Chapter 6

Bad Data Detection in Smart Grid

Authors: Haris M. Khalid, and Ahmed Al-Durra

Affiliations: H. M. Khalid is with the department of Electrical and Electronics Engineering, Higher Colleges of Technology (HCT), Sharjah 7947, UAE. Email: harism.khalid@yahoo.com, Website: www.harismkhalid.com

A. Al-Durra is with the department of Electrical Engineering, The Petroleum Institute (PI), Abu Dhabi, UAE. Email: aaldurra@pi.ac.ae

Abstract: This chapter will discuss bad data detection techniques and their application in oscillation monitoring. Utilization of synchrophasor measurements for wide-area monitoring applications enables system operators to acquire real-time grid information. However, intentional injections of false synchrophasor measurements can potentially lead to inappropriate control actions, jeopardizing the security, and reliability of power transmission networks. An attacker can compromise the integrity of the monitoring algorithms by hijacking a subset of sensor measurements and sending manipulated readings. Such approach can result to wide-area blackouts in power grids. This chapter considers bad-data detection techniques with special focus on oscillation monitoring. To achieve an accurate supervision, a Bayesian inference technique has been discussed for each monitoring node using a distributed architecture.

Index Terms: Bayesian, cyber-physical systems, cyber security, data-injection attacks, inter-area oscillations, phasor measurement unit (PMU), power system monitoring, power system stability, real-time measurements, situational awareness, smart grid, synchrophasor, wide area monitoring system (WAMS).

6.1 Introduction

Due to the increasing dependency of digital measurements for monitoring and control applications, bad-data attack is an emerging threat. If a sensor is successfully attacked, its stored information can be compromised [1-4]. Given the criticality of power systems in the context of the national security, wide area monitoring systems (WAMS) applications such as oscillation detection is an attractive attack target [5]. If a PMU is successfully attacked, its stored information can be unnoticeably compromised. This can result to significant impact on public safety and economic losses [6-10]. Currently, it is a time-consuming task to detect and identify data-attacks as an adversary can choose the site of attack judiciously and design the attack vector carefully [11].

Many methods have been proposed to identify abnormal data segments and isolate attacked sensors in recent years. Most of them are published to enhance static application like state estimation [6, 12-13], power flow analysis [8-9, 14], and electricity market [7]. Static monitoring applications primarily focus on monitoring the operating point of the system and address slow dynamics in the range of minutes to hours [15]. In contrast, few have been proposed for dynamics monitoring applications, which tracks transient dynamics in the order of seconds or less.

6.2 Possible Approaches

6.2.1 State Estimation

Several methodologies in the areas of state estimations were developed over the past decades. Literature on the types of state estimation algorithms were presented in [16-19]. State estimation also has different approaches based on application of the algorithms such as conventional state estimation [16], distributed state estimation or multi area state estimation [20]. Depending on the timing and evolution of the estimates, state estimation schemes may be broadly classified into two basic distinct paradigms: static state estimation and dynamic state estimation [21]. Another extension of static state estimation also included the Sequential state estimation which has the advantage of being able to perform updates with partial measurement set [22]. This enabled the method to address the problem of data loss and bad data. A static state estimation algorithm based on linear programming known as least absolute value was also developed in [23, 24]. Generally, under normal operating conditions, the power system is regarded as a quasi-static system that changes steadily but slowly [17]. Therefore, in order to continuously monitor the power system, state estimators must be executed at short intervals of time. But with the inherent expansion of power systems, with the increase of generations and loads, the system becomes extremely large for state estimation to be executed at short intervals of time since it requires heavy computation resources. Therefore, a technique known as tracking state estimation [25, 26] was developed. Once state estimates were calculated, the method simply update the next instant of time using a new measurement set obtained for that instant, instead of again running the entire static state estimation algorithm. Tracking estimators help energy management systems to keep track of the continuously changing power system without actually having to execute the entire state estimation algorithm. This allows continuous monitoring with reasonable utilization of computing resources.

