Signal Processing in Smart Grids: From Data to Reliable Information

Meng Wang

1 Introduction

The recent proliferation of data is revolutionizing the practice of power system monitoring and control. With the Smart Grid initiative, more than two thousand multichannel phasor measurement units (PMUs) [37] have now been installed in North America [35]. PMUs can directly measure GPS-synchronized bus voltage phasors, line current phasors, and the frequency, at a rate of 30 or 60 samples per second per channel. Compared to the conventional Supervisory Control and Data Acquisition (SCADA) systems that only provide measurements every 2–5 s, which are not accurately synchronized in time, PMUs can drastically improve the system visibility and enhance the situational awareness.

The data abundance imposes significant challenges on the power industry. Currently, the transmission grid operators decide control actions based on the output of state estimation, which is carried out at multi-second intervals in correspondence to the data acquisition rate of the SCADA system. Moreover, control actions are mostly computed offline and are not optimized for diverse real-time situations. With the recent data wealth, an important and urging question is how to convert the massive amounts of data to reliable information quickly so as to facilitate the following real-time control decisions.

PMUs are envisioned to improve wide-area situational awareness and prevent blackouts [1, 7]. Ever since the initial installation, many research efforts have been devoted to exploiting the PMU data in various applications, and the continued investigation is still ongoing. The applications include but not limited to state estimation [50], oscillation detection and electromechanical mode identification [17, 29], disturbance detection and location [28, 32], and dynamic security assessment [8, 21].

M. Wang (✉)
Rensselaer Polytechnic Institute, Troy, NY 12180, USA
e-mail: wangm7@rpi.edu

J. Stoustrup et al. (eds.), *Smart Grid Control*, Power Electronics and Power Systems, https://doi.org/10.1007/978-3-319-98310-3_11

Data quality is an inevitable issue for the control-room incorporation of PMU data. Because of the communication networks that were not designed to carry high-speed PMU data and the early deployment of older PMUs, data losses, and data quality degradations happen quite often in practice, especially in the Eastern interconnection [41]. Current PMU-based applications usually assume that the measurements are available and reliable. To incorporate PMU data into real-time operations, a data-conditioning component is needed to reconstruct missing data [12] and correct bad measurements. Alternatively, data analysis methods that are robust to data quality degradation are worth investigation. Moreover, different applications have diverse requirements on the data quality. The trust scores of the obtained and the recovered measurements should be computed and incorporated into the design of the control actions.

Developed when the measurements were scarce, conventional methods usually require the modeling of the power system. The proliferation of PMU data enables the development of data-driven methods for feature extraction without power system modeling. Data-driven methods are much investigated, especially for applications in which accurate and explicit models are difficult to obtain. Despite all the nice properties, the output of data-driven methods might lack a clear physical interpretation. In contrast, physical models of the power systems are well studied, and conventional methods are usually accompanied with clear physical intuitions. Moreover, data-driven methods usually require parameter tuning, and the computational time of these methods could be of concern for real-time applications.

Cyber data security cannot be ignored. Cyber operations have been integrated into smart grids to enhance control performance; however, such integration also increases the possibility of cyber attacks. Although attacking the control laws of the operator is relatively difficult, an intruder could alter the measurements to mislead the operator, resulting in wrong control actions. The detection of these cyber attacks requires efforts in both the communication level through the development of advanced encryption methods and the signal processing level through the development of methods that can detect these cyber data attacks based on the abnormality in the measurements.

2 Data Quality Improvement

Data losses happen due to network congestion or PMU malfunctions. The missing data rate is reduced in recent years, but data losses still happen. When the measurements were scarce, the missing data points were interpolated using observations in the same measurement channel. Another way was to run the state estimator on the partially obtained measurements and compute the missing data points based on the estimated system state.

