Recent Advances on State Estimation for Power Grids with Unconventional Measurements

Liang Hu, Zidong Wang, Xiaohui Liu, Athanasios V. Vasilakos and Fuad E. Alsaadi

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, asynchronous and missing measurements due to communication constraints, and the cyber-attacks on the communication channels. In this paper, we aim to survey some recent advances on the state estimation methods which tackle the above three issues in power grids. Traditional state estimation methods applied in power grids are first introduced. Latest results on state estimation with mixed measurements and incomplete measurements are then discussed in great detail. In addition, the techniques developed to ensure the cyber-security of the state estimation schemes for power grids are highlighted. Finally, some concluding remarks are given and some possible future research directions are pointed out.

Index Terms

Smart grids; Power grids; Dynamic state estimation; Phasor measurement units; Unconventional measurements; Cyber security.

I. Introduction

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 [1]. 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.

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

This work was supported in part by the Engineering and Physical Sciences Research Council (EPSRC) of the U.K., the Royal Society of the U.K., and the Alexander von Humboldt Foundation of Germany.

L. Hu, Z. Wang and X. Liu are with the Department of Computer Science, Brunel University London, Uxbridge, Middlesex, UB8 3PH, United Kingdom. (Email: Zidong.Wang@brunel.ac.uk)

A. V. Vasilakos is with the Department of Computer, Electrical and Space Engineering, Luea University of Technology, 97187 Lulea, Sweden, (Email: vasilako@ath.forthnet.gr)

F. E. Alsaadi is with the Faculty of Engineering, King Abdulaziz University, Jeddah 21589, Saudi Arabia, (Email: fuad_alsaadi@yahoo.com).

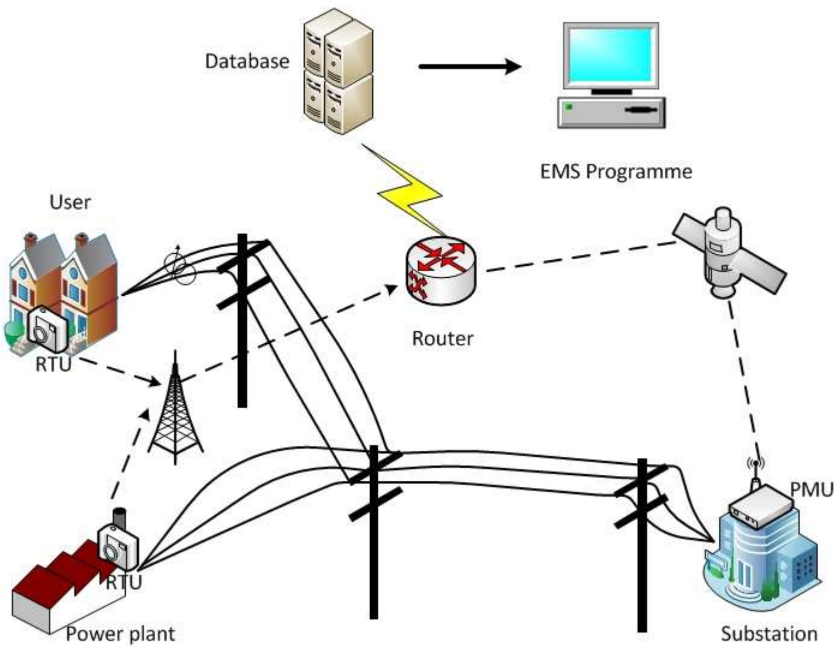


Fig. 1. A typical system structure of power grids

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 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 [1], [2]. 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 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 [3]. 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, the power system state estimation (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. In this paper, we focus our main attention on the PSSE problem by making a timely survey on the recent developments and possible future research directions.

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 [4]. 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.

It is worth mentioning that, in response to the rapid progress of the power grid technologies, the reviews on the advances of state estimation techniques have been ongoing in the past decade. Several survey papers [5]–[10] have summarized the estimation methods developed at different stages in different time periods. There have also been some survey papers on certain specific issues concerning the state estimation problems for power grids, such as [11] on the state estimation with PMUs measurements and [12] on the cyber-security issue. Most recently, the state estimation problem in power grids have been surveyed from the signal processing perspective, see [13], [14].

