timely measurements than traditional meters, they have been increasingly deployed in power grids in the past few years. For instance, it has been reported that, more than 1000 PMUs will be installed in North America by 2019 covering all 200 kV and above substations [177].

A PMU measures not only the voltage phasor of the bus where it is installed but also the current flows of the lines connecting to the bus. Similar to the traditional measurements, the PMU measurement equations can also be derived using the π model and (2.1) as follow:

$$\begin{aligned} &V_{r,s} = x_{r,s}, \quad V_{i,s} = x_{i,s}, \\ &I_{r,st} = (x_{r,s} - x_{r,t})g_{st} - (x_{i,s} - x_{i,t})b_{st} + x_{r,s}g_{st}^0 - x_{i,s}b_{st}^0, \\ &I_{i,st} = (x_{i,s} - x_{i,t})g_{st} + (x_{r,s} - x_{r,t})b_{st} + x_{i,s}g_{st}^0 + x_{r,s}b_{st}^0 \end{aligned} \tag{2.4}$$

where $V_{r,s}$ and $V_{i,s}$ are respectively the real and imaginary parts of the voltage at bus s, and $I_{r,st}$ and $I_{i,st}$ are respectively the real and imaginary parts of the current flow from bus s to t.

With the state variables and measured variables in the rectangular form, a linear PMU measurement model is obtained as follows:

$$y_2(k) = H_p x(k) + v_2(k) \tag{2.5}$$

where $y_2(k)$ is the PMU measurement and $v_2(k)$ is the PMU measurement noise.

A hot topic of research that has stirred much attention is how to make the most of PMUs in power grids [55]. On one hand, to ensure the PMU measurements compatible with existing software in power systems, the IEEE Standard C37.118-2005 on PMUs has been proposed [114]. On the other hand, to quantify the quality of PMUs, the data reliability of PMU measurements has been quantitatively analysed in [166, 82, 28]. For more details of PMU technology development, we refer the readers to the recent survey chapter [5].

2.1.2 Estimation Methods

Since the initial research conducted by F. C. Schweppe in 1970 [136], significant contributions have been made to the development in PSSE techniques. Depending on the time evolution of the estimation method, PSSE can be classified into two different paradigms: static state estimation (SSE) and dynamic state estimation (DSE). Below we provide a brief overview on the formulation, methods and development in these two PSSE paradigms.

Static State Estimation

The traditional state estimator works in a static setting where the one-scan measurement is processed to estimate the system states. In the static state estimator, the weighted least square (WLS) method is typically utilized. In particular, given the RTU measurements, the estimate of state $x(k)$ is obtained through finding

$$\hat{x}(k) = \arg\min_{x(k)} \big(y_1(k) - h(x(k))\big)^T W^{-1} \big(y_1(k) - h(x(k))\big),$$

where the weighting matrix W is commonly set as the covariance matrix of the measurement noise. Noting that the measurement model (2.3) is nonlinear, the solution of $\hat{x}(k)$ is usually obtained using the Gaussian-Newton algorithm or its variants in an iterative fashion. At each iteration, (2.3) is first linearized around the obtained state estimate and then the linear least square method is applied to the linearised model. The iterative procedures are repeated until the prescribed terminating condition has been satisfied.

The WLS method has the features of fast convergence and easy implementation, which give rise to the popularity of the static estimation approach in control centres around the world. This method, however, has certain limitations with two examples given as follows: 1) there is no guarantee for the convergence to the global or even a local minimum; and 2) the performance of the algorithm is sensitive to the initial guess. To overcome the identified weakness in WLS methods, several other improved methods have been proposed, see, the fast-decoupled WLS method [52, 67] and the robust WLS method [80, 30, 185], to name just a few. In the literature, there have been a number of survey chapters on the SSE methods. For example, the developments in the early two decades up to the year 1990 have been summarized in [19, 169], and the advances in the subsequent one decade from 1990 to 2000 have been reviewed in [122]. In addition, two textbooks [121, 2] have provided more details on SSE techniques in power grids.

Dynamic State Estimation

In the traditional SSE paradigm, to obtain the state estimate at current instant, only the new set of measurement is processed by the estimator, and the previous state estimate is not considered. In such a way, the evolution of the system state over consecutive measurement instants is ignored. Different from the SSE scheme, the DSE one utilizes the information of system dynamics in power grids. The advantage of the DSE scheme lies in its ability to provide a prediction database, which could be adopted as a set of pseudo-measurements in case of missing data or meter outages in the power grids.

There are three main steps in the DSE scheme, i.e., system modelling, state prediction and state estimation. The aim of the first step is to model the dynamical behaviour of power grids between consecutive measurement instants. When considering the PSSE problem, it is assumed that the power system operates normally in the quasi-steady regime, which is in accordance to the slow dynamics in load variations and generation changes. Various state-space power grid models have been developed in the literature. The first widely used model has been proposed by Debs and Larson [37], which is described by the following random-walk process:

$$x(k+1) = x(k) + w(k) \tag{2.6}$$

where $w(k)$ is assumed to be a zero mean Gaussian noise to represent changes of the states between consecutive instant. Several similar models were proposed as results from early attempts made in the 1970s. One common drawback in these models is that they are over-simplified as no time evolution is explicitly characterized in these models, and this might lead to poor performance in the next two steps of state prediction and state estimation. To overcome such a drawback, a more appropriate model has been put forward in [34] as follows:

$$x(k+1) = A(k)x(k) + u(k) + w(k) \tag{2.7}$$

where the diagonal matrix $A(k)$ represents how fast the state transition is, $u(k)$ is associated with the trend of the state trajectory and $w(k)$ is a zero-mean Gaussian noise. The values of $A(k)$ and $u(k)$ can be obtained by on-line or off-line methods. Different techniques have been proposed and successfully applied to estimate the parameters in the system model (2.7), including Kalman filtering, exponential smoothing and artificial neural network approaches.

Once the accurate system model is obtained, it is ready to design the dynamic state estimator. For power grids with nonlinear traditional measurements, the dynamic state estimator based on the extended Kalman filter (EKF) has been widely adopted [99, 133, 53]. In such a kind of estimator, based on the system model (2.7) and measurement model (2.3), the two steps of state prediction and state estimation are accomplished as follows:

$$\begin{aligned}\bar{x}(k+1) &= A(k)\hat{x}(k) + u(k)\\ \hat{x}(k+1) &= \bar{x}(k+1) + K(k+1)[y(k+1) - h(\bar{x}(k+1))]\end{aligned} \tag{2.8}$$

where $\bar{x}(k)$ is the state prediction at time instant k, $\hat{x}(k)$ is the state estimation at instant k, and $K(k)$ is the filter gain to be determined at time instant k. Denoting $H(k) = \frac{\partial h(x(k))}{\partial x(k)} \mid_{x(k)=\bar{x}(k)}$, the filtering gain is obtained recursively as follows:

$$\begin{aligned}K(k) &= P(k)H^T(k)R^{-1}\\ P(k) &= [H^T(k)R^{-1}H(k) + M^{-1}(k)]^{-1}\\ M(k) &= A(k)P(k-1)A^T(k) + W.\end{aligned} \tag{2.9}$$

Other alternative filtering algorithms to EKF for PSSE have also been developed, including the iterative Kalman filter [18], the unscented Kalman filter [161, 159], the particle filter [45], the robust filter [140], the disturbance filter [105, 53], the adaptive filter [178, 179] and the filter for joint estimation of state and parameter [15, 16]. Moreover, to speed up the estimation algorithm applied in large-scale power grids, parallel EKF-based dynamic state estimator has been proposed in [85–87]. In addition, computational intelligence tools (e.g. neural networks, evolutionary algorithm and fuzzy logic) have also been integrated into the DSE algorithms in [126, 147, 104]. The readers are referred to the survey papers [133, 141, 20, 21] for more details on DSE methods.

While the traditional measurements are modelled by nonlinear equations in (2.3), the PMU measurement model is linear. As such, if sufficient numbers of PMUs are installed in the power grids, the traditional Kalman filter (rather than the EKF) is needed. The performance of DSE using PMU measurements has been evaluated in [135, 88]. Different from the EKF, the Kalman filter has the desirable properties of convergence in estimation error and low computational complexity. Though the SSE and DSE methods are summarized separately above, a hybrid filter combining the static WLS and the dynamic UKF has been developed to exploit the advantages of both methods [131].

2.1.3 Bad Data Detection

In EMS, there is another process closely related to the PSSE, namely, bad data detection (BDD). On one hand, the state estimate is a prerequisite for the BDD to identify any gross errors in the measurement set. On the other hand, when the bad measurements are eliminated by the detector, the estimator can yield more accurate state estimates. Depending on static or dynamic flavours of the state estimation schemes adopted, different algorithms have been used for BDD. Nevertheless, all the algorithms are designed based on the following residual:

$$r(k) = \begin{cases} y_1(k) - h(\hat{x}(k)) & \text{traditional measurements,} \\ y_2(k) - H_p\hat{x}(k) & \text{PMU measurements,} \end{cases} \tag{2.10}$$

where the residual $r(k)$ is equal to the difference between the actual measurements and the estimated measurements.

When there are no abnormal measurements, the norm of residual $r(k)$ should follow a χ^2 distribution with known covariance and, accordingly, the χ^2 test has been widely used for bad data detection [2]. Specifically, if the condition $\|r(k)\| \leq \sigma$ is violated, an alarm will be triggered by the detector, where σ is a scalar which can be determined according to the statistical information of the residual $r(k)$.

2.2 Mixed Measurements

Recently, more advanced synchronized phasor measurement technologies have been applied in power systems, which makes it possible to measure the system states in a more accurate and timely way. Unfortunately, for economic reasons, it is not affordable to replace all the RTUs with PMUs in the foreseeable future [78]. In other words, only partial states could be measured directly by PMUs and the rest would have to be estimated by using the conventional RTUs. As such, an emerging yet promising research issue is how to integrate PMU measurements into existing SE algorithms, which is depicted in fig. 2.3.

There are several challenges that would need to be overcome in order to make it practically possible to develop PSSE methods in the presence of mixed (RTU and PMU) measurements. The challenges are outlined below:

- *High computing burden:* Due to computational limitations, most existing estimators that process traditional measurements alone (without PMU measurements) in control centre run every few minutes even though the sampling time of traditional measurements is less than one minute [122]. The inclusion of PMU measurements results in the measurement vector with an even-higher dimension and thus aggravates the computational burden greatly.

- *Big Data:* PMU measurements are obtained at a much higher (typically two order of magnitude higher) sampling rate than traditional measurements. The huge amount of measurement data put great burden on the communication networks with limited bandwidth in power grids [9]. As discussed in [180], the communication constraints

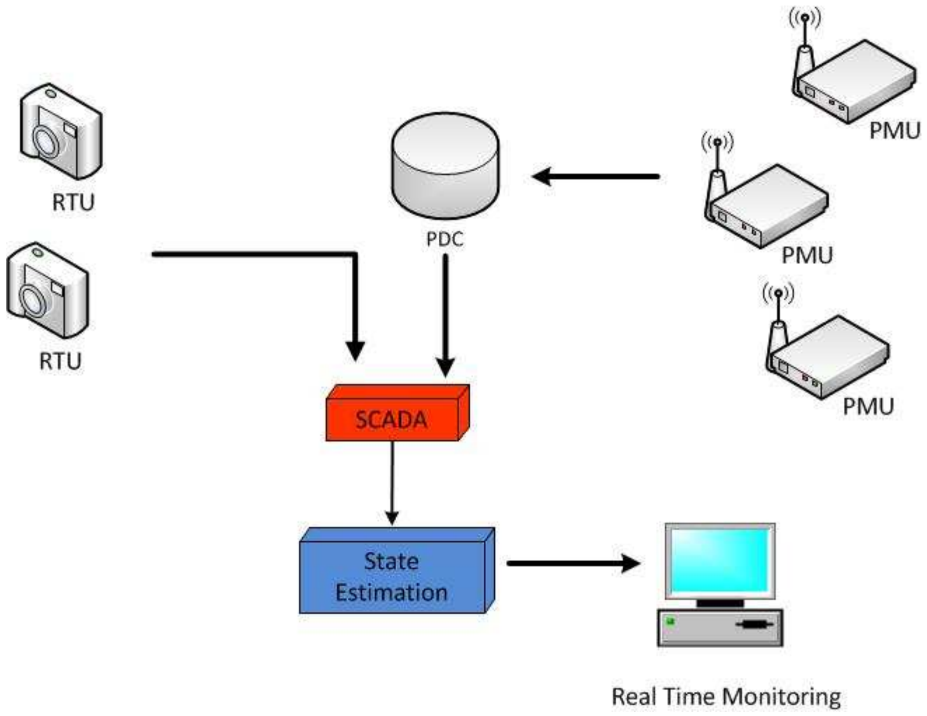


Fig. 2.3 The mixed measurements

have inevitably led to network-induced phenomena such as random communication delays, data quantization and missing measurements.

- *Numerical instability:* Since PMU measurements are significantly more accurate than traditional measurements, integration of these two kinds of measurement data often leads to the ill-condition problem for the measurement noise covariance matrices. As is known, numerical computation problem may be caused by the ill-conditioned matrices in the process of state estimation.

2.2.1 Methodologies

In this subsection, we review the state estimation methods for power grids with mixed measurements according to the following orders: first the static estimation methods, then the dynamic counterparts, and finally a hardware enhanced method through buffering PMU measurements.

Generally speaking, two static estimation schemes have been proposed . One scheme is to process both kinds of measurements simultaneously after transforming them into a common coordinate (either rectangular or polar) [188, 14, 94, 189, 175]. The other one is actually a two-stage scheme: a) estimated states are obtained by employing RTU measurements and

PMU measurements, respectively, and b) such estimates are fused based on the estimation fusion formula [143, 60, 59].

Several different techniques has been introduced to design DSE methods with mixed measurements [7, 26, 27, 42, 103, 137]. For example, the mixed-integer programming formulation has been proposed to decide whether the predicted state at buses without PMUs measurements are utilized or not [7, 26, 27], and a dynamic state estimator has been designed based on the relevance vector machine algorithm in [103], where the auto-encoder technique has been used to further reduce the data dimensionality in mixed measurement. In addition, based on the multi-agents model, a software module for DSE has been built to scan and process RTU and PMU measurements in parallel in [137].

Different from the aforementioned two methods that focus on developing estimation algorithms with mixed measurements, the third method tries to cope with the mixed measurement problem through improving the hardware design. Considering different sampling rates of the traditional and PMU measurements, a memory buffer of PMU measurements has been recommended to be installed in the state estimator. In [181], the problem that how buffering the phasor measurements can improve the state estimate has been investigated. Furthermore, the optimal buffer design and the use of the phasor measurements from that buffer have been addressed in [125].

2.3 Incomplete Information

The modern power grid is a typical complex networked system, where the widely geographically separated components such as generation plants and substations are interconnected by communication cables. The underlying communication networks in SCADA system is depicted in Fig. 2.4, from which we can find that the communication links in SCADA systems have different forms including telephone, optical fibre, satellite, microwaves, etc. Undoubtedly, it is expected that the communication network is capable of providing secure and reliable data transmission from meters to the control centre. Unfortunately, though networking technologies and systems have been greatly enhanced, network-induced phenomena still happen in practical power grids. In this chapter, the information with respect to the network-induced phenomena is customarily referred to as the incomplete information [40, 74].

The incomplete information under consideration mainly includes delayed, asynchronous and missing measurements, whose mathematical models are listed in Table 2.1, where $y(k)$ is the measurements received by the estimator, and $h(x(k))$ and $v(k)$ represents the ideal measurement and the measurement noise, respectively. The development on PSSE with

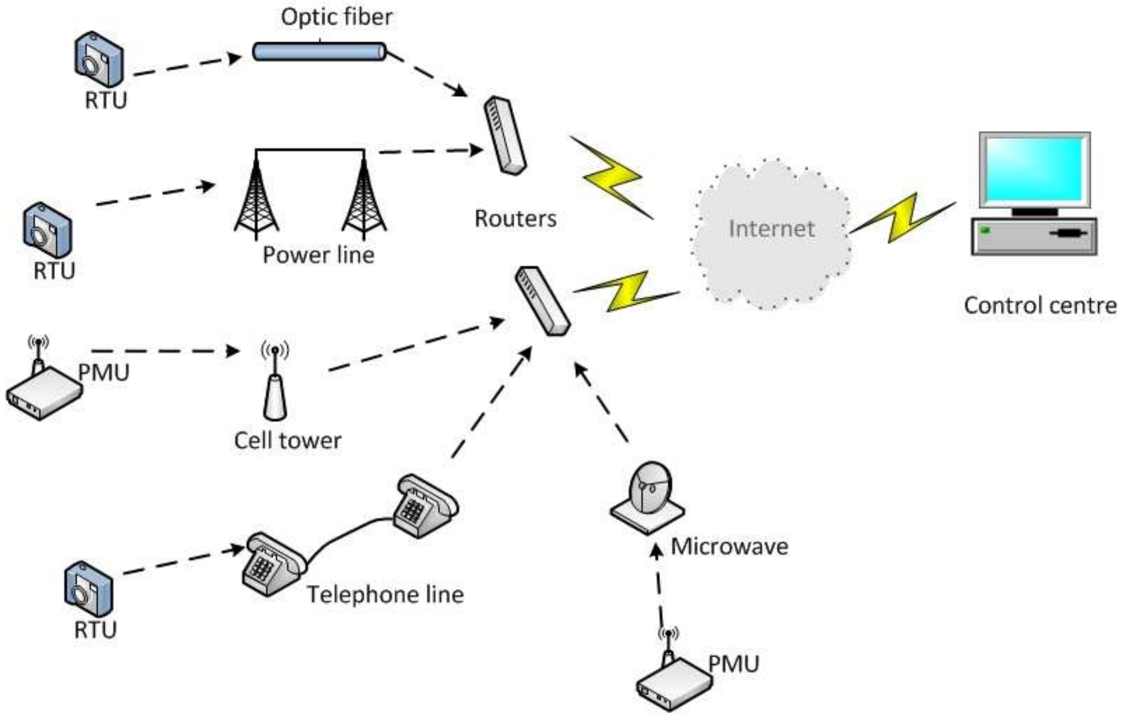


Fig. 2.4 Typical communication links in SCADA systems

Table 2.1 Mathematical models of incomplete information in measurements

Types	Mathematical models
Delayed measurements	$y(k) = \gamma(k)h(x(k)) + (1-\gamma(k))h(x(k-1)) + \nu(k)$, where $\gamma(k)$ is a stochastic variable tacking value on 0 or 1.
Asynchronous measurements	$y(k) = h\big(x(t(k))\big) + \nu(t(k))$, where $t(k) \leq k < t(k+1)$.
Missing measurements	$y(k) = \gamma(k)h(x(k)) + \nu(k)$, where $\gamma(k)$ is a stochastic variable tacking value on 0 or 1.

incomplete information will be reviewed in great detail. In particular, we will present the sources of the three kinds of incomplete information, analyse their impacts on the estimation performance, and review both the centralized and decentralized state estimation methods developed in the literature.

Delayed and Asynchronous Measurements

When considering the state estimation problem in power grids, it is explicitly assumed that the system state remains unchanged during the time interval among two successive measurement instants. In fact, this assumption may fail sometimes due to the transmission delay and time skewness among measurements from different areas. As the communication networks in power grids span wide geographic areas, the long-distance communication between different components would inevitably lead to network transmission delay. For example, non-negligible transmission delays have been observed in the communication networks of practical power grids [112]. On the other hand, time-skewness in traditional measurements, which can be viewed as a specific kind of time delays, is a common phenomenon because the measurement data from different RTUs are not synchronized. Though the asynchronous measurements can be easily removed if all traditional measuring meters are replaced by the GPS-synchronized PMUs, it cannot be realized in near future due to resource limitations.

Some researchers have observed the phenomenon of delayed measurements in experimental or practical power grids. Using the designed Ethernet-based communication platform for power systems, the transmission delays have been measured experimentally [23], and the statistical characteristics of transmission delay in some practical power grids have been obtained through analysis of real data [112]. The delayed measurements could largely affect the power systems in different aspects such as system stability [116] and power market [127]. Nevertheless, in this chapter, we focus on the effect of delay measurements on PSSE exclusively.

Missing Measurements

In power grids, the phenomenon of missing measurements occurs quite often when there are malfunction or faults in the meters and, traditionally, this issue has been investigated in the research area of fault detection for power grids. Recently, the introduction of communication networks in power grids has also stimulated the studies on missing measurements. The measurement data may be transmitted unsuccessfully due to unintentional conditions such as network traffic congestion and limited communication bandwidth. On the other hand, transmission failures can also be caused by intentional cyber-attacks. For instance, one particular type of attack called denial of service (DoS) attack can block the data transmission in communication networks. Under DoS attacks, the control centre cannot receive measurement data from certain meters. In addition, when arriving at the control centre with excessive long transmission delay, the data are usually discarded and can therefore be viewed as missing. If not adequately taken into account, the phenomenon of missing measurements could degrade the performance of the state estimator or even cause divergent estimation errors.

Some Remarks

In most of the early literature on PSSE, the perfect communication scenarios have been assumed. Recently, researchers have observed that the measurement data may not always arrive at control centre in a perfect condition. Moreover, without consideration of the incomplete information, traditional state estimators (both the static and the dynamic ones) could perform poorly especially in a networked environment. Accordingly, new PSSE methods have been proposed and applied in power grids to deal with the incomplete information in measurements.

2.3.1 Centralized State Estimation Scheme

Traditionally, the state estimator works in a centralized manner in which all remote measurements are sent to a unique control centre. In the SSE paradigm, if the measurements are delayed or lost, the static estimator may fail completely because, with fewer measurements than unknown states, the measurement equation (2.3) or (2.5) becomes undetermined. Unfortunately, in this situation, little can be done to improve the SSE scheme except viewing the delayed and missing measurements as a kind of bad data. On the contrary, in the DSE paradigm, quite a lot improved state estimation algorithms have been proposed for the power grid with incomplete information.

Delayed and Asynchronous Measurements

Several models have been used to characterize the time delays [163, 23, 152, 112, 183, 151, 63]. Of course, it would be convenient to tackle the state estimation problem by assuming that the delay is constant. Unfortunately, it is often not the case in practice. Most protocols used in the communication network of power grids (e.g. TCP/IP) do introduce time-varying delays. As such, in [163], a bounded but time-varying delay model has been proposed to capture the network-induced constraints in wide-area measurement systems. In [23], a stochastic delay that exists in power systems has been experimentally measured from an Ethernet-based communication platform. Moreover, the stochastic communication delay distribution in China southern power grids has been reported in [112]. In addition, a straightforward calculation method and model of communication delays in power system have been proposed in [151].

Based on the statistical model of delayed measurements, different state estimators have been developed. For example, a recursive estimator under one time-step random communication delay has been designed in [152]. To model the one-time step random delay, a binary switching sequence has been used which can be viewed as a Bernoulli distributed white sequence taking values of 0 and 1. In [63], a DSE algorithm has been proposed to deal with time delays that are more than one step, where the time-forward kriging model has been used to forecast the missing load data from the available measurement data. In [152, 63], it has been shown that the designed estimators exploiting statistical information of the delay perform much better than the traditional estimator without considering the delay information.

On the other hand, the issue of time skewness caused by asynchronous measurements has been taken into account in the DSE design [4, 173, 182]. Specifically, based on the credibility of each available measurement, a method has been proposed to appropriately adjust the variance of the measurement noise from different devices [4], and such an idea has been extended to calibrate the PMU measurement data received by the estimator [182]. Moreover, the imperfect synchronizations in PMU measurements have been estimated and then the estimation information has been utilized is the subsequent step of estimator design [173]. It has been shown that the proposed estimator outperforms the traditional ones.

Missing Measurements

As discussed before, the phenomenon of missing measurements may happen due to either hardware faults or communication failures. Accordingly, two different kinds of methods have been used to deal with the state estimation problems for power grids with the missing measurements.

- For the first method, to make the system resilient to sensor faults, different strategies of PMUs placement in power grids have been put forward in [6, 129, 43]. For instance, in [6], by assuming the occurrence of random sensor faults, the optimal PMU placement solution has been derived to maximize the probability of topological observability. The sensor failure problems have been considered in a deterministic way in [129, 43] whose main idea is to use backups of measurements (i.e., measurements at previous instants) to replace the lost measurements.

- The other method addressing the missing measurements caused by communication failures shares similar ideas used to tackle delayed measurements. That is, the statistics of the random missing measurements has to be utilized. The occurrence of missing measurements has been modelled as a stochastic variable satisfying the Bernoulli random binary distribution [76, 154, 155, 38]. Furthermore, the off-line state estimation algorithm has been developed in [76] where, instead of the exact occurrences of missing measurements, only the information about the statistical law (i.e., first- and second-order moments) of the stochastic variable are used for filter design. In contrast, the state estimator gains are computed on-line according to the real-time situation whether a packet is lost in [154, 155]. Moreover, in[38] the impact of dropped packets on stability of the estimator has been investigated.

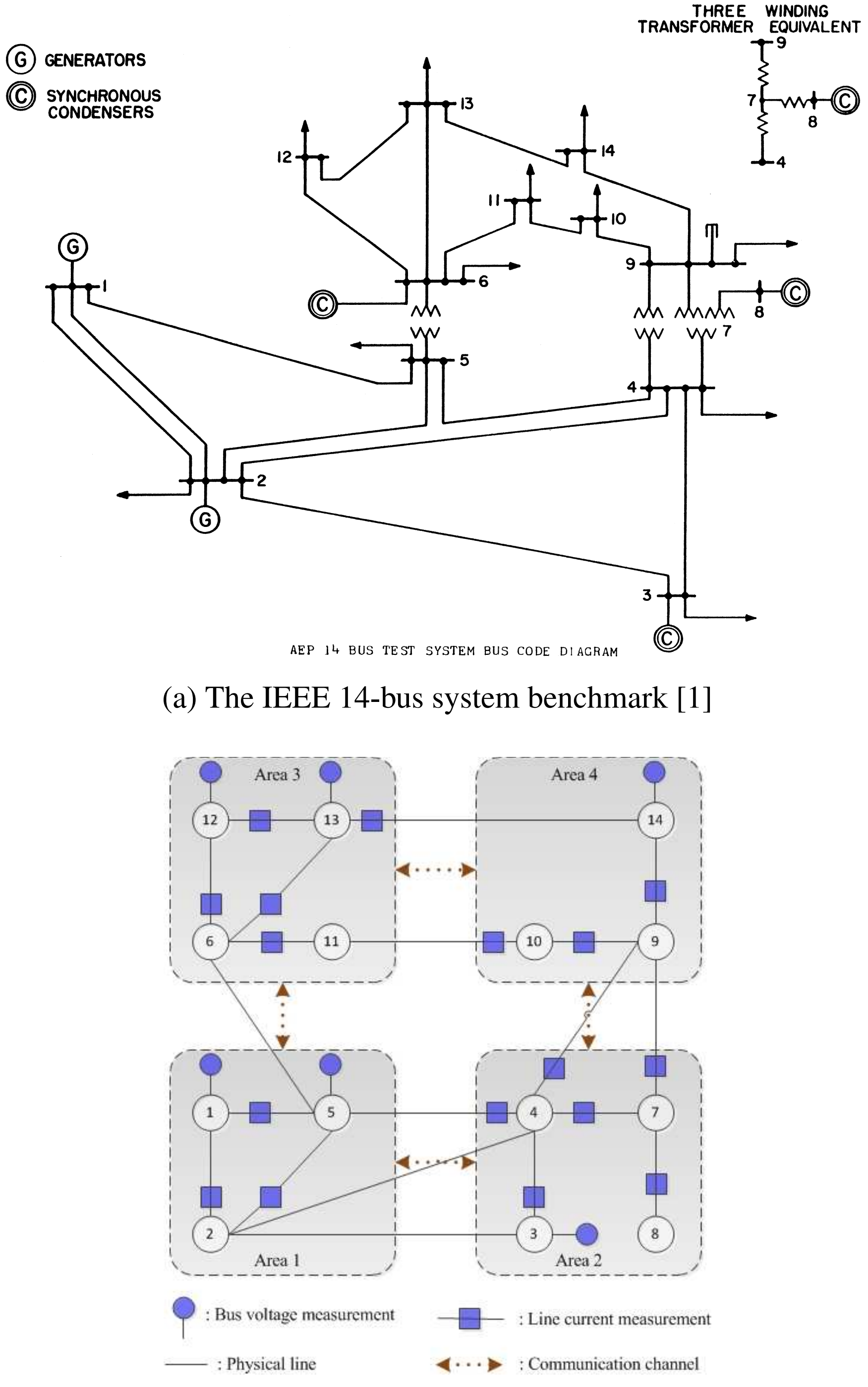
In [162, 24], both the time delays and missing measurements have been simultaneously considered. Specifically, in [162], a method using the GPS synchronized sampling technologies has been proposed to compensate both time delays and missing measurements. In [24], an integrated software package has been developed for the power grids simulation wherein the delay and the packet loss introduced by the communication systems have been taken into account.

2.3.2 Decentralized State Estimation Scheme

In the above subsection, we have reviewed the centralized state estimation methods for power grids with incomplete information. All these methods are developed based on the basic models described in Section 2.2. To deal with the incomplete information issue, another research line is to find a solution such that the phenomena of incomplete information is as less likely to happen as possible. The decentralized state estimation scheme seems to be a promising solution since it removes the necessity of a fast and reliable communication network in a power grid.

The structure in decentralized state estimation schemes has evolved from the hierarchical one to the completely distributed one. In both structures, the overall power grid is split into several geographically different areas that are electrically connected via tie-lines. Every area comprises a) a local area control centre where the local state estimator is maintained, and b) a subset of buses which are measured by meters. Due to the multi-area feature, the decentralized state estimation is also called multi-area state estimation in some papers on PSSE [187, 62]. In the hierarchical state estimation scheme, all the local area centres first perform local area state estimation and then send the local state estimates to the unique global control centre where the state estimate of the overall power grid is obtained. In this scheme, the local state estimators located remotely communicate only with the unique global one. Since research focuses in decentralized state estimation for power grids have been recently shifted from the hierarchical scheme to the completely distributed one, in this chapter, we only review recent advance in the latter scheme in detail. For the hierarchical state estimation scheme, we refer the readers to the review papers [33, 61].

Different from the hierarchical scheme where all local state estimates are directly sent to a global centre, for the distributed approach, such a global centre does not exist and, instead, every state estimator exchanges information with the estimators in its neighbouring areas. The distributed estimation approach only involves a) communication between every meter and its local estimator; and b) limited information exchange between estimators in neighbouring areas. Therefore, the heavy communication burden can be alleviated as compared to the centralized approach. A specific structure of the decentralized state estimator in the IEEE 14-bus system is depicted in Fig. 2.5.



(a) The IEEE 14-bus system benchmark [1]

(b) Decentralized estimation structure in the IEEE 14-bus system

Fig. 2.5 The IEEE 14-bus system: (a) Conventional system; (b) Decentralized estimation structure

In the following, we summarize the distributed state estimation methods in two different frameworks: the distributed static state estimation (DSSE) and the distributed dynamic state estimation (DDSE).

- Typical works in the first framework include [170, 102, 89, 81, 175, 42]. In [170], a fully distributed static estimation algorithm has been proposed where, through iterative information exchanges with estimators in neighbouring areas, all local estimators can achieve an unbiased state estimate of the entire power grid. In [102], by integrating the network gossiping algorithm into the WLS state estimation algorithm, the distributed static state estimators has worked in an adaptive re-weighted manner. In [89], the alternating direction method of multipliers (ADMM) technique has been utilized to design a distributed and robust state estimator. In addition, the DSSE methods using both PMU and traditional measurements have been presented in [81, 175, 42].

- In the DDSE framework, different estimation methods have been put forward in [145, 29, 128, 101, 132, 68]. Specifically, in [29], a factor graph has been used to model a power grid and a DDSE algorithm has been proposed based on the graphical model. As for the local estimator design, the unscented Kalman filter (UKF) has been used to process PMU measurements at each control centre in [145]. Using Gaussian approximation and stochastic linearisation techniques, the distributed point-based Gaussian approximation filters has been developed in [68]. Moreover, to improve the estimation performance, the local information exchanges of neighbouring areas based on the consensus algorithm has been introduced in [128]. In addition, a distributed Kalman filter has been developed to compensate for the information loss in the multi-rate large-scale power grids in[132], and two short survey papers on recent advances of DDSE have been given in [130, 101].

2.4 False Data Injection Attacks

To monitor and control the power grids with increasing complexities in real time, communication networks have been widely used in the SCADA system. However, due to the strong coupling between communication networks (cyber layer) and electrical networks (physical layer), the power grids are becoming vulnerable to cyber-attacks. Of all the modules in EMS, the PSSE module seems to have the highest possibility to be attacked because, through modifying the state estimation successfully, the attackers can mislead other operation decisions of the power grids and even manipulate the electric market [171].

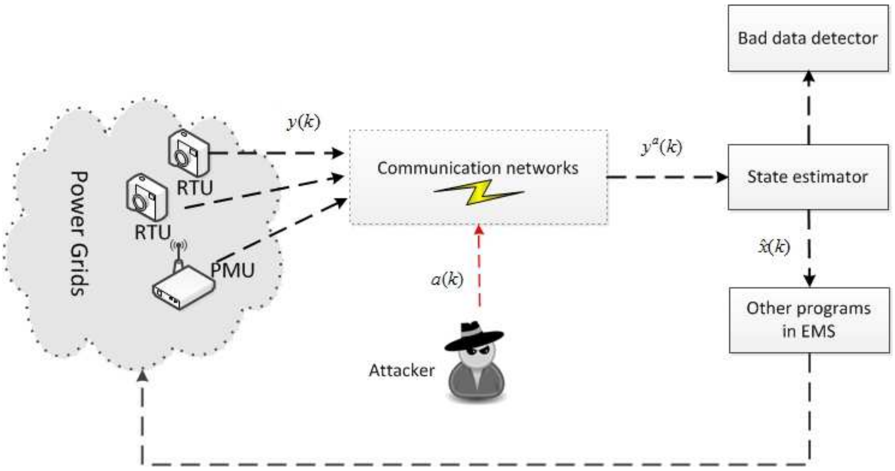


Fig. 2.6 System structure of cyber-attacks in PSSE

2.4.1 Attack Model

There are several different kinds of cyber-attacks, among which DoS attacks and false data injection (FDI) attacks are two most common ones as far as the power grids are concerned. Different from DoS attacks, FDI attacks violate the data integrity through tampering with the data. A successful FDI attack aims at the state estimator in power grids by changing the actual measurement data transmitted in the communication networks and, meanwhile, bypassing the bad data detector in EMS. The structure of PSSE problem under FDI attacks is depicted in Fig. 2.6.

Assume that the attacker has the ability to inject false data over the communication channels between the meters and the estimator. Under FDI attacks, the measurement output received by the estimator is given as follows:

$$y^a(k) = y(k) + a(k) \tag{2.11}$$

where $y(k) \in \mathbb{R}^m$ is the measurements of the PMU and/or traditional meters depending on the meter placement in practical power grids, $a(k) \in \mathbb{R}^m$ represents the false data injected by the attacker at time instant k. The attack vector is described by $a(k) = B_a a^0(k)$ where the injection matrix is defined as $B_a = \text{diag}\{\gamma_1, \dots, \gamma_m\}$ with $\gamma_i = 1$ if the attacker is able to inject false data into the ith communication channel and $\gamma_i = 0$ otherwise. Matrix B_a reflects which communication channels the attacker can compromise. Specifically, $B_a = 0$ means that no FDIAs can be injected into any communication channel and $B_a = I_m$ implies that the attacker has the ability to inject FDIA into all communication channels.

If the residual $r(k)$ in (2.10) does not change under FDI attacks, then no alarm will be triggered by the bad data detector. In formal mathematical description, the FDI attack $a(k)$ in (2.10) will not be detected if the following

$$r^a(k) - r(k) = 0 \tag{2.12}$$

is true, where $r^a(k)$ and $r(k)$ are the residuals generated by the bad data detector in the cases of a) FDI attacks on the measurements; and b) no attacks on the measurements, respectively.

2.4.2 Latest Progress

Since the initial results reported in 2009 [110], the research topic of PSSE under FDI attacks has been attracting an increasing research attention. In the following, we review the recent advances of this research topic from three different aspects: system vulnerability, attack detection and system protection.

System Vulnerability

To examine the cyber-security of the state estimator in power grids, we need to answer the question from the perspective of protector/attacker: which set of measurements (or the corresponding communication channels transmitting them) should be protected/attacked in order to make the attack detectable/undetectable by the bad data detector? To answer this question, we need to find the inherent weaknesses in the state estimator and the bad data detector in power grids.

Some representative works that would help answer the aforementioned question can be found in [110, 111, 95, 79, 148, 109]. In the context of approximate linear state estimation model (rather than the original nonlinear one), the case that the attacker has perfect knowledge of system model has been investigated in [110, 111] and the case that limited (rather than all) model knowledge is known by the attacker has been considered in [109]. Furthermore, in [95], it has been assumed that the attackers has only limited resources to manipulate either a deterministic or random subset of all measurements. The system vulnerability has been discussed from a different angle in [148] where the minimum number of sensor measurements required to be tampered with for successful attacks has been determined, and the corresponding constrained cardinality minimization problem has been solved by using some convex relaxation techniques. In addition, the system vulnerability under FDI attacks has been further investigated for the nonlinear, exact, (as opposed to linear and approximate) state estimation model in [79].