Now with the large amounts of data collected by many PMUs, the missing points can be directly and accurately estimated from the data without modeling the power system. The idea is to exploit the correlations in the spatial–temporal blocks of

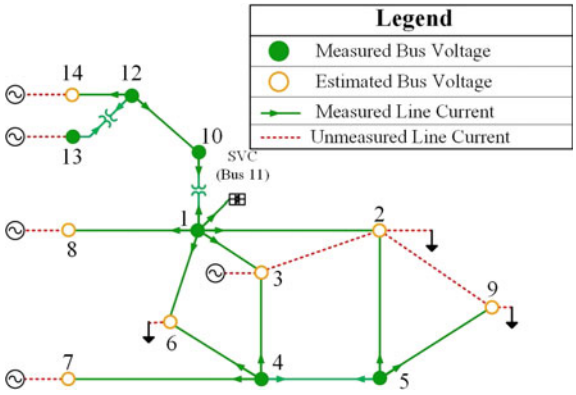

Fig. 1 Six PMUs in the Central NY Power System (reproduced from [12] ©2016 IEEE and used with permission)

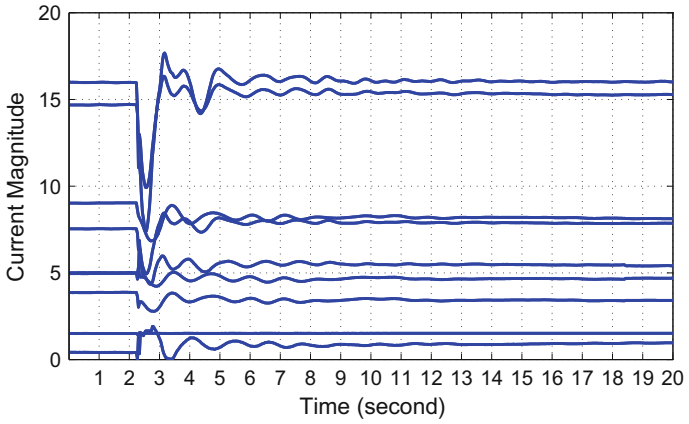

Fig. 2 Current magnitudes of PMU data (9 current phasors out of 37 phasors) (reproduced from [12] ©2016 IEEE and used with permission)

PMU data. In fact, the data correlation could be easily characterized by the low-rank property of the PMU data matrix.

Let $M \in \mathbb{C}^{m \times n}$ contain the phasor measurements (represented by complex numbers in rectangular form) from m PMU channels in n time instants. Then, M can be approximated by a low-rank matrix with a negligible error. For example, the recorded data of six multi-channel PMUs in the Central New York (NY) Power System (Fig. 1) were analyzed in [12]. M contains 37 voltage and current phasors in 20 s at a rate of 30 samples per channel per second. Figure 2 shows the current magnitudes of PMU measurements. Figure 3 shows the singular values of M. The largest 10 singular values are 894.5942, 36.8319, 20.7160, 8.3400, 3.0771, 2.4758, 1.9705, 1.3543, 0.5930, and 0.2470. We can approximate M by a rank-eight matrix with a very small error.

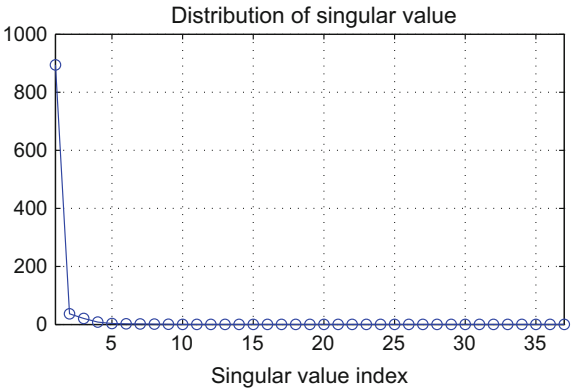

Fig. 3 Singular values of a 600×37 PMU data matrix (reproduced from [12] ©2016 IEEE and used with permission)

Table 1 Recovery performance of OLAP on NYISO data that contains disturbances. Computational time is the total time to recover missing points in 5-min data on a normal desktop. Relative recovery error is the ratio of recovery error to the actual value (both measured in ℓ_2-norm) [45]

	Voltage magnitude	Voltage angle	Frequency	Current magnitude	Current angle
Computational time (s)	1.305	1.327	1.239	8.121	9.113
Relative recovery error (%)	0.02	0.005	0.0015	0.24	0.05

The low-rank property enables computationally efficient methods with theoretical guarantees for various data analysis tasks. For instance, recovering missing points in a low-rank matrix M can be formulated as a convex optimization problem

$$\min_{X \in m \times n} \|X\|_* \text{ s.t. } X_{ij} = M_{ij}, \text{ for all } (ij) \in \Omega, \tag{1}$$

where Ω denotes the locations of the observed entries, and the matrix nuclear norm $\|\cdot\|_*$ is the sum of singular values. The original matrix M is proved to be the optimal solution to (1) under mild assumptions [5] and thus recovered in polynomial time.