In this survey, 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,

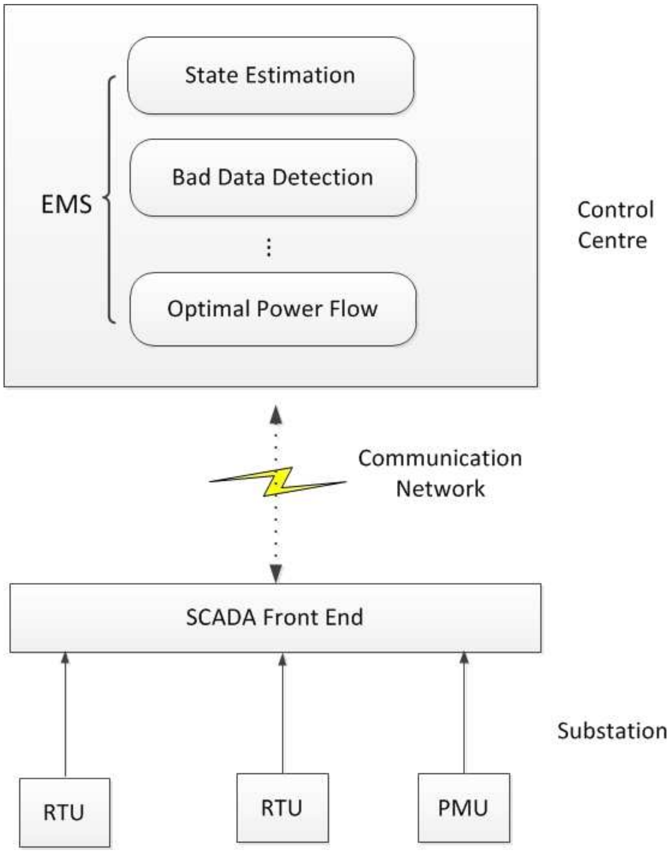


Fig. 2. The PSSE module in an EMS/SCADA system

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. This survey is organised as follows. In Section II, the measurement model is introduced and typical estimation methods used to solve the PSSE problem are discussed. The results on PSSE with mixed measurements are reviewed in Section III. Section IV provides a through summary of the research results on state estimation for power grids with three kinds of incomplete information, namely, delayed measurements, asynchronous measurements and missing measurements. Relevant literature on the cyber-security issue of PSSE is reviewed in Section V. Finally, the conclusion remarks are given and some directions for future works are pointed out in Section VI.

II. 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 shows the relation of the PSSE module with the 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.

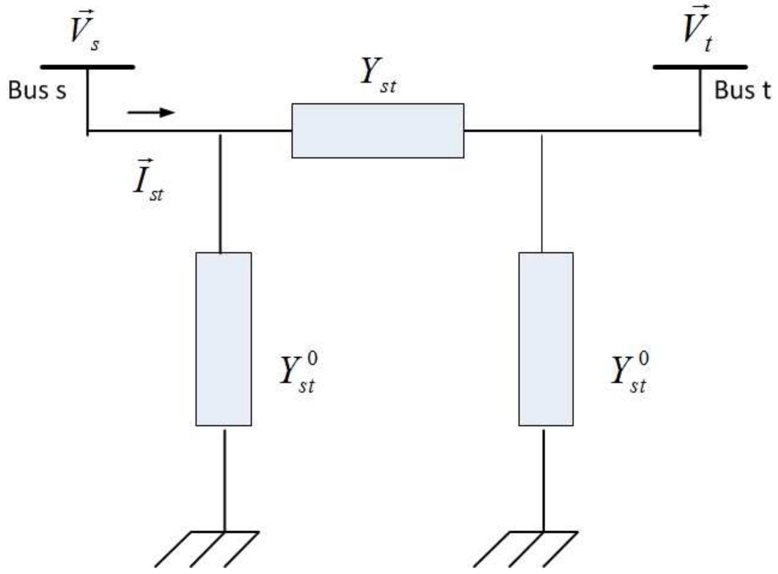


Fig. 3. The π model

A. 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. 3, 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:

$$\overrightarrow{I}_{st} = (g_{st} + jb_{st})(\overrightarrow{V}_s - \overrightarrow{V}_t) + (g_{st}^0 + jb_{st}^0)\overrightarrow{V}_s \tag{1}$$

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 paper. 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.

1) 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 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 (1), all measurement equations can be represented as follows (for the purpose of simplicity, the time instant k is omitted):

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

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:

$$y_1(k) = h\big(x(k)\big) + v_1(k) \tag{2}$$

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.

2) 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 [15].

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 (1) as follow:

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

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:

$$y_2(k) = Hx(k) + v_2(k) \tag{3}$$

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 [16]. 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 [17]. On the other hand, to quantify the quality of PMUs, the data reliability of PMU measurements has been quantitatively analysed in [18]–[20]. For more details of PMU technology development, we refer the readers to the recent survey paper [21].

B. Estimation methods

Since the initial research conducted by F. C. Schweppe in 1970 [22], 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.

1) 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

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

where the weighting matrix W is commonly set as the covariance matrix of the measurement noise. Noting that the measurement model (2) 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) is first linearized around the obtained state estimate and then the linear least square method is applied to the linearized 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 [23], [24] and the robust WLS method [25]–[27], to name just a few. In the literature, there have been a number of survey papers on the SSE methods. For example, the developments in the early two decades up to the year 1990 have been summarized in [8], [9], and the advances in the subsequent one decade from 1990 to 2000 have been reviewed in [10]. In addition, two textbooks [28], [29] have provided more details on SSE techniques in power grids.

2) 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 [30], which is described by the following random-walk process:

$$x(k+1) = x(k) + w(k) \tag{4}$$

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 [31] as follows:

$$x(k+1) = A(k)x(k) + u(k) + w(k) \tag{5}$$

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 (5), 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 [5], [32], [33]. In such a kind of estimator, based on the system model (5) and measurement model (1), the two steps of state prediction and state estimation are accomplished as follows:

$$\begin{aligned} \bar{x}(k+1) &= A(k)\hat{x}(k) + u(k) \\ \hat{x}(k+1) &= \bar{x}(k+1) + K(k+1)[y(k+1) - h(\bar{x}(k+1))] \end{aligned} \tag{6}$$

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:

$$\begin{aligned} K(k) &= P(k)H^T(k)R^{-1} \\ P(k) &= [H^T(k)R^{-1}H(k) + M^{-1}(k)]^{-1} \\ M(k) &= A(k)P(k-1)A^T(k) + W. \end{aligned} \tag{7}$$

Other alternative filtering algorithms to EKF for PSSE have also been developed, including the iterative Kalman filter [34], the unscented Kalman filter [35], [36], the particle filter [37], the robust filter [38], the disturbance filter [33], [39], the adaptive filter [40], [41] and the filter for joint estimation of state and parameter [42], [43]. Moreover, to speed up the estimation algorithm applied in large-scale power grids, parallel EKF-based dynamic state estimator has been proposed in [44]–[46]. In addition, computational intelligence tools (e.g. neural networks, evolutionary algorithm and fuzzy logic) have also been integrated into the DSE algorithms in [47]–[49]. The readers are referred to the survey papers [5]–[7], [50] for more details on DSE methods.