6.2.2 Weighted Least Squares

One of the most commonly used types of static state estimation in utilities is the weighted least squares methodology [18]. It was formulated as an optimization problem with a notion of minimizing the squares of the differences between the measured and estimated values calculated using the corresponding power flow equations. The weighted least square uses the Newton-Raphson algorithm to obtain the state estimates. There have been numerous findings on different variations of weighted least square further to improve specific aspects of the algorithm. Fast decoupled state estimator [27, 28] is an example in which voltage magnitudes and phase angles are processed separately. The voltage magnitude values are concerned with the reactive power measurements while angles were related to active power measurements. Regularized least square for power systems in [29] proposed a type of weighted least square that was able to function in cases of partial observability.

6.2.3 Dynamic State Estimation

The Extended Kalman Filter (EKF) is the most widely used algorithm to perform dynamic state estimation [30]. Other forms of Kalman filters like unscented Kalman filter [31], and Iterative EKF [32] were also proposed in the literature. Other algorithms used to perform dynamic state estimations include Artificial Neural networks (ANN) [33] and Fuzzy logic [34] which are also computationally complex. Generally dynamic state estimations are well suited when the dynamics of the power systems are smooth and follow the historical value. In other words, they could fail to accurately estimate when there exists a bigger changes in operating points.

6.2.4 Bad Data Analysis using Chi-Squares Test and Normalized Residual Test

One of the essential functions of a state estimator is to detect bad measurements and to identify and eliminate them accordingly [35]. Bad data analysis could be performed during the estimation process or post-estimation. When using the weighted least squares estimation algorithm for state estimation, detection and identification of bad data is done after the estimation process by processing the measurement residuals. The analysis is essentially based on the properties of the residuals, including their expected probability distribution.

Chi-squares test for bad data detection was presented in [36, 37]. It uses the properties of the chi-squares probability density function to compare with the objective function of weighted least squares. Chi-squares test was able to detect bad data but does not identify locations.

Alternatively, normalized residual test was able to detect as well as identify the locations of occurrences [35, 36, 38]. Normalized residual test was developed based on the statistical characteristics of the measurement residuals. Detection and identification could also be accomplished by further processing of the residuals as in the hypothesis testing identification methods [35, 36, 39]. Although both methods used the residual sensitivity matrix to represent the sensitivity of the measurement residuals to the measurement errors, hypothesis testing identification was more complex and computationally costly due to the further processing of the residuals. Hence, hypothesis testing identification was used to detect and identify bad data in this thesis. However, hypothesis testing identification was observed to exhibit some limitations as noted in [36]. The primary limitation was the inability to track bad data if it occurred at critical locations. To resolve this issue, utilizations of PMU measurements were proposed in recent literature.

6.3- Case Study: Oscillation Monitoring:

One mature dynamic monitoring application is oscillation detection [40-42]. Such low-frequency dynamics were only observable by analyzing measurements from PMUs. Today, various types of oscillation detection schemes have been installed in many transmission utilities to monitor the inter-area oscillations within critical tie-lines. Hence, oscillation detection is more likely to be subjected to intentional data-injection attacks than other dynamic monitoring applications [5]. Moreover, these data-atacks are assumed to take place in Phasor Measurement Units (PMUs) installed in substations.

6.3.2 Consequences of an Attack

In an event of an attack, the following two negative consequences can occur due to inaccurate monitoring and time complexity of the algorithms. 1) If the PMU data is altered in a way that is not detectable as false dynamics by oscillation monitoring schemes, the perceived observable state of the system will be wrong. This may lead to improper control actions endangering the security of the system. 2) The malicious intent might not be to hide the attack. An example is the denial of service, where the system operator loses the observability in a critical region.

6.3.3 Distinction between a Fault and a Cyber-Attack:

Although both types of perturbations can lead to abnormal operations, the notion of a fault and cyber-attack is distinctly different. A fault is considered as physical events that affect the power grid behavior, where the inherent transient dynamics are observable in neighboring substations and can be correlated in a time scale [43-46]. In contrast, a cyber-attack decouples from the physical world [4,6,11,12,47]. Thus, the false dynamics embedded inside attacked measurements may not correlate with other locations in time. The key is to establish a link with neighboring metering devices, and perform correlation studies.