We connected PMU data analysis with low-rank matrix theory and obtained promising results for missing PMU data recovery [9, 11, 12, 44]. We proved that the missing PMU data points can be correctly recovered under very mild assumptions [12]. The numerical evaluations of our developed online missing data recovery method, called OLAP, on recorded PMU datasets from NYISO are shown in Table 1 [45]. This 5-min dataset contains 53 voltage phasors, 53 frequencies, and 263 current phasors, with 8% missing data. Figure 4 shows the data recovery of consecutive data losses in one channel by OLAP. A capacitor-switching event during the data losses is recovered by utilizing the measurements in other channels, and this recovery is impossible by single-channel interpolations.

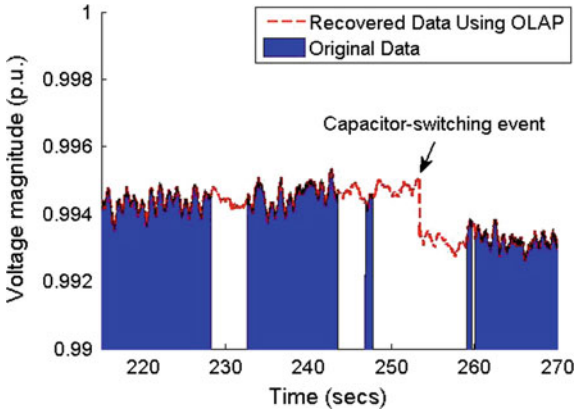

Fig. 4 Data recovery in one channel [45]

Besides missing data recovery, the low-rank property could also be exploited to detect and correct bad data. Bad data detection and identification has been an important issue for power system state estimation. It is usually integrated with the state estimation, which requires power system model. The measurements that are not consistent with the currently estimated system state are considered as bad data and removed. With the abundance of PMU data, bad data can be detected and identified directly from the data, see e.g., [10, 30, 48].

If we impose the assumption that the number of bad data is much less than the total number of measurements, the bad data detection problem can be formulated as a matrix decomposition problem. The obtained data matrix M is viewed as the sum of two matrices L^* and C^*, where the low-rank matrix L^* denotes the actual data without errors, and the sparse matrix C^* denotes the additive errors in the bad measurements. A matrix is sparse if it only has a small number of nonzero entries, while most entries are zero. The goal of matrix decomposition is to obtain L^* and C^* from M. Under mild assumptions [4], it can be achieved by solving a convex program

$$\min_{L,m\times n} \|L\|_* + \lambda \sum_{ij} |C_{ij}| \text{ s.t. } L + C = M, \tag{2}$$

where λ is a predetermined weighting factor.

The above problem formulation has been exploited to detect bad data, including injected false data by cyber attackers [10, 30]. Note that this formulation does not require any information about the system topology and the line impedances. Thus, bad data detection can be separated from state estimation. Moreover, it is shown in [10] that the topology information can be incorporated easily with minor changes to (2), resulting in a provable enhancement of the detection performance.

The above methods for data quality improvement only use PMU data. One interesting question is how to incorporate PMU data with other formats of data. For instance, conventional SCADA data provide information about power injections and power flows every 1–5 s. Is it possible to use the SCADA data to enhance the accu-

racy of the data recovery and error correction of PMU data? How shall we handle the different sampling rates of these data?

Another important question is how to differentiate data anomalies and system events. When a system event just starts, the affected measurements would be different from the nearby measurements. They might be treated as bad data if we directly apply (2). How shall we determine whether these measurements are bad data or resulting from system events? Is it possible to achieve this separation mostly based on data without much modeling of the system?

3 Model-Based and Data-Driven Analysis

Power system monitoring is conventionally model-based to compensate for the lack of measurements, as in dynamic state estimation [14, 43]. These methods degrade significantly when the model is inaccurate, which is a long-standing issue due to the complexity of power systems. Recent data abundance fosters the development of data-driven methods that do not require power system models.

Data-driven methods can extract information directly from data without modeling the power systems; however, completely ignoring the underlying dynamical system also has some limitations. First, data-driven methods might not perform as well as model-based methods when the model is correctly specified. Second, the computational complexity of machine-learning-based methods usually increases significantly when the data size increases. Lastly, the analyses are often lack of physical understandings of the power systems. An interesting research direction is how to incorporate the domain knowledge and engineering intuitions about the power system into the data-driven analyses.