While the traditional measurements are modelled by nonlinear equations in (1), 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 [51], [52]. 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 [53].

C. 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:

$$r(k) = \begin{cases} y(k) - h(\hat{x}(k)) & \text{traditional measurements,} \\ z(k) - H\hat{x}(k) & \text{PMU measurements,} \end{cases} \tag{8}$$

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 [29]. 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 $r(k)$.

III. 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 [13]. 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.

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 [10]. 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 [54]. As discussed in [55], the communication constraints 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.

A. 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) [56]–[60]. 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 [61]–[63].

Several different techniques has been introduced to design DSE methods with mixed measurements [64]–[69]. 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 [64]–[66], and a dynamic state estimator has been designed based on the relevance vector machine algorithm in [68], where the auto-encoder technique has been used to further

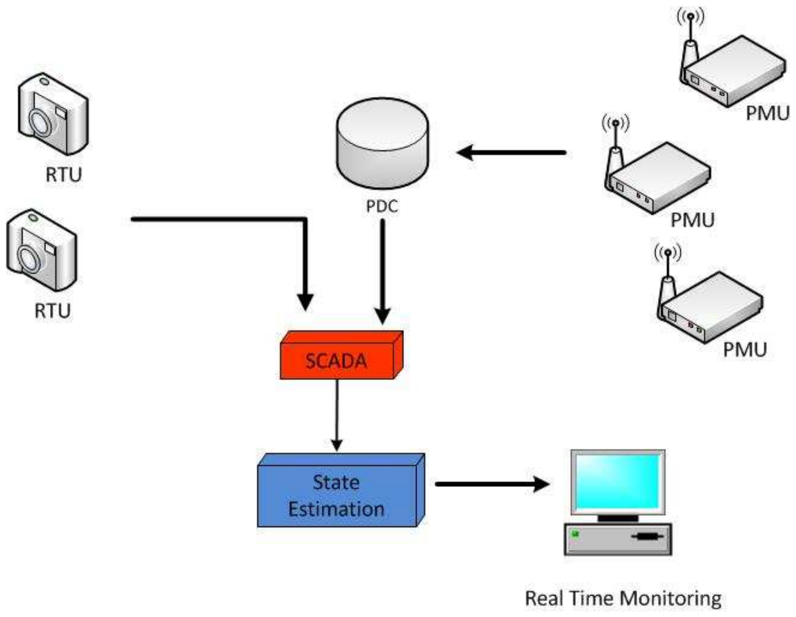


Fig. 4. The mixed measurements

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 [69].

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 [70], 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 [71].

IV. 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. 5, 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 paper, the information with respect to the network-induced phenomena is customarily referred to as the incomplete information [72], [73].

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

1) 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

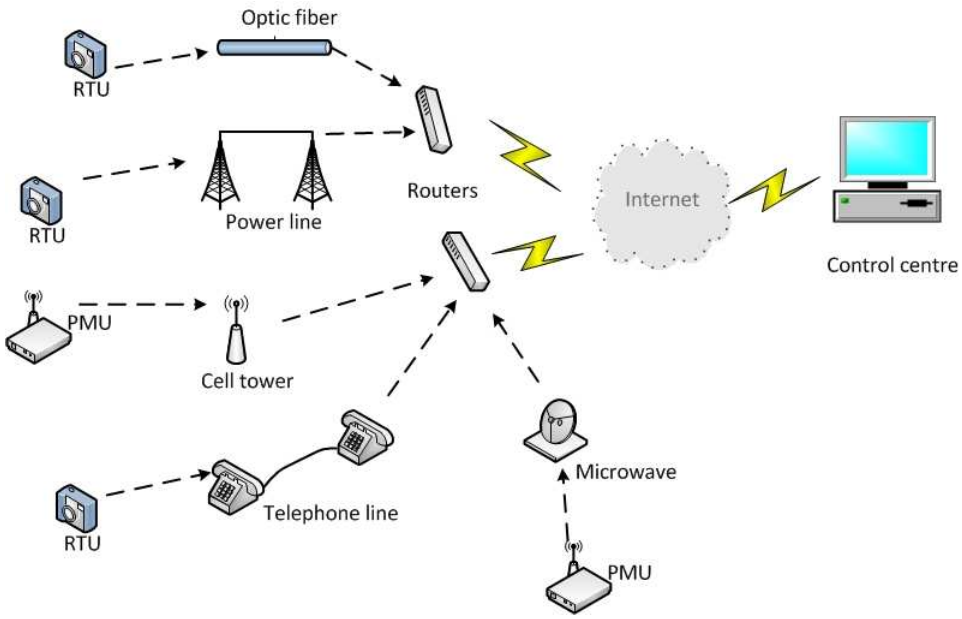


Fig. 5. Typical communication links in SCADA systems

TABLE I
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.

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 [74]. 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 [75], and the statistical characteristics of transmission delay in some practical power girds have been obtained through analysis of real data [74]. The delayed measurements could largely affect the power systems in different aspects such as system stability [76] and power market [77]. Nevertheless, in this paper, we focus on the effect of delay measurements on PSSE exclusively.

2) 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 renascence of 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.

3) 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.

A. 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) or (3) 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.

1) Delayed and asynchronous measurements: Several models have been used to characterize the time delays [3], [74], [75], [78]–[81]. 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 [3], a bounded but time-varying delay model has been proposed to capture the network-induced constraints in wide-area measurement systems. In [75], 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 [74]. In addition, a straightforward calculation method and model of communication delays in power system have been proposed in [80].