6.3.4 Difference from Static Monitoring Applications:

In contrast to static monitoring application, impacts of acting on incorrect information are experienced relatively faster leading to more destabilizing issues. The static monitoring approach of analyzing a state-space model derived from linear differential algebraic equations is not suitable for tracking transient dynamics like inter-area oscillations [5,6,13]. The fundamental issue is the linearized equations are restrictive representation of the non-linear dynamic transients caused by system perturbations. Another concern is the reaction time for addressing transient dynamics are much less in comparison with static applications like state estimation. Despite significant efforts have been invested in preventing cyber-attacks for static monitoring applications [6, 7, 8, 9, 13, 47], researchers have not fully investigated the impact of cyber-attacks for monitoring inter-area oscillations. The reason is WAMS applications for monitoring transient dynamics is still an emerging research where main focus to date has been towards application development [16-18]. Hence, novel methodologies are needed to prevent cyber-attacks in oscillation detection schemes.

6.4 Modeling an Attack in Oscillation Detection Schemes

In this section, the three critical research tasks to establish immunity towards cyber-attacks for oscillation detection schemes are described.

6.4.1 State Space Representation of a Power Grid

In the field of real-time dynamic monitoring, especially for wide-area monitoring system applications, the notion is to become less dependent on classic models and adopt real-time system identification techniques. The reason is classic differential equations are less representative of continuous random load variations, line temperature variations, and other operational uncertainties. Although using differential equation-based models are suitable for some steady-state or static applications like state estimation or automatic generation control, it is not suitable for monitoring electromechanical interactions of synchronous generators. Therefore, system parameters are not extracted from offline predetermined power system models. Instead, the proposed method extracts desired parameters from PMU measurements.

A power grid prone to data-injection attacks can be modeled as a nonlinear dynamical system. Continuous load perturbations are part of noise-induced transitions, which can be expressed as:

$$\alpha x_{t+1} = f(x_t, w_t), \quad t = 0, 1, \dots, T \tag{1}$$

where α is the constant matrix, $f(\cdot)$ is the nonlinear function representing the state transition model, $x \in \boldsymbol{R}^r$ is the state variable, and the superscript *r* is the number of monitored dynamic modes. For the case of oscillation detection, the state variable represents the electromechanical oscillation, and *r* refers to the number of oscillations in the subspace **R**. The process noise of the recursive scheme is $w \in \boldsymbol{R}^r$at the time *t* over a monitoring window of *T* time instances. Suppose a power grid described by (1) is monitored by *N* number of PMUs. We propose a distributed scheme that processes the estimated oscillatory dynamics of each PMU nodes at a centralized track fusion center. The observation vector z^i for extracting electromechanical oscillations at the i^{th} node is:

$$z_t^i = h_t^i(x_t) + v_t^i, \quad i = 1, 2, \dots, N \tag{2}$$

Note that the i^{th} node may be subjected to an attack. The term $z^i \in \boldsymbol{R}^{p^i}$ and p^i is the number of measurements made by the i^{th} PMU. The nonlinear function representing the local observation matrix of the i^{th} sensor is $h_t^i(\cdot)$, and $v^i \in \boldsymbol{R}^{p^i}$ refers to the observation noise.

6.4.2 Constraints of a Power Grid

From (1) and (2), a power grid can be governed by the following constraints:

$$x_t \in \boldsymbol{X}_t, w_t \in \boldsymbol{W}_t, and\ v_t \in \boldsymbol{V}_t \tag{3}$$

where $\mathbf{X_t}$, $\mathbf{W_t}$, and $\mathbf{V_t}$ are assumed to have Gaussian probability distribution function. Once the observation model is constructed from synchrophasor measurements corrected from the affected location, the corresponding state representation of electromechanical oscillations can be formulated in the frequency domain.

6.4.3 Electromechanical Oscillation Model Formulation

According to [48], a measured noise-induced signal containing *K* number of electromechanical oscillations can be modeled in the frequency domain. As a result, (2) can be expressed as:

$$z_t^i = \sum_{k=1}^{K} A_k e^{(-\sigma_k + j2\pi f_k)tT_s} + v_t^t, \quad t = 1, 2, \ldots, T \tag{4}$$

A_k is the complex amplitude of the kth mode, σ_k and f_k are the corresponding damping factor and oscillatory frequency respectively. The sampling time is represented as T_s.