Take disturbance identification as an example. Both model-based identification methods (see e.g., [42, 51]) and data-driven methods [3, 6, 15, 47] have been developed to identify different types of events in the system. Data-driven methods extract features (including direct features like a frequency [6] or its derivative [3], as well as indirect features like wavelet coefficients [19]) from measurements and classify those with similar features as resulting from the same event type.

We also developed a data-driven method to identify and locate events without modeling the power system [26, 27]. The key idea is to characterize an event by a low-dimensional row subspace spanned by the dominant singular vectors of the data matrix that contains spatial–temporal blocks of measurements from multiple PMUs. This subspace characterization is robust to initial system conditions and captures the system dynamics. Then an event is identified by comparing the obtained data with a pre-computed event dictionary with each dictionary atom corresponding to a row subspace of an event. The location of an event is determined based on the magnitudes of changes. Figure 5 shows the overview of this approach.

One distinctive feature of this approach is that a dictionary atom has a clear physical interpretation. It is the subspace spanned by a few dominant modes in the observation window. The subspace can be computed through Singular Value Decomposition

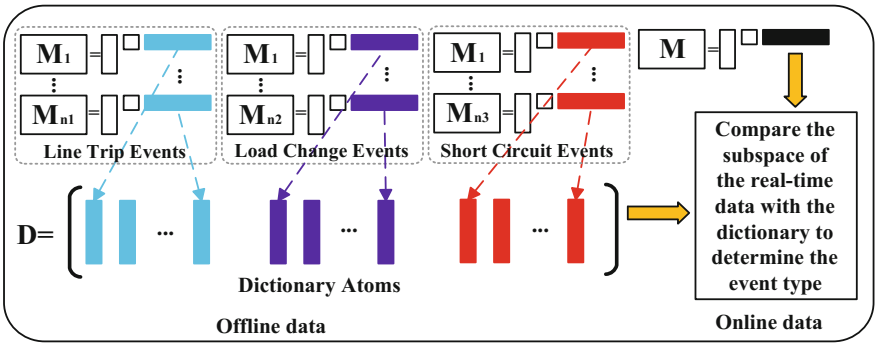

Fig. 5 Dictionary construction from historical datasets and real-time data identification through subspace comparison (reproduced from [27] ©2018 IEEE and used with permission)

Table 2 Identification results of 380 events (reproduced from [26] ©2017 IEEE and used with permission)

Type of event	IAR (%)	ELAR (%)	ALAR (%)
Line trip	100	85	94 (among 3 buses)
Short circuit	100	77	90 (among top 3 buses)
Load change	100	46	90 (among top 5 buses)

(SVD) [18]. Moreover, the dictionary size is much smaller than those of the dictionaries of time series [47] or other computed features [20]. That is because all the events will be compactly represented by a few row singular vectors to reduce the dimensionality. The reduction of the dictionary size reduces the computational complexity of both the offline training and the online event identification. The method identifies events shortly after the event starts (e.g., within 1–5 s) and can be implemented in real time, while existing methods are mostly designed for past event analysis (e.g., 30 s of data are needed in [47]).

The method is evaluated on the IEEE 68-bus test system (details see [26]). We simulate 380 events, including 160 line trip events, 100 load change events, and 120 short circuit events at different locations and with different pre-event conditions. Only one second of data is used for event identification. The constructed dictionary includes 33 events. Each event is represented by a subspace spanned by 30×6 matrix, where 30 is the number of time steps in one second and 6 is the number of dominating singular vectors.

Table 2 records the identification and location results under three criteria:

Identification Accuracy Rate (IAR): The ratio of the number of accurately identified events to the total number of events;

Approximate Location Accuracy Rate (ALAR): The ratio of the number of events with actual locations[1] among the top k buses with the most significant changes to the total number of events.

Exact Location Accuracy Rate (ELAR): A special case of ALAR when $k = 1$, i.e., the event location is exact.

The above disturbance identification method is one initial effort in incorporating physical understandings into the data-driven analyses for power system monitoring. One future direction is to extend these efforts to other aspects of power system monitoring such as state estimation and disturbance location.