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 [78]. 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 [81], 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 [78], [81], 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 [82]–[84]. 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 [82], and such an idea has been extended to calibrate the PMU measurement data received by the estimator [84]. 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 [83]. It has been shown that the proposed estimator outperforms the traditional ones.

2) 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 [85]–[87]. For instance, in [85], 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 [86], [87] 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 [88]–[91]. Furthermore, the off-line state estimation algorithm has been developed in [88] 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 [89], [90]. Moreover, in [91] the impact of dropped packets on stability of the estimator has been investigated.

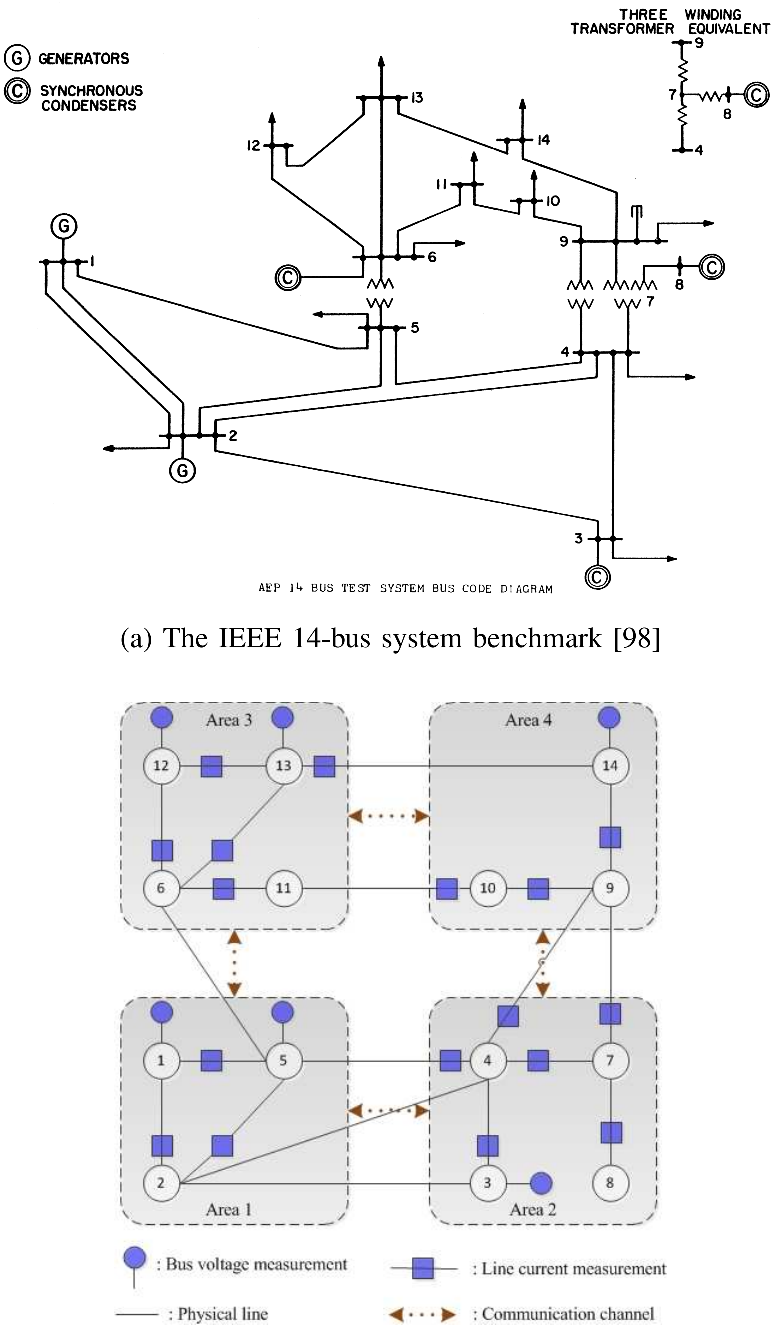
In [92], [93], both the time delays and missing measurements have been simultaneously considered. Specifically, in [92], a method using the GPS synchronized sampling technologies has been proposed to compensate both time delays and missing measurements. In [93], an integrated software package has been developed for the power grids simulation wherein the delay and the packet loss introduced by the communication systems have been taken into account.

B. 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 II. 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 [94], [95]. 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 paper, 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 [96], [97].

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


THREE WINDING TRANSFORMER EQUIVALENT
G GENERATORS
C SYNCHRONOUS CONDENSERS
1
2
3
4
5
6
7
8
9
10
11
12
13
14
AEP 14 BUS TEST SYSTEM BUS CODE DIAGRAM
Area 3
Area 4
Area 1
Area 2
: Bus voltage measurement
: Line current measurement
: Physical line
: Communication channel

(a) The IEEE 14-bus system benchmark [98]

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

Fig. 6. The IEEE 14-bus system: (a) Conventional system; (b) Decentralized estimation structure

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. 6.

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 [60], [67], [99]–[102]. In [99], 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 [100], 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 [101], 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 [60], [67], [102].

- In the DDSE framework, different estimation methods have been put forward in [103]–[108]. Specifically, in [104], 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 [103]. Using Gaussian approximation and stochastic linearization techniques, the distributed point-based Gaussian approximation filters has been developed in [108]. Moreover, to improve the estimation performance, the local information exchanges of neighbouring areas based on the consensus algorithm has been introduced in [105]. In addition, a distributed Kalman filter has been developed to compensate for the information loss in the multi-rate large-scale power grids in [107], and two short survey papers on recent advances of DDSE have been given in [106], [109].