Attack Detection

It is widely recognized that the PSSE system is typically vulnerable, and it is of great importance to detect whether the system is under FDI attacks or not. The attack detection can be achieved by improving either the BDD schemes or the state estimation algorithms. For example, In [95], a new BDD scheme has been proposed to replace the tradition one using χ^2 test and the new scheme has been shown to successfully detect a particular kind of FDI attacks. In [32], different detection methods for FDI attacks in power grids have been reviewed. On the other hand, the sparse nature of the attack vectors in power grids has been exploited in designing efficient attack detection/estimation algorithms [106, 57, 149]. Specifically, sparse optimization-based estimation methods have been proposed to detect the attacks in [106] and, under a stronger assumption that less than 6 meters/communication channels can be attacked simultaneously, an efficient FDI attack estimation method has been developed in[57]. Similarly, using the minimum-cut algorithm, the stealthy attacks on power networks have been computed exactly in[149]. Moreover, the optimal policies for attack design/detection from the adversary/defender has been investigated in a game-theoretic framework in [46].

System Protection

System protection refers to the countermeasures which remove or mitigate the existing system vulnerabilities, thus making successful attacks less likely to happen. To prevent the PSSE system from cyber-attacks, the PMUs and the communication networks which transmit measurement data should be protected. Several protection schemes have been developed [56, 56, 91, 160, 13, 123, 100, 164] by using methods such as secured PMU placements, data encryption and isolated physical transmission media. Assuming that the PMU measurements are free from cyber-attacks, the optimal placement of secured PMUs has been considered in [56, 91]. Without the above assumption, in [13], both exact and fast approximation algorithms have been derived to compute the minimum number of measurements needed to be protected, and an algorithm has been developed in [123] for determining the set of PMUs that should be disabled such that the remaining PMUs continue to maintain the observability of the power grids under FDI attacks. There have been some other research results focusing on how to secure the communication networks. For instance, schemes to reroute measurements have been used in [160] whose main idea is to change the communication network topology and make successful attacks difficult to accomplish. From the information theoretic perspective, the minimum channel capacity needed in the wireless network that ensures negligible information leakage of the power grid to the eavesdropper has been studied in [100]. In addition, another different protection mechanism has been proposed in [164] where, by strategically shutting down some preselected transmission lines by turns, the topologies of the electrical network (instead of that of the communication networks) have been switched. By doing so, the measurement model is time-varying and therefore difficult to be obtained by the attacker.

Some Remarks

Though the literature on the security of the PSSE system under FDI attacks has been classified and reviewed from three different aspects, there has been indeed some literature concentrating on more than one aspects. For example, both the system vulnerability and attack detection problems have been considered in [70] and, in [174], both the system vulnerability and system protection problem under FDI attacks have been considered simultaneously. In addition, as an interdisciplinary research area, the cyber-security of the PSSE system has drawn significant attention of researchers from a variety of communities such as power systems, computer security, communication and control. Progresses made in different research societies can be found from the survey papers [150, 165, 64, 134].

Chapter 3

A Constrained Optimization Approach to Dynamic State Estimation for Power Grids including Missing and PMU Measurements

3.1 Introduction

State estimation (SE) has long been one of the fundamental problems in the research on power systems. Traditional SE approach is typically static where the single-scan weighted least-squares estimators are adopted [2]. Static SE method exhibits the features of fast convergence and easy implementation, but it suffers from the accuracy problems since the dynamics of the power system is ignored.

With rapid development of the sensing techniques, online monitoring has recently become popular which gives rise to the renewed research interests on the design of the dynamic state estimator (DSE). Comparing with the static state estimation scheme, the DSE is capable of achieving better estimation accuracy since more information about the state evolution is utilized. Another advantage of the DSE is its potential ability to provide prediction database that could be adopted as a set of pseudo-measurements in case of missing data or meter outages in the power grids.

Note that the missing data phenomenon constitutes one of the major concerns in state estimation for power systems since data dropouts inevitably occur in the transmission channels of traditional measurements from the meters to the control centre. As discussed in [146, 163, 74], the communication constraints (e.g. limited bandwidth) have inevitably led to network-induced phenomena such as random communication delays and missing measurements. As for missing measurements, a conventional way is to treat them as normal bad data *without* in-depth characterization of the dropouts. Very recently, the missing measurement problem has been tackled in [154, 146] where a certain stochastic variable is involved in the estimator, and this renders the difficulties in the implementation. In this chapter, a recursive algorithm is developed to mitigate the effect of missing measurements through modifying the traditional DSE approaches.

The main purpose of this chapter is to design dynamic state estimators for power systems by making one of the first attempts to solve the aforementioned two challenging problems, i.e., 1) how to account for the probabilistic missing data phenomenon? 2) how to include the PMU measurements in the state estimator design? In this chapter, the phenomenon of missing measurements is assumed to occur randomly and the missing probability for each channel is governed by an individual random variable satisfying a certain probability distribution over the interval $[0,1]$. The impact of missing measurements on the overall estimation performance is considered when designing the estimator. On the other hand, to incorporate the PMU measurements into the widely used extended Kalman filter (EKF) algorithm, the PMU measurements are characterized via a set of inequality constraints based on the well-known 3-sigma rule of the Gaussian distribution, and then the EKF problem with state constraints becomes a constrained optimization problem that can be effectively solved by the particle swarming optimization (PSO) algorithm. As PSO has been developed primarily as an unconstrained optimization method, the penalty function approach is utilized to convert the constrained optimization problem into an unconstrained one.

The reminder of this chapter is organized as follows. In Section 3.2, the dynamic model of the power systems is briefly introduced, and the PMU measurement is characterized by a set of inequality constraints on systems states. In Section 3.3, the EKF estimation problem with the inequality constraints on the states is converted to a constrained optimization problem by the maximum probability method. The PSO algorithm together with the penalty function approach for the constrained optimization problem is described in Section 3.4. The results of case studies performed on the 14-bus IEEE benchmark system are presented and analysed in Section 3.5. Finally, the chapter is concluded in Section 3.6.

3.2 Problem Formulation and Preliminaries

3.2.1 System Model with Missing RTU Measurements

In this chapter, the power network is assumed to operate among quasi-steady states and such kind of steady-state dynamics is typically different from the transient ones generated by the electro-mechanical power systems. Let us consider the following model that represents the slow system dynamics of N buses ([15, 17, 20, 154, 159]:

$$x(k+1)-u=A(x(k)-u)+\omega(k) \tag{3.1}$$

where the state $x(k)\in\mathbb{R}^{2N}$ is the vector of the real parts and the imaginary parts of the voltages at all buses in the rectangular form, that is, $x(k)=\left[x_{r,1}(k)\ \cdots\ x_{r,N}(k)\ x_{i,1}(k)\ \cdots\ x_{i,N}(k)\right]^T$, and $u\in\mathbb{R}^{2N}$ is the trend behavior of the state trajectory. $\omega(k)$ is a Gaussian sequence with zero mean and covariance matrix $W(k)$. A represents how fast the transitions between states are. The initial value of state $x(0)$ is a white Gaussian noise with mean value $\bar{x}(0)$ and covariance matrix $\Sigma(0|0)$. For computational convenience, the state transition matrix A has been traditionally assumed to be diagonal in the dynamic state estimation algorithms of power systems [20].

For the purpose of simplicity, define $B\triangleq I-A$, then (3.1) can be rewritten in the following compact form:

$$x(k+1)=Ax(k)+Bu+\omega(k). \tag{3.2}$$

The ideal measurement (without missing phenomena) $z^{(r)}(k)\in\mathbb{R}^m$ collected by RTUs is given as follows

$$z^{(r)}(k)=\begin{bmatrix}V^T(k) & P^T(k) & Q^T(k) & P^{fT}(k) & Q^{fT}(k)\end{bmatrix}^T$$

Recall that the explicit element for each aforementioned measurement is given in (2.2) in Chapter 2. Taking the measurement noise into consideration, $z^{(r)}(k)$ can be rewritten as the following compact form

$$z^{(r)}(k)=h(x(k))+v_1(k) \tag{3.3}$$

The nonlinear function $h(x)$ is given as follows:

$$h(x(k))=[V^T(k),P^T(k),Q^T(k),P^{f^T}(k),Q^{f^T}(k)]^T,$$

and $v_1(k)$ is the RTU measurement noise which is also a Gaussian noise with zero mean and covariance matrix $R_1(k)$. Assume $\omega(k)$ and $v_1(k)$ are uncorrelated with $x(0)$ and with each other.

Considering missing measurements, the *actual* measurement $z(k)$ is described by

$$z(k) = \Xi(k)h(x(k)) + v_1(k) \tag{3.4}$$

where $\Xi(k) = \text{diag}\{\gamma_1(k), \gamma_2(k), \cdots, \gamma_m(k)\}$ with $\gamma_i(k)$ $(i = 1, 2, \cdots, m)$ being m unrelated random variables. $\Xi(k)$ is also unrelated with $\omega(k)$, $v_1(k)$ and $x(0)$. Furthermore, it is assumed that the stochastic variable $\gamma_i(k)$ is a Bernoulli-distributed white noise sequence taking values on 0 or 1 with:

$$\text{Prob}\{\gamma_i(k) = 0\} = 1 - \mu_i(k), \quad \text{Prob}\{\gamma_i(k) = 1\} = \mu_i(k)$$

where the value of Prob$\{\gamma_i(k) = 0\}$ is also called the missing rate of the ith measurement.

In RTU measurements, one bus is usually chosen as the reference bus for all the other buses to obtain the relative phase angles, while in PMU measurements, all PMU measurements provide the direct phase angles with respect to the time reference provided by the GPS system. In this chapter, we use both RTU and PMU measurements, and therefore all the bus phase angles are relative to the reference dictated by the GPS [94]. As a result, no reference buses are needed.

Remark 3.1 *In the state transition equation, there are three parameters to be determined, namely, A, W and u, where A is assumed to be diagonal for computational convenience. Based on a frequently used power system model, we aim to develop a new estimation algorithm so as to handle both RTU and PMU measurements in the presence of quantization effects. One of our next research topics would be to integrate the parameter identification issue with our developed state estimation algorithm.*

3.2.2 PMU Measurements and Inequality Constraints

In this chapter, both the state variables and measured variables are in the rectangular form, which makes a linear PMU measurement model. Assume that the lth PMU is installed at bus j, and recall the PMU measurement model given in (2.4) in Chapter 2. Considering the measurement noise, the PMU measurements can be presented in the following compact vector form:

$$z^{(p)}(k) = H^{(p)}x(k) + v_2(k) \tag{3.5}$$

where $z^{(p)}$ is the PMU measurement vector, and $v_2(k)$ is the PMU measurement noise, which is also a Gaussian noise with zero mean and covariance matrix $R_2(k)$. $H^{(p)}$ can be obtained directly from PMU configurations, and it can be found that the measurement $z^{(p)}(k)$ is linearly related to the state $x(k)$.

A seemingly natural idea is to treat the PMU measurements as an additional set similar to the RTU measurements. Note the fact reported in [94, 14], that the standard deviation of the errors of PMU measurements is one to two order magnitude less than the one of traditional RTU measurements. Unfortunately, since the PMU measurements are much more accurate than the RTU measurements, including these two kinds of measurements in the estimation process often results in ill-conditioned filtering procedure due primarily to the low covariance matrix for the PMU measurement noises.

As $R_2(k)$ is always a real symmetric matrix, we can find a transformation matrix $M(k)$ of appropriate dimension such that the matrix $M(k)R_2(k)M^T(k)$ is diagonal. Accordingly, we can obtain the following equation from (3.5):

$$M(k)z^{(p)}(k) = M(k)H^{(p)}x^p(k) + M(k)v_2(k) \tag{3.6}$$

where $M(k)v_2(k)$ is still a Gaussian noise with zero mean and covariance matrix $M(k)R_2(k)M^T(k)$.

Based on the well-known 3-sigma rule of Gaussian distribution, we can conclude that the following inequality sets are satisfied with probability 99.7%:

$$-3\tilde{R}_2(k) \leq M(k)z^{(p)}(k) - M(k)H^{(p)}x^p(k) \leq 3\tilde{R}_2(k) \tag{3.7}$$

where $\tilde{R}_2(k) \triangleq M(k)R_2(k)M^T(k)I_{m_1,1}$. From the perspective of engineering applications, it is reasonable to assume that the above inequality sets are satisfied all the time. So far, we have characterized the PMU measurements by a set of inequality constraints on the states for the power system.

Remark 3.2 *Traditionally, the measurement noise is usually assumed to be Gaussian. Sometimes such an assumption, however, is no longer true for PMU measurements where the probability distribution of the measurement errors (noises) is unavailable. According to [27], sometimes only the maximal measurement errors are specified by PMU manufacturers, which can be interpreted as the inequality constraints on the PMU measurements. In this case, it makes more practical sense to model the PMU measurement errors via inequality constraints in order to characterize the noise in a more accurate way.*

3.3 Filter Schemes

3.3.1 EKF Design for the System with RTU Measurements

In this subsection, we first introduce the EKF approach to estimating the system state for the system (3.2) with missing measurements (3.4). The EKF is of the following form:

$$\begin{aligned}&\hat{x}(k|k-1) = A\hat{x}(k-1|k-1)+Bu\\&\hat{x}(k|k) = \hat{x}(k|k-1)+K(k)[z(k)-\bar{\Xi}(k)h(\hat{x}(k|k-1))]\end{aligned}$$

where $\hat{x}(k|k)$ is the estimate of $x(k)$ at time instant k with $\hat{x}(0|0)=\bar{x}(0)$, and $\hat{x}(k|k-1)$ is the one-step prediction of $x(k)$ at time $k-1$. $K(k)$ is the filter gain to be determined at time instant k, and $\bar{\Xi}(k) \triangleq \mathbb{E}\{\Xi(k)\} = \mathrm{diag}\{\mu_1(k),\mu_2(k),\ldots,\mu_m(k)\}$. $P(k|k-1)$ and $P(k|k)$ are the covariance matrices of, respectively, the one-step prediction error and the filtering error defined by

$$\begin{aligned}&\tilde{x}(k|k-1) = x(k)-\hat{x}(k|k-1), \quad \tilde{x}(k|k) = x(k)-\hat{x}(k|k),\\&P(k|k-1) = \mathbb{E}\{\tilde{x}(k|k-1)\tilde{x}(k|k-1)^T\},\\&P(k|k) = \mathbb{E}\{\tilde{x}(k|k)\tilde{x}(k|k)^T\}.\end{aligned}$$

Denoting $H(k) = \frac{\partial h(x(k))}{\partial x(k)}\Big|_{x(k)=\hat{x}(k|k-1)}$, the gain $K(k)$ can be obtained using the following recursive algorithm:

$$\begin{aligned}P(k|k-1) &= AP(k-1|k-1)A^T+W(k-1) &&(3.8)\\P(k|k) &= [I-K(k)\bar{\Xi}(k)H(k)]P^{-1}(k|k-1) &&(3.9)\\S(k) &= \tilde{\Xi}(k)\circ(h(\hat{x}(k|k-1))h^T(\hat{x}(k|k-1)))\\&\quad +\tilde{\Xi}(k)\circ(H(k)P(k|k-1)H^T(k))+R(k)\\&\quad +\bar{\Xi}(k)H(k)P(k|k-1)H^T(k)\bar{\Xi}(k) &&(3.10)\\K(k) &= P(k|k-1)H^T(k)\bar{\Xi}(k)S^{-1}(k) &&(3.11)\end{aligned}$$

where $\tilde{\Xi}(k) \triangleq \mathrm{diag}\{\tilde{\mu}_1(k),\tilde{\mu}_2(k),\ldots,\tilde{\mu}_m(k)\}$ with $\tilde{\mu}_i(k) = \mu_i(k)(1-\mu_i(k))$ $(i=1,2,\ldots,m)$.

Remark 3.3 *In this chapter, the exact occurrence time for the randomly missing measurements is not required to be exactly known, and this reflects the practical situation in power system. Nonetheless, the statistical law (i.e., the first- and second- order of moments) of the random occurrence of missing measurements is needed in the filter design, where the statistical law could be obtained through statistic tests.*

Remark 3.4 *There are mainly two kinds of DSE paradigms in power system state estimation. These two paradigms differ from each other in system dynamics model and time scale. In one paradigm (see e.g. [159, 20, 17] and the references therein) called forecasting-aided state estimation, the bus voltages are chosen as state variables and a succession of the quasi steady-states is assumed to evolve in time. Therefore, a dynamic model is adopted to describe the slow time evolution of the quasi steady-state. In the other paradigm (see e.g. [48] and the references therein), rotor angles and rotor speeds of generators are chosen as state variables, and the classic dynamic model of generators is considered. The DSE of such a paradigm is concerned with the low frequency electromechnical dynamics.*

3.3.2 The Probability-Maximum Method

For the constrained estimation problem, it is difficult to incorporate the inequality/equality constraint of system states into traditional EKF estimator. Fortunately, the probability-maximum method has been successfully exploited in [144] to convert the constrained estimation problem into a constrained optimization one after each step of the EKF algorithm and, therefore, this method is chosen to handle the constrained EKF problem in this chapter.

For presentation conciseness, the notation for time instant, k, is omitted in this subsection. It is known from [8] that, based on the Kalman filter theory, the state estimate of x maximizes the conditional probability density

$$\mathbb{P}(x|Z) = (2\pi)^{-\frac{n}{2}}|P|^{-\frac{1}{2}}\exp\{-\frac{1}{2}(x-\bar{x})^T P^{-1}(x-\bar{x}) - \frac{1}{2}(h(x)-h(\bar{x}))^T R^{-1}(h(x)-h(\bar{x}))\} \tag{3.12}$$

where n is the dimension of x, P is the covariance of the Kalman filter estimate, $Z \triangleq \{z(0), z(1), \dots, z(k)\}$ denotes the set of measurements available at time instant $0, 1, \dots, k$, and $\bar{x}$ is the conditional mean of x given Z.

The constrained EKF can be derived by finding an estimate $\hat{x}$ such that the conditional probability $\mathbb{P}(\hat{x}|Z)$ is maximized and $\hat{x}$ satisfies the constraint (3.7). Since maximizing $\mathbb{P}(\hat{x}|Z)$ is equivalent to maximizing its natural logarithm, the problem to be solved can be expressed as

$$\begin{aligned} &\max \ln \mathbb{P}(\hat{x}|Y) \Rightarrow \min(\hat{x}-\bar{x})^T P^{-1}(\hat{x}-\bar{x}) + (h(x)-h(\bar{x}))^T R^{-1}(h(x)-h(\bar{x})) \\ &\text{subject to} - 3\tilde{R}_2 \leq Mz^{(p)} - MH^{(p)}C\hat{x} \leq 3\tilde{R}_2. \end{aligned} \tag{3.13}$$

So far, the constrained state estimation problem has been converted into an equivalent constrained optimization problem that can be solved after each time step of the EKF algorithm. As is impossible to develop a deterministic method for the constrained nonlinear optimization

Table 3.1 The nominal voltage at normal states

Bus	1	2	3	4	5	6	7	8	9	10	11	12	13	14
R.V	1.0600	1.0368	0.9609	0.9858	0.9958	1.0016	1.0022	1.0270	0.9827	0.9769	0.9850	0.9806	0.9755	0.9552
I.V	0	0.0943	0.2173	0.1821	0.1563	0.2694	0.2512	0.2643	0.2743	0.2744	0.2724	0.2759	0.2748	0.2812

problem (3.13) in the global optimization category, we adopt the PSO algorithm, which is a popular evolutionary algorithm in solving the nonlinear optimization problem.

3.4 PSO for Constrained Optimization Problem

Particle Swarm optimization (PSO) is a metaheuristic that optimizes a problem by iteratively searching in a large spaces of candidate solutions [90]. In PSO, a population of candidate solutions (called as particles) moves in the search space according to two simple mathematic formulae over the particle's position and velocity. More specifically, each particle's movement is influenced by its local best known position and also the best known positions, which are updated by other particles, in the search space. By such an iterate approach, the swarm of the particles moves towards the best solutions. The velocity and position of the particle at the next iteration are updated according to the following equations:

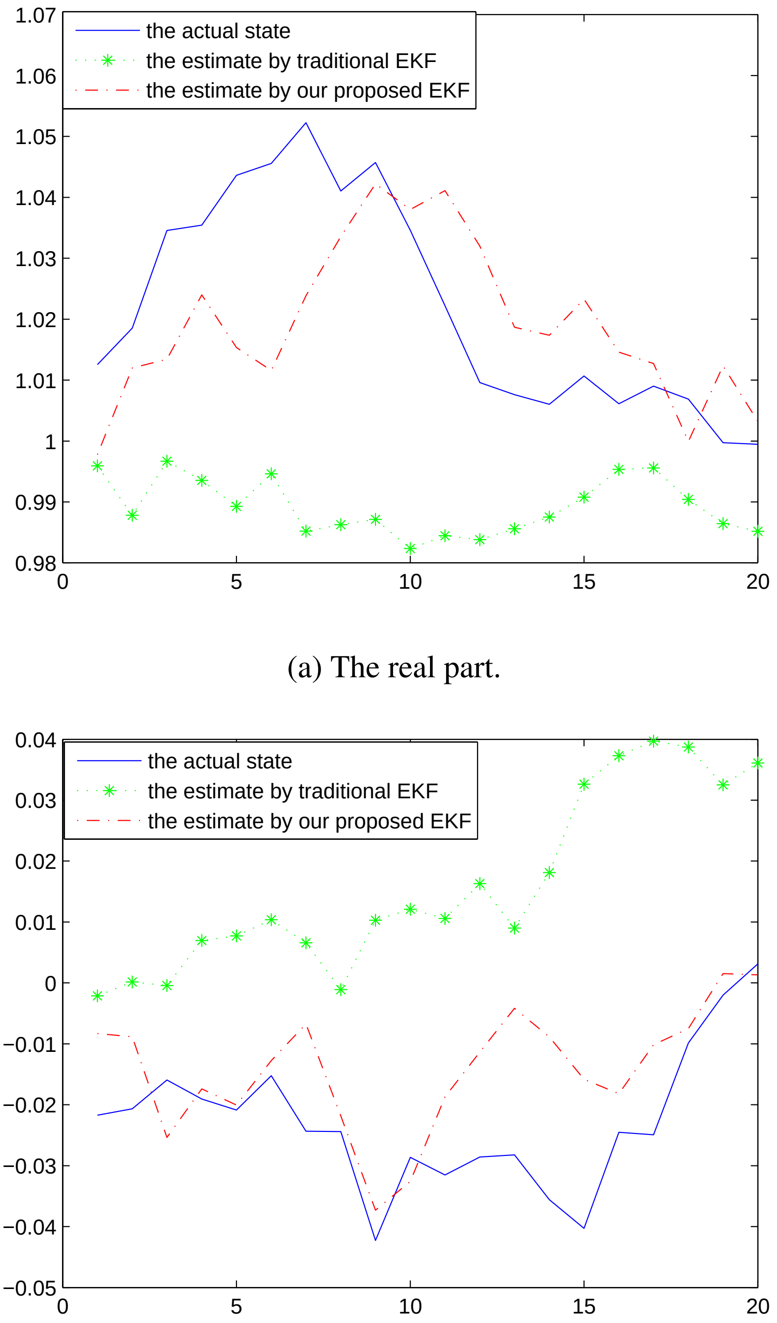
$$\begin{cases} v_i(s+1) = \omega v_i(s) + c_1 r_1 (p_i(s) - x_i(s)) + c_2 r_2 (p_g(s) - x_i(s)) \\ x_i(s+1) = x_i(s) + v_i(s+1) \end{cases} \tag{3.14}$$

where $x_i(s) = [x_{i1}(s), \ldots, x_{id}(s)]$, $x_i(s)$ is the position of the ith particle at the sth iteration, and $x_i(s) \in [x_{min,n}, x_{max,n}]$, with $x_{min,n}$ and $x_{max,n}$ being the lower and the upper bounds for all particles' positions. $v_i(s) = [v_{i1}(s), \ldots, v_{id}(s)]$, $v_i(s)$ is the velocity of the ith particle at the sth iteration. ω is the inertia weight, c_1 and c_2 are called acceleration coefficients, namely, cognitive and social parameters, respectively. r_1 and r_2 are two uniform random number samples from $[0,1]$. $p_i(s)$ is the local best position encountered by ith particle at the sth iteration, and $p_g(s)$ is the global best position in the swarm at the sth iteration.

PSO has been successfully applied to various optimization problems. As to constrained optimization problem, PSO is still valid with the aid of the popular constraint-handling technique: the penalty function approach. By using the penalty function approach, a constrained optimization problem can be converted into a corresponding unconstrained optimization one by adding a penalty term to the original objective function [176].

In this chapter, the penalty function $F(x)$ is defined as

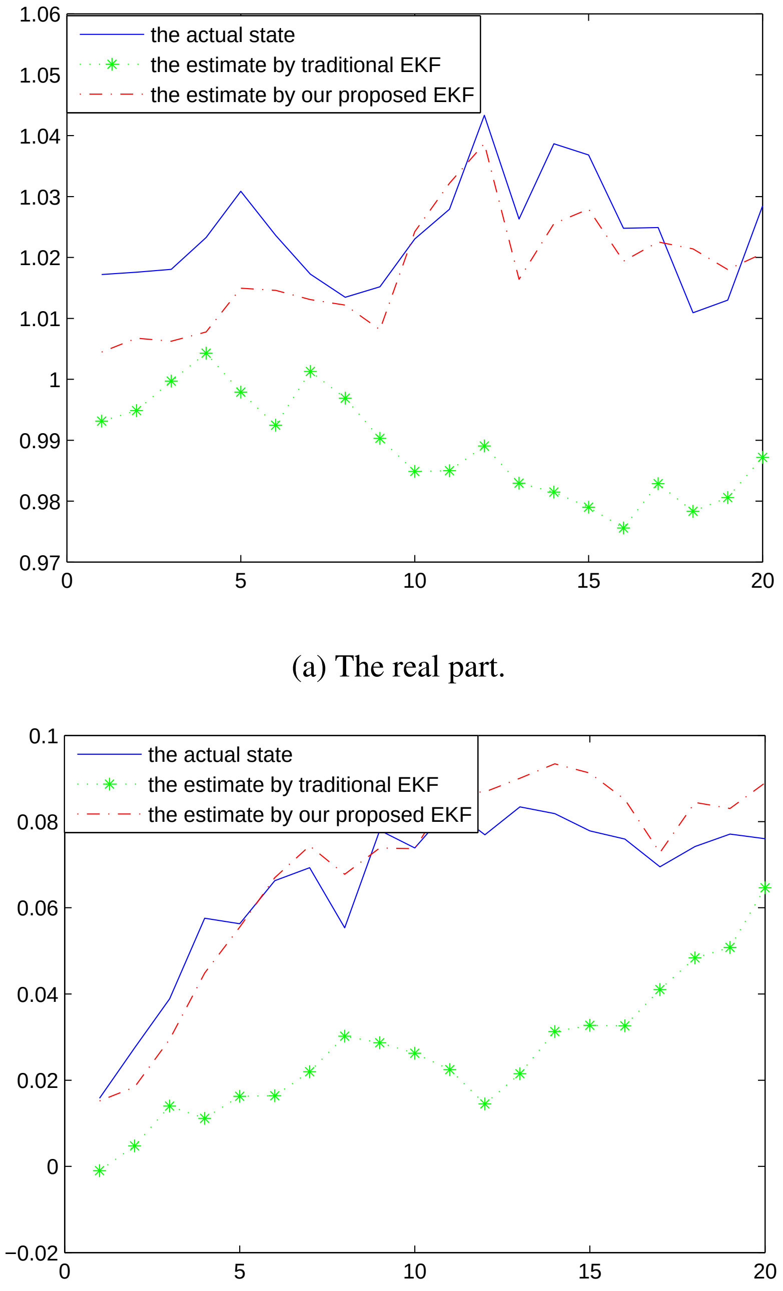
$$F(x) = f(x) + h(s)g(x), x \in \mathbb{R}^n \tag{3.15}$$



(a) The real part.

(b) The imaginary part.

Fig. 3.1 The estimated states of bus 2 from the traditional EKF and our proposed EKF



(a) The real part.

(b) The imaginary part.

Fig. 3.2 The estimated states of bus 5 from the traditional EKF and our proposed EKF

where $f(x)$ is the original objective function of the constrained optimization problem in (3.13), $h(s)$ is a dynamic penalty coefficients with the sth iteration steps, $g(x)$ is a penalty factor defined as $g(x) = \theta \sum_{i=1}^{m_1} q_i^2(x)$. Here $q_i(x) = \max\{0, c_i(x)\}$ with $c_i(x) = \frac{|M_i(k)(z^{(p)} - H^{(p)} x^p)|}{3\tilde{R}_{2i}(k)} - 1$, $i = 1, \ldots, m_1$, where $M_i(k)$ and $\tilde{R}_{2i}(k)$ are the ith row of $M(k)$ and $\tilde{R}_2(k)$ in inequality (3.7).

3.5 Simulation Results

In this section, the proposed hybrid algorithm of EKF and PSO is tested in the case study of the IEEE 14-bus test system. The simulation is implemented in Matlab with the Matpower package[190]. First, the IEEE 14-bus test system can be model as (3.1) with parameters $A = \text{diag}_{28}\{0.98\}$, $B = \text{diag}_{28}\{0.02\}$ and $W(k) = \text{diag}_{28}\{0.01^2\}$. The trend u of the normal state is the base-case voltages given in Table 3.1. Furthermore, assume that the initial voltages of all buses are at flat start, that is, $x_{r,l}(0) = 1$ p.u, $x_{i,l}(0) = 0$ for all $l = 1, 2, \ldots, 14$.

The measurement configuration is the same as the one used in [94], where RTU measurements consist of three categories: the voltage magnitude at bus 1, power injections at bus 3, 5, 13 and 14, and power flows at branches 1-2, 1-5, 2-5, 3-4, 4-7, 4-9, 6-11, 6-12, 6-13, 7-8, 7-9, 9-10, 9-14, 10-11, 12-13 and 13-14. In addition, PMUs are deployed at buses 2, 7 and 9. Furthermore, the covariance matrices of the traditional RTU measurement and PMU measurement noise are $R_1(k) = \text{diag}_{43}\{0.1^2\}$ and $R_2(k) = \text{diag}_{28}\{0.01^2\}$, respectively.

The algorithm is implemented in Matlab R2010a. The simulation is performed on a PC with a Intel(R) Core(TM) CPU i5-2500 @3.30 GHz and 4 GB RAM. The time required by the proposed EKF without PSO algorithm at each step is 0.81 seconds. For the proposed EKF with PSO algorithm, the computation time is related to the population of the swarm (ps) and the iterations (iter). In the simulation, we have set $ps = 100$ and $iter = 200$, and the time required by the proposed EKF with PSO algorithm at each step is 1.47 seconds. It can be concluded that the proposed EKF with PSO algorithm is quite fast and hence is suitable for online implementations. Moreover, the integration of PSO into EKF slows the computational speed slightly, yet improves the performance of state estimation obviously.

In this test system, three comparative experiments regarding the estimation accuracy are carried out as follows:

Case 1) Both the proposed EKF considering measurements with certain missing rate and the traditional EKF ignoring the missing measurements are implemented for the system with missing measurements;

Case 2) When the missing rate of the measurements varies from zero to higher values, the proposed EKF is implemented in all the cases;

Case 3) The state estimations based on the proposed EKF with/without PSO algorithm are compared.

In order to have more general and significant experimental results, 100 Monte-Carol simulations are run in Cases 2 and 3. The notion mean square error (MSE) is adopted to evaluate the estimation accuracy, where MSE_i denotes MSE for the estimate of the ith state, i.e. $\mathrm{MSE}_i(k) = \frac{1}{100}\sum_{j=1}^{100}(x_i(k) - \hat{x}_i(k))^2$. To evaluate the average estimation performance of all states, average mean square error (AMSE) is defined as $\mathrm{AMSE}(k) \triangleq \frac{1}{n}\sum_{j=1}^{n}\mathrm{MSE}_j(k)$, where n is the number of the state variables. In all the figures, “R.V” and “I.V” denote the real and imaginary part of voltage, respectively.

3.5.1 Traditional EKF vs. the Proposed EKF

In this case, the probability density function for the missing $\Xi(k)$ is $\mathrm{Prob}\{\Xi_i(k) = 0\} = 0.5, \quad \mathrm{Prob}\{\Xi_i(k) = 1\} = 0.5$. The expectation can be easily calculated as $\mu_i(k) = 0.5$. The estimated states of the representative buses $2,5$ obtained from traditional EKF without considering the missing measurements and our proposed EKF considering missing measurements are plotted in Figs. 3.1 and 3.2, respectively. From the comparison, it can be found that our proposed EKF algorithm performs well in the presence of missing measurements, whereas the state estimate obtained from the traditional EKF cannot track the real states when missing measurements occur randomly.

3.5.2 EKF with Individual Missing Measurements

In order to see how different missing rates impact on the estimation accuracy, three missing rates of 0.15, 0.02 and 0 (without missing measurements) are considered. The MSEs of the estimated states of buses $2,5$ for all the three missing rates are compared in Figs. 3.3 and 3.4. The $\mathrm{AMSE}(k)$ in all three cases are given in the first three rows of Table 3.2, for $k = 1,\dots,15$. From the comparisons, it can be found the less the missing rate is, the more accurate the state estimation obtained from the proposed EKF algorithm will be.

Table 3.2 The AMSE for estimated states by different algorithms with different missing rates

Time instant	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
MR = 0.00 (EKF)	0.1350	0.1609	0.1748	0.2121	0.2342	0.2432	0.2366	0.2564	0.2767	0.2651	0.2707	0.2601	0.2572	0.2503	0.2751
MR = 0.02 (EKF)	0.1344	0.1784	0.2091	0.2134	0.2123	0.2356	0.2550	0.2425	0.2787	0.2884	0.2851	0.3136	0.3202	0.3253	0.3578
MR = 0.15 (EKF)	0.1416	0.1836	0.2152	0.2596	0.2673	0.2913	0.3341	0.3350	0.3590	0.3813	0.3858	0.4410	0.4615	0.4801	0.4612
MR = 0.15 (Hybrid)	0.1342	0.1725	0.2066	0.2047	0.2226	0.2450	0.2682	0.2818	0.3135	0.2985	0.2958	0.2950	0.3050	0.3199	0.3049

Note that MR denotes the missing rate, and the results in the table are magnified 10^3 times for clarity.

3.5.3 EKF vs. Hybrid EKF and PSO Algorithm

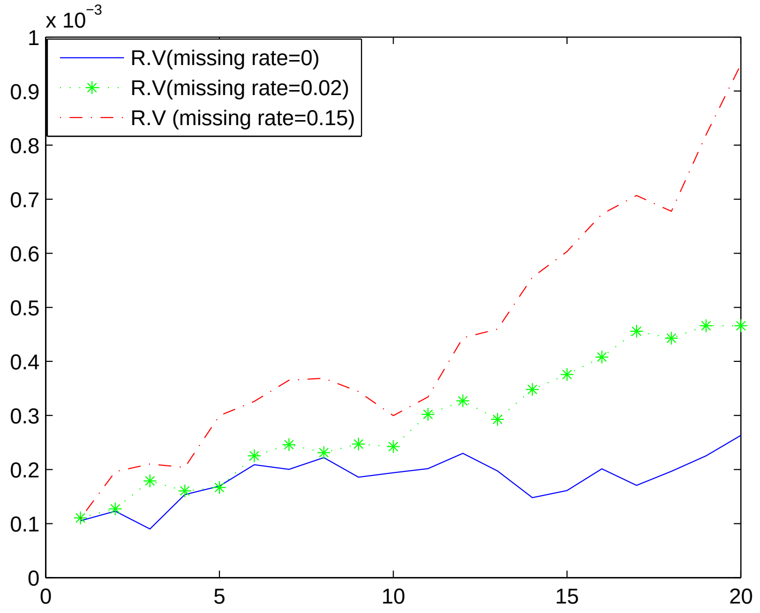
We are now in a position to evaluate the effectiveness of including the PSO scheme in the EKF design. A comparison is made between the EKF algorithm alone and the hybrid EKF and PSO algorithm. For this purpose, the missing rate is fixed as 0.15. Regarding the penalty function parameters, $\theta = 1000$ and $h(s) = s$ are chosen in all the iteration steps.

For the same test system, one realization of the EKF and one realization of the hybrid algorithm are simulated simultaneously, and the estimated states of bus voltages $2,5$ obtained from the two algorithms are illustrated in Figs. 3.5 and 3.6. It is seen that the trajectory by the proposed hybrid approach is much closer to the true state trajectory than the one only by the EKF. The MSE_2 and MSE_5 at all time instants for both algorithms are plotted in Fig. 3.7. It can be found that for the same state variable, the MSE of EKF-based state estimation is bigger than the MSE of the state estimation obtained from the hybrid algorithm. Especially, when the accumulated error of EKF-based state estimation becomes bigger after several integrations, the subsequent PSO algorithm can refine the state estimation and diminish the error. The AMSEs of EKF and of the proposed hybrid algorithm are given in the last two rows of Table II. It can be found the $\text{AMSE}(k)$ of EKF is bigger than the one of the proposed hybrid algorithm at each step.