However, estimating oscillatory parameters for an accurate WAMS will require the complete observability of the observation matrix. This is quiet challenging in the presence of data-injection attacks. Locational awareness for each node is required, considering the fact that installed PMUs may also malfunction during an attack. This requires classification of the attack, followed by its characterization and modeling.

6.4.4 Characterization of an Attack: An Example

An initial characterization about the unobservable attacks can be possibly induced by Bayesian inference. Assume a bus of power grid is attacked as shown in Fig. 1. Considering the Bayesian inference, the probabilities on *a-prior* distribution over the oscillatory states at ith node are p(x_t^i), and the observation matrix is p($H_t^i|x_t^i$).

The resultant posterior distribution over the observations can be represented by the Bayesian inference as:

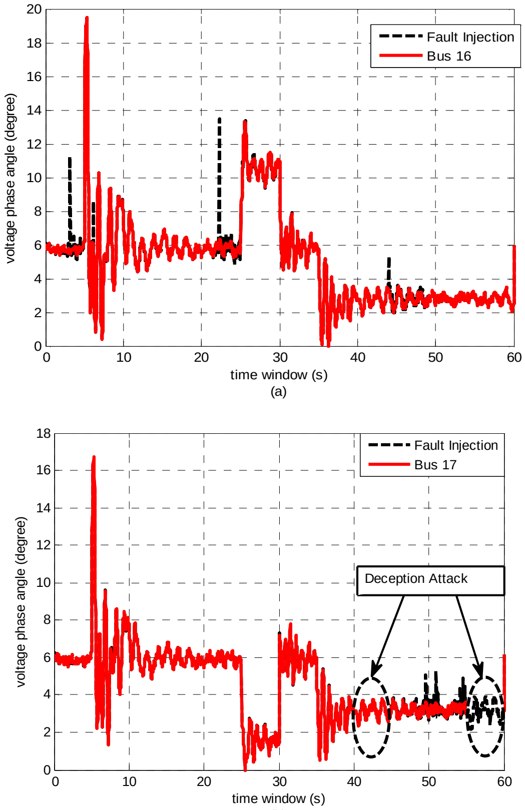
$$p(x_t^i \mid z_t^i) = \frac{p(x_t^i)\, p(z_t^i \mid x_t^i)}{p(z_t^i)} \tag{5}$$

To quantify the uncertainty of possible data-injection attacks, the density of the predicted synchrophasor observations is required to be computed. This can be obtained by averaging over the uncertainty of data-injection attacks on the oscillatory states and the observation matrix. Let z_{pr}^i represent the predicted synchrophasor observations at ith node, then $z_{pr,t}^i$ can be presented in the form of predictive distribution as:

$$p(z_{pr,t}^i \mid z_t^i) = \sum_{x_t^i} \int dH_t^i\, p(z_{pr}^i \mid H_t^i, x_t^i, z_t^i)\, p(H_t^i \mid x_t^i, z_t^i)\, p(x_t^i \mid z_t^i) \tag{6}$$

H_t^i is a hypothesis extracted from the observation signal about the presence or absence of the attack signal.

This distribution will later assist in the development of the probability of attack vectors.



(a)

(b)

Fig. 1 Profile of a) Bus 16 and b) Bus 17 with random fault injections

Once all the information about the covariance and estimated states are collected from local PMU nodes, they will be treated at the distributed fusion center which is an integral part of attack tolerant monitoring system.

6.4.5 Significance of Distributed Architecture towards Information of Cyber-Attack

To create a cascading failure caused by lightly damped electromechanical oscillations, the injected data can be assumed to imitate regular small-amplitude load variations as seen in daily operations. Therefore, characterizing a plausible attack or loss of information needs to be done. Furthermore, from a practical viewpoint, we can assume attacked nodes are local as wide-area attacks are less feasible from a geographical perspective. Based on these considerations, it is not possible to identify abnormalities if a monitoring scheme utilizes one or local PMU measurements. Conventionally, an oscillation monitoring scheme can be installed in the PMU or local Phasor Data Concentrator (PDC). Estimated oscillatory parameters are transmitted to the control center to optimize the communication bandwidth. Building on top of this configuration, we intend to request each recursive monitoring scheme to send additional information of its estimated covariance matrix and state vector. As a result, a centralized track fusion center is proposed. Similar to (5), the observation model of the track fusion center z_t^{TF}can be expressed as:

$$z_t^{TF} = H_t^{TF} x_t + \omega_t^{TF} \tag{10}$$

Estimating oscillatory parameters in the presence of abnormal or attacked nodes will require the complete observability of the oscillation observation matrix. This requires the calculation of correlation information from the initial estimates of the observation model. Treated correlation information will then assist in the removal of faulty oscillatory parameters to ensure an attack-free update of oscillatory parameters to the system operators. Based on this concept, a refined covariance matrix generated is then sent back to each monitoring node to improve the observability of the wide-area dynamics of inter-area oscillations. However, an accurate power oscillation monitoring scheme is required to operate near real-time. This can be very challenging in the presence of data-injection attacks. To reduce the computational effort of determining the initial estimates and the error covariance matrix at each PMU node, diagonalization of the system model into subsystems can be proposed.

6.4.6 Diagonalization of a System into Subsystems:

Note the attacked system at node *i* can be diagonalized up to *N* number of subsystems. Considering the diagonalization of *N*=2 subsystems, using the theory of robust eigenvalue placement, the system (4) and (5) can be decomposed into *L* and *R* non-singular matrices.

$$L\alpha R = \begin{bmatrix} \alpha_1 & 0 \\ \alpha_2 & 0 \end{bmatrix}, L\kappa R = \begin{bmatrix} \kappa_1 & 0 \\ \kappa_2 & \kappa_3 \end{bmatrix}, L\psi R = \begin{bmatrix} \psi_1 \\ \psi_2 \end{bmatrix}, H^i R = \begin{bmatrix} H_1^i \\ H_2^i \end{bmatrix}^* \tag{11}$$

where $\alpha_1 \in R^{n_1 \times n_2}$ is a non-singular lower-triangular, $\kappa_1 \in R^{n_1 \times n_1}$ is quasi-lower-triangular, $\kappa_3 \in R^{n_2 \times n_2}$ is non-singular lower-triangular. Transforming $x_t = R[x_{1,t}^* \;\; x_{2,t}^*]^*$, where $x_{1,t} \in R^{n_1}, x_{2,t} \in R^{n_2}$. The system can be transformed into the following two diagonalizable subsystems by taking the inverse of high dimensional matrices of (1) and (2) using linear minimum variance:

$$x_{1,t+1} = \kappa_0 x_{1,t} + \psi_0 w_t \tag{12}$$

$$x_{2,t} = \overline{\kappa} x_{1,t} + \overline{\psi} w_t \tag{13}$$

$$z_t^i = \overline{H}_t^i x_{1,t} + \overline{v}_t^i \tag{14}$$

where $x_{1,t}$ and $x_{2,t}$ are the states of subsystem 1 and subsystem 2, respectively. $\kappa_0, \psi_0, \overline{\kappa}, \overline{\psi}, \overline{H}$ and $\overline{v}$ are diagonalized variables, which are computed from the inverse of weighted matrices α_1 and κ_3. Note in the subsystem transformation, only first subsystem will have the prediction and filtering stage, whereas the rest of *N −1* subsystems will only have filtering stage. Each subsystem is a smaller matrix than the original model, which would then improve the computing speed required to update the covariance matrix at each monitoring instance. Once the subsystems are constructed from the system affected by the data-injection attacks, the interactions between them shall be evaluated. Moreover, by handling the noise and state constraints of (3), the immunity of the estimation results during data-injection can be increased. Referring to (12)–(14), the resultant noises w_t and v_t will have the diagonalizable expected value:

$$E\left[\begin{bmatrix} \overline{w}_t \\ \overline{v}_t^{1} \end{bmatrix}, \begin{bmatrix} \overline{w}_t^{*} & \overline{v}_t^{2*} \end{bmatrix}\right] = Q_t^{1,2}\delta_t^{1,2}$$

where $Q_t^{1,2}$ is the process noise correlation factor between subsystem 1 and 2, $\delta_t^{1,2}$ is the Kronecker delta function used for shifting the integer variable after the presence or absence of noise.

In this step, we will integrate a centralized filter to remove estimated parameters from attacked sensor nodes while providing accurate covariance matrix for the individual monitoring nodes. This established a closed loop monitoring system. Thus, the resilience of inter-area oscillation detection against data-injection attacks can be improved.