V. 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 [110].

A. 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. 7.

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:

$$y^a(k) = y(k) + a(k) \tag{9}$$

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 (8) 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 (8) will not be detected if the following

$$r^a(k) - r(k) = 0 \tag{10}$$

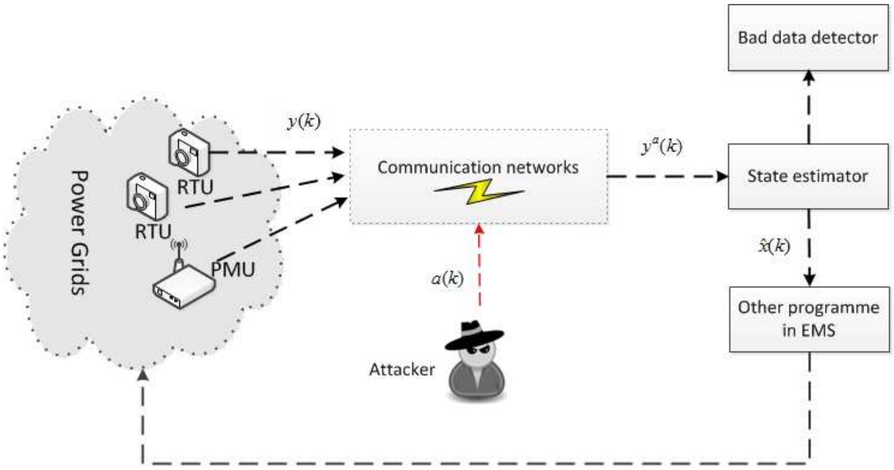


Fig. 7. System structure of cyber-attacks in PSSE

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.

B. Latest progress

Since the initial results reported in 2009 [111], 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.

1) 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 [111]–[116]. 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 [111], [112] and the case that limited (rather than all) model knowledge is known by the attacker has been considered in [116]. Furthermore, in [113], 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 [115] 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 [114].

2) 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 [113], 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 [117], different detection methods for FDI attacks in power girds have been reviewed. On the other hand, the sparse nature of the attack vectors in power girds has been exploited in designing efficient attack detection/estimation algorithms [118]–[120]. Specifically, sparse optimization-based estimation methods have been proposed to detect the attacks in [118] 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 [119]. Similarly, using the minimum-cut algorithm, the stealthy attacks on power networks have been computed exactly in [120]. Moreover, the optimal policies for attack design/detection from the adversary/defender has been investigated in a game-theoretic framework in [121].

3) 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 [122], [122]–[128] 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 [122], [123]. Without the above assumption, in [125], 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 [126] 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 [124] 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 [127]. In addition, another different protection mechanism has been proposed in [128] 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.

4) 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 [129] and, in [130], 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 [4], [12], [131], [132].

VI. Conclusion and future works

In this paper, we have reviewed 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. Section II has provided the background knowledge on the topic of power system state estimation. Following that, the state estimation problem with the above mentioned three issues have been discussed one by one from Section III-V. We have analysed the motivation for each issue, presented their impact on the estimation performance and provided overviews on the corresponding research results. In Section III, the research works on mixed measurements have been categorized into three frameworks, namely, the dynamic state estimation framework, the static state estimation framework and the hardware-enhanced framework. In Section IV, three kinds of incomplete information in measurements (i.e., delayed measurements, asynchronous measurements and missing measurements) have been considered, and the methods for dealing with the incomplete information have been 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. In Section V, we have summarized the research work on state estimation with FDI attacks from three aspects, namely, system vulnerability, attack detection and system protection.

Based on the literature review, some related topics for the future research work are listed as follows.

- *Data quantization:* The quantization naturally exists in the measurement data due to the essence of digital meters in power grids. In addition, network-induced quantization phenomenon may exist when the measurements are sent to the control centre via the bandwidth-constrained communication networks [133]. Both the device-induced and the network-induced quantized measurements should be properly taken in account when designing the state estimation algorithms.
- *Event-based state estimation:* Many state estimation methods have been proposed to handle the networked-induced incomplete information. In fact, the event-based estimation could be a promising approach to maintaining the estimation performance under limited communication resources [134], [135]. 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. So far, the event-based state estimation problem for power grids has seldom been addressed except some preliminary results reported in [136], [137].
- *Cyber-security of the dynamic state estimator:* The PSSE problem under FDI attacks has been extensively addressed in the context of static state estimation. However, such a problem has not been adequately investigated in the context of dynamic state estimators, and only scattered results have appeared in [138], [139]. In fact, both the SSE and DSE schemes are currently used in practical power grids and, therefore, more attentions should be paid to the DSE schemes under cyber-attacks. Compared with FDI attacks with static models, the FDI attacks on dynamic models are more difficult to detect because the attacks can be mixed with system noises. In this regard, it is challenging to investigate the cyber-security of the DSE problem in power grids.

References

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

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

[3] Wang, S., Meng, X., Chen, T.: 'Wide-area control of power systems through delayed network communication', *IEEE Transactions on Control Systems Technology*, 2012, **20**, (2), pp. 495–503.

[4] Sridhar, S., Hahn, A., Govindarasu, M.: 'Cyber–physical system security for the electric power grid', *Proceedings of the IEEE*, 2012, **100**, (1), pp. 210–224.

[5] Rousseaux, P., Van Cutsem, T., Liacco, T. D.: 'Whither dynamic state estimation?', *International Journal of Electrical Power & Energy Systems*, 1990, **12**, (2), pp. 104–116.

[6] Shivakumar, N., Jain, A.: 'A review of power system dynamic state estimation techniques', *Proc. Joint International Conference on Power System Technology and IEEE Power India Conference*, 2008, pp. 1–6.

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

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

[9] Wu, F. F.: 'Power system state estimation: a survey', *International Journal of Electrical Power & Energy Systems*, 1990, **12**, (2), pp. 80–87.