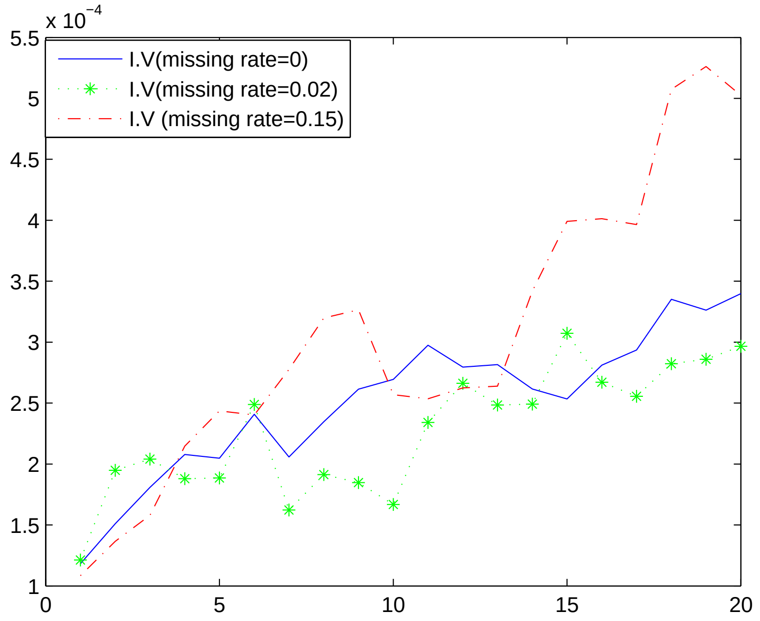
From the comparative experiments, it can be concluded that our proposed hybrid EKF and PSO algorithm outperforms the traditional EKF algorithm in the presence of probabilistic missing measurements by including PMU measurements.

3.6 Conclusion

In this chapter, a hybrid filter algorithm is developed to deal with the state estimation problem for power systems by taking into account the impact from the PMUs. Our aim is to include PMU measurements when designing the dynamic state estimators for power systems with traditional measurements. Also, as data dropouts inevitably occur in the transmission channels of traditional measurements from the meters to the control centre, the missing measurement phenomenon is also tackled in the state estimator design. In the framework of EKF algorithm, the PMU measurements are treated as inequality constraints on the states with the aid of the statistical criterion, and then the addressed state estimation problem becomes a constrained optimization one based on the probability-maximization method. The resulting constrained optimization problem is then solved by using the PSO algorithm together with the penalty function approach. The proposed algorithm is applied to estimate the states of the power systems with both traditional and PMU measurements in the presence of probabilistic data missing phenomenon. Extensive simulations are carried out on the

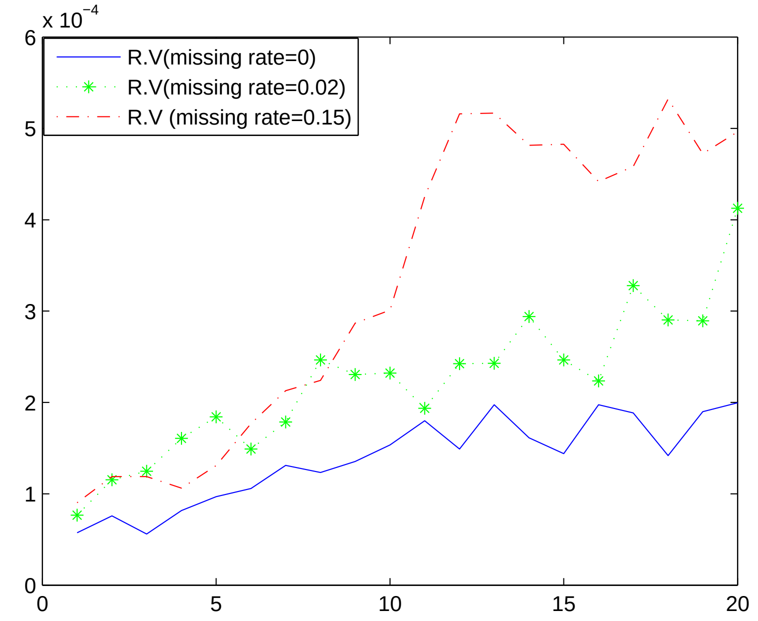


(a) The real part.

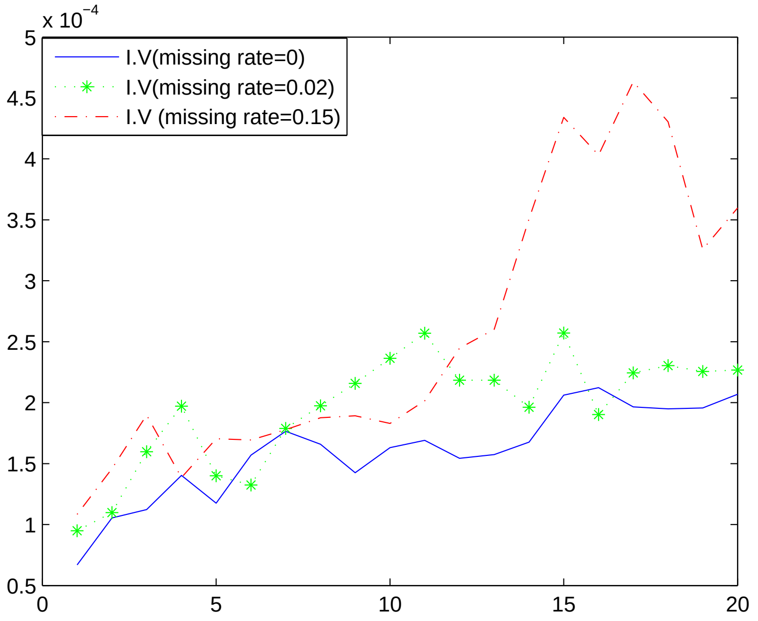


(b) The imaginary part.

Fig. 3.3 The MSEs of the estimated state at bus 2 under different missing rates

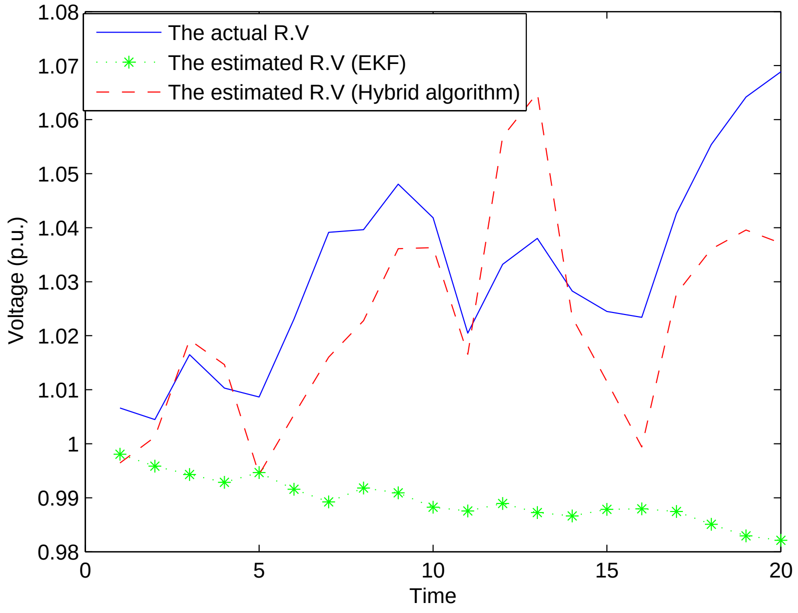


(a) The real part.

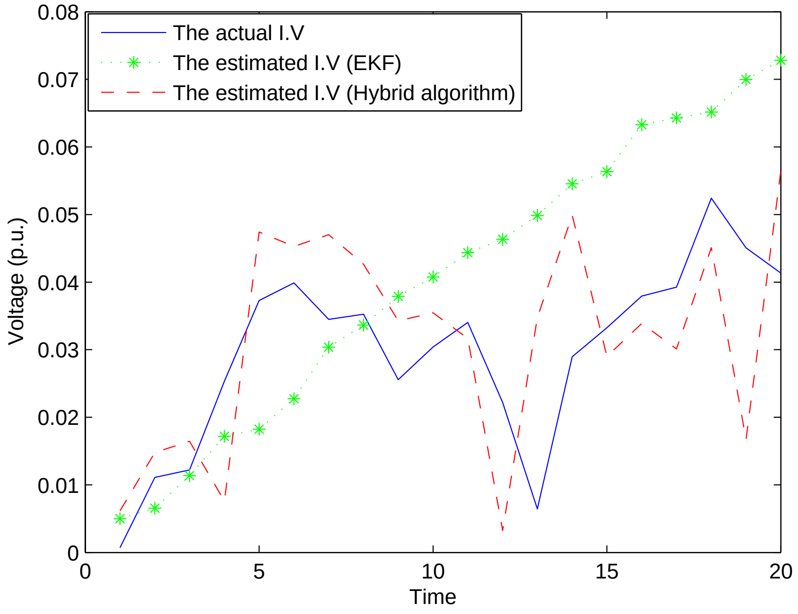


(b) The imaginary part.

Fig. 3.4 The MSEs of the estimated state at bus 5 under different missing rates

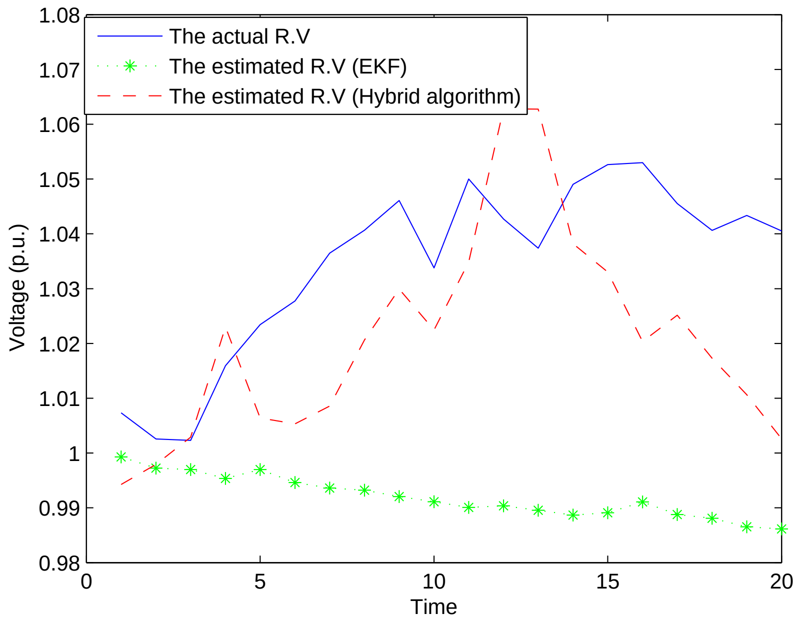


(a) The real part.

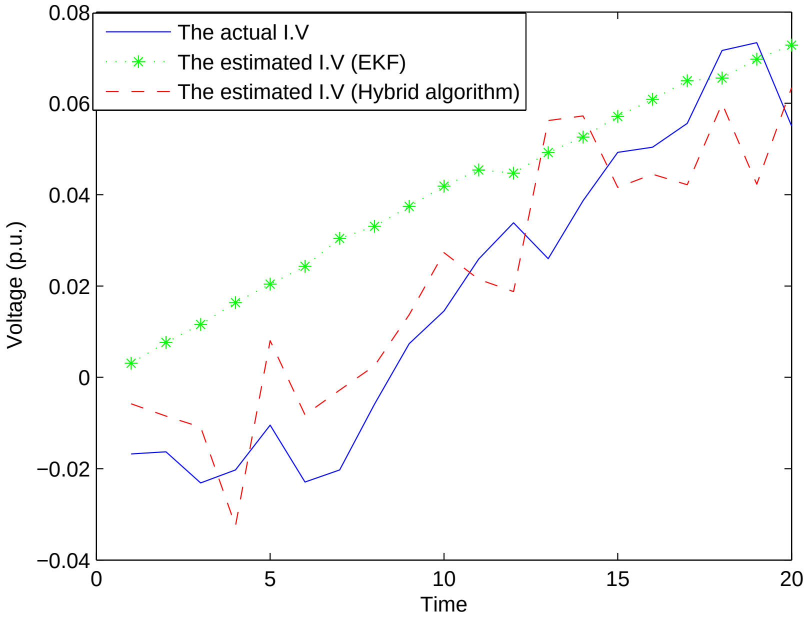


(b) The imaginary part.

Fig. 3.5 The estimated state at bus 2 by EKF and the proposed hybrid algorithm

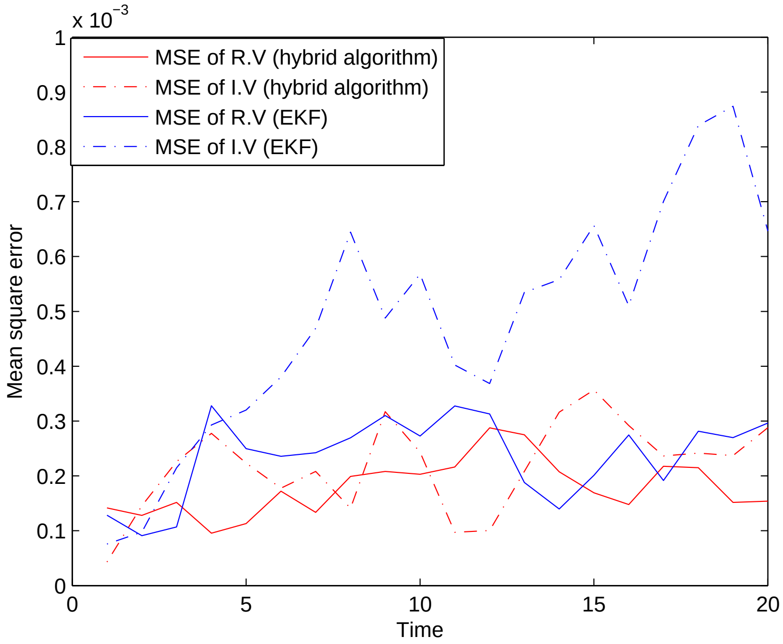


(a) The real part.

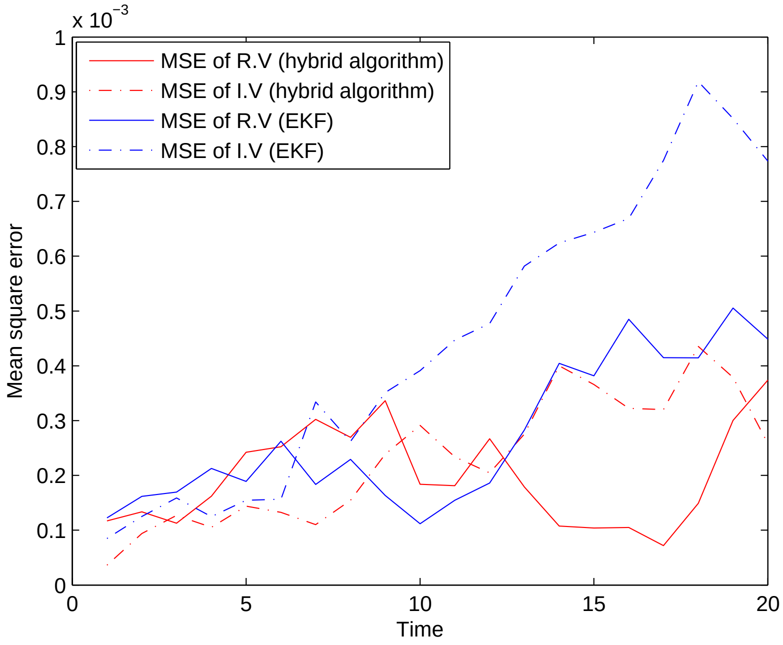


(b) The imaginary part.

Fig. 3.6 The estimated state at bus 5 by EKF and the proposed hybrid algorithm



(a) Bus 2.



(b) Bus 5.

Fig. 3.7 The MSEs of estimated states by EKF and the proposed hybrid algorithm

IEEE 14-bus test system and it is shown that the proposed algorithm gives much improved estimation performances over the traditional EKF method.

Chapter 4

Dynamic State Estimation of Power Grids with Quantization Effects: A Recursive Filter Approach

4.1 Motivation

Quantization phenomenon is ubiquitous in power systems. Considering the measurements in power systems, the readings provided by digital meters (e.g., PMU and RTU) are practically the quantized values converted by the analog-to-digital converter (ADC) from the continuous original measurement signals. Quantization by the ADC adds errors to the measurement values. Due to its effects on power system monitoring, the quantization error has attracted a great deal of research attention. In [96], the effects of ADC-induced quantization error on the recovery of harmonic amplitudes and phases have been examined by theoretical investigation and simulation validation in order to determine the error limits of the instrumentation system design for power system monitoring and harmonic power-flow measurement. In [25], it has been revealed that, despite its impressive dynamic range, the 12-bit state-of-the-art digital recorder is insufficient to achieve the required precision of the measured loss in high voltage thyristor valves.

To mitigate the effects on quantization errors, a seemly natural way is to evaluate and improve the measurement reliability by re-calibrating the measurements. In [166], the reliability issue of PMU has been investigated by taking into account the data uncertainty representing the quantization error. In order to enhance the overall accuracy of measurements in a power transmission system, several mathematical techniques have been utilized in [182] within an integrated calibration process. Furthermore, on the software side, new algorithms for power system monitoring and control have been developed in consideration of the effects of quantization errors. In [47], the authors have proposed a fault location algorithm and tested its performance against the quantization error introduced by ADCs. In [93], the inherent limitation of quantization errors incurred by low-precision sensors on the accuracy of estimated fault locations has been further investigated. In [3, 27], the quantization errors have been assumed to be a range uncertainty with uniform distribution and new least-square state estimation algorithms have been developed. However, such an assumption is quite coarse as no prior knowledge on quantization process is utilized.

On the other hand, todays' power system together with the tightly integrated hi-tech devices constitutes a complex networked cyber-physical system, for which some practical issues are emerging that have rarely been considered before for the traditional power systems. One of these issues is to do with the transmission of massive measurement data over the communication network with limited capacity. For example, PMUs update the measurements with high frequency, and this puts enormous strain on the communication and data processing infrastructure of the grid. It has been recently reported in [9] that, a single PMU can take up almost 10% of the bandwidth of the substation. Due to the limited bandwidth of the communication networks, the measurement signals in the networked environment are typically quantized before being transmitted to the substation, and such a network-induced quantization phenomenon (in addition to the aforementioned device-induced one) should be properly taken in account when designing DSEs.

It is worth pointing out that, in the communities of system control and signal processing, a series of theoretical results have been obtained on quantized control and estimation [44, 51, 50, 84, 138, 75, 167, 10]. In [44], it has been proved that the logarithmic quantizer performs better than the linear quantizer in the quantized control problem. The sector bound approach, which was first introduced in [51], has been extensively employed to solve the quantized control problem. Parallel to the quantized control problem, the quantized estimation problem has been widely investigated as well. In [50], the state estimation problem has been investigated for linear discrete-time systems with quantized measurements. In [75], a recursive filter has been designed for the systems with nonlinear dynamics subject to multiplicative noise, missing measurements and quantization effects such that the estimation error covariance has an upper bound. However, almost all published results on quantized estimation have been concerned with systems with the *linear* measurement model only. In reality, lots of practical systems have *nonlinear* measurements. Taking the power system as an example, the RTU measurements are strongly nonlinear with respect to the state variables, see Section 4.2 of this chapter for more details. As such, there is a gap between the theoretical results and the practical application of DSE design problems in power systems due to the quantization issue, and our aim of this chapter is to shorten this gap by initiating a study on this challenging issue.

Motivated by the above discussion, we aim to design a recursive filter algorithm for power systems with quantized nonlinear measurement. First, the quantized nonlinear measurement model of power systems is presented where the quantization is assumed to be of logarithmic type. In the filter design, the composite errors caused by linearization of nonlinear measurements and quantization effects are taken into consideration and represented by several norm-bounded uncertainty matrices. Subsequently, a recursive filter algorithm is designed for the system with the introduced uncertainties such that an upper bound of the estimation error is guaranteed and then minimized by appropriately designing the filter gains.

The remainder of this chapter is organized as follows. In Section 4.2, the dynamic model of power systems with quantized measurements is briefly introduced, and the structure of the proposed filter is presented. In Section 4.3, the gain matrices of the recursive filter are derived, which minimize the upper bound of the covariance matrix of the estimation errors, and the upper bound at each time instant is given explicitly. In Section 4.4, the results of case studies performed on the 14-bus IEEE benchmark system are presented and analyzed. Finally, the chapter is concluded in Section 4.5.

4.2 Problem Formulation and Preliminaries

4.2.1 Dynamic System Model

First, recall that the dynamic system model of the power system with both RTU and PMU measurements (without considering the quantized measurements) is described in (3.2) -(3.5) in Chapter 3.

Next, let's consider the quantization effect on measurements, where the map of the quantization process is given by

$$\tilde{z}(k) = q(z(k)) = [q_1(z^{(1)}(k))\ q_2(z^{(2)}(k))\ \ldots\ q_m(z^{(m)}(k))].$$

The quantizer is assumed to be of the logarithmic type, that is, for each $q_j(\cdot)(j = 1, 2, \ldots, m)$, the set of the quantization levels is described by

$$\mathscr{U}_j = \left\{ \pm u_i^{(j)}, u_i^{(j)} = \chi_j{}^i u_0^{(j)}, i = 0,\ \pm 1,\ \pm 2,\ \cdots \right\} \cup \{0\},$$
$$0 < \chi_j < 1, \quad u_0^{(j)} > 0,$$

where $\chi_j (j = 1,2,\ldots,m)$ is called the quantization density. Each of the quantization level corresponds to a segment such that the quantizer maps the whole segment to this quantization level. The logarithmic quantizer $q_j(\cdot)$ is defined as

$$q_j(z^{(j)}(k)) = \begin{cases} u_i^{(j)}, \ \frac{1}{1+\delta_j}u_i^{(j)} < z^{(j)}(k) \le \frac{1}{1-\delta_j}u_i^{(j)} \\ 0, \ z^{(j)}(k) = 0 \\ -q_j(-z^{(j)}(k)), \ z^{(j)}(k) < 0 \end{cases}$$

with $\delta_j = (1-\chi_j)/(1+\chi_j)$.

It can be easily seen from the above definition that $q_j(z^{(j)}(k)) = (1+\Delta_k^{(j)})z^{(j)}(k)$ for certain $\Delta_k^{(j)}$ satisfying $|\Delta_k^{(j)}| \le \delta_j$. According to the above transformation, the quantization effects have been transformed into sector-bounded uncertainties [51]. Defining $\Delta_k = \text{diag}\{\Delta_k^{(1)},\cdots,\Delta_k^{(m)}\}$, the measurement after quantization can be expressed as

$$\tilde{z}(k) = (I+\Delta_k)z(k). \tag{4.1}$$

By defining $\Lambda = \text{diag}\{\delta_1,\ldots,\delta_m\}$ and setting $F(k) = \Delta_k\Lambda^{-1}$, we can know that $F(k)$ is a real-value time-varying matrix satisfying $F(k)F^T(k) \le I$.

Remark 4.1 *As for state estimation with quantized measurements in power systems, the conventional way is to treat the quantization error as a range uncertainty with uniform distribution without in-depth characterization of the error [3, 27]. This assumption in quantization errors is quite coarse, hence making the estimation conservative. In addition, to the best of the author's knowledge, all the results on quantized PSSE have been done in the frame of static state estimation while none has been done in the frame of DSE, and this chapter initializes the first attempt on DSE with quantized measurements in power systems.*

4.3 Main Results

4.3.1 Filter Structure

In this chapter, we aim to design a filter with the following two properties: 1) the filter has a recursive structure and hence is suitable for online DSE in power systems; 2) despite the nonlinear measurement and quantization effects, the estimated state should be precise with a confidence interval, that is, the estimation error covariance should fall in a bounded interval. Meanwhile, we want to minimize such a bound by appropriately designing the filter gain at every time instant.

For the system (3.2) with measurement model (4.1), the recursive filter is designed as follows:

$$\begin{aligned} \hat{x}(k+1|k) &= A\hat{x}(k|k)+Bu && (4.2)\\ \hat{x}(k+1|k+1) &= \hat{x}(k+1|k)+K(k+1)\Big(\tilde{z}(k+1)-g(\hat{x}(k+1|k))\Big) && (4.3) \end{aligned}$$

where $\hat{x}(k+1|k+1)$ is the estimate of $x(k+1)$ with $\hat{x}(0|0)=\bar{x}(0)$, $\hat{x}(k+1|k)$ is the one-step state prediction at time instant k, $K(k+1)$ is the filter gain to be determined. The one-step prediction and filtering error and the corresponding covariance matrices are defined as

$$\begin{aligned} &\tilde{x}(k+1|k)=x(k+1)-\hat{x}(k+1|k),\\ &\Sigma(k+1|k)=\mathbb{E}\{\tilde{x}(k+1|k)\tilde{x}^T(k+1|k)\}\\ &\tilde{x}(k+1|k+1)=x(k+1)-\hat{x}(k+1|k+1),\\ &\Sigma(k+1|k+1)=\mathbb{E}\{\tilde{x}(k+1|k+1)\tilde{x}^T(k+1|k+1)\} \end{aligned} \tag{4.4}$$

Remark 4.2 *The filter presented above inherits the basic recursive structure of the Kalman filter, and hence it is suitable for online computation. However, due to the nonlinear RTU measurement function and the nonlinearity induced by quantization effects, to design an appropriate filter gain K is quite challenging, which is accomplished in the subsequent subsection.*

4.3.2 Filter Design

To introduce our main results, we need the following two lemmas.

Lemma 4.1 *[172] Given matrices A, H, F, and M with compatible dimensions such that $FF^T \leq I$. Let U be a symmetric positive-definite matrix and a be an arbitrary positive constant such that $a^{-1}I-MUM^T>0$, then the following matrix inequality holds:*

$$\begin{aligned} &(A+HFM)U(A+HFM)^T\\ &\leq A(U^{-1}-aM^TM)^{-1}A^T+a^{-1}HH^T. \end{aligned} \tag{4.5}$$

Lemma 4.2 *For $0\leq k\leq N$, suppose that $X=X^T>0$, $Y=Y^T>0$, $S_k(X)=S_k^T(X)\in\mathbb{R}^{n\times n}$. If*

$$S_k(Y)\geq S_k(X),\quad \forall X\leq Y, \tag{4.6}$$

then the solutions M_k and N_k to the following difference equations

$$M_{k+1}\leq S_k(M_k),\ N_{k+1}=S_k(N_k),\ M_0=N_0>0 \tag{4.7}$$

satisfy

$$M_k \leq N_k.$$

This lemma can be easily derived from Lemma 3.2 in [158], and hence the derivation is omitted here.

In this section, the filter is designed for the power system with quantized nonlinear measurements. First, the one-step prediction and filtering error covariances are calculated, wherein the specific difficulties caused by the composite of the measurement nonlinearity and the quantization are pointed out. Second, a special effort is made to cope with these difficulties in terms of some robust filtering techniques. At last, an upper bound of the filtering error covariance is obtained and a filter gain is designed to guarantee that such an upper bound is minimized.

To begin with, substituting (4.3) into (4.4), we have

$$\tilde{x}(k+1|k) = A\tilde{x}(k|k) + \omega(k), \tag{4.8}$$

and the corresponding covariance matrix is easily obtained,

$$\Sigma(k+1|k) = A\Sigma(k|k)A^T + W(k). \tag{4.9}$$

Similarly, the filtering error can be written as

$$\tilde{x}(k+1|k+1) = \tilde{x}(k+1|k) - K(k+1)(\tilde{z}(k+1) - g(\hat{x}(k+1|k)))$$

where

$$\begin{aligned} &\tilde{z}(k+1) - g(\hat{x}(k+1|k)) \\ =&q(g(x(k+1)) + v(k+1)) - g(\hat{x}(k+1|k)) \\ =&(I+\Delta_{k+1})(g(x(k+1)) + v(k+1)) - g(\hat{x}(k+1|k)). \end{aligned} \tag{4.10}$$

Expanding $g(x(k+1))$ in a Taylor series around $\hat{x}(k+1|k)$, we can have

$$\begin{aligned} g(x(k+1)) =&g(\hat{x}(k+1|k)) + G(k+1)\tilde{x}(k+1|k) \\ &+ o(|\tilde{x}(k+1|k)|) \end{aligned} \tag{4.11}$$

where $G(k+1) \triangleq \frac{\partial g(x)}{\partial x}|_{x=\hat{x}(k+1|k)}$ and $o(|\tilde{x}(k+1|k)|)$ represents the high-order terms of the Taylor series expansion. From the results of [22, 83], the high-order terms are transformed into the following easy-to-handle formulation:

$$o(|\tilde{x}(k+1|k)|) = C(k+1)\aleph(k+1)L(k+1)\tilde{x}(k+1|k) \tag{4.12}$$

where $C(k+1) \in \mathbb{R}^{m\times n}, L(k+1) \in \mathbb{R}^{n\times n}$ are problem-dependent scaling matrices, and $\aleph(k+1) \in \mathbb{R}^{n\times n}$ is an unknown time-varying matrix representing the linearization errors of the measurement model that satisfies

$$\aleph(k+1)\aleph^T(k+1) \leq I. \tag{4.13}$$

Combining the equations (4.10), (4.11), (4.12) and(4.13), we can obtain the filtering errors in the following form:

$$\begin{aligned}&\tilde{x}(k+1|k+1)\\ =&\Phi(k+1)\tilde{x}(k+1|k) - K(k+1)(I+\Delta_{k+1})v(k+1)\\ &-K(k+1)F(k+1)\Lambda g(\hat{x}(k+1|k))\end{aligned} \tag{4.14}$$

where

$$\begin{aligned}\Phi(k+1) \triangleq\ & I - K(k+1)\big(C(k+1)\aleph(k+1)L(k+1)\\ & G(k+1) + F(k+1)\Lambda G(k+1) + M(k+1)L(k+1)\big)\\ M(k+1) \triangleq\ & F(k+1)\Lambda C(k+1)\aleph(k+1)\end{aligned}$$

It can be easily found that $M(k+1)$ satisfies

$$M^T(k+1)M(k+1) \leq \gamma I \tag{4.15}$$

for certain scalar γ. To ensure the condition (4.15) is fulfilled, γ is chosen as $\gamma = 10\sigma_{\max}(\Lambda C)$, where $\sigma_{\max}(\cdot)$ indicates the maximum singular value (of a matrix). The covariance of the filtering error can be written as follows:

$$\begin{aligned}&\Sigma(k+1|k+1)\\ =&\Phi(k+1)\Sigma(k+1|k)\Phi^T(k+1)\\ &-\Phi(k+1)\tilde{x}(k+1|k)g^T(\hat{x}(k+1|k))\Lambda F^T(k+1)K^T(k+1)\\ &-K(k+1)F(k+1)\Lambda g(\hat{x}(k+1|k))\tilde{x}^T(k+1|k)\Phi^T(k+1)\\ &+K(k+1)F(k+1)\Lambda g(\hat{x}(k+1|k))g^T(\hat{x}(k+1|k))\Lambda F^T(k+1)K^T(k+1)\\ &+K(k+1)(I+F(k+1)\Lambda)R(k+1)(I+F(k+1)\Lambda)^T K^T(k+1)\end{aligned} \tag{4.16}$$

$$
\begin{aligned}
K(k+1) &= (1+\varepsilon_1)\big(P^{-1}(k+1|k)-\lambda_{1,k+1}\tilde{L}^T(k+1)\tilde{L}(k+1)\big)^{-1}G^T(k+1) \\
&\quad \times\Big[(1+\varepsilon_1)G(k+1)\big(P^{-1}(k+1|k)-\lambda_{1,k+1}\tilde{L}^T(k+1)\tilde{L}(k+1)\big)^{-1} \\
&\quad \times G^T(k+1)+(R^{-1}(k+1)-\lambda_{2,k+1}\Lambda\Lambda)^{-1}+\lambda_{2,k+1}^{-1}I+(1+\varepsilon_1)\lambda_{1,k+1}^{-1} \\
&\quad \times\tilde{C}(k+1)\tilde{C}^T(k+1)+(1+\varepsilon_1^{-1})\mathrm{tr}\big(\Psi(k+1|k)I\big)\Big]^{-1}, \qquad (4.17)\\
P(k+1|k) &= AP(k|k)A^T+W(k), \qquad (4.18)\\
P(k+1|k+1) &= (1+\varepsilon_1)(I-K(k+1)G(k+1))\times \\
&\quad \big(P^{-1}(k+1|k)-\lambda_{1,k+1}\tilde{L}^T(k+1)\tilde{L}(k+1)\big)^{-1}(I-K(k+1)G(k+1))^T \\
&\quad +(1+\varepsilon_1)\lambda_{1,k+1}^{-1}K(k+1)\tilde{C}(k+1)\tilde{C}^T(k+1)K^T(k+1) \\
&\quad +(1+\varepsilon_1^{-1})K(k+1)\mathrm{tr}\big(\Psi(k+1|k)\big)K^T(k+1) \\
&\quad +K(k+1)\Big[(R^{-1}(k+1)-\lambda_{2,k+1}\Lambda\Lambda)^{-1}+\lambda_{2,k+1}^{-1}I\Big]K^T(k+1). \qquad (4.19)
\end{aligned}
$$

The main result of this section is summarized in the following theorem.

Theorem 4.1 *Consider the one-step prediction error and the filtering error covariances in (4.9) and (4.16), respectively. Assume that (4.13) holds. Let γ, $\lambda_{1,k}$, $\lambda_{2,k}$ and ε_1 be positive scalars, and $K(k)$ be calculated recursively shown in (4.17) at the top of this page. If there exist positive-definite solutions $P(k+1|k)$, $P(k+1|k+1)$ with initial condition $P(0|0)=\Sigma(0|0)$ to the Riccati difference equations shown in (4.18)-(4.19) at the top of the next page, subject to*

$$
\begin{cases}
\lambda_{1,k+1}^{-1}I-\tilde{L}(k+1)P(k+1|k)\tilde{L}^T(k+1)>0 \\
\lambda_{2,k+1}^{-1}I-\Lambda R(k+1)\Lambda>0
\end{cases} \tag{4.20}
$$

where

$$\tilde{L}(k+1)\triangleq\big[L^T(k+1)\ (\Lambda G(k+1))^T\ L^T(k+1)\ \big]^T \tag{4.21}$$

$$\tilde{C}(k+1)\triangleq[C(k+1)\ \ I\ \ \gamma I] \tag{4.22}$$

$$\Psi(k+1|k)\triangleq\Lambda g(\hat{x}(k+1|k))g^T(\hat{x}(k+1|k))\Lambda \tag{4.23}$$

then the matrix $P(k|k)$ is an upper bound for $\Sigma(k|k)$, that is,

$$\Sigma(k|k)\leq P(k|k).$$

Moreover, the filter with gain $K(k+1)$ given by (4.17) minimizes the upper bound $P(k|k)$.

Proof. To begin with, from (4.18) and (4.19), we can view the covariance matrices $P(k+1|k+1)$ as a function of $P(k|k)$, that is

$$P(k+1|k+1) = \varphi_k\{P(k|k)\} \tag{4.24}$$

where $\varphi_k\{\,\cdot\,\}$ denotes the specific functional relationship between $P(k+1|k+1)$ and $P(k|k)$. Then, it is not difficult to verify that

$$\varphi_k(Y) \geq \varphi_k(X), \tag{4.25}$$

for all $X \leq Y$, $X = X^T > 0$, and $Y = Y^T > 0$.

Now, let's consider the right side of (4.16) term by term. Representing $\Phi(k+1)$ in the following form:

$$\begin{aligned}
&\Phi(k+1)\\
=&I - K(k+1)G(k+1) - K(k+1)\tilde{C}(k+1)\\
&\times \begin{bmatrix} \aleph(k+1) & 0 & 0 \\ 0 & F_{k+1} & 0 \\ 0 & 0 & 1/\gamma M(k+1) \end{bmatrix} \tilde{L}(k+1)
\end{aligned}$$

from Lemma 6.1, we can obtain

$$\begin{aligned}
&\Phi(k+1)\Sigma(k+1|k)\Phi^T(k+1)\\
\leq&\big(I - K(k+1)G(k+1)\big)\big(\Sigma^{-1}(k+1|k)\\
&-\lambda_{1,k+1}\tilde{L}^T(k+1)\tilde{L}(k+1)\big)^{-1}\big(I - K(k+1)G(k+1)\big)^T\\
&+\lambda_{1,k+1}^{-1}K(k+1)\tilde{C}(k+1)\tilde{C}^T(k+1)K^T(k+1)
\end{aligned} \tag{4.26}$$

if

$$\lambda_{1,k+1}^{-1}I - \tilde{L}(k+1)P(k+1|k)\tilde{L}^T(k+1) > 0$$

for arbitrary positive scalars $\lambda_{1,k+1}$.

Recall the following fundamental inequality

$$ab^T + ba^T \leq \varepsilon_1 aa^T + \varepsilon_1^{-1}bb^T \tag{4.27}$$

where $\varepsilon_1 > 0$ is a scalar, a and b are two vectors with arbitrary dimension. Taking (4.27) into consideration, and noticing $F(k+1)F^T(k+1) \leq I$, the second and third terms on the right side of (4.16) can be rearranged as follows:

$$\begin{aligned}&-\Phi(k+1)\tilde{x}(k+1|k)g^T(\hat{x}(k+1|k))\Lambda F^T(k+1)K^T(k+1)\\&-K(k+1)F(k+1)\Lambda g(\hat{x}(k+1|k))\tilde{x}^T_{k+1|k}\Phi^T(k+1)\\&\leq \varepsilon_1\Phi(k+1)\Sigma(k+1|k)\Phi^T(k+1)\\&+\varepsilon_1^{-1}K(k+1)F(k+1)\Psi(k+1|k)F^T(k+1)K^T(k+1)\\&\leq \varepsilon_1\Phi(k+1)\Sigma(k+1|k)\Phi^T(k+1)\\&+\varepsilon_1^{-1}K(k+1)\mathrm{tr}(\Psi(k+1|k))K^T(k+1)\end{aligned} \tag{4.28}$$

Similarly, the fourth term on the right side of (4.16) can be tackled as follows:

$$\begin{aligned}&K(k+1)F(k+1)\Lambda g(\hat{x}(k+1|k))\\&\quad\times g^T(\hat{x}(k+1|k))\Lambda F^T(k+1)K^T(k+1)\\&\leq\ K(k+1)\mathrm{tr}\big(\Psi(k+1|k)\big)K^T(k+1).\end{aligned} \tag{4.29}$$

As to the last term of the right side of (4.16), the following inequality can be easily derived from Lemma 6.1,

$$\begin{aligned}&K(k)(I+F(k)\Lambda)R(k)(I+F(k)\Lambda)^TK^T(k)\\&\leq K(k)\big[(R^{-1}(k)-\lambda_{2,k}\Lambda\Lambda)^{-1}+\lambda_{2,k}^{-1}I\big]K^T(k)\end{aligned} \tag{4.30}$$

if

$$\lambda_{2,k}^{-1}I-\Lambda R(k)\Lambda > 0$$

for arbitrary positive scalars $\lambda_{2,k+1}$.