6.4.7 Detection Bad-Data using Initial Observation Analysis:

Once the probability of attack vectors is developed, the attack can be detected by doing an initial observation analysis of the measurements. This can be achieved by taking the difference between the given and predicted observation of the oscillation state:

$$Z^i_{t+1} = [z^i_{t+1} - z^i_{pr,t+1}] = \sum_{t=1}^{T} \psi^*_{t-1}\theta_t^{H(1)}\Delta H^i_t + \upsilon^i_t \qquad (15)$$

where the vector Z^i_{t+1} is the innovation calculated for i-th node. $z^i_{t+1}$and $z^i_{pr,t+1}$ are the data-injection free (nominal) and predicted affected observation outputs, respectively.$\Delta H^i_t = \Delta H^i_{d,t} - H^i_t$ is the perturbation in H^i_t. $\theta^i_t = \dfrac{\delta z^i_t}{\delta H^{i*}_t}$ is the gradient used to identify the perturbation due to data-injection attacks. ψ_t is the data vector formed from past outputs and reference inputs at each node.

Bibliography

[1] A. G. Tartakovsky, B. L. Rozovskii, R. B. Blažek, and H. Kim, "A novel approach to detection of intrusions in computer networks via adaptive sequential and batch-sequential change-point detection methods," IEEE Transactions on Signal Processing, vol. 54, pp. 3372-3382, 2006.

[2] S. Zhu, S. Setia, S. Jajodia, and P. Ning, "An interleaved hop-by-hop authentication scheme for filtering of injected false data in sensor networks," in IEEE symposium on security and privacy, 2004, pp. 259-271.

[3] V. Shukla and D. Qiao, "Distinguishing data transience from false injection in sensor networks," in 4th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks, 2007, pp. 41-50.

[4] F. Pasqualetti, F. Dorfler, and F. Bullo, "Control-Theoretic Methods for Cyberphysical Security: Geometric Principles for Optimal Cross-Layer Resilient Control Systems," IEEE Control Systems, vol. 35, pp. 110-127, 2015.

[5] H. M. Khalid and J. C.-H. Peng, "Immunity toward data-injection attacks using multisensor track fusion-based model prediction," IEEE Transactions on Smart Grid, in press.

[6] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," IEEE Transactions on Automatic Control, vol. 58, pp. 2715-2729, 2013.

[7] X. Le, M. Yilin, and B. Sinopoli, "Integrity data attacks in power market operations," IEEE Transactions on Smart Grid, vol. 2, pp. 659-666, 2011.

[8] A. H. Mohsenian-Rad and A. Leon-Garcia, "Distributed internet-based load altering attacks against smart power grids," IEEE Transactions on Smart Grid, vol. 2, pp. 667-674, 2011.

[9] H. Yi, M. Esmalifalak, N. Huy, Z. Rong, H. Zhu, L. Husheng, et al., "Bad data injection in smart grid: attack and defense mechanisms," IEEE Communications Magazine, vol. 51, pp. 27-33, 2013.

[10] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," IEEE Transactions on Smart Grid, vol. 2, pp. 326-333, 2011.

[11] 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, vol. 29, pp. 106-115, 2012.

[12] M. Ozay, I. Esnaola, F. Vural, S. R. Kulkarni, and H. V. Poor, "Sparse attack construction and state estimation in the smart grid: Centralized and

distributed models," IEEE Journal on Selected Areas in Communications, vol. 31, pp. 1306-1318, 2013.

[13] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," IEEE Transactions on Automatic Control, vol. 59, pp. 1454-1467, 2014.

[14] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," IEEE Transactions on Smart Grid, vol. 2, pp. 382-390, 2011.

[15] C. Rehtanz, J. Béland, G. Benmouyal, S. Boroczky, C. Candia, D. Cirio, et al., "Wide area monitoring and control for transmission capability enhancement," CIGRE Technical Brochure, 2007.

[16] A. Monticelli, "Electric power system state estimation," Proceedings of the IEEE, vol. 88, pp. 262-282, 2000.

[17] N. Shivakumar and A. Jain, "A review of power system dynamic state estimation techniques," in Power System Technology and IEEE Power India Conference, 2008. POWERCON 2008. Joint International Conference on, 2008, pp. 1-6.