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

[11] Phadke, A., Thorp, J., Nuqui, R., Zhou, M.: 'Recent developments in state estimation with phasor measurements', *Proc. IEEE/PES Power Systems Conference and Exposition*, 2009, pp. 1–7.

[12] Guan, Z., Sun, N., Xu, Y., Yang, T.: 'A comprehensive survey of false data injection in smart grid', *International Journal of Wireless and Mobile Computing*, 2015, **8**, (1), pp. 27–33.

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

[14] Giannakis, G. B., Kekatos, V., Gatsis, N., Kim, S.-J., Zhu, H., Wollenberg, B.: ‘Monitoring and optimization for power grids: A signal processing perspective’, *IEEE Signal Processing Magazine*, 2013, **30**, (5), pp. 107–128.

[15] Zhang, J., Domínguez-García, A. D.: ‘On the impact of communication delays on power system automatic generation control performance’, *North American Power Symposium (NAPS)*, 2014, pp. 1–6.

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

[17] Martin, K., Hamai, D., Adamiak, M., et al: ‘Exploring the IEEE standard c37.118–2005 synchrophasors for power systems’, *IEEE Transactions on Power Delivery*, 2008, **23**, (4), pp. 1805–1811.

[18] Wang, Y., Li, W., Zhang, P., Wang, B., Lu, J.: ‘Reliability analysis of phasor measurement unit considering data uncertainty’, *IEEE Transactions on Power Systems*, 2012, **27**, (3), pp. 1503–1510.

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

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

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

[22] Schweppe, F. C.: ‘Power system static-state estimation, part I, II and III’, *IEEE Transactions on Power Apparatus and Systems*, 1970, (1), pp. 120–135.

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

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

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

[26] Chen, Y., Ma, J., Zhang, P., Liu, F., Mei, S.: ‘Robust state estimator based on maximum exponential absolute value’, *IEEE Transactions on Smart Grid*, (in press).

[27] Zhao, J., Zhang, G., Das, K., Korres, G., Manousakis, N., Sinha, A., He, Z.: ‘Power system real-time monitoring by using PMU-based robust state estimation method’, *IEEE Transactions on Smart Grid*, 2016, **7**, (1), pp. 300–309.

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

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

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

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

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

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

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

[35] Wang, S., Gao, W.,: ‘An alternative method for power system dynamic state estimation based on unscented transform’, *IEEE Transactions on Power Systems*, 2012, **27**, (2), pp. 942–950.

[36] Valverde, G., Terzija, V.: ‘Unscented Kalman filter for power system dynamic state estimation’, *IET Generation, Transmission & Distribution*, 2011, **5**, (1), pp. 29–37.

[37] Emami, K., Fernando, T., Iu, H.-C., Trinh, H., Wong, K.: ‘Particle filter approach to dynamic state estimation of generators in power systems’, *IEEE Transactions on Power Systems*, 2015, **30**, (5), pp. 2665–2675.

[38] Shih, K.-R., Huang, S.-J.: ‘Application of a robust algorithm for dynamic state estimation of a power system’, *IEEE Transactions on Power Systems*, 2002, **17**, (1), pp. 141–147.

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

[40] Zhang, J., Welch, G., Bishop, G., Huang, Z.: ‘A two-stage Kalman filtering approach for robust and real-time power systems state tracking’, *IEEE Transactions on Sustainable Energy*, 2014, **5**, (2), pp. 629–636.

[41] Zhang, J., Welch, G., Ramakrishnan, N., Rahman, S.: ‘Kalman filters for dynamic and secure smart grid state estimation’, *Intelligent Industrial Systems*, 2015, pp. 1–8.

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

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

[44] Karimipour, H., Dinavahi, V.: 'Extended Kalman filter-based parallel dynamic state estimation', *IEEE Transactions on Smart Grid*, (In press), **6**, (3), pp. 1539–1549.

[45] Karimipour, H., Dinavahi, V.: 'Parallel relaxation-based joint dynamic state estimation of large-scale power systems', *IET Generation, Transmission & Distribution*, (In press).

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

[47] Nejati, M., Amjady, N., Zareipour, H.: 'A new stochastic search technique combined with scenario approach for dynamic state estimation of power systems', *IEEE Transactions on Power Systems*, 2012, **27**, (4), pp. 2093–2105.

[48] Sinha, A., Mondal, J.: 'Dynamic state estimator using ann based bus load prediction', *IEEE Transactions on Power Systems*, 1999, **14**, (4), pp. 1219–1225.

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

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

[51] Sarri, S., Zanni, L., Popovic, M., Le Boudec, J.-Y., Paolone, M.: 'Performance assessment of linear state estimators using synchrophasor measurements', *IEEE Trans. Sustain. Energy*, 2016.

[52] Kashyap, N., Werner, S., Huang, Y.-F., Riihonen, T.: 'Power system state estimation under incomplete PMU observabilitya reduced-order approach', *IEEE Journal of Selected Topics in Signal Processing*, 2014, **8**, (6), pp. 1051–1062.

[53] Risso, M., Rubiales, A. J., Lotito, P. A.: 'Hybrid method for power system state estimation', *IET Generation, Transmission & Distribution*, 2015, **9**, (7), pp. 636–643.

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

[55] Zhang, L., Gao, H., Kaynak, O.: 'Network-induced constraints in networked control systems: a survey', *IEEE Transactions on Industrial Informatics*, 2013, **9**, (1), pp. 403–416.

[56] Zhou, M., Centeno, V., Thorp, J., Phadke, A.: 'An alternative for including phasor measurements in state estimators', *IEEE Transactions on Power Systems*, 2006, **21**, (4), pp. 1930–1937.