It then follows from (4.26), (4.28), (4.29) and (4.30) that

$$\begin{aligned}&\Sigma(k+1|k+1)\\&\leq\ (1+\varepsilon_1)\big(I-K(k+1)G(k+1)\big)\\&\quad\times\big(\Sigma^{-1}(k+1|k)-\lambda_{1,k+1}\tilde{L}^T(k+1)\tilde{L}(k+1)\big)^{-1}\big(I-K(k+1)G(k+1)\big)^T\\&\quad+(1+\varepsilon_1)\lambda_{1,k+1}^{-1}K(k+1)\tilde{C}(k+1)\tilde{C}^T(k+1)K^T(k+1)\\&\quad+(1+\varepsilon_1^{-1})K(k+1)\mathrm{tr}\big(\Psi(k+1|k)\big)K^T(k+1)\\&\quad+K(k+1)\big[\big(R^{-1}(k+1)-\lambda_{2,k+1}\Lambda\Lambda\big)^{-1}+\lambda_{2,k+1}^{-1}I\big]K^T(k+1)\end{aligned} \tag{4.31}$$

In other words, we have obtained that $\Sigma(k+1|k+1) \leq \varphi_k\big\{\Sigma(k|k)\big\}$. Recall the condition (4.24) and (4.25). Based on Lemma 6.2, we can therefore conclude that

$$\Sigma(k|k) \leq P(k|k).$$

Having determined the upper bound $P(k|k)$, we are now ready to show the filter gain given by (4.17) is optimal as it minimizes the upper bound $P(k|k)$. Taking partial derivatives of $P(k+1|k+1)$ with respect to $K(k+1)$ as follows:

$$\begin{aligned}
&\frac{\partial tr\big(P(k+1|k+1)\big)}{\partial K(k+1)} \\
=&-2(1+\varepsilon_1)\big(I-K(k+1)G(k+1)\big) \\
&\big(P^{-1}(k+1|k)-\lambda_{1,k+1}\tilde{L}^T(k+1)\tilde{L}(k+1)\big)^{-1}G^T(k+1) \\
&+2(1+\varepsilon_1)\lambda_{1,k+1}^{-1}K(k+1)\tilde{C}(k+1)\tilde{C}^T(k+1) \\
&+2(1+\varepsilon_1^{-1})K(k+1)\mathrm{tr}\big(\Psi(k+1|k)\big) \\
&+2K(k+1)\big[(R^{-1}(k+1)-\lambda_{2,k+1}\Lambda\Lambda)^{-1}+\lambda_{2,k+1}^{-1}I\big]
\end{aligned} \tag{4.32}$$

and setting $\frac{\partial tr(P(k+1|k+1))}{\partial K(k+1)}=0$, through some straightforward algebraic manipulation, we obtain the optimal filter gain, as shown in (4.17). This completes the proof of Theorem 1. ■

Remark 4.3 *It can be seen that the linearization has been enforced to facilitate the recursive filtering algorithm developments. From (4.9) and (4.16), the filtering error covariance can be obtained in consideration of the quantization effect. Unfortunately, due to the simultaneous presences of the measurement nonlinearity and the quantization, the uncertainty matrices* $\aleph(k)$*,* $M(k)$*, and* $F(k)$ *are involved in the error covariance in (4.16). As such, it is impossible to calculate the accurate covariance matrix* $\Sigma(k|k)$*, and an alternative approach is proposed to find an upper bound of the covariance matrix at every time instant through designing an appropriate filtering gain* $K(k|k)$ *for the filter.*

4.4 Simulation Results

In this section, as did in Chapter 3, the proposed algorithm is tested in the case study of the IEEE 14-bus test system. The simulation is implemented in Matlab with the Matpower package[190]. First, the IEEE 14-bus test system can be model as (3.2) with parameters $A=\mathrm{diag}_{28}\{0.98\}$, $B=\mathrm{diag}_{28}\{0.02\}$ and $W(k)=\mathrm{diag}_{28}\{0.1^2\}$. The nominal centre u of the normal state is the base-case voltages given in Table 3.1 in Chapter 3. Furthermore, assume that the initial voltages of all buses are at flat start, that is, $x_{r,l}(0) = 1$ p.u, $x_{i,l}(0) = 0$ for all $l = 1, 2, \ldots, 14$, and $\Sigma(0|0) = 10^{-4}I_{28}$.

The measurement configuration is shown in Fig. 4.1, which has been adopted in [94]. The measurement system includes both conventional RTUs and PMUs, in which RTU measurements consist of three categories: the voltage magnitude at bus 1, power injections at the bus 3, 5, 13 and 14, and power flows at branches 1-2, 1-5, 2-5, 3-4, 4-7, 4-9, 6-11, 6-12, 6-13, 7-8, 7-9, 9-10, 9-14, 10-11, 12-13 and 13-14, and PMUs are deployed at buses 2, 7 and 9. Furthermore, the covariance matrices of RTU and PMU measurement noise are $R_1(k) = \text{diag}_{43}\{0.1^2\}$ and $R_2(k) = \text{diag}_{28}\{0.01^2\}$, respectively.

In the simulation, the default parameters are chosen as $C(k) = \begin{bmatrix} 0.01I_{28\times 43} & 0_{28} \end{bmatrix}^T, L(k) = 0.001I_{28}, \varepsilon_1 = 0.6, \lambda_{1,k} = 0.01, \lambda_{2,k} = 100$, if not specifically mentioned. The parameters of the logarithmic quantizers are $u_0^i = 1$ and $\chi_i = 0.8$, for $i = 1, \ldots, 71$.

Of all the buses, we choose bus 7 and 11 as the representative buses, as both PMU and RTU are installed at bus 7 while only RTU at bus 11. In this test system, two experiments regarding the estimation accuracy are carried out as follows:

Case 1) The proposed filter is implemented for the system with quantized measurements;

Case 2) The state estimations based on the proposed quantized filter and the traditional EKF without considering quantization effects are compared.

In order to have more general and significant experimental results, 100 Monte-Carol simulations are run. The notion mean square error (MSE) is adopted to evaluate the estimation accuracy, where MSE_i denotes MSE for the estimate of the ith state, i.e. $\text{MSE}_i(k) = \frac{1}{100}\sum_{j=1}^{100}(x_i(k) - \hat{x}_i(k))^2$. To evaluate the average estimation performance of all states, average mean square error (AMSE) is defined as $\text{AMSE}(k) \triangleq \frac{1}{n}\sum_{j=1}^{n}\text{MSE}_j(k)$, where n is the number of the state variables. In all the figures, "R.V" and "I.V" denote the real and imaginary parts of voltage, respectively.

4.4.1 Estimation Performance of the Proposed Filter

In this case, both the RTU and PMU measurements are assumed to be quantized according to the same quantizer level.

The algorithm is implemented in Matlab R2010a. The simulation is performed on a PC with a Intel(R) Core(TM) CPU i5-2500 @3.30 GHz and 4 GB RAM. The algorithm is run for 30 time steps, The corresponding time required by the algorithm is 61.5 seconds. We can conclude that the algorithm is quite fast and hence is suitable for online implementations.

In Fig. 4.2, $P_{7,8}$ is the RTU measurement of active power flow from bus 7 to bus 8, while $I_{7,8}$ is the PMU measurement of the real part of the current from bus 7 to bus 8. From

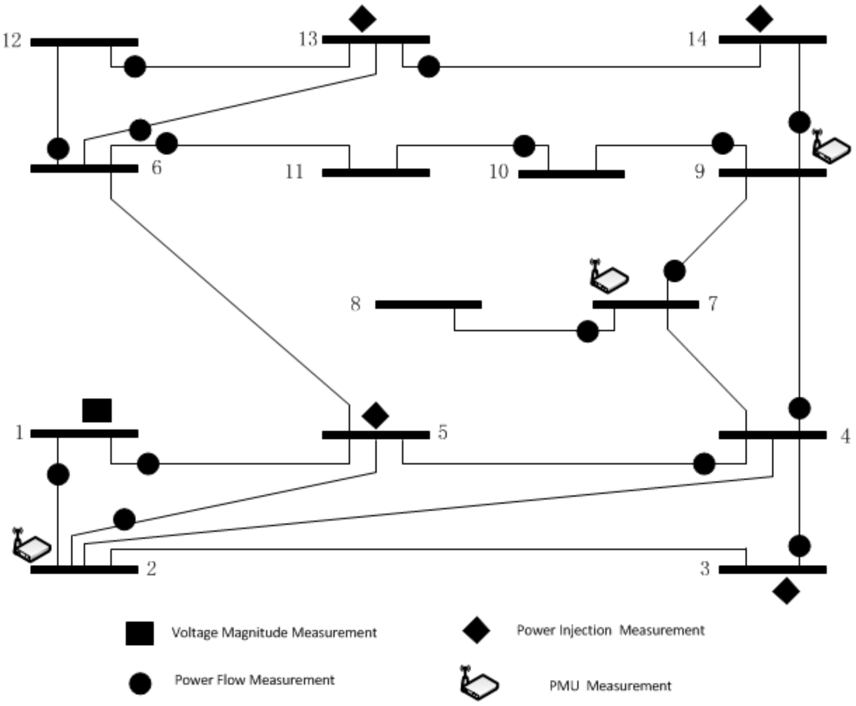


Fig. 4.1 IEEE 14 bus system and measurement configuration

the comparison, we can see that even with the same quantization level, the quantized RTU measurement is less accurate than the PMU counterpart. This is due to the nonlinearity of RTU measurement model which aggravates the quantization errors of RTU measurements, as the PMU measurements are linear functions of state variables while the RTU measurements are nonlinear functions of state variables.

Fig. 4.3 shows the log(MSE) for the state at bus 7 and 11 as well as the upper bound, which confirms that the MSEs stay below their upper bounds. That means the estimated voltages of the systems are always close to the real values with a known upper bound on the estimate error. Moreover, to show how the parameter $L(k)$ affects the upper bound of error covariance, different values of $L(k)$ are considered. From Fig. 4.4, it can be seen that, the upper bound of of error covariance with $L(k) = 0.01 * I$ and the one with with $L(k) = 0.001 * I$ are almost the same, but the one with with $L(k) = 0.1 * I$ are larger than the former two. Since the value of parameter $L(k)$ reflects the linearisation error of the measurement function, we can conclude that the performance of our algorithm is related to the linearisation error and generally the smaller the linearisation error is, the less conservative the upper bound is.

The trajectories of the actual state $x_j(k), j = 7, 11$ and their estimation are plotted in Fig. 4.5, which illustrate the good performance of our proposed algorithm in estimating the system states. This is due to the specific efforts we have made to compensate the linearization errors of the nonlinear measurements as well as the quantization errors.

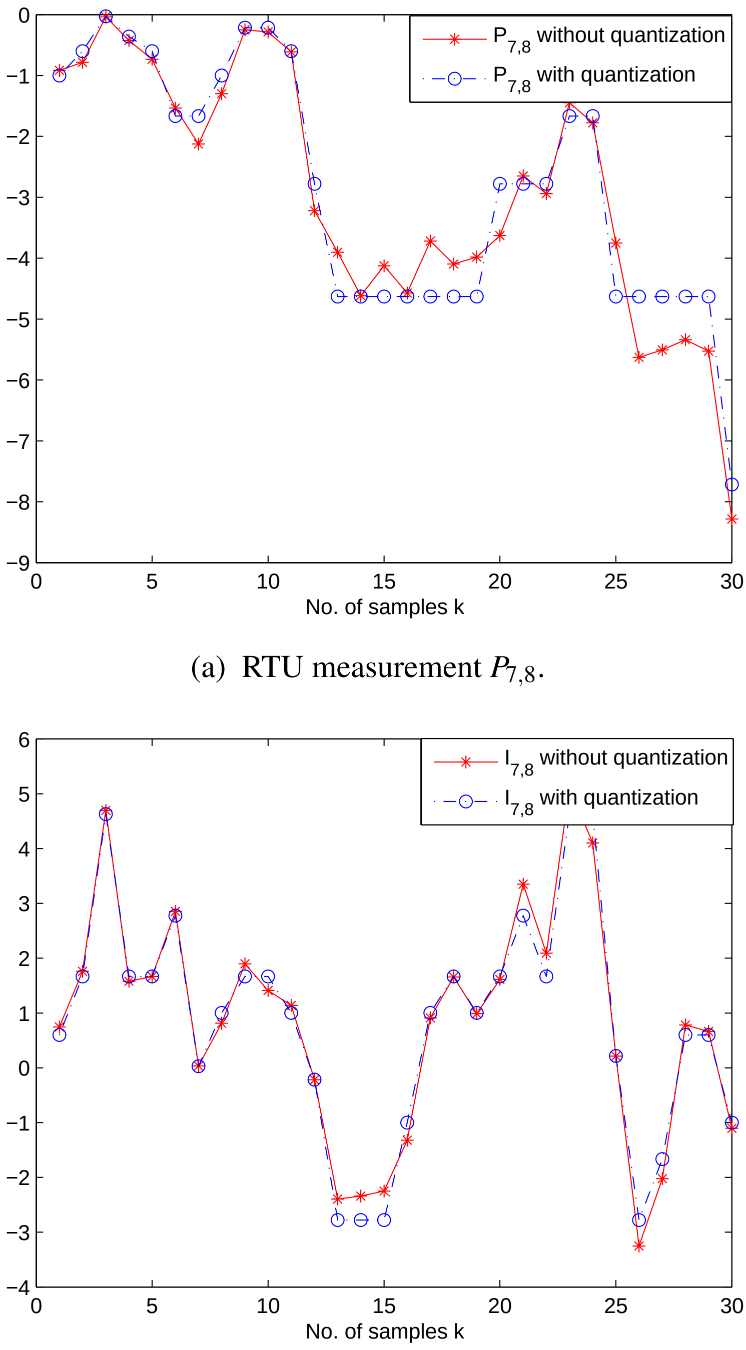
4.4.2 Traditional EKF VS the Proposed Filter

In Fig. 4.6, the estimation performances of the standard EKF and our proposed quantized filter algorithm are compared. In our simulation settings, the system parameters are given. In this case, the traditional FASE [98] implemented in the test system reduces to the traditional EKF. In this sense, We have compared the performance of proposed filter with that of the traditional approach to FASE [98] in the simulation.

One realization of the EKF and one realization of the proposed algorithm are simulated simultaneously, and the estimate errors of the real part of the voltage at bus 7 at both cases are illustrated in Fig. 4.6. We can find that, during the most of the time, the estimate error of EKF-based state estimation is bigger than the one of our proposed algorithm. Especially, when the accumulated error of EKF-based state estimation becomes bigger after several integrations, our proposed algorithm still yields accurate estimated states without accumulating the errors. The AMSEs of EKF and of the proposed algorithm are plotted in Fig. 4.6, from which we can find that our proposed algorithm performs much better than the EKF one. This is because the traditional EKF is sensitive to the quantization and linearization errors in measurements. However, due to specific considerations of these errors of measurement model and the designed robust filter gain, our proposed algorithm performs better.

4.5 Conclusion

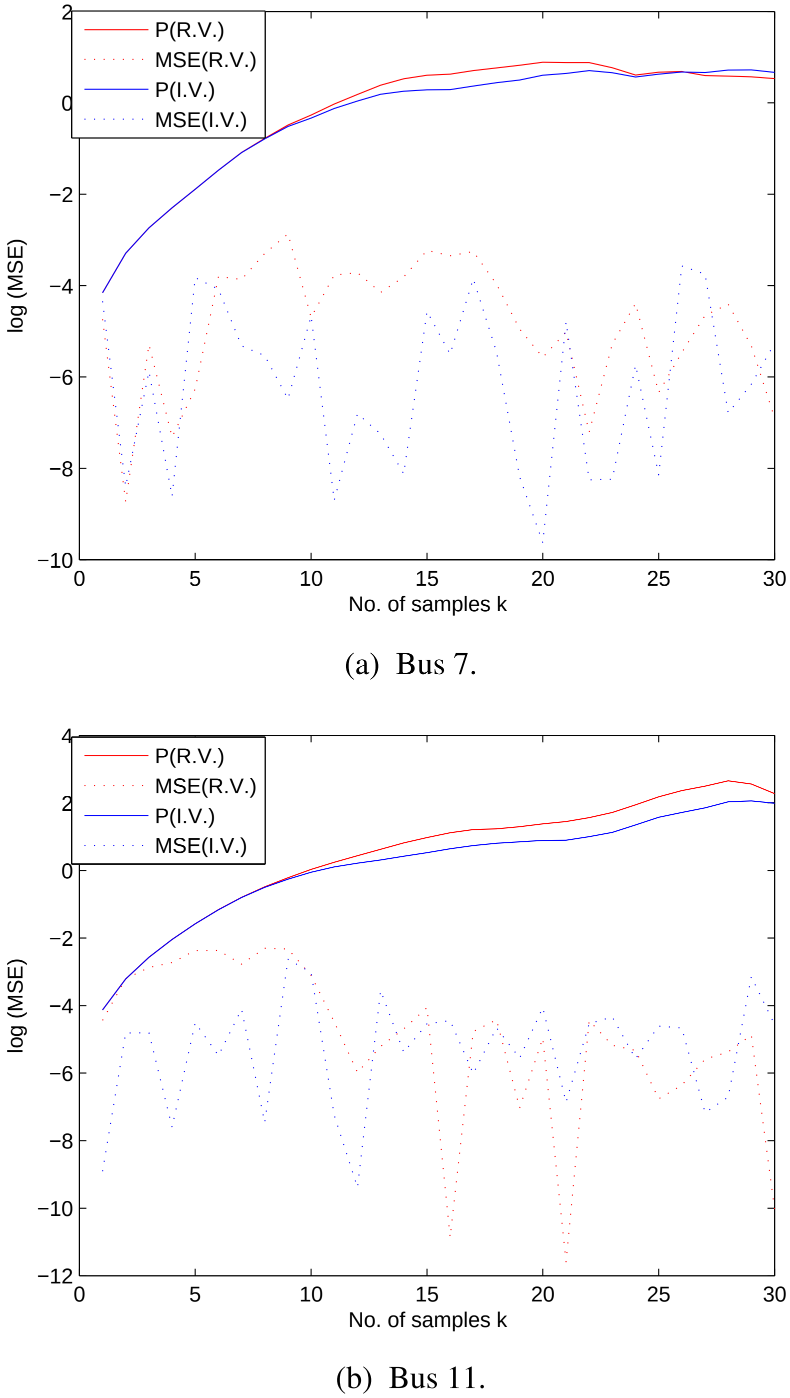
In this chapter, we have developed a recursive filter algorithm for power system dynamic state estimation. The system model with quantized RTU and PMU measurements is first proposed. In consideration of the quantization effect of nonlinear measurement, both the linearization and quantization errors are represented in terms of norm-bounded uncertainty matrices. Then, in the frame of robust estimation, a recursive filter is designed to guarantee that, despite the uncertainties existing in the derived model, the estimation error covariances are always less than a finite upper bound. Furthermore, the filter gain is designed such that the upper bound is minimized. Simulations have illustrated the performance of our proposed algorithm. Higher estimation accuracy can be achieved with our algorithm than that from the traditional EKF algorithm, which has confirmed the effectiveness of the propose filter algorithm.



(a) RTU measurement $P_{7,8}$.

(b) PMU measurement $I_{7,8}$.

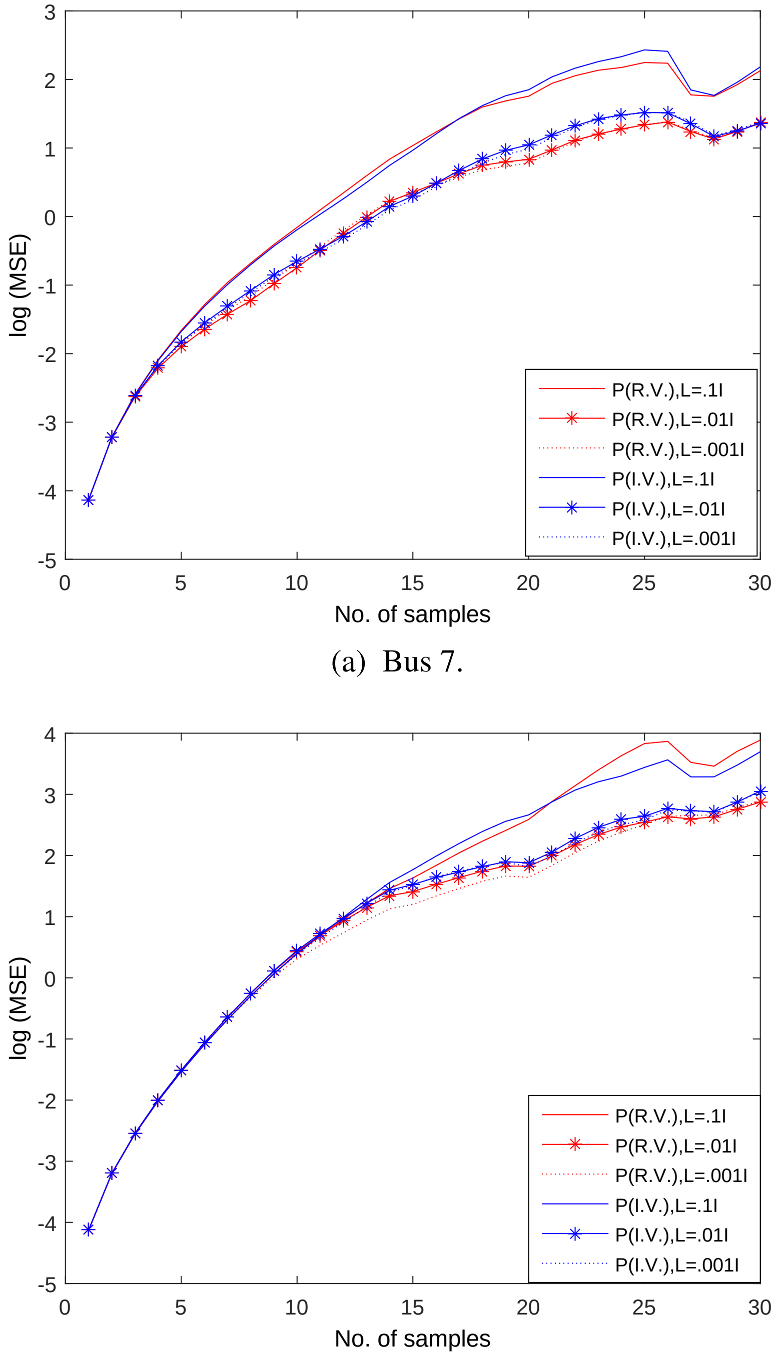
Fig. 4.2 The measurements with/without quantization



(a) Bus 7.

(b) Bus 11.

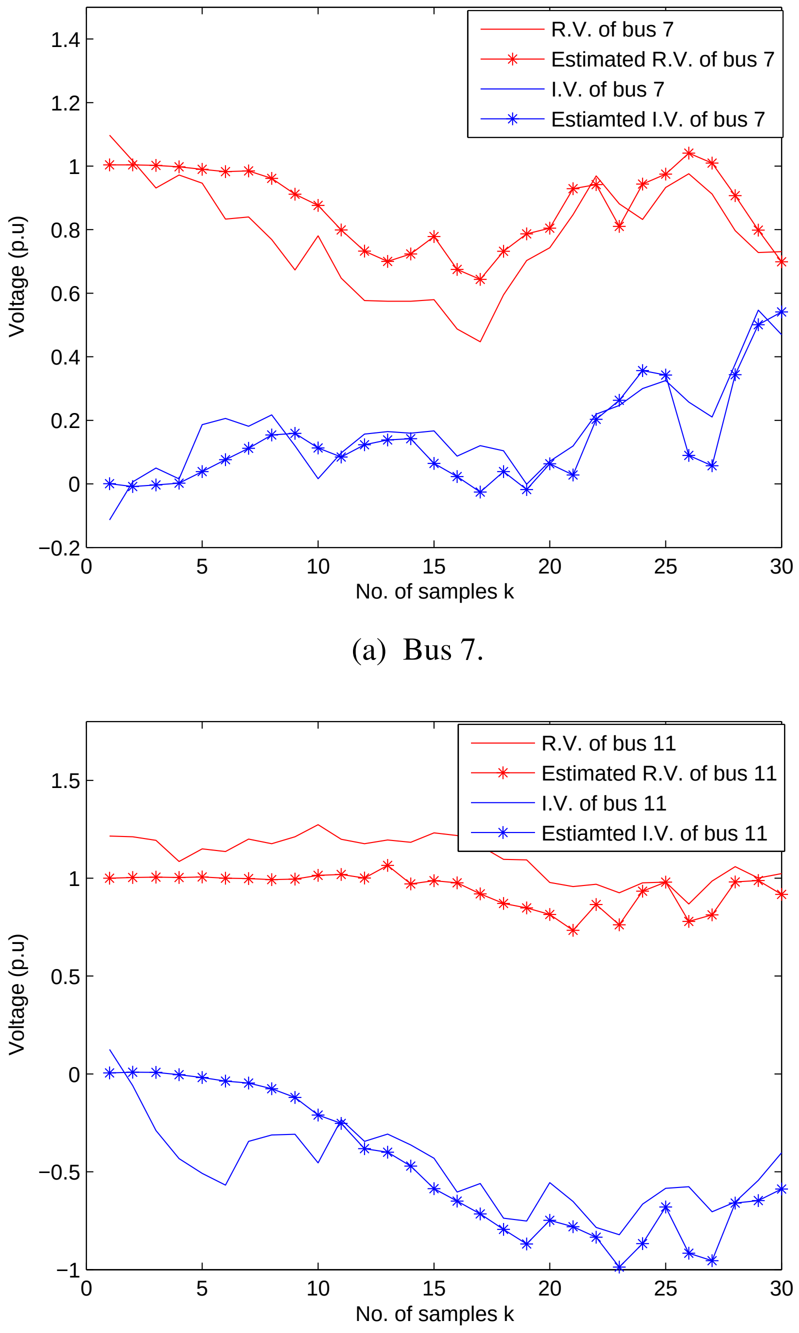
Fig. 4.3 Log(MSE) and its upper bound



(a) Bus 7.

(b) Bus 11.

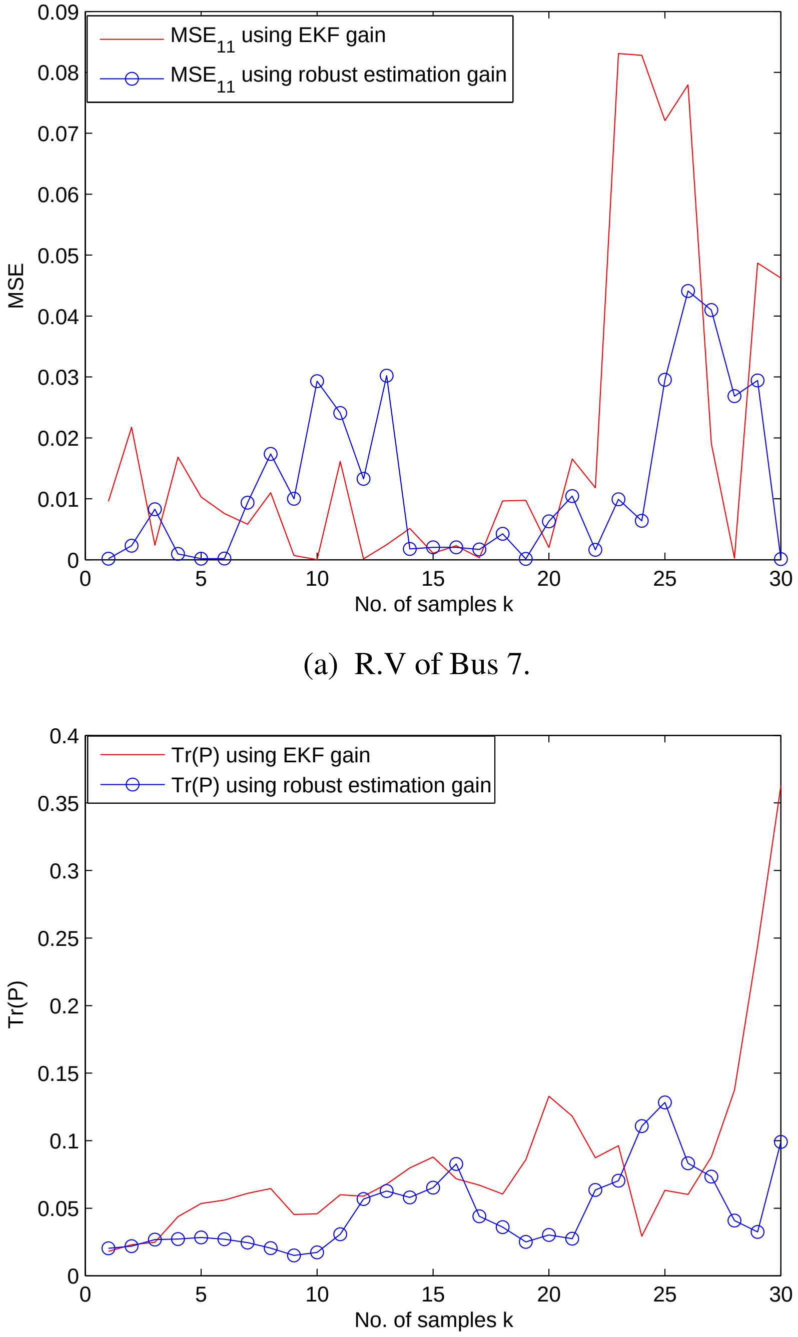
Fig. 4.4 The upper bound under different parameters $L(k)$



(a) Bus 7.

(b) Bus 11.

Fig. 4.5 The actual state and its estimation



(a) R.V of Bus 7.

(b) AMSE of all states.

Fig. 4.6 The estimate error comparison

Chapter 5

Event-triggered Input and State Estimation for Power Grids

5.1 Motivation

The extended Kalman filter has been widely used to estimate the state of the power grid, and accurate state estimates can be obtained if the exact values of the system parameters and the input/output data are known [8]. However, the exogenous input, which represents the unknown disturbances or unmodeled dynamics, may not be known a prior. In this case, both the traditional Kalman filter and the H_∞ filter [11, 168, 39, 74] do not yield an optimal state estimation. As such, a new kind of filter, which is applicable for power grids with unknown inputs, is desirable.

Motivated by it wide range of applications of the state and unknown input estimation, considerable research efforts have been devoted to optimal filtering in the presence of unknown inputs during the last few years [92, 35, 36, 31, 73, 58]. Recently, the unknown input state estimation algorithms have been applied in power systems [53, 15]. However, all the results has implicitly adopted the time based strategy. That is, the meters send the measurement data to the state estimator at a fixed time interval. However, as discussed in previous two chapters, in this case networked-induced phenomena such as missing and quantized measurements may occur especially when the bandwidth of the communication networks in power grids is limited and precious [65, 66].

Governed by the event-based strategy, a sensor is triggered to send the measurement data if and only if some events occur. The event-based strategy provides the possibility to maintain system performance under limited communication resources and has attracted considerable research attention for the past decade. Accordingly, the event-based state estimation problem has been investigated extensively [107, 108, 69, 115, 153, 142, 139, 77, 184]. However, the event-based transmission scheme complicates the estimation problem considerably, especially when no measurements are received by the estimator between two consecutive event-triggered instants. As such, the Gaussian approximation is a typical assumption in the existing work. For example, in [153], a modified Kalman filter has been proposed for the discrete time-invariant system with a send-on-delta (SOD) event triggering mechanism; in [142], with a general description of the event-based strategy, an event-based estimator has been designed for the discrete time-invariant system using Gaussian sum approximations; the maximum likelihood event-based estimation problem has been investigated in [139]. This assumption simplifies the estimator development, but makes the estimator with only approximate minimum mean square error. In this chapter, we try to develop the estimator and investigate the estimation performance without making such an assumption.

Summarizing the above discussion, although the event-based estimation problem has been investigated for the linear system, the corresponding estimation problem for the power grids *with unknown input* has not yet been investigated due mainly to the difficulty in handling the unknown input with no prior information. In addition, when the adoption of the event-based mechanism, the unbiasedness of both the input and the state estimate cannot be guaranteed in general, and the traditional time-based unbiased input/state estimator design methods are no longer applicable. As such, we are motivated to challenge the design problem of the joint input/state estimators according to the event-based strategy by employing a SOD concept [117]. Our aim is to the joint input/state estimates that are precise within a known confidence interval even though only partial measurements at the event-triggered instants are accessible by the estimator.

The remainder of this chapter is organized as follows. In Section 5.2,a general linear time-varying system with unknown inputs is briefly introduced, and the structure of the proposed filter is presented. In Section 5.3, An algorithm is proposed to choose scalar parameters which facilitates the estimator design, and the filter gain is chosen to minimize the upper bound of the covariance matrix of the estimation errors. In Section 5.4, the asymptotic boundedness of the obtained upper bounds is analysed for the time-invariant linear systems. The results of case studies performed on a three-bus power grids are presented and analysed in Section 5.5. Finally, the chapter is concluded in Section 5.6.

5.2 Problem Formulation and Preliminaries

In the section, we first consider the following linear discrete-time system which describes the dynamics of the power grid:

$$\begin{cases} x(k+1) = A(k)x(k) + G(k)d(k) + \omega(k) \\ \quad y(k) = C(k)x(k) + \nu(k) \end{cases} \tag{5.1}$$

where $x(k) \in \mathbb{R}^n$ is s the vector of the real parts and the imaginary parts of the voltages at all buses in the rectangular form, $d(k) \in \mathbb{R}^p$ is the unknown system input and $y(k) \in \mathbb{R}^m$ is the PMU measurement output. The initial value $x(0)$ has mean $\bar{x}(0)$ and covariance $P(0|0)$, the process noise $\omega(k) \in \mathbb{R}^n$ and the measurement noise $\nu(k) \in \mathbb{R}^m$ are assumed to be mutually uncorrelated, zero-mean random signals with known covariance matrices $W(k)$ and $R(k)$, respectively. We assume that $m \geq p$ and, without loss of generality, $\mathrm{Rk}\{C(k)G(k-1)\} = \mathrm{Rk}\{G(k)\} = p$.

Remark 5.1 *Comparing* (5.1) *with the dynamic model used to describe the system dynamics of the power grid in Chapter 3, it can be found that the linear system model in* (5.1) *is more general. In* (5.1)*, the input $u(k)$ is not assumed to be known beforehand but instead is estimated in real time.*

5.2.1 Traditional Unknown Input and State Estimator

Up to now, lots of results have been developed with respect to the estimation problem with unknown input. The traditional unknown input and state estimator has the following general form:

$$\mathscr{E}_1 : \begin{cases} \hat{d}_t(k-1) = M_t(k)\big(y(k) - C(k)A(k-1)\hat{x}_t(k-1|k-1)\big) \\ \hat{x}_t(k|k-1) = A(k-1)\hat{x}_t(k-1|k-1) + G(k-1)\hat{d}_t(k-1) \\ \hat{x}_t(k|k) = \hat{x}_t(k|k-1) + K_t(k)\big(y(k) - C(k)\hat{x}_t(k|k-1)\big) \end{cases} \tag{5.2}$$

where $\hat{d}_t(k-1)$ is the estimate of the unknown input at time instant $k-1$, $\hat{x}_t(k|k-1)$ is the one-step prediction of $x(k)$ at time instant $k-1$, and $\hat{x}_t(k|k)$ is the estimate of $x(k)$ at time instant k with $\hat{x}_t(0|0) = \bar{x}(0)$. $M_t(k)$ and $K_t(k)$ are the estimator gain matrices to be determined at time instant k.

So far, to the best of the author's knowledge, almost all established results on unknown input and state estimation problem have been obtained according to the time-based mechanism whose idea is to send the measurements to the estimator at every time instant. Due to the resource limits on energy-consumption and communication bandwidth especially in wireless communication, the control system needs more energy-efficient and lower bitrate data transmission mechanisms than the time-based one. The event-based data transmission mechanism stands out as a promising solution to this issue because, with such a mechanism, only important measurements (rather than all measurements) are transmitted to accomplish the control/estimation tasks.

5.2.2 Event-based Unknown Input and State Estimator

In order to reduce the energy consumption and communication burden, the measurement $y(k)$ is transmitted only when certain event generator is triggered. In this chapter, the send-on-delta (SOD) triggering mechanism is adopted and characterized as follows.

Assume that the event triggering instants are $k_0, k_1, \ldots$, where $k_0 = 0$ is the initial time. Define $y_e(k) = y(k_j)$ for $k \in [k_j, k_{j+1})$ with the subscript "e" indicating event triggering. The sequence of event triggering instants $0 = k_0 \leq k_1 \leq \cdots \leq k_i \leq \ldots$ is determined iteratively by

$$k_{i+1} = \min\{k \in \mathbb{N} | k > k_i, \|y_e(k) - y(k)\| > \sigma\} \tag{5.3}$$

where the threshold σ is a positive scalar.