[18] W.-g. Li, J. Li, A. Gao, and J.-h. Yang, "Review and Research Trends on State Estimation of Electrical Power Systems," in Power and Energy Engineering Conference (APPEEC), 2011 Asia-Pacific, 2011, pp. 1-4.

[19] A. Leite da Silva and D. Falcao, "Bibliography on power system state estimation (1968-1989)," Power Systems, IEEE Transactions on, vol. 5, pp. 950-961, 1990.

[20] 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, vol. 81, pp. 1060-1069, 2011.

[21] Y.-F. Huang, S. Werner, J. Huang, N. Kashyap, and V. Gupta, "State estimation in electric power grids: Meeting new challenges presented by the requirements of the future grid," Signal Processing Magazine, IEEE, vol. 29, pp. 33-43, 2012.

[22] A. Simoes-Costa and V. Quintana, "An orthogonal row processing algorithm for power system sequential state estimation," Power Apparatus and Systems, IEEE Transactions on, pp. 3791-3800, 1981.

[23] A. Abur and M. K. Celik, "Least absolute value state estimation with equality and inequality constraints," Power Systems, IEEE Transactions on, vol. 8, pp. 680-686, 1993.

[24] M. K. Celik and A. Abur, "A robust WLAV state estimator using transformations," Power Systems, IEEE Transactions on, vol. 7, pp. 106-113, 1992.

[25] A. S. Debs and R. Larson, "A dynamic estimator for tracking the state of a power system," Power Apparatus and Systems, IEEE Transactions on, pp. 1670-1678, 1970.

[26] D. Falcao, P. Cooke, and A. Brameller, "Power system tracking state estimation and bad data processing," Power Apparatus and Systems, IEEE Transactions on, pp. 325-333, 1982.

[27] A. Garcia, A. Monticelli, and P. Abreu, "Fast decoupled state estimation and bad data processing," Power Apparatus and Systems, IEEE Transactions on, pp. 1645-1652, 1979.

[28] A. Monticelli, "Fast Decoupled State Estimator," in State Estimation in Electric Power Systems, ed: Springer, 1999, pp. 313-342.

[29] M. C. de Almeida, A. V. Garcia, and E. N. Asada, "Regularized least squares power system state estimation," Power Systems, IEEE Transactions on, vol. 27, pp. 290-297, 2012.

[30] T. Zhai, H. Ruan, and E. E. Yaz, "Performance evaluation of extended Kalman filter based state estimation for first order nonlinear dynamic systems," in Decision and Control, 2003. Proceedings. 42nd IEEE Conference on, 2003, pp. 1386-1391.

[31] G. Valverde and V. Terzija, "Unscented Kalman filter for power system dynamic state estimation," IET generation, transmission & distribution, vol. 5, pp. 29-37, 2011.

[32] M. Brown Do Coutto Filho and J. S. de Souza, "Forecasting-aided state estimation—Part I: Panorama," Power Systems, IEEE Transactions on, vol. 24, pp. 1667-1677, 2009.

[33] A. Sinha and J. Mondal, "Dynamic state estimator using ANN based bus load prediction," Power Systems, IEEE Transactions on, vol. 14, pp. 1219-1225, 1999.

[34] 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," Power Systems, IEEE Transactions on, vol. 18, pp. 570-577, 2003.

[35] E. Handschin, F. Schweppe, J. Kohlas, and A. Fiechter, "Bad data analysis for power system state estimation," Power Apparatus and Systems, IEEE Transactions on, vol. 94, pp. 329-337, 1975.

[36] A. Abur and A. G. Exposito, Power system state estimation: theory and implementation: CRC Press, 2004.

[37] H. M. Merrill and F. C. Schweppe, "Bad data suppression in power system static state estimation," Power Apparatus and Systems, IEEE Transactions on, pp. 2718-2725, 1971.

[38] J. Chen and A. Abur, "Placement of PMUs to enable bad data detection in state estimation," Power Systems, IEEE Transactions on, vol. 21, pp. 1608-1615, 2006.

[39] T. Van Cutsem, M. Ribbens-Pavella, and L. Mili, "Hypothesis testing identification: a new method for bad data analysis in power system state estimation," Power Apparatus and Systems, IEEE Transactions on, pp. 3239-3252, 1984.