[57] Bi, T., Qin, X., Yang, Q.: 'A novel hybrid state estimator for including synchronized phasor measurements', *Electric Power Systems Research*, 2008, **78**, (8), pp. 1343–1352.

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

[59] Zhu, H., Giannakis, G.: 'Power system nonlinear state estimation using distributed semidefinite programming', *IEEE Journal of Selected Topics in Signal Processing*, 2014, **8**, (6), pp. 1039–1050.

[60] Yang, X., Zhang, X.-P., Zhou, S.: 'Coordinated algorithms for distributed state estimation with synchronized phasor measurements', *Applied Energy*, 2012, **96**, pp. 253–260.

[61] Simoes Costa, A., Albuquerque, A., Bez, D.: 'An estimation fusion method for including phasor measurements into power system real-time modeling', *IEEE Transactions on Power Systems*, 2013, **28**, (2), pp. 1910–1920.

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

[63] Glavic, M., Van Cutsem, T.: 'Reconstructing and tracking network state from a limited number of synchrophasor measurements', *IEEE Transactions on Power Systems*, 2013, **28**, (2), pp. 1921–1929.

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

[65] Chakhchoukh, Y., Vittal, V., Heydt, G. T.: 'PMU based state estimation by integrating correlation', *IEEE Transactions on Power Systems*, 2014, **29**, (2), pp. 617–626.

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

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

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

[69] Sharma, A., Srivastava, S. C., Chakrabarti, S.: 'A multi-agent-based power system hybrid dynamic state estimator', *IEEE Intelligent Systems*, 2015, **30**, (3), pp. 52–59.

[70] Zhang, Q., Chakhchoukh, Y., Vittal, V., Heydt, G. T., Logic, N., Sturgill, S.: 'Impact of PMU measurement buffer length on state estimation and its optimization', *IEEE Transactions on Power Systems*, 2013, **28**, (2), pp. 1657–1665.

[71] Murugesan, V., Chakhchoukh, Y., Vittal, V., Heydt, G. T., Logic, N., Sturgill, S.: 'PMU data buffering for power system state estimators', *IEEE Power and Energy Technology Systems Journal*, 2015, **2**, (3), pp. 94–102.

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

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

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

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

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

[77] Nutaro, J., Protopopescu, V.: 'The impact of market clearing time and price signal delay on the stability of electric power markets', *IEEE Transactions on Power Systems*, 2009, **24**, (3), pp. 1337–1345.

[78] Su, C., Lu, C.: 'Interconnected network state estimation using randomly delayed measurements', *IEEE Transactions on Power Systems*, 2001, **16**, (4), pp. 870–878.

[79] Zhang, X., Lu, C., Xie, X., Dong, Z. Y.: 'Stability analysis and controller design of a wide-area time-delay system based on the expectation model method', *IEEE Transactions on Smart Grid*, 2016, **7**, (1), pp. 520–529.

[80] Stahlhut, J., Browne, T., Heydt, G., Vittal, V.: 'Latency viewed as a stochastic process and its impact on wide area power system control signals', *IEEE Transactions on Power Systems*, 2008, **23**, (1), pp. 84–91.

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

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

[83] Yang, P., Tan, Z., Wiesel, A., Nehora, A.: 'Power system state estimation using PMUs with imperfect synchronization', *IEEE Transactions on Power Systems*, 2013, **28**, (4), pp. 4162–4172.

[84] Zhang, Q., Vittal, V., Heydt, G. T., Logic, N., Sturgill, S.: 'The integrated calibration of synchronized phasor measurement data in power transmission systems', *IEEE Transactions on Power Delivery*, 2011, **26**, (4), pp. 2573–2581.

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

[86] Rakpenthai, C., Premrudeepreechacharn, S., Uatrongjit, S., Watson, N. R.: 'An optimal PMU placement method against measurement loss and branch outage', *IEEE Transactions on Power Delivery*, 2007, **22**, (1), pp. 101–107.

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

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

[89] Tai, X., Marelli, D., Fu, M.: 'Power system dynamic state estimation with random communication packets loss', *Proc. International Symposium on Advanced Control of Industrial Processes*, pp. 359–362, IEEE, Hangzhou, China, 2011.

[90] Tai, X., Marelli, D., Rohr, E., Fu, M.: 'Optimal PMU placement for power system state estimation with random component outages', *International Journal of Electrical Power & Energy Systems*, 2013, **51**, pp. 35–42.

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

[92] Wang, S., Gao, W., Wang, J., Lin, J.: 'Synchronized sampling technology-based compensation for network effects in wams communication', *IEEE Transactions on Smart Grid*, 2012, **3**, (2), pp. 837–845.

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

[94] Zhao, L., Abur, A.: 'Multi area state estimation using synchronized phasor measurements', *IEEE Transactions on Power Systems*, 2005, **20**, (2), pp. 611–617.

[95] Gómez-Expósito, A., de la Villa Jaén, A., Gómez-Quiles, C., Rousseaux, P., Van Cutsem, T.: 'A taxonomy of multi-area state estimation methods', *Electric Power Systems Research*, 2011, **81**, (4), pp. 1060–1069.

[96] Cutsem, T. V., Pavella, M. R.: 'Critical survey of hierarchical methods for state estimation of electric power systems', *IEEE Transactions on Power Apparatus and Systems*, (1983), , (10), pp. 3415–3424.

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

[98] 'Power systems test case archive', [Online]. Available: http://www.ee.washington.edu/research/pstca/.

[99] Xie, L., Choi, D.-H., Kar, S., Poor, H. V.: 'Fully distributed state estimation for wide-area monitoring systems', *IEEE Transactions on Smart Grid*, 2012, **3**, (3), pp. 1154–1169.