Define $\delta(k) = y(k) - y_e(k)$. Under the event-based strategy, $\delta(k)$ will be reset to zero if the triggering condition is fulfilled. Consequently, the following inequality holds all the time:

$$\delta^T(k)\delta(k) \leq \sigma. \tag{5.4}$$

With the event-based communication strategy, a recursive estimator for the system (5.1) as follows:

$$\mathscr{E}_2 : \begin{cases} \hat{d}_e(k-1) = M_e(k)\big(y_e(k) - C(k)A(k-1)\hat{x}_e(k-1|k-1)\big) \\ \hat{x}_e(k|k-1) = A(k-1)\hat{x}_e(k-1|k-1) + G(k-1)\hat{d}_e(k-1) \\ \hat{x}_e(k|k) = \hat{x}_e(k|k-1) + K_e(k)\big(y_e(k) - C(k)\hat{x}_e(k|k-1)\big) \end{cases} \tag{5.5}$$

where $\hat{d}_e(k-1)$ is the estimate of the unknown input at time instant $k-1$, $\hat{x}_e(k|k-1)$ is the one-step prediction of $x(k)$ at time instant $k-1$, and $\hat{x}_e(k|k)$ is the estimate of $x(k)$ at time instant k with $\hat{x}_e(0|0) = \bar{x}(0)$. $M_e(k)$ and $K_e(k)$ are the estimator gain matrices to be determined at time instant k.

In the event-based estimator $\mathscr{E}_2$, the input estimate $\hat{d}_e(k-1)$ is first obtained from $y_e(k)$ since $y_e(k)$ is the first event-triggered measurement that contains information about $d_e(k-1)$. Then, using both $\hat{d}_e(k-1)$ and the state estimate $\hat{x}_e(k-1|k-1)$, the a prior estimate $\hat{x}_e(k|k-1)$ is obtained. Finally, a posteriori estimate $\hat{x}_e(k|k)$ is obtained by updating $\hat{x}_e(k|k-1)$ with a correction term.

Substituting the first two equations into the last one in (5.5) leads to

$$\hat{x}_e(k|k) = A(k-1)\hat{x}_e(k-1|k-1) + L_e(k)\big(y_e(k) - C(k)A(k-1)\hat{x}_e(k-1|k-1)\big) \tag{5.6}$$

where

$$L_e(k) \triangleq K_e(k) + E(k)G(k-1)M_e(k), \quad E(k) \triangleq I - K_e(k)C(k). \tag{5.7}$$

Letting $\tilde{x}_e(k|k) = x(k) - \hat{x}_e(k|k)$, we have the following system that governs the estimation error dynamics:

$$\tilde{x}_e(k|k) = E(k)\big(A(k-1)\tilde{x}_e(k-1|k-1) + G(k-1)d(k-1) + \omega(k-1)\big) - L_e(k)(\nu(k) + \delta(k)). \tag{5.8}$$

To eliminate the effect of the unknown input $d(k)$ on the state estimation error $\tilde{x}_e(k|k)$ in (5.8), the following lemma is needed.

Lemma 5.1 *For the designed event-based estimator $\mathscr{E}_2$ in* (5.5)*, the estimation error $\hat{x}_e(k|k)$ is unrelated to the unknown input $d(k)$ if the gain matrix $M_e(k)$ satisfies*

$$M_e(k)C(k)G(k-1) = I_p. \tag{5.9}$$

Proof. Substituting (5.6) and (5.9) into (5.8) yields

$$\tilde{x}_e(k|k) = E(k)\big(A(k-1)\tilde{x}_e(k-1|k-1) + \omega(k-1)\big) - L_e(k)(\nu(k) + \delta(k)). \tag{5.10}$$

Comparing with (5.8), it can be found that, when condition (5.9) holds, the state estimation error $\tilde{x}_e(k|k)$ in (5.10) is not related to the unknown input $d(k)$. ■

When the condition (5.9) holds, the estimated input can be represented as follows:

$$\hat{d}_e(k) = M_e(k)(y_e(k) - C(k)A(k-1)\hat{x}_e(k-1|k-1)).$$

Accordingly, the input estimation error $\tilde{d}_e(k-1)$ can be given as follows:

$$\tilde{d}_e(k-1) = -M_e(k)\big(C(k)A(k-1)\tilde{x}_e(k-1|k-1) + C(k)\omega(k-1) + \nu(k) + \delta(k)\big) \tag{5.11}$$

where $\tilde{d}_e(k-1) \triangleq d(k) - \hat{d}_e(k)$.

For presentation convenience, we denote

$$\begin{aligned}
\tilde{d}_e^u(k) &= \mathbb{E}\{\tilde{d}_e(k)\}, & \tilde{d}_e^s(k) &= \tilde{d}_e(k) - \tilde{d}_e^u(k),\\
\tilde{x}_e^u(k|k) &= \mathbb{E}\{\tilde{x}_e(k|k)\}, & \tilde{x}_e^s(k|k) &= \tilde{x}_e(k|k) - \tilde{x}_e^u(k|k),\\
\Sigma_e^u(k) &= \tilde{d}_e^u(k)(\tilde{d}_e^u(k))^T, & \Sigma_e^s(k) &= \mathbb{E}\{\tilde{d}_e^s(k)(\tilde{d}_e^s(k))^T\},\\
P_e(k|k) &= \mathbb{E}\{\tilde{x}_e(k|k)(\tilde{x}_e(k|k))^T\}, & \Sigma_e(k) &= \mathbb{E}\{\tilde{d}_e(k)(\tilde{d}_e(k))^T\},\\
P_e^u(k|k) &= \tilde{x}_e^u(k|k)(\tilde{x}_e^u(k|k))^T, & P_e^s(k|k) &= \mathbb{E}\{\tilde{x}_e^s(k|k)(\tilde{x}_e^s(k|k))^T\},
\end{aligned}$$

and then (5.10)-(5.11) can be rewritten in the following form:

$$\begin{aligned}
\tilde{x}_e^s(k|k) &= E(k)(A(k-1)\tilde{x}_e^s(k-1|k-1) + \omega(k-1)) - L_e(k)\nu(k),\\
\tilde{x}_e^u(k|k) &= E(k)A(k-1)\tilde{x}_e^u(k-1|k-1) - L_e(k)\delta(k),\\
\tilde{d}_e^s(k) &= -M_e(k)C(k)A(k-1)\tilde{x}_e^s(k-1|k-1) - M_e(k)C(k)\omega(k-1)\\
&\quad -M_e(k)\nu(k),\\
\tilde{d}_e^u(k) &= -M_e(k)C(k)A(k-1)\tilde{x}_e^u(k-1|k-1) - M_e(k)\delta(k)
\end{aligned}$$

where $\tilde{x}_e^s(k|k)$ and $\tilde{x}_e^u(k|k)$ represent the stochastic and deterministic parts of the state estimation error, respectively. Similarly, $\tilde{d}_e^s(k)$ and $\tilde{d}_e^u(k)$ represent the stochastic and deterministic parts of the input estimation error, respectively.

Remark 5.2 *As pointed out in [58], in the traditional time-based estimator design, the estimator $\mathscr{E}_1$ is unbiased if and only if* (5.9) *is satisfied. On the other hand, in the event-based scenario, the state estimation error is not affected by the unknown input $d(k)$ when* (5.9) *holds.*

5.3 Estimator Design

In this section, for the system (5.1) with the event-based estimator $\mathscr{E}_2$, we will first obtain the upper bounds of the error covariances of both the input and state estimates, and then look for appropriate gain matrices $M_e(k)$ and $K_e(k)$ such that the obtained upper bounds are minimized.

Before proceeding further, we introduce the following lemmas which will be used in subsequent developments.

Lemma 5.2 *Given two vectors $x, y \in \mathbb{R}^m$, the following inequality holds,*

$$(x+y)(x+y)^T \leq (1+\varepsilon)xx^T + (1+\varepsilon^{-1})yy^T \tag{5.12}$$

where ε is an arbitrary positive scalar.

Proof. (5.12) follows from $(\sqrt{\varepsilon}x - \sqrt{\varepsilon^{-1}}y)(\sqrt{\varepsilon}x - \sqrt{\varepsilon^{-1}}y)^T \geq 0$ immediately. ■

Lemma 5.3 *Define a matrix function $f : \mathbb{S}^n_+ \mapsto \mathbb{R}$ as follows:*

$$f(X) = Tr\{(A^T X^{-1} A)^{-1}\}$$

where A is a given matrix of appropriate dimension and $A^T X^{-1} A$ is nonsingular. For two matrices $X_1, X_2 \in \mathbb{S}^n_+$, if $X_1 < X_2$, then $f(X_1) < f(X_2)$.

Proof. For two arbitrary positive definite matrices $X_1, X_2 \in \mathbb{S}^n_+$, assume that $X_1 < X_2$, then the following are true:

$$\begin{aligned} &0 < X_1 < X_2 \Rightarrow 0 < X_2^{-1} < X_1^{-1} \Rightarrow 0 < A^T X_1^{-1} A < A^T X_2^{-1} A \\ &\Rightarrow 0 < (A^T X_2^{-1} A)^{-1} < (A^T X_1^{-1} A)^{-1} \Rightarrow f(X_1) < f(X_2), \end{aligned}$$

and the proof is then completed. ■

Lemma 5.4 *[8] Consider the following recursion equation*

$$P(k+1) = FP(k)F^T + Q$$

where matrix $P(k) \in \mathbb{R}^{n\times n}$, and F and Q are known matrices of appropriate dimensions. If $|\lambda(F)| < 1$, for arbitrary initial $P(0)$, we have $\lim_{k\to\infty} P(k) = \bar{P}$ where $\bar{P}$ is the solution to $\bar{P} - F\bar{P}F^T = Q$.

Lemma 5.5 *[108] For $0 \leq k \leq N$, suppose that $X, Y \in \mathbb{R}^{n\times n}$, $X = X^T > 0$, $Y = Y^T > 0$, $\phi(X,k) = \phi^T(X,k) \in \mathbb{R}^{n\times n}$. If*

$$\phi(X,k) \leq \phi(Y,k), \quad \forall X \leq Y, \tag{5.13}$$

then the solutions $M(k)$ and $N(k)$ to the following difference equations

$$M(k+1) \leq \phi(M(k),k),\ N(k+1) = \phi(N(k),k),\ M(0) = N(0) > 0 \tag{5.14}$$

satisfy

$$M(k) \leq N(k).$$

5.3.1 Input Estimation

In this section, we consider the unknown input estimation problem. At time instant k, given the event-based measurement $y_e(k)$, we aim to obtain the input estimate $\hat{d}_e(k)$ and an upper bound on the error covariance of the input estimate, and then we look for an appropriate estimation gain $M_e(k)$ which minimizes such an upper bound.

An upper bound on the error covariance of the input estimate is given in the following theorem.

Theorem 5.1 *Consider the linear system (5.1) and the event-based estimator* $\mathscr{E}_2$ *in* (5.5) *with event generator condition (5.3). Assume that the condition (5.9) is satisfied. For a given positive scalar sequence* $\{\varepsilon_1(k), k \in \mathbb{N}\}$, *an upper bound on the error covariance matrix of the input estimation* $\hat{\Sigma}_e(k-1)$ *is given by*

$$\hat{\Sigma}_e(k-1) = M_e(k)\Phi(k)M_e^T(k) \tag{5.15}$$

where

$$\begin{aligned}\Phi(k) &= C(k)Q(k-1|k-1)C^T(k) + R(k) + (1+\varepsilon_1^{-1}(k))\sigma I,\\ Q(k-1|k-1) &= A(k-1)\big(P_e^s(k-1|k-1) + (1+\varepsilon_1(k))\hat{P}_e^u(k-1)\big)A^T(k-1) + W(k-1).\end{aligned}$$

Proof. First, let us derive the expression of $\Sigma_e(k-1)$. It follows from (5.12) and (5.12) that

$$\begin{aligned}\Sigma_e(k-1) &= \Sigma_e^s(k-1) + \Sigma_e^u(k-1) &(5.16)\\ \Sigma_e^s(k-1) &= M_e(k)\Big(C(k)(A(k-1)P_e^s(k-1|k-1)A^T(k-1) + W(k-1))C^T(k)\\ &\quad +R(k)\Big)M_e^T(k) &(5.17)\\ \Sigma_e^u(k-1) &= \delta(k)\delta^T(k) + M_e(k)C(k)A(k-1)P_e^u(k-1|k-1)A^T(k-1)C^T(k)(M_e(k))^T\\ &\quad +\big(M_e(k)C(k)A(k-1)\tilde{x}^u(k-1|k-1)\big)(M_e(k)\delta(k))^T\\ &\quad +M_e(k)\delta(k)\big(M_e(k)C(k)A(k-1)\tilde{x}^u(k-1|k-1)\big)^T. &(5.18)\end{aligned}$$

Using Lemma 6.1, we obtain

$$\begin{aligned}&\big(M_e(k)C(k)A(k-1)\tilde{x}_e^u(k-1|k-1)\big)(M_e(k)\delta(k))^T\\ &\quad + M_e(k)\delta(k)\big(M_e(k)C(k)A(k-1)\tilde{x}_e^u(k-1|k-1)\big)^T\\ &\leq M_e(k)\big(\varepsilon_1(k)C(k)A(k-1)P_e^u(k-1|k-1)A^T(k-1)C^T(k) + \varepsilon_1^{-1}(k)\delta(k)\delta^T(k)\big)M_e^T(k).\end{aligned} \tag{5.19}$$

Substituting (5.19) into (5.18) and noting that $P_e^u(k-1|k-1) \leq \hat{P}_e^u(k-1|k-1)$, we have

$$\Sigma_e(k-1) \leq \hat{\Sigma}_e(k-1),$$

where $\hat{\Sigma}_e(k-1)$ is given in (5.15). ■

Now, we are ready to minimize the upper bound $\hat{\Sigma}_e(k-1)$ at each time instant by appropriately designing the estimator parameter $M_e(k)$.

Theorem 5.2 *Consider the linear system (5.1) and the event-based estimator $\mathscr{E}_2$ in* (5.5) *with event generator condition (5.3). Assume that the condition (5.9) is satisfied. The upper bound $\hat{\Sigma}_e(k-1)$ (given in* (5.15)*) on the error covariance of the input estimation is minimized if the parameter $M_e(k)$ is chosen as*

$$M_e(k) = \Pi^{-1}(k)G^T(k-1)C^T(k)\Phi^{-1}(k), \tag{5.20}$$

and the minimized upper bound is given by

$$\hat{\Sigma}_e(k-1) = \Pi^{-1}(k) \tag{5.21}$$

where $\Pi(k) = G^T(k-1)C^T(k)\Phi^{-1}(k)C(k)G(k-1)$.

Proof. We need to search for an appropriate gain matrix $M_e(k)$ which minimizes the upper bound matrix $\hat{\Sigma}_e(k-1)$, and the corresponding problem can be equivalently written as the following constrained optimization problem:

$$\begin{gathered}\min_{M_e(k)} \hat{\Sigma}_e(k-1),\\ \text{subject to } M_e(k)C(k)G(k-1) = I_p.\end{gathered} \tag{5.22}$$

Using the completion-of-squares method, $\hat{\Sigma}_e(k-1)$ can be rearranged as follows:

$$\begin{aligned}\hat{\Sigma}_e(k-1) =& \big(M_e(k) - \Pi^{-1}(k)G^T(k-1)C^T(k)\Phi^{-1}(k)\big)\Phi(k)\\ &\times \big(M_e(k) - \Pi^{-1}(k)G^T(k-1)C^T(k)\Phi^{-1}(k)\big)^T + \Pi^{-1}(k)\end{aligned} \tag{5.23}$$

By choosing

$$M_e(k) = \Pi^{-1}(k)G^T(k-1)C^T(k)\Phi^{-1}(k),$$

it can be easily found that the equality constraint in (5.22) is satisfied and $\hat{\Sigma}_e(k-1)$ is minimized as

$$\hat{\Sigma}_e(k-1) = \Pi^{-1}(k).$$

This completes the proof. ■

5.3.2 State Estimation

In this section, we consider the estimation problem of the system state. We are interested in finding an appropriate gain matrix $K_e(k)$ for the event-based estimator $\mathscr{E}_2$ such that the upper bound on the error covariance of the state estimation is minimized. First, an upper bound on the error covariance of the state estimation is given in the following theorem.

Theorem 5.3 *Consider the linear system (5.1) and the event-based estimator $\mathscr{E}_2$ in* (5.5) *with event generator condition (5.3). Let the condition* (5.9) *be satisfied. Assume that, for a given positive scalar sequence $\{\varepsilon_2(k), k \in \mathbb{N}\}$, there exist two sets of real-valued matrices $\hat{P}_e^u(k|k)$ and $L_e(k)$ satisfying the following Riccati-like difference equation with the initial condition $\hat{P}_e^u(k|k) = 0$:*

$$\hat{P}_e^u(k|k) = \phi(\hat{P}_e^u(k-1|k-1), k-1), \tag{5.24}$$

where

$$\phi(\hat{P}_e^u(k-1|k-1), k-1) = (1+\varepsilon_2(k))\bar{A}_e(k-1)\hat{P}_e^u(k-1|k-1)\bar{A}_e^T(k-1) + (1+\varepsilon_2^{-1}(k))\sigma L_e(k)L_e^T(k),$$

$$\bar{A}_e(k-1) = E(k)A(k-1), \quad L_e(k) = K_e(k) + E(k)G(k-1)M_e(k).$$

Then, we have $\hat{P}_e^u(k|k) \geq P_e^u(k|k)$. Accordingly, an upper bound $\hat{P}_e(k|k)$ on the estimation error covariance matrix $P_e(k|k)$ is given as follows:

$$\hat{P}_e(k|k) = P_e^s(k|k) + \hat{P}_e^u(k|k) \tag{5.25}$$

where

$$\begin{aligned} P_e^s(k|k) =& \bar{A}(k-1)P_e^s(k-1|k-1)\bar{A}^T(k-1) + L_e(k)R(k)L_e^T(k) \\ &+ E(k)W(k-1)E^T(k), \quad P_e^s(0|0) = P(0|0). \end{aligned}$$

Proof. From (5.12) and (5.12), it is straightforward to obtain that

$$\begin{aligned} P_e^s(k|k) &= \bar{A}(k-1)P_e^s(k-1|k-1)\bar{A}^T(k-1)+L_e(k)R(k)L_e^T(k) && (5.26)\\ &\quad +E(k)W(k-1)E^T(k), && (5.27)\\ P_e^u(k|k) &= \bar{A}(k-1)P_e^u(k-1|k-1)\bar{A}^T(k-1)+\bar{A}(k-1)\tilde{x}_e^u(k-1|k-1)(L_e(k)\delta(k))^T\\ &\quad +\sigma L_e(k)L_e^T(k)+L_e(k)\delta(k)(\bar{A}(k-1)\tilde{x}_e^u(k-1|k-1))^T. && (5.28)\end{aligned}$$

For an arbitrary positive scalar $\varepsilon_2(k)$, it follows from Lemma 6.1 that

$$\begin{aligned} &\bar{A}(k-1)\tilde{x}_e^u(k-1|k-1)(L_e(k)\delta(k))^T+L_e(k)\delta(k)(\bar{A}(k-1)\tilde{x}_e^u(k-1|k-1))^T\\ \leq&\varepsilon_2(k)\bar{A}(k-1)P_e^u(k-1|k-1)\bar{A}^T(k-1)+\varepsilon_2^{-1}(k)\sigma L_e(k)L_e^T(k)\end{aligned}$$

which, together with (5.28), indicates that $\phi(P_e^u(k-1|k-1)) \geq P_e^u(k|k)$. As $\hat{P}_e^u(k|k) = P_e^u(k|k) = 0$, and $\hat{P}_e^u(k|k)$ can be calculated iteratively by the Riccati-like difference equation $\hat{P}_e^u(k|k) = \phi(\hat{P}_e^u(k-1|k-1),k-1)$. It follows from Lemma 6.4 that

$$\hat{P}_e^u(k|k) \geq P_e^u(k|k), \forall k>0, \tag{5.29}$$

and, furthermore, we can easily obtain from (5.25) and (5.29) that

$$\hat{P}_e(k|k) \geq P_e(k|k), \forall k>0$$

and the proof is now complete. ■

Before we design the estimator, we denote

$$\begin{aligned} \Omega(k) &\triangleq \left\{\left[\tilde{P}_e(k-1|k-1)+\Lambda(k)G^T(k-1)\right]C^T(k)\Xi^{-1}(k)-G(k)M_e(k)\right\} && (5.30)\\ &\quad \times\left\{I-\left[I-C(k)G(k-1)M_e(k)\right]^+\left[I-C(k)G(k-1)M_e(k)\right]\right\} && (5.31)\end{aligned}$$

In the following theorem, the upper bound matrix $\hat{P}_e(k|k)$ at each time instant is minimized by appropriately designing the estimator parameter $K_e(k)$.

Theorem 5.4 *Consider the linear system (5.1) and the event-based estimator* $\mathscr{E}_2$ (5.5) *with event generator condition (5.3). Assume that the condition (5.9) is satisfied. The matrix $\hat{P}_e(k|k)$ given in (5.25), which is an upper bound on the error covariance $P_e(k|k)$ of the state estimation, can be minimized at the iteration when $\Omega(k)=0$ with the parameter $K_e(k)$ given* *by*

$$\begin{aligned}K_e(k) =&\Big(\big(\tilde{P}_e(k-1|k-1)+\Lambda(k)G^T(k-1)\big)C^T(k)\Xi^{-1}(k)-G(k)M_e(k)\Big)\\&\times\big(I-C(k)G(k-1)M_e(k)\big)^+\end{aligned} \tag{5.32}$$

and the minimum given by

$$\begin{aligned}\hat{P}_e(k|k) =&\Lambda(k)G^T(k-1)C^T(k)\Xi^{-1}(k)C(k)G(k-1)\Lambda^T(k)+\tilde{P}_e(k-1|k-1)\\&-\tilde{P}_e(k-1|k-1)C^T(k)\Xi^{-1}(k)C(k)\tilde{P}_e(k-1|k-1)\end{aligned} \tag{5.33}$$

where

$$\begin{aligned}\tilde{P}_e(k-1|k-1) =&A(k-1)\big(P_e^s(k-1|k-1)+(1+\varepsilon_2(k))\hat{P}_e^u(k-1|k-1)\big)A^T(k-1)+W(k-1),\\ \Xi(k) =&C(k)\tilde{P}_e(k-1|k-1)C^T(k)+R(k)+(1+\varepsilon_2^{-1}(k))\sigma I,\\ \Lambda(k) =&\big(G(k-1)-\tilde{P}_e(k-1|k-1)C^T(k)\Xi^{-1}(k)C(k)G(k-1)\big)\\&\times\big(G^T(k-1)C^T(k)\Xi^{-1}(k)C(k)G(k-1)\big)^{-1}.\end{aligned}$$

In the special case that the two set of positive scalar sequences are identical, that is, $\varepsilon_2(k)=\varepsilon_1(k),\forall k\in\mathbb{N}$, *the expression of* $K_e(k)$ *reduces to the following equation,*

$$K_e(k)=\tilde{P}_e(k-1|k-1)C^T(k)\Xi^{-1}(k). \tag{5.34}$$

Proof. For locally minimum-variance estimation, we first look for $L_e(k)$ which minimizes $\hat{P}_e(k|k)$ subject to the constraint $L_e(k)C(k)G(k-1)=G(k-1)$. Using the completion-of-squares method, $\hat{P}_e(k|k)$ can be rewritten as follows:

$$\begin{aligned}\hat{P}_e(k|k) =&\Big(L_e(k)\Xi(k)-\tilde{P}_e(k-1|k-1)C^T(k)-\Lambda(k)G^T(k-1)C^T(k)\Big)\Xi^{-1}(k)\\&\times\Big(L_e(k)\Xi(k)-\tilde{P}_e(k-1|k-1)C^T(k)-\Lambda(k)G^T(k-1)C^T(k)\Big)^T+\tilde{P}_e(k-1|k-1)\\&+\Lambda(k)G^T(k-1)C^T(k)\Xi^{-1}(k)C(k)G(k-1)\Lambda^T(k)\\&-\tilde{P}_e(k-1|k-1)C^T(k)\Xi^{-1}(k)C(k)\tilde{P}_e(k-1|k-1)\end{aligned} \tag{5.35}$$

By choosing

$$L_e(k)=\big(\tilde{P}_e(k-1|k-1)+\Lambda(k)G^T(k-1)\big)C^T(k)\Xi^{-1}(k), \tag{5.36}$$

it can be found that $\hat{P}_e(k|k)$ is minimized and the minimum of $\hat{P}_e(k|k)$ is given by

$$\begin{aligned}\hat{P}_e(k|k) =&\Lambda(k)G^T(k-1)C^T(k)\Xi^{-1}(k)C(k)G(k-1)\Lambda^T(k)+\tilde{P}_e(k-1|k-1)\\&-\tilde{P}_e(k-1|k-1)C^T(k)\Xi^{-1}(k)C(k)\tilde{P}_e(k-1|k-1).\end{aligned}$$

Note that $L_e(k) = K_e(k) + \big(I - K_e(k)C(k)\big)G(k-1)M_e(k)$ and $\Omega k = 0$, it is easy to see that the minimum-norm solution $K_e(k)$ to

$$\big(\tilde{P}_e(k-1|k-1)+\Lambda(k)G^T(k-1)\big)C^T(k)\Xi^{-1}(k) = K_e(k)+\big(I-K_e(k)C(k)\big)G(k-1)M_e(k)$$

exists and is given by

$$\begin{aligned}K_e(k) =&\Big(\big(\tilde{P}_e(k-1|k-1)+\Lambda(k)G^T(k-1)\big)C^T(k)\Xi^{-1}(k)-G(k)M_e(k)\Big)\\&\times\big(I-C(k)G(k-1)M_e(k)\big)^+\end{aligned}$$

When $\varepsilon_2(k) = \varepsilon_1(k)$, we have $\Phi(k) = \Xi(k)$ and then obtain $K_e(k)$ as follows:

$$K_e(k) = \tilde{P}_e(k-1|k-1)C^T(k)\Xi^{-1}(k).$$

This completes the proof. ■

Remark 5.3 *In case that $\Omega(k) \neq 0$, the estimator gain (5.32) would lead to a practical (not necessarily minimum-variance) solution with guaranteed upper bound $\hat{P}_e(k|k)$. On the other hand, if the threshold of event-triggering σ is set to be zero, then the event-based mechanism reduces to the traditional time-based mechanism and, accordingly, our proposed estimator reduces to the optimal time-based estimator proposed in [58].*

5.3.3 Discussion on Choosing Scalar Parameters

From Theorems 5.1 and 5.3, it is clear that the estimation performance at time instant k depends on system data and the scalar sequences $\varepsilon_i(0),\varepsilon_i(1),\dots,\varepsilon_i(k), i = 1,2$. It means that, to compute an optimal event-based estimator at time k, the scalar sequences $\varepsilon_i(0),\varepsilon_i(1),\dots,\varepsilon_i(k-1), i = 1,2$, need to be re-computed, and so do the corresponding estimator gain matrices (5.20) and (5.32). The optimization over the scalar sequences becomes numerically intractable as the time instant k tends to $+\infty$.

To reduce the computation complexity, instead of optimizing the performance over all the k scalar parameters, a practical way is to optimize the trace of matrices $\hat{\Sigma}_e(k)$ and $\hat{P}_e(k|k)$ over a fixed length of scalar parameters $\varepsilon_i(k+1-i),\varepsilon_i(k+2-i),\dots,\varepsilon_i(k), i = 1,2$. For the special case that the length is equal to 1, an optimal and suboptimal algorithms on how to choose the scalar parameters are given below respectively.

Proposition 5.1 *For the event-based estimator $\mathscr{E}_2$ in* (5.5) *with the parameters $M_e(k)$ and $K_e(k)$ given in (5.20) and (5.32), respectively, $Tr\{\hat{\Sigma}_e(k)\}$ and $Tr\{\hat{P}_e(k|k)\}$ are minimized if the scalars $\varepsilon_1(k)$ and $\varepsilon_2(k)$ are given as follows:*

$$\varepsilon_1(k) = \arg\min_{\varepsilon_1(k)} Tr\{\Pi^{-1}(k)\} \tag{5.37}$$

$$\begin{aligned}\varepsilon_2(k) =& \arg\min_{\varepsilon_2(k)} Tr\Big\{\Lambda(k)G^T(k-1)C^T(k)\Xi^{-1}(k)C(k)G(k-1)\Lambda^T(k)+\tilde{P}_e(k-1|k-1)\\ &-\tilde{P}_e(k-1|k-1)C^T(k)\Xi^{-1}(k)C(k)\tilde{P}_e(k-1|k-1)\Big\}.\end{aligned} \tag{5.38}$$

An analytical suboptimal scalar $\varepsilon_1(k)$ can be chosen as follows:

$$\varepsilon_1(k) = \begin{cases} \sqrt{\frac{\sigma}{\bar{\rho}(k)}}, & if\, \Phi\big(\sqrt{\frac{\sigma}{\bar{\rho}(k)}},k\big) < \Phi\big(\sqrt{\frac{\sigma}{\underline{\rho}(k)}},k\big) \\ \sqrt{\frac{\sigma}{\underline{\rho}(k)}}, & \qquad otherwise. \end{cases} \tag{5.39}$$

where $\bar{\rho}(k), \underline{\rho}(k)$ are the minimum and the maximum eigenvalues of $C(k)A(k-1)\hat{P}_e(k-1|k-1)A^T(k-1)C^T(k)$, respectively.

Proof. With the obtained optimal gain matrices $M_e(k)$ and $K_e(k)$, we search for the optimal/suboptimal scalar parameters $\varepsilon_1(k)$ and $\varepsilon_2(k)$. From (5.21) and (5.35), it is straightforward to derive the optimal $\varepsilon_1(k)$ and $\varepsilon_2(k)$, which are given in (5.37) and (5.38), respectively. However, since it is numerical intractable to compute the analytical solution for the optimal $\varepsilon_1(k)$ from (5.37), we would like to look for a suboptimal $\varepsilon_1(k)$. Instead of searching for the optimal $\varepsilon_1(k)$ from the interval $(0,+\infty)$, in the following, a suboptimal $\varepsilon_1(k)$ belonging to the interval $\Big(0,\sqrt{\frac{\sigma}{\bar{\rho}(k)}}\Big] \bigcup \Big[\sqrt{\frac{\sigma}{\underline{\rho}(k)}},+\infty\Big)$, is derived in the analytical form.

Choosing two arbitrary scalar variables $\varepsilon_2(k) > \tilde{\varepsilon}_1(k) > 0$, we have

$$\begin{aligned}&\Phi(\tilde{\varepsilon}_1(k),k)-\Phi(\varepsilon_1(k),k)\\ =&(\tilde{\varepsilon}_1(k)-\varepsilon_1(k))C(k)A(k-1)\hat{P}_e(k|k)A^T(k-1)C^T(k)+\sigma(\tilde{\varepsilon}_1^{-1}(k)-\varepsilon_1^{-1}(k))I_m\\ =&(\tilde{\varepsilon}_1(k)-\varepsilon_1(k))\big(C(k)A(k-1)\hat{P}_e(k|k)A^T(k-1)C^T(k)-\frac{\sigma}{\varepsilon_1(k)\tilde{\varepsilon}_1(k)}I_m\big),\end{aligned}$$

from which we conclude the following:

(i) if $\varepsilon_1(k), \tilde{\varepsilon}_1(k) \in \Big(0,\sqrt{\frac{\sigma}{\bar{\rho}(k)}}\Big]$, then $\Phi(\tilde{\varepsilon}_1(k),k) < \Phi(\varepsilon_1(k),k)$;

Algorithm 5.1 Event-based Simultaneous Input and State Estimation (ESISE)

```
Initialize:
    $k = 0, \hat{P}_e^u(0) = 0, \hat{P}_e^s(0) = P(0|0)$ ;
while $k \geq 1$ do
    if opt="optimal" then
        Choose the scalar $\varepsilon_1(k)$ via (5.37) ;
        Calculate the input estimate gain $M_e(k)$ via (5.20);
        Calculate the upper bound of the input estimation $\hat{\Sigma}_e(k-1)$ via (5.21);
        Choose the scalar $\varepsilon_2(k)$ via (5.38) ;
        Calculate the state estimate gain $K_e(k)$ via (5.32) ;
        Calculate $\hat{P}_e(k|k)$ via (5.33) ;
    else if opt="sub-optimal" then
        Choose the scalar $\varepsilon_1(k)$ via (5.39) ;
        Calculate the input estimate gain $M_e(k)$ via (5.20);
        Calculate the upper bound of the input estimation $\hat{\Sigma}_e(k-1)$ via (5.21);
        Set the scalar $\varepsilon_2(k) = \varepsilon_1(k)$;
        Calculate the state estimate gain $K_e(k)$ via (5.34) ;
        Calculate $\hat{P}_e(k|k)$ via (5.33) ;
    end if
    Input and state estimate $\hat{d}_e(k)$, $\hat{x}_e(k|k)$ via (5.5);
    $k = k + 1$;
end while
```

(ii) if $\varepsilon_1(k), \tilde{\varepsilon}_1(k) \in \left[\sqrt{\frac{\sigma}{\underline{\rho}(k)}}, +\infty\right)$, then $\Phi(\tilde{\varepsilon}_1(k), k) > \Phi(\varepsilon_1(k), k)$;

(iii) if $\varepsilon_1(k), \tilde{\varepsilon}_1(k) \in \left[\sqrt{\frac{\sigma}{\bar{\rho}(k)}}, \sqrt{\frac{\sigma}{\underline{\rho}(k)}}\right]$, then $\Phi(\tilde{\varepsilon}_1(k), k)$ and $\Phi(\varepsilon_1(k), k)$ are not dominated by each other.

On the other hand, it follows from Lemma 6.2 that $\mathrm{Tr}\{\Sigma_e(k)\}$ is a strictly increasing function of $\Phi(k)$. Hence, it is known that, for $\varepsilon_1(k) \in \left(0, \sqrt{\frac{\sigma}{\bar{\rho}(k)}}\right] \cup \left[\sqrt{\frac{\sigma}{\underline{\rho}(k)}}, +\infty\right)$, $\mathrm{Tr}\{\Sigma_e(k)\}$ attains the minimum when

$$\varepsilon_1(k) = \begin{cases} \sqrt{\frac{\sigma}{\bar{\rho}(k)}}, & \text{if } \Phi(\sqrt{\frac{\sigma}{\bar{\rho}(k)}}, k) < \Phi(\sqrt{\frac{\sigma}{\underline{\rho}(k)}}, k) \\ \sqrt{\frac{\sigma}{\underline{\rho}(k)}}, & \text{otherwise.} \end{cases}$$

This completes the proof. ∎

The complete procedure of our proposed estimation algorithm is described in Algorithm 5.1.

5.4 Boundedness Analysis

In the section, we investigate the asymptotic boundedness properties of the upper bound $\hat{P}_e(k|k)$ for the time-invariant system. Without notation confusion, when referring to the time invariant system (5.1), it is explicitly assumed that the parameter matrices are fixed as constant matrices, that is, $A(k) = A$, $G(k) = G$, $C(k) = C$, $W(k) = W$, and $R(k) = R$.

To facilitate our analysis, existing results on time-based estimation problems for time-invariant systems are summarized in the following lemma.

Lemma 5.6 *[35] Consider the linear time-invariant system with unknown input (5.1) and the time-based estimator $\mathscr{E}_1$ in (5.2). The corresponding error covariance matrix $P_t(k|k)$ of the state estimation converges to a unique fixed positive semi-definite matrix $\bar{P}_t$ for any given initial condition $P_t(0|0)$ if and only if the following two equations hold,*

$$\text{Rk}\left\{\begin{bmatrix} zI_n - A & G \\ C & 0 \end{bmatrix}\right\} = n + p, \forall z \in \mathbb{C}, |z| \geq 1. \tag{5.40}$$

$$\text{Rk}\left\{\begin{bmatrix} A - e^{j\omega}I & G & W^{\frac{1}{2}} & 0 \\ e^{j\omega}C & 0 & 0 & R^{\frac{1}{2}} \end{bmatrix}\right\} = n + m, \forall \omega \in [0, 2\pi]. \tag{5.41}$$

Moreover, with the associate limiting gain matrices $K_t \triangleq \lim_{k\to\infty} K_t(k)$, $M_t \triangleq \lim_{k\to\infty} M_t(k)$, the time-invariant estimator is stable as well, i.e., all the eigenvalues of $\bar{A}_t \triangleq (I - L_t C)A$ satisfy $|\lambda(\bar{A}_t)| < 1$, where $L_t = K_t + (I - K_t C)GM_t$.

Theorem 5.5 *Consider the linear time-invariant system with unknown input (5.1) and event generator condition (5.3). Assume that both (5.40) and (5.41) are satisfied and an event-based estimator is designed according to Algorithm 5.1. With an arbitrarily chosen constant scalar $\varepsilon_2 \in (0, \bar{\varepsilon})$, where $\bar{\varepsilon} = \rho_{\max}^{-2}(\bar{A}_t) - 1$, the state error covariance matrix $P_e(k|k)$ is bounded and the upper bound $\hat{P}_e(k|k)$ is asymptotically convergent.*

Proof. 1). First, we prove that, for the event-based state estimator, when the filter gain $K_e(k)$ is set to be equivalent to the optimal gain $K_t(k)$ obtained in the time-based scenario, then the state estimation error covariance is bounded.