[40] C. Lu, B. Shi, X. Wu, and H. Sun, "Advancing China's smart grid: Phasor measurement units in a wide-area management system," IEEE Power and Energy Magazine, vol. 13, pp. 60-71, 2015.

[41] W. Sattinger and G. Giannuzzi, "Monitoring continental europe: An overview of WAM systems used in Italy and Switzerland," IEEE Power and Energy Magazine, vol. 13, pp. 41-48, 2015.

[42] V. Madani, J. Giri, D. Kosterev, D. Novosel, and D. Brancaccio, "Challenging changing landscapes: Implementing synchrophasor technology in

grid operations in the WECC region," IEEE Power and Energy Magazine, vol. 13, pp. 18-28, 2015.

[43] Y. Zhang and J. Jiang, "Bibliographical review on reconfigurable fault-tolerant control systems," Annual reviews in control, vol. 32, pp. 229-252, 2008.

[44] M. Blanke and J. Schröder, Diagnosis and fault-tolerant control vol. 2: Springer, 2006.

[45] C. Hajiyev and F. Caliskan, Fault diagnosis and reconfiguration in flight control systems vol. 2: Springer Science & Business Media, 2013.

[46] F. García-Nocetti, Reconfigurable Distributed Control: Springer Science & Business Media, 2005.

[47] F. Skopik and P. D. Smith, Smart grid security: Innovative solutions for a modernized grid: Elsevier Science, 2015.

[48] J. F. Hauer, "Application of Prony analysis to the determination of modal content and equivalent models for measured power system response," IEEE Transactions on Power Systems, vol. 6, pp. 1062-1068, 1991.

Haris M. Khalid (M'13) received his B.S. (Hons.) degree in Mechatronics and Control Systems Engineering from University of Engineering and Technology (UET), Lahore, Pakistan, in 2007, and the M.S. and Ph.D. degrees in Control Systems Engineering from King Fahd University of Petroleum and Minerals (KFUPM), Dhahran, Kingdom of Saudi Arabia, in 2009 and 2012, respectively. He then joined Distributed Control Research Group (DCRG) at KFUPM, as a Research Fellow. In 2013, he joined as a Research Fellow with the Power Systems Research Laboratory (PSRL) at Department of Electrical Engineering and

Computer Science, Institute Center for Energy, Masdar Institute of Science and Technology (MI), Masdar City, United Arab Emirates, which is a MI-MIT Cooperative Program with Massachusetts Institute of Technology (MIT), Cambridge, MA, USA. Currently, he is a Visiting Scholar with Petroleum Institute, Abu Dhabi, UAE.

His research interests are power systems, cyber-physical systems, electric vehicles, signal processing, applied mathematics, fault diagnostics, filtering, estimation, performance monitoring, and battery management systems. He has authored 40+ peer-reviewed publications, which includes 1 Monograph, 6 IEEE Transactions, 3 IET Journals, 2 Elsevier Journals, 3 Springer Journals and 15+ peer-reviewed International Conferences.

Ahmed Al-Durra (S'07-M'10-SM'14) received the B.S., M.S., and PhD in Electrical and Computer Engineering from the Ohio State University in 2005, 2007, and 2010, respectively. For his M. Sc. degree, he investigated the application of several nonlinear control techniques on automotive traction PEM fuel cell systems. He conducted his PhD research at the Center for Automotive Research in the Ohio State University on the applications of modern estimation and control theories to automotive propulsion systems. At the present, he is an Associate Professor in the Electrical Engineering Department at the Petroleum Institute, Abu Dhabi, UAE. He obtained the PI Research & Scholarship Award for Junior Faculty in 2014. He has one U.S. Patent Application and co-published one book titled “Modeling and Control Aspects of Wind Power Systems.” His research interests are application of estimation and control theory in power system stability, Micro and Smart Grids, renewable energy, and process control. He has published over 80 scientific articles in Journals, International Conferences, and book chapters. Dr. Ahmed has successfully accomplished several research projects at international and national levels. He has supervised/co-supervised over 20 PhD and Master students. He is the co-founder of Renewable Energy Laboratory at the Petroleum Institute, and Senior Member in IEEE.