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

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

[102] Jiang, W., Vittal, V., Heydt, G. T.: 'A distributed state estimator utilizing synchronized phasor measurements', *IEEE Transactions on Power Systems*, 2007, **22**, (2), pp. 563–571.

[103] Singh, A. K., Pal, B. C.: 'Decentralized dynamic state estimation in power systems using unscented transformation', *IEEE Transactions on Power Systems*, 2014, **29**, (2), pp. 794–804.

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

[105] Qing, X., Karimi, H. R., Niu, Y., Wang, X.: '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*, 2015, **65**, pp. 26–33.

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

[107] Roshany-Yamchi, S., Cychowski, M., Negenborn, R. R., De Schutter, B., Delaney, K., Connell, J.: 'Kalman filter-based distributed predictive control of large-scale multi-rate systems: Application to power networks', *IEEE Transactions on Control Systems Technology*, 2013, **21**, (1), pp. 27–39.

[108] Guo, Z., Li, S., Wang, X., Heng, W.: 'Distributed point-based gaussian approximation filtering for forecasting-aided state estimation in power systems', *IEEE Transactions on Power Systems*, (in press).

[109] Rana, M. M., Li, L.: 'An overview of distributed microgrid state estimation and control for smart grids', *Sensors*, 2015, **15**, (2), pp. 4302–4325.

[110] Xie, L., Mo, Y., Sinopoli, B.: 'Integrity data attacks in power market operations', *IEEE Transactions on Smart Grid*, 2011, **2**, (4), pp. 659–666.

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

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

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

[114] Hug, G., Giampapa, J. A.: 'Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks', *IEEE Transactions on Smart Grid*, 2012, **3**, (3), pp. 1362–1370.

[115] Sou, K. C., Sandberg, H., Johansson, K. H.: 'On the exact solution to a smart grid cyber-security analysis problem', *IEEE Transactions on Smart Grid*, 2013, **4**, (2), pp. 856–865.

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

[117] Cui, S., Han, Z., Kar, S., Kim, T. T., Poor, H. V., Tajer, A.: 'Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions', *IEEE Signal Processing Magazine*, 2012, **29**, (5), pp. 106–115.

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

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

[120] Sou, K. C., Sandberg, H., Johansson, K. H.: 'Data attack isolation in power networks using secure voltage magnitude measurements', *IEEE Transactions on Smart Grid*, 2014, **5**, (1), pp. 14–28.

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

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

[123] Kim, T. T., Poor, H. V.: 'Strategic protection against data injection attacks on power grids', *IEEE Transactions on Smart Grid*, 2011, **2**, (2), pp. 326–333.

[124] Vuković, O., Sou, K. C., Dán, G., Sandberg, H.: 'Network-aware mitigation of data integrity attacks on power system state estimation', *IEEE Journal on Selected Areas in Communications*, 2012, **30**, (6), pp. 1108–1118.

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

[126] Mousavian, S., Valenzuela, J., Wang, J.: 'A probabilistic risk mitigation model for cyber-attacks to PMU networks', *IEEE Transactions on Power Systems*, 2015, **30**, (1), pp. 156–165.

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

[128] Wang, S., Ren, W., Al-Saggaf, U.: 'Effects of switching network topologies on stealthy false data injection attacks against state estimation in power networks', *IEEE Systems Journal*, (in press).

[129] Hao, J., Piechocki, R. J., Kaleshi, D., *et al.*: 'Sparse malicious false data injection attacks and defense mechanisms in smart grids', *IEEE Transactions on Industrial Informatics*, 2015, **11**, (5), pp. 1198–1209.

[130] Yang, Q., Yang, J., Yu, W., *et al.*: 'On false data-injection attacks against power system state estimation: Modeling and countermeasures', *IEEE Transactions on Parallel and Distributed Systems*, 2014, **25**, (3), pp. 717–729.

[131] Wang, W., Lu, Z.: 'Cyber security in the smart grid: Survey and challenges', *Computer Networks*, 2013, **57**, (5), pp. 1344–1371.

[132] Sandberg, H., Amin, S., Johansson, K.: 'Cyberphysical security in networked control systems: an introduction to the issue', *IEEE Control Systems Magazine*, 2015, **35**, (1), pp. 20–23.

[133] Wang, Z., Dong, H., Shen, B., Gao, H.: 'Finite-horizon H_∞ filtering with missing measurements and quantization effects', *IEEE Transactions on Automatic Control*, 2013, **58**, (7), pp. 1707–1718.

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

[135] Dong, H., Wang, Z., Ding, S. X., Gao, H.: 'Event-based filter design for a class of nonlinear time-varying systems with fading channels and multiplicative noises', *IEEE Transactions on Signal Processing*, 2015, **63**, (13), pp. 3387–3395.

[136] Francy, R. C., Farid, A. M., Youcef-Toumi, K.: 'Event triggered state estimation techniques for power systems with integrated variable energy resources', *ISA transactions*, 2015, **56**, pp. 165–172.

[137] Werner, S., Lundén, J.: 'Event-triggered real-time metering in smart grids', *Proc. the 23rd European Signal Processing Conference (EUSIPCO)*, 2015, pp. 2701–2705.

[138] Zhao, J., Zhang, G., La Scala, M., Dong, Z. Y., Chen, C., Wang, J.: 'Short-term state forecasting-aided method for detection of smart grid general false data injection attacks', *IEEE Transactions on Smart Grid*, (in press).

[139] Manandhar, K., Cao, X., Hu, F., Liu, Y.: 'Detection of faults and attacks including false data injection attack in smart grid using Kalman filter', *IEEE Transactions on Control of Network Systems*, 2014, **1**, (4), pp. 370–379.