When the filter parameters are chosen as $K_e(k) = K_t(k)$, $L_e(k) = L_t(k)$, then $\bar{A}_e = \bar{A}_t$. From Lemma 6.3, it is known that $\bar{A}_e$ is a stable matrix and $\lim_{k\to\infty} P_t(k|k) = \bar{P}$. Moreover, it is easily found that $P_e^s(k|k)$ coincides with $P_t(k|k)$ and hence $P_e^s(k|k)$ converges to matrix $\bar{P}_t$. As $\bar{A}_e$ is a stable matrix and $\varepsilon \in (0, \bar{\varepsilon})$, then $\tilde{A}_e \triangleq \sqrt{1 + \varepsilon}\bar{A}_e$ is a stable matrix as well.

Noting that $\hat{P}_e^u(k|k)$ satisfies

$$\hat{P}_e^u(k|k) = \tilde{A}_e\hat{P}_e^u(k-1|k-1)\tilde{A}_e^T + (1+\varepsilon^{-1})\sigma L_e L_e^T,$$

it follows from Lemma 6.5 that $\hat{P}_e^u(k|k) \to \bar{P}_e^u$ when $k \to \infty$, where $\bar{P}_e^u = \tilde{A}_e\bar{P}_e^u\tilde{A}_e^T + (1+\varepsilon^{-1})\sigma L_e L_e^T$. Furthermore, by noticing the fact that $\hat{P}_e(k|k) = \hat{P}_e^s(k|k) + \hat{P}_e^u(k|k)$, we have $\lim\limits_{k\to\infty} P_e(k|k) = \bar{P}_t + \bar{P}_e^u$.

2). Next, through the induction approach, we aim to prove that, with the proposed optimal filter parameters $K_e(k)$ and $M_e(k)$, the upper bound matrix $\hat{P}^u(k|k)$ is always less than the one with the gain $K_t(k)$. That is, we would like to show that

$$\hat{P}_e\Big(k|k, K_e(k), \hat{P}_e\big(k-1|k-1, K_e(k-1)\big)\Big) \le \hat{P}_e\Big(k|k, K_t(k), \hat{P}_e\big(k-1|k-1, K_t(k-1)\big)\Big). \tag{5.42}$$

When $k=0$, $P_e^s(0|0) = P(0|0)$, and $P_e^u(0|0) = 0$, it is easy to find that $\hat{P}_e(0|0, K_e(0)) = \hat{P}_e(0|0, K_t(0))$. Suppose that, when $k = i-1$, $\hat{P}_e(i-1|i-1, K_e(i-1)) \le \hat{P}_e(i-1|i-1, K_t(i-1))$ and we like to prove that (5.42) holds for $k=i$. In this case, since $K_e(i)$ minimizes $\hat{P}_e(i|i)$ given $\hat{P}_e(i-1|i-1)$, we can see that

$$\hat{P}_e\Big(i|i, K_e(i), \hat{P}_e\big(i-1|i-1, K_e(i-1)\big)\Big) \le \hat{P}_e\Big(i|i, K_t(i), \hat{P}_e\big(i-1|i-1, K_e(i-1)\big)\Big). \tag{5.43}$$

On the other hand, it can be found that

$$\begin{aligned} &\hat{P}_e\Big(i|i, K_t(i), \hat{P}_e\big(i-1|i-1, K_t(i-1)\big)\Big) - \hat{P}_e\Big(i|i, K_t(i), \hat{P}_e\big(i-1|i-1, K_e(i-1)\big)\Big) \\ &= \bar{A}_e(i-1)\Big((1+\varepsilon)\big(\hat{P}_e^u(i-1|i-1, K_t(i-1)) - \hat{P}_e^u(i-1|i-1, K_e(i-1))\big) \\ &- \big(P_e^s(i-1|i-1, K_e(i-1)) - P_e^s(i-1|i-1, K_t(i-1))\big)\Big)\bar{A}_e^T(i-1). \end{aligned} \tag{5.44}$$

Noting that $P_e^s(i-1|i-1, K_t(i-1)) \le P_e^s(i-1|i-1, K_e(i-1))$, and $\hat{P}_e(i-1|i-1, K_e(i-1)) \le \hat{P}_e(i-1|i-1, K_t(i-1))$, it can be inferred that

$$\begin{aligned} 0 &\le P_e^s\big(i-1|i-1, K_e(i-1)\big) - P_e^s\big(i-1|i-1, K_t(i-1)\big) \\ &\le \hat{P}_e^u\big(i-1|i-1, K_t(i-1)\big) - \hat{P}_e^u\big(i-1|i-1, K_e(i-1)\big). \end{aligned}$$

Substituting the above inequalities into (5.44), one obtains

$$\hat{P}_e\Big(i|i, K_t(i), \hat{P}_e\big(i-1|i-1, K_e(i-1)\big)\Big) \le \hat{P}_e\Big(i|i, K_t(i), \hat{P}_e\big(i-1|i-1, K_t(i-1)\big)\Big). \tag{5.45}$$

Combining the inequalities (5.43) and (5.45) leads to (5.42).

3). In this step, we aim to prove that the upper bound is asymptotically bounded. Noting that

$$\lim_{k\to\infty} \hat{P}_e\Big(k|k, K_t(k), \hat{P}_e\big(k-1|k-1, K_t(k-1)\big)\Big) = \hat{P},$$

it follows from (5.45) that

$$\lim_{k\to\infty} \hat{P}_e\Big(k|k, K_e(k), \hat{P}_e\big(i-1|i-1, K_e(i-1)\big)\Big) \leq \hat{P}.$$

This completes the proof.

5.5 Numerical Example

In this section, we consider the state estimation system of a three-bus system that is depicted in Fig. 5.1. For the 3-bus test system, we choose the state $x(k)$ as

$$x(k) = \big[x_{r,1}(k)\; x_{r,2}(k)\; x_{r,3}(k)\; x_{i,1}(k)\; x_{i,2}(k)\; x_{i,3}(k)\big]^T$$

where $x_{r,l}(k)$ and $x_{i,l}(k)$ represent the real and imaginary parts of voltage of the lth bus, respectively, then the system is modelled as (5.1) with parameters $A = \text{diag}_6\{1.0\}$, $G = \Big[0,1,0,0,0,1\Big]^T$, $W(k) = \text{diag}_6\{0.01^2\}$ and $R(k) = \text{diag}_{10}\{0.1^2\}$. The unknown input is given by

$$d(k) = 0.1u_s(k) - 0.2u_s(k-20)$$

where $u_s(k)$ is the unit-step function. The simulation time is 20 time steps. Assume that the initial voltages of all buses are at flat start, that is, $x_{r,l}(0) = 1$ p.u, $x_{i,l}(0) = 0$ for all $l = 1, 2, \ldots, 3$.

The values of branch parameters in the three-bus system are the same as the ones in [15]. We assume that each PMU measurement either one bus voltage or one branch current. Three PMUs measure the voltages at bus 1, 2 and 3, and two PMUs measure the current at line 1-2 and 3-1.

To show that the threshold of the event-generator affects both the communication rate and the estimation performance, four different values of the threshold σ $(0, 0.5, 1.5, and 10)$ are considered. Let us choose the bus 3 as the representative bus.

Figs. 5.2 shows the actual and the estimated values of the system states $3, 6$ with different thresholds respectively. Figs. 5.3 shows the actual and the estimated value of the unknown input. It can be seen, the smaller the threshold is, the more accurate both the state and the input estimates are.

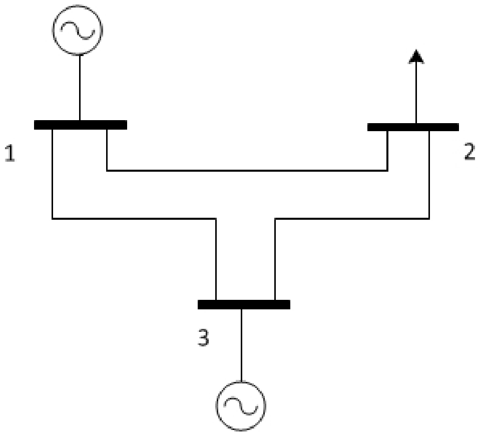


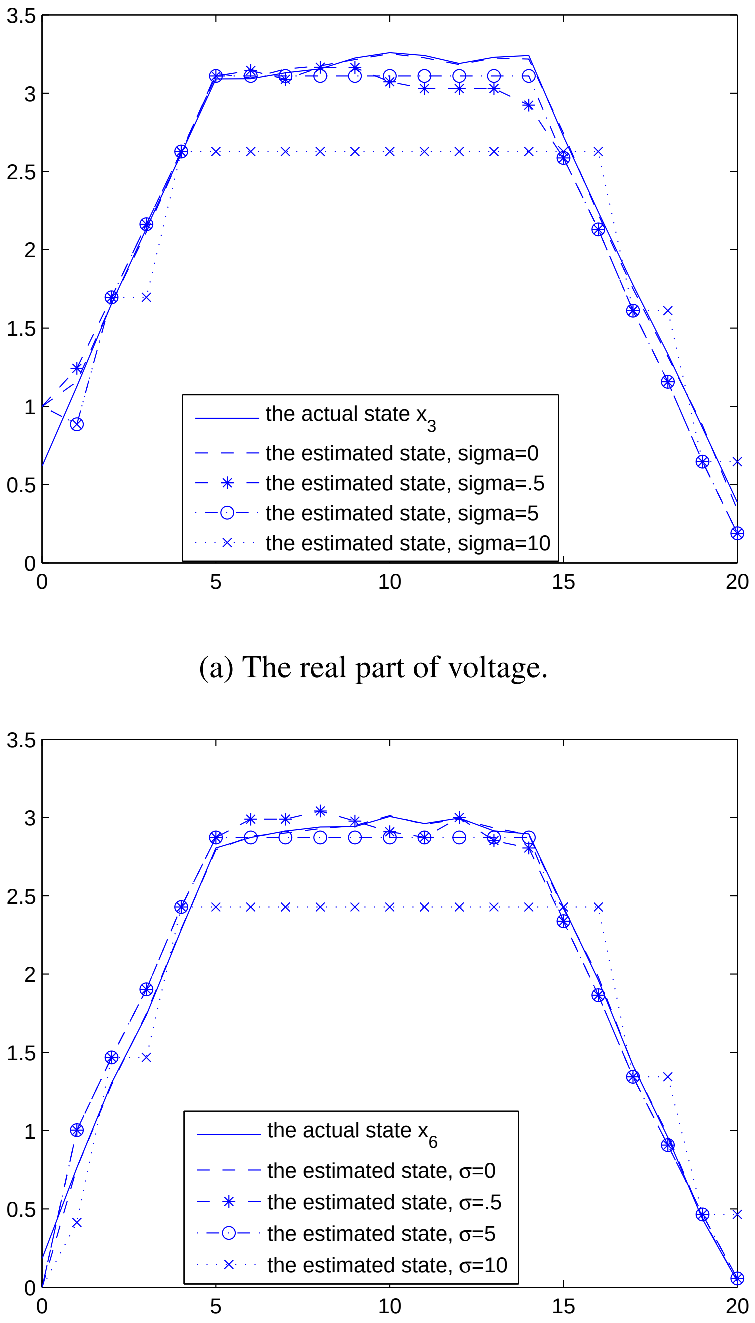
Fig. 5.1 The simplified 3-bus system

Fig. 5.4 shows the triggering events during the whole simulation period. Compared with the time-based mechanism, it can be found that the transmission times are significantly reduced, which clearly shows the superiority of the proposed event-based mechanism. Moreover, the larger the threshold is, the less data transmission is.

From the observations of the simulation results, we can conclude that the event-triggered estimation paradigm provides a flexible way to trade off the communication rate and the estimation performance. Optimizing of one objective usually worsen the performance on the other objective, and hence the threshold of the event triggering should be tuned carefully with considerations of performance specifics.

5.6 Conclusion

In this chapter, an event-based joint input/state estimator has been proposed for the sake of reducing the sensor data transmission rate and the energy consumption. Based on a SOD concept, the sensors transmit the measurements when the prescribed conditioned is violated. By using the inductive method and intensive analysis on the estimation error, upper bounds of the estimation error covariances are obtained recursively. Subsequently, by choosing some scalar parameters properly, such upper bounds are reduced. In addition, for linear time-invariant system, the upper bounds are proved to be asymptotically bounded under certain conditions. Finally, through a numerical simulation, we have demonstrated that the proposed event-based estimator yields acceptable estimation performance while reduces the number of transmission greatly.



(a) The real part of voltage.

(b) The imaginary part of voltage.

Fig. 5.2 The actual and estimated state at Bus 3 under different event-triggering thresholds

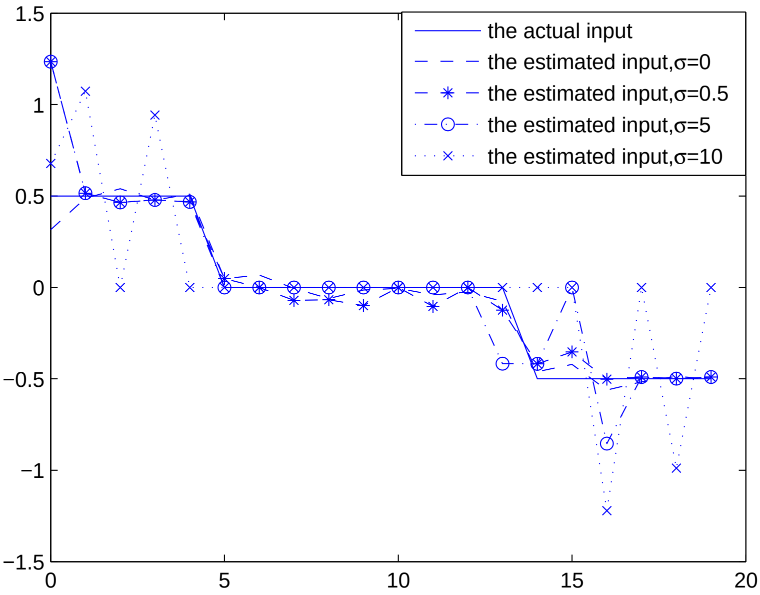


Fig. 5.3 The actual and estimated unknown input under different event-triggering thresholds

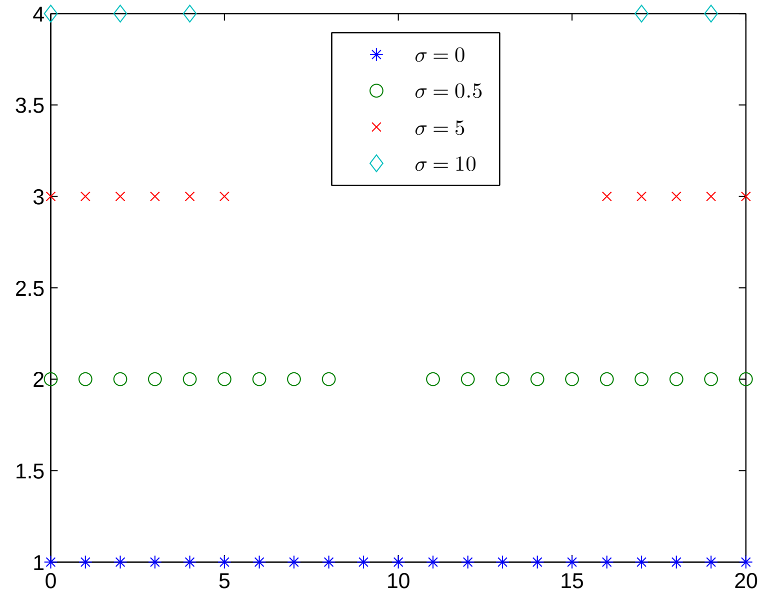


Fig. 5.4 The triggering sequence under different event-triggering thresholds

Chapter 6

State Estimation under False Data Injection Attacks: Security Analysis and System Protection

6.1 Motivation

the cyber-security in the state estimation problem of power grids has been a hot topic of research that stirs considerable interest. In general, two kinds of attacks have been considered [157], one is the denial-of-service (DoS) attack that violates data *availability* through blocking information flows between meters and the control centre, and the other is the false data injection (FDI) attack that violates data *integrity* through modifying the data packets. Compared with DoS attacks, FDI attacks are more difficult to detect because the adversary could keep the attacks stealthy to the bad data detector in EMS through deliberately designing the attack sequences.

The FDI attacks have been first considered in [110] for the state estimation problems of power grids where the *static* SE scheme is adopted. Since then, the cyber-security issue of the PSSE program has been extensively addressed from different aspects such as system vulnerability, attack detection and system protection. For example, the minimum number of comprised sensors that needed to launch deception attacks has been investigated in [95, 79, 148, 109] from the attackers' perspective, and some attack detection methods have been proposed in [156, 106, 57] from defenders' points of view.

Though the cyber-security under FDI attacks has been extensively addressed in the context of static state estimation, such a problem has not been sufficiently investigated in the context of *dynamic* state estimators, except some scattered results in [186, 113]. In fact, both the SSE and DSE schemes are currently used in practical power grids, and thus more attentions should be paid to the DSE schemes under cyber-attacks. Compared with FDI attacks in static model, the FDI attacks in dynamic models are more difficult to detect because the attacks can be mistaken as a type of noises by the protection devices. On the other hand, due to the system dynamics of power grids related with the behaviours in communication networks , the cyber-security issue in DSE cannot be solved using only classical systems and control approaches or existing information security methods [150]. As such, it is important yet challenging to investigate the cyber-security of the DSE program in power grids.

In this chapter, we focus on the dynamical state estimation problem for power grids under possible FDI attacks where a χ^2 detector is employed to monitor the state estimates. Note that FDI attacks have been considered in [119, 118, 120, 97] for state estimation problems of stochastic systems equipped with χ^2 detectors. In particular, an approximation method has been proposed in [118, 120] to analyse the cyber-security of the system by calculating the estimation error bound caused by the FDI attacks, and some *insecurity* conditions have been derived in [97, 119] to determine whether or not there exists FDI attacks which can cause unbounded estimation error for the state estimation system. Nevertheless, a thorough investigation reveals that 1) there is still room to improve the existing insecurity conditions; and 2) there is also an engineering need to develop system protection scheme by using only necessary number of communication channels requiring protection against FDI attacks.

The main purpose of the present research is to propose new insecurity conditions for state estimation problems under FDI attacks. Specifically, for the case when all communication channels are compromised by the adversary, we propose a *new* necessary and sufficient condition under which the system is insecure in the sense that the estimation error caused by FDI attacks is unbounded. Such new condition improves the existing ones as demonstrated by an example. For the case when only parts of the communication channels are compromised by the adversary, a sufficient condition is proposed as well. Furthermore, to protect the overall power grid from FDI attacks, we propose a criterion which determines a sufficient number of communication channels that require protection. According to the criterion, only necessary number of (rather than all) communication channels need to be protected in order to make the overall system secure against the FDI attacks.

The remainder of this chapter is organized as follows. The security problem of state estimation system under cyber-attacks are formulated in Section 6.2. In Section 6.3, we analyse the system security under FDI attacks for two cases and further propose the system protection scheme. Examples for illustration are given in Section 6.4 and we conclude the chapter in Section 6.5.

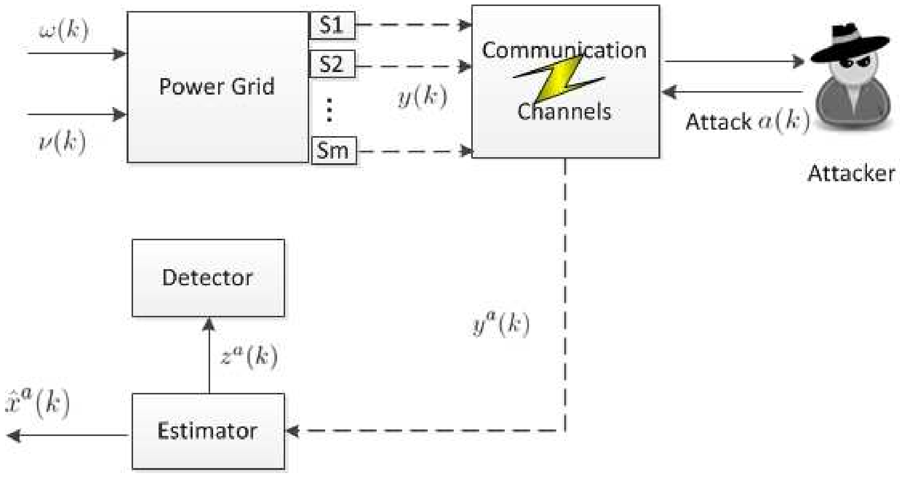


Fig. 6.1 Diagram of state estimation problem under cyber-attacks

6.2 Problem Formulation

In this section, we describe the model of false data injection (FDI) attack and analyse how the injected attacks affect the estimation system in power grids. The structure of the state estimation system under cyber-attacks is shown in Fig. 6.1. For presentation convenience, we first introduce the estimation system without cyber-attacks (i.e., $y^a(k) = y(k)$ in Fig. 6.1).

6.2.1 State Estimation without Cyber-attacks

The following dynamic equation is used to model the power system containing N buses

$$\mathscr{P}: \begin{cases} x(k+1) = Ax(k) + \omega(k) \\ \quad\;\; y(k) = Cx(k) + \nu(k) \end{cases} \tag{6.1}$$

where $x(k) \in \mathbb{R}^n$ is the voltages at all buses in the rectangular form and $n = 2N$, $y(k) = [y_1(k), \ldots, y_m(k)]^T \in \mathbb{R}^m$ is the PMU measurement output, and $y_i(k)$ is the output of the ith PMU (labelled as S_i in Fig. 6.1) at time instant k. The initial state $x(0)$ has mean $\bar{x}(0)$ and covariance $\Sigma(0)$, the process noise $\omega(k) \in \mathbb{R}^n$ and the measurement noise $\nu(k) \in \mathbb{R}^m$ are assumed to be mutually uncorrelated zero-mean random signals with known covariance matrices W and R, respectively. It is assumed that (A, C) is observable.

The following time-invariant state estimator is proposed:

$$\mathscr{E}: \begin{cases} \hat{x}(k+1) = A\hat{x}(k) + Kz(k+1) \\ z(k+1) = y(k+1) - CA\hat{x}(k) \end{cases} \tag{6.2}$$

where $\hat{x}(k+1)$ and $z(k+1)$ are the state estimate and the estimation residual at time instant $k+1$, respectively. Throughout this chapter, we assume that the estimator converges to its steady state.

Defining the estimation error $\tilde{x}(k+1) \triangleq x(k+1) - \hat{x}(k+1)$, the dynamics of the estimation error follows from (6.1) and (6.2) as follows:

$$\tilde{x}(k+1) = (I - KC)(A\tilde{x}(k) + \omega(k)) - K\nu(k+1). \tag{6.3}$$

It is well known that the estimator is stable if and only if the matrix $(I - KC)A$ is stable [71]. In this chapter, it is assumed that the estimator is stable by choosing appropriate estimator gain K.

Failure detectors are often used to detect abnormal operations. In this chapter, we assume that a χ^2 failure detector is deployed. At each time instant k, the χ^2 failure detector first computes the value $g(k) = z^T(k)(C\Sigma C^T + R)^{-1}z(k)$ where Σ is the steady estimation error covariance, and then compares $g(k)$ with a prescribed threshold α. If $g(k) > \alpha$, then an alarm will be triggered. When the system operates normally (i.e. without attacks), $g(k)$ satisfies a χ^2 distribution implying low probability of a large $g(k)$ [8].

From Fig. 6.1, we can see that there is a communication channel between each PMU S_i and the estimator $\mathscr{E}$. In practice, the PMUs and the estimator are mainly connected through wired or wireless network, and such networked communication makes the transmitted data prone to be attacked by the adversary.

6.2.2 False Data Injection Attack

In this subsection, we introduce the model of false data injection (FDI) attack and then investigate how it affects the estimation dynamics. Assume that the adversary has perfect knowledge about the system model, that is, the values of all the matrices A, C, K, W and R described in Subsection 6.2.1 are known by the attacker. We also assume that the attacker has the ability to inject false data over the communication channels between the PMUs and the estimator. Under FDI attacks, the measurement output received by the estimator is given as follows:

$$y^a(k) = Cx(k) + a(k) + \nu(k) = Cx(k) + B_a a^0(k) + \nu(k) \tag{6.4}$$

where $a(k) \in \mathbb{R}^m$ represents the false data injected by the attacker at time instant k. The attack vector is described by $a(k) = B_a a^0(k)$ where the injection matrix $B_a = \text{diag}\{\gamma_1, \ldots, \gamma_m\}$. Here, $\gamma_i = 1$ if the attacker is able to inject false data into the ith communication channel, otherwise $\gamma_i = 0$. The matrix B_a reflects which communication channels can be compromised by the attacker. Specifically, $B_a = 0$ means that no FDI attacks can be injected into any communication channel, and $B_a = I_m$ implies that the attacker has the ability to inject FDI attacks into all communication channels.

With the compromised measurement $y^a(k)$, based on the estimator $\mathscr{E}$ in (6.2), the dynamics of state estimation can be derived as follows:

$$\begin{aligned} \hat{x}^a(k+1) =& A\hat{x}^a(k) + Kz^a(k+1) \\ z^a(k+1) =& y^a(k+1) - CA\hat{x}^a(k) \end{aligned} \tag{6.5}$$

where $\hat{x}^a(k+1)$ and $z^a(k+1)$ are the state estimation and the estimation residual of system (6.1) at time $k+1$ using the compromised measurement (6.4), respectively. Without loss of generality, we assume that the attack begins at time instant 1 and $\hat{x}^a(0) = \hat{x}(0)$.

To take into account the effect of FDI attacks on the state estimation of system (6.1), we define the difference between the state estimates of system (6.1) (without FDI attacks) and system (6.4) (with FDI attacks) as

$$\Delta\hat{x}(k+1) \triangleq \hat{x}^a(k+1) - \hat{x}(k+1),$$

and the difference between the estimation residuals of system (6.1) and (6.4) as

$$\Delta z(k+1) \triangleq z^a(k+1) - z(k+1).$$

For convenience, we call $\Delta\hat{x}(k+1)$ and $\Delta z(k+1)$ as the state estimation difference and the estimation residual difference, respectively. The dynamics of $\Delta z(k+1)$ and $\Delta\hat{x}(k+1)$ can be derived from (6.2) and (6.5) as follows:

$$\Delta z(k+1) = -CA\Delta\hat{x}(k) + a(k+1), \tag{6.6}$$

$$\begin{aligned} \Delta\hat{x}(k+1) &= A\Delta\hat{x}(k) + K\Delta z(k+1) \\ &= (I - KC)A\Delta\hat{x}(k) + Ka(k+1) \end{aligned} \tag{6.7}$$

where $\Delta\hat{x}(0) = \hat{x}^a(0) - \hat{x}(0) = 0$.

In the considered FDI attack model, the purpose of the attacker is to launch a “special” FDI attack sequence under which the state estimation difference $\Delta\hat{x}(k)$ will diverge to ∞ without any alarm triggered by the χ^2 detector. In other words, the attacker aims to inject false data which would largely degrade the estimation performance without being detected by the detector.

It is known from the triangular inequality $\|z^a(k)\| \leq \|z(k)\| + \|\Delta z(k)\|$ that, if $\|\Delta z(k)\|$ is small, then the χ^2 detector cannot distinguish between $z^a(k)$ and $z(k)$ with high probability. As such, to make the attack sequence stealthy, the attacker launching the FDI attacks should avoid causing a large change in estimation residual difference $\Delta z(k)$ [119], which means that the inequality $\|\Delta z(k)\| \leq M$ should hold all the time, where M represents the tolerant level of the χ^2 detector. Obviously, a smaller value of M would result in a higher probability for the corresponding attack to be undetected. We assume that M is predetermined by the attacker. On the other hand, the attacker should design the attack sequence deliberately such that the sequence $\{\Delta\hat{x}(k)\}$ becomes unbounded, i.e, $\lim_{k\to\infty} \Delta\hat{x}(k) = \infty$.

Throughout the chapter, the definition on system security is given as follows.

Definition 6.1 *The system $\mathscr{P}$ in (6.1) with estimator $\mathscr{E}$ in (6.2) is called insecure if there exists at least one FDI attack sequence $\{a(k)\}$ such that the following two conditions are satisfied simultaneously:*

1) for the state estimation difference $\Delta\hat{x}(k)$,

$$\lim_{k\to\infty} \|\Delta\hat{x}(k)\| \to \infty; \tag{6.8}$$

2) for the estimation residual difference $\Delta z(k)$,

$$\|\Delta z(k)\| \leq M, \tag{6.9}$$

where M is a prescribed small positive constant scalar.

In case that (6.8)-(6.9) do not hold simultaneously under FDI attacks (6.4), the system $\mathscr{P}$ in (6.1) with estimator $\mathscr{E}$ in (6.2) is called secure under FDI attacks (6.4).

The aim of the addressed system security problem is to analyse under what conditions there exists an FDI attack that is undetectable by the fault detector but drives the bias in state estimation to infinity.

6.3 Security Analysis

In this section, we investigate the security of system $\mathscr{P}$ in (6.1) with estimator $\mathscr{E}$ in (6.2) for the following two cases: 1) the attacker is able to inject FDI attacks into all communication channels, *i.e.*, $B_a = I_m$; and 2) the attacker can inject FDI attacks into only part of the communication channels, *i.e.*, $B_a \neq I_m$.

Assume that the system matrix A in (6.1) has p independent eigenvectors and its Jordan form J is given by

$$J = P^{-1}AP \tag{6.10}$$

where

$$J = \begin{bmatrix} J_1 & 0 & 0 & \dots & 0 \\ 0 & J_2 & 0 & \dots & 0 \\ 0 & 0 & J_3 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & J_p \end{bmatrix}, \quad J_i = \begin{bmatrix} \lambda_i & 1 & & & \\ & \lambda_i & 1 & & \\ & & \ddots & \ddots & \\ & & & \ddots & 1 \\ & & & & \lambda_i \end{bmatrix},$$

the Jordan block $J_i \in \mathbb{C}^{n_i \times n_i}$ $(i = 1,\dots,p)$ with $|\lambda_1| \geq |\lambda_2| \geq \dots \geq |\lambda_p|$ and $\sum_{i=1}^{i=p} n_i = n$. Denote $P = \begin{bmatrix} P_1,\dots,P_p \end{bmatrix}$ and $Q = P^{-1} = \begin{bmatrix} Q_1^T,\dots,Q_p^T \end{bmatrix}^T$, where $P_i \in \mathbb{C}^{n \times n_i}$ and $Q_i \in \mathbb{C}^{n_i \times n}$.

If $\rho(A) \geq 1$, there exists a positive integer l satisfying $1 \leq l \leq p$ such that the inequality $|\lambda_1| \geq \dots \geq |\lambda_l| \geq 1 > |\lambda_{l+1}| \geq \dots \geq |\lambda_p|$ is true. Furthermore, defining $\bar{l} = \sum_{i=1}^{l} n_i$, we have

$$A = PJQ = \left[\begin{array}{c:c} P_o & P_c \end{array}\right] \left[\begin{array}{c:c} \Lambda_1 & 0 \\ \hdashline 0 & \Lambda_2 \end{array}\right] \left[\begin{array}{c} Q_o \\ \hdashline Q_c \end{array}\right], \tag{6.11}$$

where block matrices $\Lambda_1 = \text{diag}\{J_1,\dots,J_l\} \in \mathbb{C}^{\bar{l} \times \bar{l}}$, $\Lambda_2 = \text{diag}\{J_{l+1},\dots,J_p\} \in \mathbb{C}^{(n-\bar{l}) \times (n-\bar{l})}$, $P_o = \begin{bmatrix} P_1,\dots,P_l \end{bmatrix}$, $P_c = \begin{bmatrix} P_{l+1},\dots,P_p \end{bmatrix}$, $Q_o = \begin{bmatrix} Q_1^T,\dots,Q_l^T \end{bmatrix}^T$ and $Q_c = \begin{bmatrix} Q_{l+1}^T,\dots,Q_p^T \end{bmatrix}^T$ are of appropriate dimensions.

6.3.1 Case 1: $B_a = I_m$

To introduce our main results, we need the following lemmas.

Lemma 6.1 *[72] For two matrices $M,N \in \mathbb{C}^{n \times n}$, $det(MN) = det(M)det(N)$. Moreover, matrices MN and NM have the same non-zero eigenvalues.*

Lemma 6.2 *For the system (6.1) with estimator (6.2), if $\rho(A) \geq 1$, the following matrix equation*

$$P_c X = K \tag{6.12}$$

has no solution, where matrix K is the estimator gain of state estimator (6.2) and matrix P_c is given in (6.11).

Proof. It is known from Lemma 6.1 that the matrices $(I-KC)A$ and $A(I-KC)$ have the same eigenvalues. Then, it follows from $\rho((I-KC)A)<1$ that the inequality $\rho(A(I-KC))<1$ holds.

Let us prove the lemma by contradiction. Assume that there exists a matrix solution $\tilde{X}$ to equation (6.12), then we have

$$A(I-KC)=\left[\begin{array}{c:c} P_o & P_c \end{array}\right]\left[\begin{array}{c:c} \Lambda_1 & 0 \\ \hdashline 0 & \Lambda_2 \end{array}\right]\left[\begin{array}{c} Q_o \\ \hdashline Q_c \end{array}\right](I-P_c\tilde{X}C),$$

and it follows from $Q_oP_c=0$ and $Q_cP_c=I$ that

$$A(I-KC)=\left[\begin{array}{c:c} P_o & P_c \end{array}\right]\left[\begin{array}{c:c} \Lambda_1 & 0 \\ \hdashline 0 & \Lambda_2 \end{array}\right]\left[\begin{array}{c} Q_o \\ \hdashline Q_c-\tilde{X}C \end{array}\right].$$

Accordingly, the characteristic polynomial of matrix $A(I-KC)$, denoted by $\det(\lambda I-A(I-KC))$, can be given as follows:

$$\begin{aligned}\det(\lambda I-A(I-KC))&=\det\left(\left[\begin{array}{c:c} P_o & P_c \end{array}\right]\lambda I\left[\begin{array}{c} Q_o \\ \hdashline Q_c \end{array}\right]-\left[\begin{array}{c:c} P_o & P_c \end{array}\right]\left[\begin{array}{c:c} \Lambda_1 & 0 \\ \hdashline 0 & \Lambda_2 \end{array}\right]\left[\begin{array}{c} Q_o \\ \hdashline Q_c-\tilde{X}C \end{array}\right]\right)\\&=\det\left(\left[\begin{array}{c:c} P_o & P_c \end{array}\right]\left[\begin{array}{c} (\lambda I-\Lambda_1)Q_o \\ \hdashline (\lambda I-\Lambda_2)Q_c+\Lambda_2\tilde{X}C \end{array}\right]\right)\\&=\det(P)\det\left(\left[\begin{array}{c} (\lambda I-\Lambda_1)Q_o \\ \hdashline (\lambda I-\Lambda_2)Q_c+\Lambda_2\tilde{X}C \end{array}\right]\right).\end{aligned} \tag{6.13}$$

Setting $\lambda=\lambda_i$ $(i\in\{1,\dots,l\})$, we can see that the last row of matrix $\lambda I-J_i$ is a zero row, which implies that there is at least a zero row in the sub-matrix $(\lambda I-\Lambda_1)Q_o$ and hence $\det(\lambda I-A(I-KC))=0$. In other words, we conclude that λ_i $(i=1,\dots,l)$ is the eigenvalue of matrix $A(I-KC)$. Noting that $|\lambda_i|\geq 1$ $(i=1,\dots,l)$, this conclusion contradicts the inequality $\rho(A(I-KC))<1$. As a result, there is no solution to the matrix equation (6.12) and the proof is complete. ■

From Lemma 6.2, the following lemma can be easily obtained.

Lemma 6.3 *For the system (6.1) with estimator (6.2), let $\rho(A)\geq 1$ and $E_{s,t}$ represent the element of matrix E in the sth row and tth column. Define matrix $E=P^{-1}K$. Then, there exists at least one non-zero component in matrix E, that is, there exist integers $s\in\{1,\dots,\bar{l}\}$ and $t\in\{1,\dots,m\}$ with $\bar{l}\triangleq\sum_{i=1}^{l}n_i$ such that $E_{s,t}\neq 0$.*

Algorithm 6.1 The algorithm for generating false date Injection attacks (FDI attacks)

```
Initialize:
    Decompose matrix $A$ in (6.1) as the Jordan normal form (6.10), Choose
    arbitrarily a scalar $\sigma \in (0,1)$ and the positive scalar $M$;
Determine the integers $t$, $r$ and $q$ according to Lemma 6.3, (6.18) and (6.19), respectively;
Set $\bar{t}_r(0) = 0$;
while $k \geq 0$ do
    if $\mathrm{Re}\{\lambda_q \bar{t}_r(k)\} \geq 0$ then
        Set $\sigma(k+1) = \sigma$;
        Set the attack sequence $a(k+1) = CA\Delta\hat{x}(k) + \sigma(k+1)MI_m^t$ ;
    else
        Set $\sigma(k+1) = -\sigma$;
        Set the attack sequence $a(k+1) = CA\Delta\hat{x}(k) + \sigma(k+1)MI_m^t$ ;
    end if
    Calculate the state estimation difference $\Delta\hat{x}(k+1)$ according to (6.7);
    Calculate $\bar{t}_r(k+1)$ according to (6.21);
    $k = k+1$;
end while
```

Proof. Let us prove the lemma by contradiction. Assume that $E_{s,t} = 0$, $\forall s \in \{1,\ldots,\bar{l}\}$, $\forall t \in \{1,\ldots,m\}$. That is, $E = \begin{bmatrix} 0 \\ \hdashline \bar{E} \end{bmatrix}$ where $\bar{E} \in \mathbb{C}^{(n-\bar{l})\times m}$ is the sub-matrix forming by the last $n-\bar{l}$ rows of E. Then, the equation $K = PE$ can be rewritten as follows:

$$K = PE = \begin{bmatrix} P_o \,\vdots\, P_c \end{bmatrix} \begin{bmatrix} 0 \\ \hdashline \bar{E} \end{bmatrix} = P_c\bar{E}.$$

The above equation implies that $\bar{E}$ is the solution of equation (6.12), which contradicts the statement in Lemma 6.2 that equation (6.12) has no solution. The proof is now complete. ■

Before we present the necessary and sufficient condition under which the system (6.1) with estimator (6.2) is *insecure*, a procedure for generating a certain sequence of FDI attacks is outlined in Algorithm 6.1.

Theorem 6.1 *Assume that the attacker is able to attack all communication channels, that is, $B_a = I_m$. The system (6.1) with state estimator (6.2) is insecure if and only if $\rho(A) \geq 1$.*

Proof. (**Sufficiency**) We start by proving that, if $\rho(A) \geq 1$, the system (6.1) state estimator (6.2) is *insecure*. According to Definition 6.1, we need to prove that there exists at least one FDI attack sequence satisfying both (6.8) and (6.9) if $\rho(A) \geq 1$. In the following, we prove that (6.8) and (6.9) are true under the attacks generated by Algorithm 6.1.

According to Algorithm 6.1, it is known that

$$a(k+1) = CA\Delta\hat{x}(k) + \sigma(k+1)MI_m^t \tag{6.14}$$

where $\sigma(k+1)$ takes value on either σ or $-\sigma$ with $\sigma \in (0,1)$. It follows from (6.6) and (6.14) that

$$\Delta z(k+1) = \sigma(k+1)MI_m^t, \tag{6.15}$$

from which we can easily see that $\|\Delta z(k+1)\| = \sigma M < M$, and this implies that condition (6.9) is satisfied.

To show that the condition (6.8) is satisfied, we define vector $t(k) = Q\Delta\hat{x}(k)$ where $t(k) = [t_1^T(k), \dots, t_p^T(k)]^T$ with $t_i(k) \in \mathbb{C}^{n_i}$ $(i \in \{1,2,\dots,p\})$. Based on (6.7), (6.11) and Lemma 6.3, the dynamics of $t(k)$ can be derived as follows:

$$\begin{aligned} t(k+1) &= Jt(k) + QK\Delta z(k+1) = Jt(k) + QPE\Delta z(k+1) \\ &= Jt(k) + E\Delta z(k+1). \end{aligned} \tag{6.16}$$

Substituting (6.15) into (6.16) gives

$$t(k+1) = Jt(k) + \sigma(k+1)MEI_m^t.$$

Define $\bar{t}(k) = \left[t_1^T(k), \dots, t_l^T(k)\right]^T$ and $\underline{t}(k) = \left[t_{l+1}^T(k), \dots, t_p^T(k)\right]^T$. Noting that $J = \left[\begin{array}{c:c} \Lambda_1 & 0 \\ \hdashline 0 & \Lambda_2 \end{array}\right]$, one has

$$\bar{t}(k+1) = \Lambda_1 \bar{t}(k) + \sigma(k+1)Md, \tag{6.17}$$

where $d = \left[I_{\bar{l}}, 0_{\bar{l}\times(n-\bar{l})}\right] EI_m^t$, *i.e.*, vector d is formed by the first $\bar{l}$ elements of the tth column of matrix E. From Lemma 6.3, it is known that $d \neq 0$.

Define $d = \left[d_1, \dots, d_{\bar{l}}\right]^T$ and

$$r =_{1\leq j\leq \bar{l}} \ (d_j \neq 0), \tag{6.18}$$

that is, d_r is the non-zero element of vector d with the maximal index. Since $1 \leq r \leq \bar{l}$, there exists an integer q $(1 \leq q \leq l)$ such that

$$\sum_{i=1}^{q} n_i - n_q < r \leq \sum_{i=1}^{q} n_i. \tag{6.19}$$

It follows from (6.17) that

$$\begin{bmatrix} \bar{t}_r(k+1) \\ \bar{t}_{r+1}(k+1) \\ \vdots \\ \bar{t}_{n_q}(k+1) \end{bmatrix} = \begin{bmatrix} \lambda_q & 1 & & \\ & \lambda_q & \ddots & \\ & & \ddots & 1 \\ & & & \lambda_q \end{bmatrix} \begin{bmatrix} \bar{t}_r(k) \\ \bar{t}_{r+1}(k) \\ \vdots \\ \bar{t}_{n_q}(k) \end{bmatrix} + \sigma(k+1)M \begin{bmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}, \tag{6.20}$$

where $\bar{t}_j(k)$ is the jth element of vector $\bar{t}(k)$, $j \in \{r, r+1, \dots, n_q\}$.

Noting the initial condition $\bar{t}_{r+1}(0) = 0$, it can be easily derived from (6.20) that $\bar{t}_{i+1}(k) = 0$ and

$$\bar{t}_r(k+1) = \lambda_q \bar{t}_r(k) + \sigma(k+1)M, \tag{6.21}$$

and therefore

$$|\bar{t}_r(k+1)|^2 = |\lambda_q|^2 |\bar{t}_r(k)|^2 + \sigma^2(k+1)M^2 + 2\sigma(k+1)M\mathrm{Re}\{\lambda_q \bar{t}_r(k)\} \tag{6.22}$$

According to Algorithm 6.1, it is known that $\sigma(k+1)\mathrm{Re}\{\lambda_q \bar{t}_i(k)\} \geq 0$ and $\sigma^2(k+1) = \sigma^2$. Furthermore, noticing that $|\lambda_q| \geq 1$, we have

$$|\bar{t}_r(k+1)|^2 \geq |\lambda_q|^2 |\bar{t}_r(k)|^2 + \sigma^2 M^2 \geq |\bar{t}_r(k)|^2 + \sigma^2 M^2. \tag{6.23}$$

Based on the inequality $|\bar{t}_r(k+1)|^2 \geq |\bar{t}_r(k)|^2 + \sigma^2 M^2$ and the initial condition $\bar{t}_r(0) = 0$, it can be inferred that $|\bar{t}_r(k+1)|^2 \geq (k+1)\sigma^2 M^2$, which implies that $\lim_{k\to\infty} |\bar{t}_r(k+1)| = \infty$ and therefore $\lim_{k\to\infty} t(k+1) = \infty$. Since $t(k+1) = Q\Delta\hat{x}(k+1)$, it can be deduced that at least one component of vector $\Delta\hat{x}(k+1)$ is unbounded, and $\lim_{k\to\infty} \|\Delta\hat{x}(k+1)\| = \infty$. To this end, the condition (6.8) is satisfied and we finally reach the conclusion that the system is *insecure* under the attacks generated by Algorithm 6.1 if $\rho(A) \geq 1$.

(**Necessity**). To prove the necessity, we just need to show that the system $\mathscr{P}$ in (6.1) with estimator $\mathscr{E}$ in (6.2) is *secure* if matrix $\rho(A) < 1$. Again, let us prove by contradiction. Assume that the system (6.1) with estimator (6.2) is *insecure*, that is, there exist attacks sequences satisfying (6.8) and (6.9). It follows from (6.9) that $\Delta z(k+1)$ is norm-bounded. Since $\rho(A) < 1$, based on the equation $\Delta\hat{x}(k+1) = A\Delta\hat{x}(k) + K\Delta z(k+1)$, it can be inferred that $\Delta\hat{x}(k+1)$ is norm-bounded as well. That is, condition (6.8) is violated and the proof is now complete. ■

Remark 6.1 *In the main results of [119, 97], it has been stated that the necessary and sufficient conditions for the state error by FDI attacks to be unbounded are that a) the system matrix A should be unstable; and b) at least one eigenvector v corresponding to the unstable* *system mode satisfies $v \in Q_{oa}$ where Q_{oa} is the controllability matrix associated with the pair $(A-KCA, KB_a)$. Note that Condition b) has been removed in Theorem 6.1 of this chapter and we will use a simple example to show that the removal of such a condition is deemed to be necessary.*

Example 1: Consider the system given in (6.1) where the parameters are given by

$$A = \begin{bmatrix} 1.5 & 0 \\ 0.6 & 0.8 \end{bmatrix}, W = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, C = \begin{bmatrix} 0 & 1 \end{bmatrix}, Q = 1,$$

and the linear estimator is given in (6.2) with estimator gain $K = \begin{bmatrix} 1.4 & 1.2 \end{bmatrix}^T$.

Since matrix A has an unstable eigenvalue $\lambda = 1.5$ with eigenvector $p = \begin{bmatrix} 4 & -3 \end{bmatrix}^T$, it is known from Theorem 6.1 that the system is *insecure*. A specific FDI attack sequence is generated according to Algorithm 6.1, where the parameters are chosen as $\sigma = 0.1, M = 2$. It can be found from Fig. 6.2 that the norm of estimation error $||\Delta\hat{x}(k)||$ tends to unbounded while the norm of residual error $||\Delta\hat{z}(k)||$ is always less the prescribed scalar M.

On the other hand, from (6.7), the dynamics of estimation error $||\Delta\hat{x}(k)||$ can be given by

$$\Delta\hat{x}(k+1) = (I-KC)A\Delta\hat{x}(k) + Ka(k),\ \Delta\hat{x}(0) = 0, \tag{6.24}$$

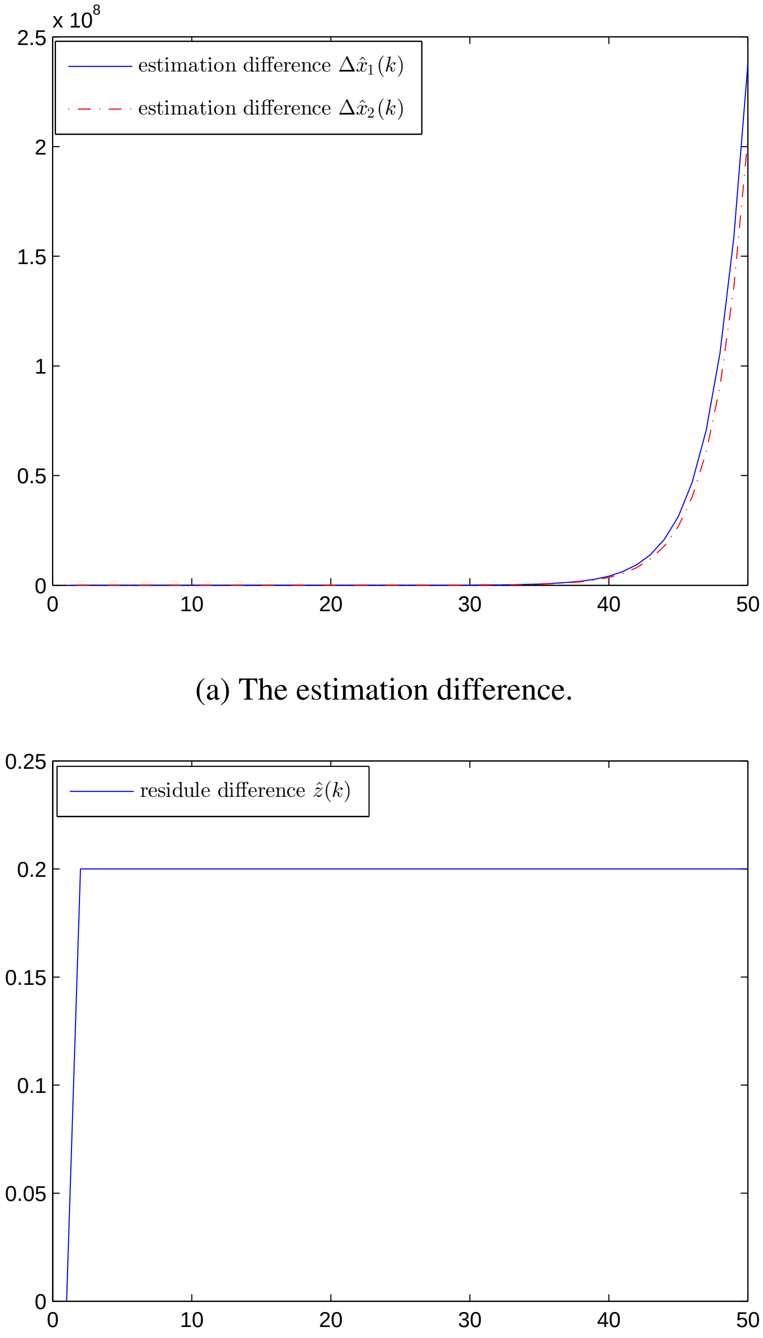
where $(I-KC)A = \begin{bmatrix} 0.66 & 1.12 \\ -0.12 & -0.16 \end{bmatrix}$. Through straightforward calculation, it can be found that $\Delta\hat{x}(k) \in \text{span}\left\{ \begin{bmatrix} 7 \\ 6 \end{bmatrix} \right\}$, and therefore the eigenvector p is not a reachable state of the dynamics system (6.24). According to the main results in [119, 97], the system is *secure* but this is not actually the case as evidenced from the simulation results.

6.3.2 Case 2: $B_a \neq I_m$

In this case, we assume that the attacker is able to inject false data to *only a part of* (rather than all) communication channels, i.e., $\text{Rk}\{B_a\} < m$. It can be easily seen from Theorem 6.1 that, if $\rho(A) < 1$, the system (6.1) with estimator (6.2) is *secure* no matter how many communication channels the attacker could hijack. As such, in this subsection, we only consider the case when $\rho(A) \geq 1$.

The following lemmas are useful in subsequent analysis.

Lemma 6.4 *[12] Let $A \in \mathbb{C}^{n\times m}$, $B \in \mathbb{C}^{m\times l}$ and $C \in \mathbb{C}^{k\times n}$. Assume that B has full row rank and C has full column rank. Then, $Rk\{AB\} = Rk\{A\} = Rk\{CA\}$.*



(a) The estimation difference.

(b) The residual difference.

Fig. 6.2 The estimation and residual differences under FDI attacks

Lemma 6.5 *If the system $\mathscr{P}$ in (6.1) with estimator $\mathscr{E}$ in (6.2) is insecure, then 1) the attack sequence $\{a_k\}$ leading to the insecurity is unbounded, and 2) the state estimation difference $\Delta\hat{x}(k)$ can be represented in the following form:*

$$\Delta\hat{x}(k) = P_o\zeta_1(k) + P_c\zeta_2(k) \tag{6.25}$$

for some $\zeta_1(k) \in \mathbb{C}^{\bar{l}}$ satisfying $\lim_{k\to\infty}\zeta_1(k) = \infty$ and some bounded vector sequence $\zeta_2(k) \in \mathbb{C}^{n-\bar{l}}$, where P_o and P_c are defined in (6.11).

Proof. Assume that the attack sequence $\{a_k\}$ leading to the insecurity is bounded. Noting that $\rho((I-KC)A) < 1$, it follows from the dynamics of $\Delta\hat{x}(k)$ in (6.7) that $\Delta\hat{x}(k+1)$ is bounded. According to Definition 6.1, the boundedness of $\Delta\hat{x}(k+1)$ contradicts the insecurity assumption of this lemma. As such, the attack sequence $\{a_k\}$ is unbounded.

Next, we proceed to prove that $\Delta\hat{x}(k)$ can be represented as (6.25) and we use the same notations for P,Q, P_o, P_c, Q_o and Q_c as defined in (6.10)-(6.11). Similar to the proof of Theorem 6.1, we define vector $t(k) \triangleq Q\Delta\hat{x}(k)$ and write $t(k) = \left[t_1^T(k),\ldots,t_p^T(k)\right]^T$ with $t_i(k) \in \mathbb{C}^{n_i}$ ($i \in \{1,2,\ldots,p\}$). According to (6.11), the dynamics of $t(k)$ can be given by

$$t(k+1) = \left[\begin{array}{c} \bar{t}(k+1) \\ \hdashline \underline{t}(k+1) \end{array}\right] = \left[\begin{array}{c:c} \Lambda_1 & 0 \\ \hdashline 0 & \Lambda_2 \end{array}\right]\left[\begin{array}{c} \bar{t}(k) \\ \hdashline \underline{t}(k) \end{array}\right] + \left[\begin{array}{c} Q_oK \\ \hdashline Q_cK \end{array}\right]\Delta z(k+1), \tag{6.26}$$

where $\bar{t}(k) \triangleq \left[t_1^T(k),\ldots,t_l^T(k)\right]^T$ and $\underline{t}(k) \triangleq \left[t_{l+1}^T(k),\ldots,t_p^T(k)\right]^T$.

As $\rho(\Lambda_2) < 1$ and $\Delta z(k)$ is norm-bounded, it can be inferred that $\underline{t}(k)$ is norm-bounded. On the other hand, it is easy to see that $\Delta\hat{x}(k) = Pt(k) = \left[\begin{array}{c:c} P_o & P_c \end{array}\right]\left[\begin{array}{c} \bar{t}(k) \\ \hdashline \underline{t}(k) \end{array}\right] = P_o\bar{t}(k) + P_c\underline{t}(k)$. Since $P_c\underline{t}(k)$ is bounded and $\lim_{k\to\infty}\Delta\hat{x}(k) = \infty$, it follows that $\lim_{k\to\infty}\bar{t}(k) = \infty$ and therefore expression (6.25) holds for $\zeta_1(k) = \bar{t}(k)$ and $\zeta_2(k) = \underline{t}(k)$, which completes the proof. ■

Theorem 6.2 *For the system $\mathscr{P}$ in (6.1), assume that $\rho(A) \geq 1$, $Rk\{CP_o\} = r$ and the attacker is able to inject FDI attacks to a part of (but not all) communication channels, i.e., $Rk\{B_a\} < m$. The system $\mathscr{P}$ in (6.1) with estimator $\mathscr{E}$ in (6.2) is secure if the following condition holds:*

$$Rk\big\{(I-B_a)CP_o\big\} = r. \tag{6.27}$$

Proof. Again, we prove the theorem by contradiction. Suppose that the system is *insecure* when condition (6.27) holds. It follows from Lemma 6.5 that (6.25) is true. Furthermore, noting that $\Delta z(k+1)$ is bounded, it follows from (6.6) and (6.25) that

$$a(k+1) = CA\Delta\hat{x}(k) + \Delta z(k+1) = CP_o\Lambda_1\zeta_1(k) + O(k), \tag{6.28}$$

where $O(k) \triangleq CP_c\Lambda_2\zeta_2(k) + \Delta z(k+1)$ which is obviously bounded.

Define matrix $\Phi = \left[\phi_1, \ldots, \phi_{\bar{l}}\right] = CP_o$ where the vector ϕ_i is equal to the ith column of the matrix CP_o $(1 \leq i \leq \bar{l})$. Since $\mathrm{Rk}\{CP_o\} = r$, there exists a matrix $\Psi = \left[\phi_{i_1}, \phi_{i_2}, \ldots, \phi_{i_r}\right]$ satisfying $\mathrm{Rk}\{\Psi\} = r$ where $1 \leq i_1 < i_2 \leq \ldots < i_r \leq \bar{l}$. Moreover, the matrix CP_o can be represented as $CP_o = \Psi X$ where $X \in \mathbb{C}^{r\times\bar{l}}$. For matrix X, $X_s = I_{\bar{l}}^s$, $s \in \{i_1, \ldots, i_r\}$, where X_s represents the sth column of matrix X. It can be easily found that $\mathrm{Rk}\{X\} = r$, *i.e.*, matrix X has full row rank. As a result, (6.28) can be represented as follows

$$a(k+1) = \Psi\xi(k) + O(k), \tag{6.29}$$

where $\xi(k) = X\Lambda_1\zeta_1(k)$.

According to Lemma 6.5, the attack sequence $\{a(k)\}$ is unbounded, the sequence $\{O(k)\}$ is bounded, and therefore the vector sequence $\{\xi(k)\}$ is unbounded.

Left-multiplying both sides of (6.29) by $I - B_a$ gives rise to

$$(I-B_a)a(k+1) = (I-B_a)\Psi\xi(k) + (I-B_a)O(k),$$

and then it follows from $a(k+1) = B_a a^0(k+1)$ and $(I-B_a)B_a = 0$ that

$$(I-B_a)\Psi\xi(k) + (I-B_a)O(k) = 0. \tag{6.30}$$

Since $(I-B_a)CP_o = (I-B_a)\Psi X$ and X is full row rank, it is known from Lemma 6.4 that $\mathrm{Rk}\big\{(I-B_a)\Psi\big\} = \mathrm{Rk}\big\{(I-B_a)\Psi X\big\} = \mathrm{Rk}\big\{(I-B_a)CP_o\big\}$. Note the fact $\mathrm{Rk}\big\{(I-B_a)\Psi\big\} = r$ in (6.27) or, in other words, the matrix $(I-B_a)\Psi$ has full column rank. As $\lim_{k\to\infty}\xi(k) = \infty$, we have $\lim_{k\to\infty}(I-B_a)\Psi\xi(k) = \infty$ that contradicts (6.30), and the proof is now complete. ■

It is known From Theorem 6.1 that the system $\mathscr{P}$ in (6.1) with estimator $\mathscr{E}$ in (6.2) is *insecure* when $\rho(A) \geq 1$. In this case, it is important to ensure the security by protecting some communication channels. The following corollary provides an efficient method on which communication channels need to protected.

Corollary 6.1 *For the system (6.1), assume that $\rho(A) \geq 1$ and Rk$\{CP_o\} = r$. The system $\mathscr{P}$ in (6.1) with estimator $\mathscr{E}$ in (6.2) is secure if*

1) r communication channels are protected;

2) $Rk\Big\{\Big[\varphi_{i_1}^T,\cdots,\varphi_{i_r}^T\Big]^T\Big\} = r$*, where* $i_1,\ldots,i_r$ *are the indexes of the protected communication channels and* φ_j *is the jth row of matrix* CP_o $(i_1 \leq j \leq i_r)$*.*

Proof. Since the communication channels $i_1,\ldots,i_r$ are protected (i.e., free from cyber-attacks), according to the definition of matrix B_a, it is known that $\gamma_{i_1} = \ldots = \gamma_{i_r} = 0$ and $(I - B_a)CP_o = \Big[\gamma_1\varphi_1^T,\ldots,\gamma_m\varphi_m^T\Big]^T$.

On one hand, $\mathrm{Rk}\Big\{\Big[\varphi_{i_1}^T,\cdots,\varphi_{i_r}^T\Big]^T\Big\} = r$ implies that $\mathrm{Rk}\big\{(I-B_a)CP_o\big\} \geq r$. On the other hand, we have $\mathrm{Rk}\big\{(I-B_a)CP_o\big\} \leq \mathrm{Rk}\{CP_o\} = r$. As a result, $\mathrm{Rk}\big\{(I-B_a)CP_o\big\} = r$ and it follows from Theorem 6.2 that the system (6.1) with state estimator (6.2) is *secure*, which completes the proof. ■

Remark 6.2 *It is clear that* $Rk\{CP_o\} = r \leq \bar{l}$ *and it can be found from (6.11) that* $\bar{l}$ *is the number of unstable eigenvalues of matrix A (counted up to multiplicity). As such, Corollary 6.1 implies that the number of communication channels that should be protected is not more than the number of unstable eigenvalues of matrix A (counted up to multiplicity).*

6.4 Simulation Results

In this section, we consider the state estimation system of the three-bus system described in the simulation section of Chapter 5. For the 3-bus test system, we choose the state $x(k)$ as

$$x(k) = \big[x_{r,1}(k)\, x_{r,2}(k)\, x_{r,3}(k)\, x_{i,1}(k)\, x_{i,2}(k)\, x_{i,3}(k)\big]^T$$

where $x_{r,l}(k)$ and $x_{i,l}(k)$ represent the real and imaginary parts of voltage of the lth bus, respectively, then the system is modelled as (3.1) with parameters $A = \mathrm{diag}_6\{1.0\}$, $B = \mathrm{diag}_6\{0.02\}$, $W(k) = \mathrm{diag}_6\{0.01^2\}$ and $R(k) = \mathrm{diag}_{10}\{0.1^2\}$. The trend

$$u = \Big[0, -0.008, 0.02, -0.026, -0.01, -0.014\Big]$$

. Furthermore, assume that the initial voltages of all buses are at flat start, that is, $x_{r,l}(0) = 1$ p.u, $x_{i,l}(0) = 0$ for all $l = 1,2,\ldots,3$.

The values of branch parameters are the same as the ones in [15]. We assume that each PMU measurement either one bus voltage or one branch current. Three PMUs measure the voltages at bus 1,2 and 3, and two PMUs measure the current at line 1-2 and 3-1. Each PMU send the measurements to the estimator using its own communication channel. A stationary Kalman filter is employed in the remote estimator and a χ^2 fault detector is employed as

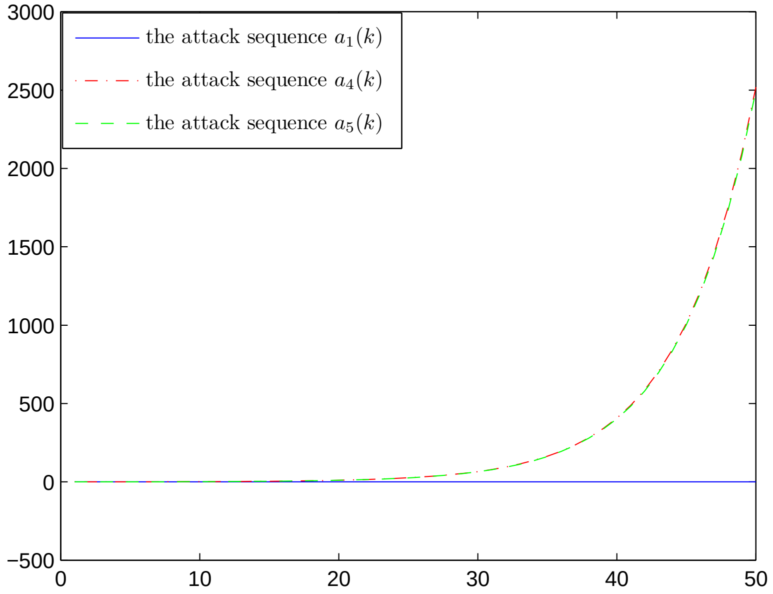


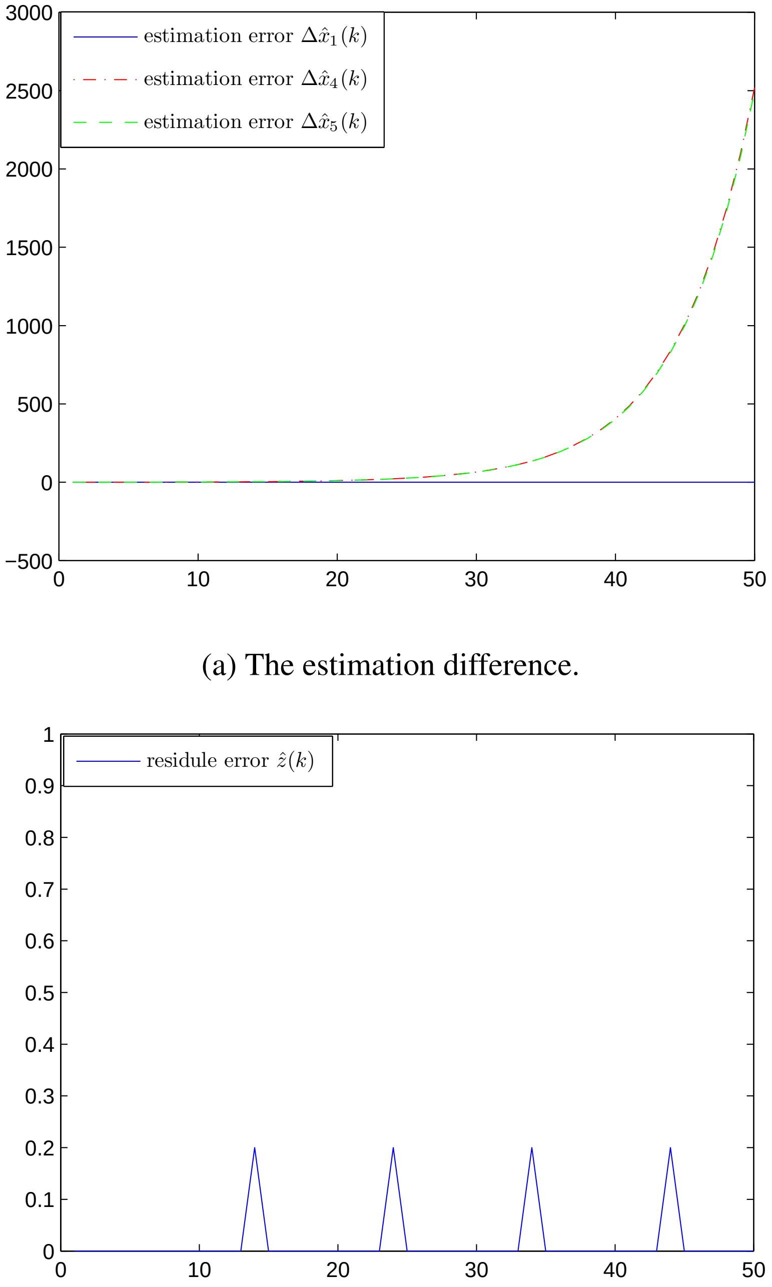
Fig. 6.3 The generated FDI attacks

well. Our purpose is to 1) analyse the security of the system, and 2) protect the system from cyber-attacks if it is insecure.

It can be computed that the eigenvalues of system matrix are all 1.0. According to Theorem 6.1, the estimation system of the power grid is insecure. To confirm this conclusion via simulation, a specific deceptive FDI attacks sequence is generated according to Algorithm 6.1 where the parameters are chosen as $\sigma = 0.1, M = 2$. Fig. 6.3 shows the generated FDI attack sequence $\{a(k)\}$.

Fig. 6.4 depicts the state estimation difference $\Delta\hat{x}(k)$ and the estimation residual difference $\Delta\hat{z}(k)$ under the designed attack sequences $\{a(k)\}$, respectively. From Figs. 6.3-6.4, it can be seen that the sequence $\{\Delta\hat{x}(k)\}$ diverges to ∞ while the sequence $\{\|\Delta\hat{z}(k)\|\}$ is always less the prescribed scalar M. Here, the estimated state of the 3-bus system under the designed FDI attacks deviates significantly from its nominal one but this cannot be detected by the χ^2 fault detector. In other words, the state of the power gird cannot be tracked at all under the attacks by the adversary.

Next, let us consider how to protect the system from cyber-attacks. It can be computed that $\text{Rank}(CP_o) = 6$, according to Corollary 6.1, it is known that the state estimate system of the power grid is secure if the communication channel between the three PMUs that measure bus voltages and the estimator is protected.



(a) The estimation difference.

(b) The residual difference.

Fig. 6.4 The estimation and residual differences under FDI attacks

6.5 Conclusion

In this chapter, we have considered the security issues in state estimation of power grids, where the adversary can inject false data into the communication channels between PMUs and the state estimator in a remote control centre. For the case that the adversary can compromise all communication channels, a necessary and sufficient condition has been derived under which the estimation error caused by the attacks is unbounded all the time. For the case that the adversary can only compromise a part of the communication channels, a sufficient condition ensuring the security is derived as well. Moreover, a criterion on protecting a sufficient number of channels such that the estimation error is kept bounded under FDI attacks has been proposed. A simulation example has been proposed to demonstrate the usefulness of the developed results and algorithms.

Chapter 7

Conclusions and Future Research

In this chapter, we first summarize our work in this thesis and then point out some directions of further research that follow from this thesis.

7.1 Concluding Remarks

The unconventional measurements pose great challenges to the state estimation program of power grids. The inability of processing mixed (RTU and PMU) measurements makes the traditional state estimation method outdated. The disregard of incomplete information in measurement data degrades the estimation performance. The vulnerability of the state estimation scheme exposes itself to cyber-attacks.

In this thesis, we propose a series of new state estimation methods. Specifically, considering of the missing measurements, a novel EKF state estimator is designed, in which the PMU measurements are incorporated as well (Chapter 3); an explicit model for the power grid with quantized nonlinear measurement is proposed, and based on the model a recursive estimation algorithm is developed for the system with consideration of quantization effects (Chapter 4); an event-based state estimator is designed which could maintain the estimation performance under limited communication resources (Chapter 5); the cyber-security of the DSE scheme in power grids is examined and the corresponding system protection scheme against FDI attacks is developed (Chapter 6). Next, we summarise the research results presented in each of these chapters.

Chapter 3 presents a hybrid EKF and PSO algorithm which can be used for state estimation of power grids. In consideration of the missing traditional measurements, a novel EKF estimator is designed for the power system. The PMU measurements is incorporated in the designed EKF estimator via the characterization of a set of inequality constraints. The constrained state estimation problem is transformed to a constrained optimization problem. Then, the PSO algorithm together with the penalty function is employed to solve the constrained optimization problem. Simulations confirm the effectiveness of the propose method.

Chapter 4 presents a recursive dynamic state estimation algorithm for power grids. The system model with quantized RTU and PMU measurements is first proposed. In consideration of the quantization effect of nonlinear measurement, both the linearisation and quantization errors is represented in terms of norm-bounded uncertainty matrices. Then, in the frame of robust estimation, a recursive filter is designed to guarantee that, despite the uncertainties existing in the derived model, the estimation error covariances are always less than a finite upper bound. Furthermore, the filter gain is designed such that the upper bound is minimized. Simulations illustrate the performance of our proposed algorithm. Higher estimation accuracy can be achieved with our algorithm than that from the traditional EKF algorithm, which has confirmed the effectiveness of the propose filter algorithm.

In Chapter 5, the joint input and state estimation problem is considered for power grids. For the sake of reducing the PMU data transmission rate, an event-based transmission scheme is proposed, with which the current measurement is released to the estimator only when the difference from the previously transmitted one is greater than a prescribed threshold. The purpose of this chapter is to design an event-based recursive input and state estimator such that the estimation error covariances have guaranteed upper bounds at all times. The estimator gains are calculated by solving two constrained optimization problems and the upper bounds of the estimation error covariances are obtained in form of the solution to Riccati-like difference equations. Special efforts are made on the choices of appropriate scalar parameter sequences in order to reduce the upper bounds. In the special case of linear time-invariant system, sufficient conditions are acquired under which the upper bound of the error covariance of the state estimation is asymptomatically bounded. Numerical simulations are conducted to illustrate the effectiveness of the proposed estimation algorithm.

In Chapter 6, the security issue in the dynamic state estimation problem for power grids is investigated. The communication channels between the meters of PMUs and the remote estimator in the control centre are vulnerable to attacks from malicious adversaries. The FDI attacks are considered. We aim to find the so-called *insecurity* conditions under which the estimation system is insecure in the sense that there exist FDI attacks that can bypass the anomaly detector but still lead to unbounded estimation errors. In particular, a *new* necessary and sufficient condition for the insecurity is derived in the case that all communication channels are compromised by the adversary. Furthermore, a specific attack algorithm is proposed with which the estimation system is insecure. Moreover, for the insecure system, we propose a system protection scheme through which only a few (rather than all) communication channels require protection against FDI attacks. A simulation example is utilized to demonstrate the usefulness of the proposed conditions/algorithms in the secure estimation problem for power grids.

7.2 Recommendations for Future Research

Although we have presented several new state estimation algorithms that are capable to deal with the challenges caused by unconventional measurements in power grids, the work may be further developed in a number of ways:

- Two specific network-induced incomplete information phenomena, namely, the missing measurements and quantized measurements, have been considered in Chapter 3 and Chapter 4, respectively. In the communication networks of practical power grids, some other phenomena such as time delay, time-varying sampling intervals may emerge as well, resulting incomplete information of measurements received by the control centre. Moreover, different incomplete information phenomena may emerge simultaneously. For example, due to traffic congestion in the networked environment, some data packets may be transmitted successfully but with a time delay and some others may be totally lost. As such, one future research direction is to consider the different kinds of incomplete information phenomena in a unified framework.

- In this thesis, all the developed state estimators works in the traditional *centralized* estimation manner. One of the future research directions is the *decentralized* DSE of power grids with unconventional measurements. Compared with the centralized estimation algorithm, the decentralized one is much faster and its speed remains independent of the size of the system[145]. However, the limited bandwidth of communication networks may cause network-induced phenomena in the decentralized DSE as well. Recently, some theoretical results on distributed dynamic state estimation problem under limited communication bandwidth have been obtained in [124, 41]. How to extend these theoretical results to the practical application of DSE design in power grids will be the next topic in our future research.

- Building dynamics model of the power grid is an indispensable part of the DSE scheme. Though several effective models have been proposed and applied, there is still a lack of rigorous validations to decide whether the proposed models are optimal or not. Moreover, in almost all system models used in DSE schemes, it is assumed that 1) the system state variables are uncoupled such that a diagonal transition matrix is used, and 2) the system noise is a Gaussian white noise. Are these assumptions reasonable? There is a need to justify the models through extensive experimental design and data analysis. In this regard, model verification of the DSE scheme is another future research direction.

- Since the DSE is a model-based estimation scheme, its performance relies on the accuracy of real-time system parameters. In this thesis since we focus on the impact of unconventional measurements on the estimation performances, we adopt the conventional assumption that all system parameters keep constant. In fact, system parameters may be time-varying and the constant values of system parameters stored in the database may be incorrect [15]. In order to further improve the estimation performance, there is a need to jointly estimate the parameters and state of the power grids in real time, which could be another future research direction.

- Though the cyber-security in state estimation of power grids has attracted lots of research attentions, it is still a relatively young research area. Up to now, almost all research results are based on the *approximately linearised* state estimation model of power grids. However, the countermeasure schemes developed using the approximate model may fail to protect the state estimation program in practical power grids due to the inherent difference between the approximate and the exact models. To shorten the gap between current research and practical application, future researches should be done to re-examine the cyber-secuity of state estimation for power grids based on the exact nonlinear model.

References

[1] Power systems test case archive. *http://www.ee.washington.edu/research/pstca/*.

[2] A. Abur and A. G. Exposito. *Power System State Estimation: Theory and Implementation*. Marcel Decker, New York, 2004.

[3] A. Al-Othman and M. Irving. Uncertainty modelling in power system state estimation. *IEE Generation, Transmission & Distribution*, 152(2):233–239, 2005.

[4] A. Alimardani, F. Therrien, D. Atanackovic, J. Jatskevich, and E. Vaahedi. Distribution system state estimation based on nonsynchronized smart meters. *IEEE Transactions on Smart Grid*, 6(6):2919–2928, 2015.

[5] F. Aminifar, M. Fotuhi-Firuzabad, A. Safdarian, A. Davoudi, and M. Shahidehpour. Synchrophasor measurement technology in power systems: panorama and state-of-the-art. *IEEE Access*, 2:1607–1628, 2014.

[6] F. Aminifar, M. Fotuhi-Firuzabad, M. Shahidehpour, and A. Khodaei. Observability enhancement by optimal PMU placement considering random power system outages. *Energy Systems*, 2(1):45–65, 2011.

[7] F. Aminifar, M. Shahidehpour, M. Fotuhi-Firuzabad, and S. Kamalinia. Power system dynamic state estimation with synchronized phasor measurements. *IEEE Transactions on Instrumentation and Measurement*, 63(2):352–363, 2014.

[8] B. D. Anderson and J. B. Moore. *Optimal Filtering*. Courier Dover Publications, 2005.

[9] P. M. Ashton, G. A. Taylor, M. R. Irving, I. Pisica, A. M. Carter, and M. E. Bradley. Novel application of detrended fluctuation analysis for state estimation using synchrophasor measurements. *IEEE Transactions on Power Systems*, 28(2):1930–1938, 2013.

[10] M. Basin, S. Elvira-Ceja, and E. N. Sanchez. Mean-square H_∞ filtering for stochastic systems: Application to a 2dof helicopter. *Signal Processing*, 92(3):801–806, 2012.

[11] M. Basin, P. Shi, D. Calderon-Alvarez, and J. Wang. Central suboptimal H_∞ filter design for linear time-varying systems with state or measurement delay. *Circuits, Systems & Signal Processing*, 28(2):305–330, 2009.

[12] D. S. Bernstein. *Matrix Mathematics: Theory, Facts, and Formulas*. Princeton University Press, 2009.

[13] S. Bi and Y. J. Zhang. Graphical methods for defense against false-data injection attacks on power system state estimation. *IEEE Transactions on Smart Grid*, 5(3):1216–1227, 2014.

[14] T. Bi, X. Qin, and Q. Yang. A novel hybrid state estimator for including synchronized phasor measurements. *Electric Power Systems Research*, 78(8):1343–1352, 2008.

[15] X. Bian, X. Li, H. Chen, D. Gan, and J. Qiu. Joint estimation of state and parameter with synchrophasors part I: State tracking. *IEEE Transactions on Power Systems*, 26(3):1196–1208, 2011.

[16] X. Bian, X. Li, H. Chen, D. Gan, and J. Qiu. Joint estimation of state and parameter with synchrophasors part II: Parameter tracking. *IEEE Transactions on Power Systems*, 26(3):1209–1220, 2011.

[17] E. Blood, B. Krogh, and M. Ilic. Electric power system static state estimation through Kalman filtering and load forecasting. In *Proc. Power and Energy Society General Meeting*, pages 1–6, Pittsburgh, USA, 2008. IEEE.

[18] N. Bretas. An iterative dynamic state estimation and bad data processing. *International Journal of Electrical Power & Energy Systems*, 11(1):70–74, 1989.

[19] M. Brown Do Coutto Filho, A. da Silva, and D. Falcao. Bibliography on power system state estimation (1968-1989). *IEEE Transactions on Power Systems*, 5(3):950–961, 1990.

[20] M. Brown Do Coutto Filho and J. de Souza. Forecasting-aided state estimation Part I: Panorama. *IEEE Transactions on Power Systems*, 24(4):1667–1677, 2009.

[21] M. Brown Do Coutto Filho, J. de Souza, and R. Freund. Forecasting-aided state estimation part II: Implementation. *IEEE Transactions on Power Systems*, 24(4):1678–1685, 2009.

[22] G. Calafiore. Reliable localization using set-valued nonlinear filters. *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, 35(2):189–197, 2005.

[23] S. P. Carullo and C. O. Nwankpa. Experimental validation of a model for an information-embedded power system. *IEEE Transactions on Power Delivery*, 20(3):1853–1863, 2005.

[24] G. Celli, P. Pegoraro, F. Pilo, G. Pisano, and S. Sulis. DMS cyber-physical simulation for assessing the impact of state estimation and communication media in smart grid operation. *IEEE Transactions on Power Systems*, 29(5):2436–2446, 2014.

[25] M. Cepek, J. Douville, G. Fecteau, and R. Malewski. Loss measurement in high voltage thyristor valves. *IEEE Transactions on Power Delivery*, 9(3):1222–1236, 1994.

[26] Y. Chakhchoukh, V. Vittal, and G. T. Heydt. PMU based state estimation by integrating correlation. *IEEE Transactions on Power Systems*, 29(2):617–626, 2014.

[27] S. Chakrabarti and E. Kyriakides. PMU measurement uncertainty considerations in WLS state estimation. *IEEE Transactions on Power Systems*, 24(2):1062–1071, 2009.

[28] S. Chakrabarti, E. Kyriakides, and M. Albu. Uncertainty in power system state variables obtained through synchronized measurements. *IEEE Transactions on Instrumentation and Measurement*, 58(8):2452–2458, 2009.

[29] P. Chavali and A. Nehorai. Distributed power system state estimation using factor graphs. *IEEE Transactions on Signal Processing*, 63(11):2864–2876, 2015.

[30] Y. Chen, J. Ma, P. Zhang, F. Liu, and S. Mei. Robust state estimator based on maximum exponential absolute value. *IEEE Transactions on Smart Grid*, in press.

[31] Y. Cheng, H. Ye, Y. Wang, and D. Zhou. Unbiased minimum-variance state estimation for linear systems with unknown input. *Automatica*, 45(2):485–491, 2009.

[32] S. Cui, Z. Han, S. Kar, T. T. Kim, H. V. Poor, and A. Tajer. Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions. *IEEE Signal Processing Magazine*, 29(5):106–115, 2012.

[33] T. V. Cutsem and M. R. Pavella. Critical survey of hierarchical methods for state estimation of electric power systems. *IEEE Transactions on Power Apparatus and Systems*, (10):3415–3424, 1983.

[34] A. L. Da Silva, M. B. Do Coutto Filho, and J. De Queiroz. State forecasting in electric power systems. *IEE Generation, Transmission & Distribution*, 130(5):237–244, 1983.

[35] M. Darouach and M. Zasadzinski. Unbiased minimum variance estimation for systems with unknown exogenous inputs. *Automatica*, 33(4):717–719, 1997.

[36] M. Darouach, M. Zasadzinski, and M. Boutayeb. Extension of minimum variance estimation for systems with unknown inputs. *Automatica*, 39(5):867–876, 2003.

[37] A. Debs and R. Larson. A dynamic estimator for tracking the state of a power system. *IEEE Transactions on Power Apparatus and Systems*, (7):1670–1678, 1970.

[38] S. Deshmukh, B. Natarajan, and A. Pahwa. State estimation and voltage/var control in distribution network with intermittent measurements. *IEEE Transactions on Smart Grid*, 5(1):200–209, 2014.

[39] D. Ding, Z. Wang, B. Shen, and H. Shu. H_∞ state estimation for discrete-time complex networks with randomly occurring sensor saturations and randomly varying sensor delays. *IEEE Transactions on Neural Networks and Learning Systems*, 23(5):725–736, 2012.

[40] H. Dong, Z. Wang, X. Chen, and H. Gao. A review on analysis and synthesis of nonlinear stochastic systems with randomly occurring incomplete information. *Mathematical Problems in Engineering*, 2012, 2012.

[41] H. Dong, Z. Wang, and H. Gao. Distributed filtering for a class of time-varying systems over sensor networks with quantization errors and successive packet dropouts. *IEEE Transactions on Signal Processing*, 60(6):3164–3173, 2012.

[42] J. Du, S. Ma, Y.-C. Wu, and H. V. Poor. Distributed hybrid power state estimation under PMU sampling phase errors. *IEEE Transactions on Signal Processing*, 62(16):4052–4063, 2014.

[43] D. Dua, S. Dambhare, R. K. Gajbhiye, and S. Soman. Optimal multistage scheduling of PMU placement: An ILP approach. *IEEE Transactions on Power Delivery*, 23(4):1812–1820, 2008.

[44] N. Elia and S. K. Mitter. Stabilization of linear systems with limited information. *IEEE Transactions on Automatic Control*, 46(9):1384–1400, 2001.

[45] K. Emami, T. Fernando, H.-C. Iu, H. Trinh, and K. Wong. Particle filter approach to dynamic state estimation of generators in power systems. *IEEE Transactions on Power Systems*, 30(5):2665–2675, 2015.

[46] M. Esmalifalak, G. Shi, Z. Han, and L. Song. Bad data injection attack and defense in electricity market using game theory study. *IEEE Transactions on Smart Grid*, 4(1):160–169, 2013.

[47] C. Y. Evrenosoglu and A. Abur. Travelling wave based fault location for teed circuits. *IEEE Transactions on Power Delivery*, 20(2):1115–1121, 2005.

[48] L. Fan, Z. Miao, and Y. Wehbe. Application of dynamic state and parameter estimation techniques on real-world data. *IEEE Transactions on Smart Grid*, 4(2):1133–1141, 2013.

[49] X. Fang, S. Misra, G. Xue, and D. Yang. Smart grid – the new and improved power grid: A survey. *IEEE Communications Surveys & Tutorials*, 14(4):944–980, 2012.

[50] M. Fu and C. E. de Souza. State estimation for linear discrete-time systems using quantized measurements. *Automatica*, 45(12):2937–2945, 2009.

[51] M. Fu and L. Xie. The sector bound approach to quantized feedback control. *IEEE Transactions on Automatic Control*, 50(11):1698–1711, 2005.

[52] A. Garcia, A. Monticelli, and P. Abreu. Fast decoupled state estimation and bad data processing. *IEEE Transactions on Power Apparatus and Systems*, (5):1645–1652, 1979.

[53] E. Ghahremani and I. Kamwa. Dynamic state estimation in power system by applying the extended Kalman filter with unknown inputs to phasor measurements. *IEEE Transactions on Power Systems*, 26(4):2556–2566, 2011.

[54] H. Gharavi and B. Hu. Multigate communication network for smart grid. *Proceedings of the IEEE*, 99(6):1028–1045, 2011.

[55] S. G. Ghiocel, J. H. Chow, G. Stefopoulos, B. Fardanesh, D. Maragal, B. Blanchard, M. Razanousky, and D. B. Bertagnolli. Phasor-measurement-based state estimation for synchrophasor data quality improvement and power transfer interface monitoring. *IEEE Transactions on Power Systems*, 29(2):881–888, 2014.

[56] A. Giani, R. Bent, and F. Pan. Phasor measurement unit selection for unobservable electric power data integrity attack detection. *International Journal of Critical Infrastructure Protection*, 7(3):155–164, 2014.

[57] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, K. Poolla, et al. Smart grid data integrity attacks. *IEEE Transactions on Smart Grid*, 4(3):1244–1253, 2013.

[58] S. Gillijns and B. De Moor. Unbiased minimum-variance input and state estimation for linear discrete-time systems. *Automatica*, 43(1):111–116, 2007.

[59] M. Glavic and T. Van Cutsem. Reconstructing and tracking network state from a limited number of synchrophasor measurements. *IEEE Transactions on Power Systems*, 28(2):1921–1929, 2013.

[60] M. Gol and A. Abur. A hybrid state estimator for systems with limited number of PMUs. *IEEE Transactions on Power Systems*, 30(3):1511–1517, 2015.

[61] A. Gómez-Expósito, A. Abur, A. De La Villa Jaén, and C. Gómez-Quiles. A multilevel state estimation paradigm for smart grids. *Proceedings of the IEEE*, 99(6):952–976, 2011.

[62] A. Gómez-Expósito, A. de la Villa Jaén, C. Gómez-Quiles, P. Rousseaux, and T. Van Cutsem. A taxonomy of multi-area state estimation methods. *Electric Power Systems Research*, 81(4):1060–1069, 2011.

[63] C. Gu and P. Jirutitijaroen. Dynamic state estimation under communication failure using kriging based bus load forecasting. *IEEE Transactions on Power Systems*, 30(6):2831–2840, 2015.

[64] Z. Guan, N. Sun, Y. Xu, and T. Yang. A comprehensive survey of false data injection in smart grid. *International Journal of Wireless and Mobile Computing*, 8(1):27–33, 2015.

[65] V. C. Gungor and G. P. Hancke. Industrial wireless sensor networks: Challenges, design principles, and technical approaches. *IEEE Transactions on Industrial Electronics*, 56(10):4258–4265, 2009.

[66] V. C. Gungor, B. Lu, and G. P. Hancke. Opportunities and challenges of wireless sensor networks in smart grid. *IEEE Transactions on Industrial Electronics*, 57(10):3557–3564, 2010.

[67] Y. Guo, W. Wu, B. Zhang, and H. Sun. An efficient state estimation algorithm considering zero injection constraints. *IEEE Transactions on Power Systems*, 28(3):2651–2659, 2013.

[68] Z. Guo, S. Li, X. Wang, and W. Heng. Distributed point-based Gaussian approximation filtering for forecasting-aided state estimation in power systems. *IEEE Transactions on Power Systems*, in press.

[69] D. Han, Y. Mo, J. Wu, S. Weerakkody, B. Sinopoli, and L. Shi. Stochastic event-triggered sensor schedule for remote state estimation. *IEEE Transactions on Industrial Electronics*, 60(10):2661–2675, 2015.

[70] J. Hao, R. J. Piechocki, D. Kaleshi, W. H. Chin, and Z. Fan. Sparse malicious false data injection attacks and defense mechanisms in smart grids. *IEEE Transactions on Industrial Informatics*, 11(5):1198–1209, 2015.

[71] J. P. Hespanha. *Linear Systems Theory*. Princeton university press, 2009.

[72] R. Horn and C. Johnson. *Matrix Analysis*. Cambridge University Press, 1985.

[73] C.-S. Hsieh. Robust two-stage Kalman filters for systems with unknown inputs. *IEEE Transactions on Automatic Control*, 45(12):2374–2378, 2000.

[74] J. Hu, Z. Wang, H. Gao, and L. Stergioulas. Extended Kalman filtering with stochastic nonlinearities and multiple missing measurements. *Automatica*, 48(9):2007–2015, 2012.

[75] J. Hu, Z. Wang, B. Shen, and H. Gao. Quantised recursive filtering for a class of nonlinear systems with multiplicative noises and missing measurements. *International Journal of Control*, 86(4):650–663, 2013.

[76] L. Hu, Z. Wang, I. Rahman, and X. Liu. A constrained optimization approach to dynamic state estimation for power systems including PMU and missing measurements. *IEEE Transactions on Control Systems Technology*, in press.

[77] S. Hu and D. Yue. Event-based H_∞ filtering for networked system with communication delay. *Signal Processing*, 92(9):2029–2039, 2012.

[78] Y. Huang, S. Werner, J. Huang, and V. Gupta. State estimation in electric power grids: Meeting new challenges presented by the requirements of the future grid. *IEEE Signal Processing Magazine*, 29(5):33–43, 2012.

[79] 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*, 3(3):1362–1370, 2012.

[80] M. Irving. Robust state estimation using mixed integer programming. *IEEE Transactions on Power Systems*, 23(3):1519–1520, 2008.

[81] W. Jiang, V. Vittal, and G. T. Heydt. A distributed state estimator utilizing synchronized phasor measurements. *IEEE Transactions on Power Systems*, 22(2):563–571, 2007.

[82] K. D. Jones, A. Pal, and J. S. Thorp. Methodology for performing synchrophasor data conditioning and validation. *IEEE Transactions on Power Systems*, 30(3):1121–1130, 2015.

[83] X. Kai, C. Wei, and L. Liu. Robust extended Kalman filtering for nonlinear systems with stochastic uncertainties. *IEEE Transactions on Systems, Man and Cybernetics, Part A: Systems and Humans*, 40(2):399–405, 2010.

[84] H. R. Karimi. Robust H_∞ filter design for uncertain linear systems over network with network-induced delays and output quantization. *Modeling, Identification and Control*, 30(1):27–37, 2009.

[85] H. Karimipour and V. Dinavahi. Extended Kalman filter-based parallel dynamic state estimation. *IEEE Transactions on Smart Grid*, 6(3):1539–1549, 2015.

[86] H. Karimipour and V. Dinavahi. Parallel relaxation-based joint dynamic state estimation of large-scale power systems. *IET Generation, Transmission & Distribution*, 2015.

[87] H. Karimipour and V. Dinavahi. Parallel domain decomposition based distributed state estimation for large-scale power systems. *IEEE Transactions on Industry Applications*, In press.

[88] N. Kashyap, S. Werner, Y.-F. Huang, and T. Riihonen. Power system state estimation under incomplete PMU observability—a reduced-order approach. *IEEE Journal of Selected Topics in Signal Processing*, 8(6):1051–1062, 2014.

[89] V. Kekatos and G. Giannakis. Distributed robust power system state estimation. *IEEE Transactions on Power Systems*, 28(2):1617–1626, 2013.

[90] J. Kennedy and R. Eberhart. Particle swarm optimization. In *Proc. IEEE International Conference on Neural Networks*, volume 4, pages 1942–1948, Hawaii, USA, 1995. IEEE.

[91] T. T. Kim and H. V. Poor. Strategic protection against data injection attacks on power grids. *IEEE Transactions on Smart Grid*, 2(2):326–333, 2011.

[92] P. K. Kitanidis. Unbiased minimum-variance linear state estimation. *Automatica*, 23(6):775–778, 1987.

[93] M. Korkalı and A. Abur. Robust fault location using least-absolute-value estimator. *IEEE Transactions on Power Systems*, 28(4):4384–4392, 2013.

[94] G. N. Korres and N. M. Manousakis. State estimation and bad data processing for systems including PMU and SCADA measurements. *Electric Power Systems Research*, 81(7):1514–1524, 2011.

[95] O. Kosut, L. Jia, R. J. Thomas, and L. Tong. Malicious data attacks on the smart grid. *IEEE Transactions on Smart Grid*, 2(4):645–658, 2011.

[96] V. Kuhlmann, A. Sinton, M. Dewe, and C. Arnold. Effects of sampling rate and ADC width on the accuracy of amplitude and phase measurements in power-quality monitoring. *IEEE Transactions on Power Delivery*, 22(2):758–764, 2007.

[97] C. Kwon, W. Liu, and I. Hwang. Security analysis for cyber-physical systems against stealthy deception attacks. In *Proc. American Control Conference (ACC)*, pages 3344–3349. IEEE, 2013.

[98] A. Leite da Silva, M. Do Coutto Filho, and J. De Queiroz. State forecasting in electric power systems. *IEE Proceedings C Generation, Transmission & Distribution*, 130(5):237–244, 1983.

[99] A. M. Leite da Silva, M. Do Coutto Filho, and J. Cantera. An efficient dynamic state estimation algorithm including bad data processing. *IEEE Transactions on Power Systems*, 2(4):1050–1058, 1987.

[100] H. Li, L. Lai, and W. Zhang. Communication requirement for reliable and secure state estimation and control in smart grid. *IEEE Transactions on Smart Grid*, 2(3):476–486, 2011.

[101] X. Li and A. Scaglione. Advances in decentralized state estimation for power systems. In *the 5th International Workshop on Computational Advances in Multi-Sensor Adaptive Processing (CAMSAP)*, pages 428–431. IEEE, 2013.

[102] X. Li and A. Scaglione. Robust decentralized state estimation and tracking for power systems via network gossiping. *IEEE Journal on Selected Areas in Communications*, 31(7):1184–1194, 2013.

[103] Y. Li, B. Wang, Y. Wang, and X. Wang. A dynamic state estimation method based on mixed measurements for power system. *Przeglad Elektrotechniczny*, 89(5):222–227, 2013.

[104] J.-M. Lin, S.-J. Huang, and K.-R. Shih. Application of sliding surface-enhanced fuzzy control for dynamic state estimation of a power system. *IEEE Transactions on Power Systems*, 18(2):570–577, 2003.

[105] J. Liu, A. Benigni, D. Obradovic, S. Hirche, and A. Monti. State estimation and branch current learning using independent local Kalman filter with virtual disturbance model. *IEEE Transactions on Instrumentation and Measurement*, 60(9):3026–3034, 2011.

[106] L. Liu, M. Esmalifalak, Q. Ding, V. Emesih, Z. Han, et al. Detecting false data injection attacks on power grid by sparse optimization. *IEEE Transactions on Smart Grid*, 5(2):612–621, 2014.

[107] Q. Liu, Z. Wang, X. He, and D. Zhou. A survey of event-based strategies on control and estimation. *Systems Science & Control Engineering: An Open Access Journal*, 2(1):90–97, 2014.

[108] Q. Liu, Z. Wang, X. He, and D. Zhou. Event-based recursive distributed filtering over wireless sensor networks. *IEEE Transactions on Automatic Control*, 60(9):2470–2475, 2015.

[109] X. Liu, Z. Bao, D. Lu, and Z. Li. Modeling of local false data injection attacks with reduced network information. *IEEE Transactions on Smart Grid*, 6(4):1686–1696, July 2015.

[110] Y. Liu, P. Ning, and M. K. Reiter. False data injection attacks against state estimation in electric power grids. In *Proc. the 16th ACM conference on Computer and Communications Security*, pages 21–32. ACM, 2009.

[111] Y. Liu, P. Ning, and M. K. Reiter. False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security*, 14(1):13, 2011.

[112] C. Lu, X. Zhang, X. Wang, and Y. Han. Mathematical expectation modeling of wide-area controlled power systems with stochastic time delay. *IEEE Transactions on Smart Grid*, 6(3):1511–1519, 2015.

[113] 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*, 1(4):370–379, 2014.

[114] K. Martin, D. Hamai, M. Adamiak, S. Anderson, M. Begovic, G. Benmouyal, G. Brunello, J. Burger, J. Cai, B. Dickerson, et al. Exploring the IEEE standard c37.118–2005 synchrophasors for power systems. *IEEE Transactions on Power Delivery*, 23(4):1805–1811, 2008.

[115] X. Meng and T. Chen. Event triggered robust filter design for discrete-time systems. *IET Control Theory & Applications*, 8(2):104–113, 2014.

[116] F. Milano and M. Anghel. Impact of time delays on power system stability. *IEEE Transactions on Circuits and Systems I: Regular Papers*, 59(4):889–900, 2012.

[117] M. Miskowicz. Send-on-delta concept: an event-based data reporting strategy. *Sensors*, 6(1):49–63, 2006.

[118] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli. False data injection attacks against state estimation in wireless sensor networks. In *Proc. IEEE Conference on Decision and Control (CDC)*, pages 5967–5972. IEEE, 2010.

[119] Y. Mo and B. Sinopoli. False data injection attacks in cyber physical systems. In *First Workshop on Secure Control Systems*, 2010.

[120] Y. Mo and B. Sinopoli. On the performance degradation of cyber-physical systems under stealthy integrity attacks. *IEEE Transactions on Automatic Control*, in press.

[121] A. Monticelli. *State Estimation in Electric Power Systems: A Generalized Approach*. Kluwer, Norwell, MA, 1999.

[122] A. Monticelli. Electric power system state estimation. *Proceedings of the IEEE*, 88(2):262–282, 2000.

[123] S. Mousavian, J. Valenzuela, and J. Wang. A probabilistic risk mitigation model for cyber-attacks to PMU networks. *IEEE Transactions on Power Systems*, 30(1):156–165, 2015.

[124] E. J. Msechu, S. I. Roumeliotis, A. Ribeiro, and G. B. Giannakis. Decentralized quantized Kalman filtering with scalable communication cost. *IEEE Transactions on Signal Processing*, 56(8):3727–3741, 2008.

[125] V. Murugesan, Y. Chakhchoukh, V. Vittal, G. T. Heydt, N. Logic, and S. Sturgill. PMU data buffering for power system state estimators. *IEEE Power and Energy Technology Systems Journal*, 2(3):94–102, 2015.

[126] M. Nejati, N. Amjady, and H. Zareipour. A new stochastic search technique combined with scenario approach for dynamic state estimation of power systems. *IEEE Transactions on Power Systems*, 27(4):2093–2105, 2012.

[127] J. Nutaro and V. Protopopescu. The impact of market clearing time and price signal delay on the stability of electric power markets. *IEEE Transactions on Power Systems*, 24(3):1337–1345, 2009.

[128] X. Qing, H. R. Karimi, Y. Niu, and X. Wang. Decentralized unscented Kalman filter based on a consensus algorithm for multi-area dynamic state estimation in power systems. *International Journal of Electrical Power & Energy Systems*, 65:26–33, 2015.

[129] C. Rakpenthai, S. Premrudeepreechacharn, S. Uatrongjit, and N. R. Watson. An optimal PMU placement method against measurement loss and branch outage. *IEEE Transactions on Power Delivery*, 22(1):101–107, 2007.

[130] M. M. Rana and L. Li. An overview of distributed microgrid state estimation and control for smart grids. *Sensors*, 15(2):4302–4325, 2015.

[131] M. Risso, A. J. Rubiales, and P. A. Lotito. Hybrid method for power system state estimation. *IET Generation, Transmission & Distribution*, 9(7):636–643, 2015.

[132] S. Roshany-Yamchi, M. Cychowski, R. R. Negenborn, B. De Schutter, K. Delaney, and J. Connell. Kalman filter-based distributed predictive control of large-scale multi-rate systems: Application to power networks. *IEEE Transactions on Control Systems Technology*, 21(1):27–39, 2013.

[133] P. Rousseaux, T. Van Cutsem, and T. D. Liacco. Whither dynamic state estimation? *International Journal of Electrical Power & Energy Systems*, 12(2):104–116, 1990.

[134] H. Sandberg, S. Amin, and K. Johansson. Cyberphysical security in networked control systems: an introduction to the issue. *IEEE Control Systems Magazine*, 35(1):20–23, 2015.

[135] S. Sarri, L. Zanni, M. Popovic, J.-Y. Le Boudec, and M. Paolone. Performance assessment of linear state estimators using synchrophasor measurements. *IEEE Trans. Sustain. Energy*, 2016.

[136] F. C. Schweppe. Power system static-state estimation, part I, II and III. *IEEE Transactions on Power Apparatus and Systems*, (1):120–135, 1970.

[137] A. Sharma, S. C. Srivastava, and S. Chakrabarti. A multi-agent-based power system hybrid dynamic state estimator. *IEEE Intelligent Systems*, 30(3):52–59, 2015.

[138] B. Shen, Z. Wang, H. Shu, and G. Wei. Robust H_∞ finite-horizon filtering with randomly occurred nonlinearities and quantization effects. *Automatica*, 46(11):1743–1751, 2010.

[139] D. Shi, T. Chen, and L. Shi. Event-triggered maximum likelihood state estimation. *Automatica*, 50(1):247–254, 2014.

[140] K.-R. Shih and S.-J. Huang. Application of a robust algorithm for dynamic state estimation of a power system. *IEEE Transactions on Power Systems*, 17(1):141–147, 2002.

[141] N. Shivakumar and A. Jain. A review of power system dynamic state estimation techniques. In *Proc. Joint International Conference on Power System Technology and IEEE Power India Conference*, pages 1–6. IEEE, 2008.

[142] J. Sijs and M. Lazar. Event based state estimation with time synchronous updates. *IEEE Transactions on Automatic Control*, 57(10):2650–2655, 2012.

[143] A. Simoes Costa, A. Albuquerque, and D. Bez. An estimation fusion method for including phasor measurements into power system real-time modeling. *IEEE Transactions on Power Systems*, 28(2):1910–1920, 2013.

[144] D. Simon. Kalman filtering with state constraints: a survey of linear and nonlinear algorithms. *IET Control Theory & Applications*, 4(8):1303–1318, 2010.

[145] A. K. Singh and B. C. Pal. Decentralized dynamic state estimation in power systems using unscented transformation. *IEEE Transactions on Power Systems*, 29(2):794–804, 2014.

[146] A. K. Singh, R. Singh, and B. C. Pal. Stability analysis of networked control in smart grids. *IEEE Transactions on Smart Grid*, 6(1):381–390, 2015.

[147] A. Sinha and J. Mondal. Dynamic state estimator using ann based bus load prediction. *IEEE Transactions on Power Systems*, 14(4):1219–1225, 1999.

[148] K. C. Sou, H. Sandberg, and K. H. Johansson. On the exact solution to a smart grid cyber-security analysis problem. *IEEE Transactions on Smart Grid*, 4(2):856–865, 2013.

[149] K. C. Sou, H. Sandberg, and K. H. Johansson. Data attack isolation in power networks using secure voltage magnitude measurements. *IEEE Transactions on Smart Grid*, 5(1):14–28, 2014.

[150] S. Sridhar, A. Hahn, and M. Govindarasu. Cyber–physical system security for the electric power grid. *Proceedings of the IEEE*, 100(1):210–224, 2012.

[151] J. Stahlhut, T. Browne, G. Heydt, and V. Vittal. Latency viewed as a stochastic process and its impact on wide area power system control signals. *IEEE Transactions on Power Systems*, 23(1):84–91, 2008.

[152] C. Su and C. Lu. Interconnected network state estimation using randomly delayed measurements. *IEEE Transactions on Power Systems*, 16(4):870–878, 2001.

[153] Y. S. Suh, V. H. Nguyen, and Y. S. Ro. Modified Kalman filter for networked monitoring systems employing a send-on-delta method. *Automatica*, 43(2):332–338, 2007.

[154] X. Tai, D. Marelli, and M. Fu. Power system dynamic state estimation with random communication packets loss. In *Proc. International Symposium on Advanced Control of Industrial Processes*, pages 359–362, Hangzhou, China, 2011. IEEE.

[155] X. Tai, D. Marelli, E. Rohr, and M. Fu. Optimal PMU placement for power system state estimation with random component outages. *International Journal of Electrical Power & Energy Systems*, 51:35–42, 2013.

[156] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, and S. S. Sastry. Cyber security analysis of state estimators in electric power systems. In *Proc. IEEE Conference on Decision and Control (CDC)*, pages 5991–5998. IEEE, 2010.

[157] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson. A secure control framework for resource-limited adversaries. *Automatica*, 51:135–148, 2015.

[158] Y. Theodor and U. Shaked. Robust discrete-time minimum-variance filtering. *IEEE Transactions on Signal Processing*, 44(2):181–189, 1996.

[159] G. Valverde and V. Terzija. Unscented Kalman filter for power system dynamic state estimation. *IET Generation, Transmission & Distribution*, 5(1):29–37, 2011.

[160] O. Vuković, K. C. Sou, G. Dán, and H. Sandberg. Network-aware mitigation of data integrity attacks on power system state estimation. *IEEE Journal on Selected Areas in Communications*, 30(6):1108–1118, 2012.

[161] S. Wang, W. Gao, et al. An alternative method for power system dynamic state estimation based on unscented transform. *IEEE Transactions on Power Systems*, 27(2):942–950, 2012.

[162] S. Wang, W. Gao, J. Wang, and J. Lin. Synchronized sampling technology-based compensation for network effects in wams communication. *IEEE Transactions on Smart Grid*, 3(2):837–845, 2012.

[163] S. Wang, X. Meng, and T. Chen. Wide-area control of power systems through delayed network communication. *IEEE Transactions on Control Systems Technology*, 20(2):495–503, 2012.

[164] S. Wang, W. Ren, and U. Al-Saggaf. Effects of switching network topologies on stealthy false data injection attacks against state estimation in power networks. *IEEE Systems Journal*, in press.

[165] W. Wang and Z. Lu. Cyber security in the smart grid: Survey and challenges. *Computer Networks*, 57(5):1344–1371, 2013.

[166] Y. Wang, W. Li, P. Zhang, B. Wang, and J. Lu. Reliability analysis of phasor measurement unit considering data uncertainty. *IEEE Transactions on Power Systems*, 27(3):1503–1510, 2012.

[167] Z. Wang, H. Dong, B. Shen, and H. Gao. Finite-horizon H_∞ filtering with missing measurements and quantization effects. *IEEE Transactions on Automatic Control*, 58(7):1707–1718, 2013.

[168] Z. Wang, B. Shen, and X. Liu. H_∞ filtering with randomly occurring sensor saturations and missing measurements. *Automatica*, 48(3):556–562, 2012.

[169] F. F. Wu. Power system state estimation: a survey. *International Journal of Electrical Power & Energy Systems*, 12(2):80–87, 1990.

[170] L. Xie, D.-H. Choi, S. Kar, and H. V. Poor. Fully distributed state estimation for wide-area monitoring systems. *IEEE Transactions on Smart Grid*, 3(3):1154–1169, 2012.

[171] L. Xie, Y. Mo, and B. Sinopoli. Integrity data attacks in power market operations. *IEEE Transactions on Smart Grid*, 2(4):659–666, 2011.

[172] L. Xie, Y. C. Soh, and C. E. de Souza. Robust Kalman filtering for uncertain discrete-time systems. *IEEE Transactions on Automatic Control*, 39(6):1310–1314, 1994.

[173] P. Yang, Z. Tan, A. Wiesel, and A. Nehora. Power system state estimation using PMUs with imperfect synchronization. *IEEE Transactions on Power Systems*, 28(4):4162–4172, 2013.

[174] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao. On false data-injection attacks against power system state estimation: Modeling and countermeasures. *IEEE Transactions on Parallel and Distributed Systems*, 25(3):717–729, 2014.

[175] X. Yang, X.-P. Zhang, and S. Zhou. Coordinated algorithms for distributed state estimation with synchronized phasor measurements. *Applied Energy*, 96:253–260, 2012.

[176] N. Zeng, Z. Wang, Y. Li, M. Du, and X. Liu. A hybrid EKF and switching PSO algorithm for joint state and parameter estimation of lateral flow immunoassay models. *IEEE/ACM Transactions Computational Biology and Bioinformatics*, 9(2):321–329, 2012.

[177] J. Zhang and A. D. Domínguez-García. On the impact of communication delays on power system automatic generation control performance. In *Proc. North American Power Symposium (NAPS)*, pages 1–6. IEEE, 2014.

[178] J. Zhang, G. Welch, G. Bishop, and Z. Huang. A two-stage Kalman filtering approach for robust and real-time power systems state tracking. *IEEE Transactions on Sustainable Energy*, 5(2):629–636, 2014.

[179] J. Zhang, G. Welch, N. Ramakrishnan, and S. Rahman. Kalman filters for dynamic and secure smart grid state estimation. *Intelligent Industrial Systems*, pages 1–8, 2015.

[180] L. Zhang, H. Gao, and O. Kaynak. Network-induced constraints in networked control systems: a survey. *IEEE Transactions on Industrial Informatics*, 9(1):403–416, 2013.

[181] Q. Zhang, Y. Chakhchoukh, V. Vittal, G. T. Heydt, N. Logic, and S. Sturgill. Impact of PMU measurement buffer length on state estimation and its optimization. *IEEE Transactions on Power Systems*, 28(2):1657–1665, 2013.

[182] Q. Zhang, V. Vittal, G. T. Heydt, N. Logic, and S. Sturgill. The integrated calibration of synchronized phasor measurement data in power transmission systems. *IEEE Transactions on Power Delivery*, 26(4):2573–2581, 2011.

[183] X. Zhang, C. Lu, X. Xie, and Z. Y. Dong. Stability analysis and controller design of a wide-area time-delay system based on the expectation model method. *IEEE Transactions on Smart Grid*, 7(1):520–529, 2016.

[184] X.-M. Zhang and Q.-L. Han. Event-based H_∞ filtering for sampled-data systems. *Automatica*, 51:55–69, 2015.

[185] J. Zhao, G. Zhang, K. Das, G. Korres, N. Manousakis, A. Sinha, and Z. He. Power system real-time monitoring by using PMU-based robust state estimation method. *IEEE Transactions on Smart Grid*, 7(1):300–309, 2016.

[186] J. Zhao, G. Zhang, M. La Scala, Z. Y. Dong, C. Chen, and J. Wang. Short-term state forecasting-aided method for detection of smart grid general false data injection attacks. *IEEE Transactions on Smart Grid*, in press.

[187] L. Zhao and A. Abur. Multi area state estimation using synchronized phasor measurements. *IEEE Transactions on Power Systems*, 20(2):611–617, 2005.

[188] M. Zhou, V. Centeno, J. Thorp, and A. Phadke. An alternative for including phasor measurements in state estimators. *IEEE Transactions on Power Systems*, 21(4):1930–1937, 2006.

[189] H. Zhu and G. Giannakis. Power system nonlinear state estimation using distributed semidefinite programming. *IEEE Journal of Selected Topics in Signal Processing*, 8(6):1039–1050, 2014.

[190] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas. Matpower: Steady-state operations, planning, and analysis tools for power systems research and education. *IEEE Transactions on Power Systems*, 26(1):12–19, 2011.