4 Resilience to Cyber Data Attacks

Cyber operations have been integrated into power systems to enhance control performance; however, such integration also increases the possibility of cyber attacks. In early 2016, hackers caused a power outage for the first time in Ukraine during holiday season [36]. The development of a trustworthy power system requires developing new technologies in various aspects, such as a secured communication infrastructure and protected sensing and control devices. Here we focus on data security from a signal processing perspective.

Cyber data attacks can change the measurements obtained by the operator such that the operator would obtain a wrong estimate of the system state, resulting in harmful control actions and potential failures. These data attacks may also lead to significant financial impacts in the electricity market [49]. A malicious intruder with sufficient system configuration information can manipulate multiple measurements simultaneously, and the resulting injected false data can be are viewed as "the worst interacting bad data injected by an adversary" [25, 31].

State estimation in the presence of false data injection attacks has attracted much research attention recently. These attacks are carefully selected, and the interacting erroneous measurements cannot be detected by conventional bad data detections that only use measurements at one time instant. Many efforts have been devoted to studying the requirements to launch a cyber data attack [39] and preventing these attacks by protecting critical measurement units [2, 24]. A few recent works proposed detection methods for cyber data attacks [10, 30, 40]. Since the attacks cannot be detected only using measurements at one time instant, these methods exploit the temporal correlations in the data and detect the attacks as anomalies in time series.

Eavesdropping attacks are another form of security concerns [34]. An adversary might obtain sensitive information about the grid by monitoring the network traffic. The gathered information could be used for future crimes. Data privacy [23, 33] is an emerging issue in smart grids. PMU data are owned by regional transmission owners and considered to be private and sensitive. Privacy-guaranteed PMU data

[1] The location of line trip events are considered as successful if one of the two related buses are correctly identified.

communication has not yet been seriously investigated. Besides enhancing the data privacy by improving communication technologies for smart meter data [16, 22], the tools at the signal level to increase data privacy need to be developed. One can enhance data privacy by adding random noise [46] or applying quantization to the measurements [38], usually at a cost of data distortion. Some initial efforts have been devoted to developing data recovery methods from noisy and quantized measurements with a small data distortion for large amounts of PMU data [13].

Since cyber attacks can happen in various aspects of power system monitoring and control [34], it is very important to be precautious and develop the corresponding protection schemes in advance. The vulnerabilities of individual components of the system against cyber attacks should be constantly estimated, and attack prevention and detection methods should be incorporated into power system monitoring.

5 Conclusion

In summary, the data wealth brings multidisciplinary research opportunities of power engineering, signal processing, and machine learning. Data-oriented approaches, ideally incorporated with physical understandings of the power systems, can extract information from the data and enable real-time control operations. Data quality enhancement is a necessary pre-conditioning step to recover missing points and correct bad measurements. Data security issues should be taken into account in the design of these methods.

References

1. F. Aminifar, M. Fotuhi-Firuzabad, A. Safdarian, A. Davoudi, M. Shahidehpour, Synchrophasor measurement technology in power systems: Panorama and state-of-the-art. IEEE Access **2**, 1607–1628 (2014)
2. R.B. Bobba, K.M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, T.J. Overbye, Detecting false data injection attacks on DC state estimation, in *Proceedings of the First Workshop on Secure Control Systems (SCS)* (2010)
3. A. Bykhovsky, J.H. Chow, Power system disturbance identification from recorded dynamic data at the northfield substation. Int. J. Electr. Power Energy Syst. **25**(10), 787–795 (2003)
4. E.J. Candès, X. Li, Y. Ma, J. Wright, Robust principal component analysis? J. ACM (JACM) **58**(3), 11 (2011)
5. E.J. Candès, B. Recht, Exact matrix completion via convex optimization. Found. Comput. Math. **9**(6), 717–772 (2009)
6. O.P. Dahal, S.M. Brahma, H. Cao, Comprehensive clustering of disturbance events recorded by phasor measurement units. IEEE Trans. Power Del. **29**(3), 1390–1397 (2014)
7. J. De La Ree, V. Centeno, J.S. Thorp, A.G. Phadke, Synchronized phasor measurement applications in power systems. IEEE Trans. Smart Grid **1**(1), 20–27 (2010)
8. R. Diao, K. Sun, V. Vittal, R.J. O'Keefe, M.R. Richardson, N. Bhatt, D. Stradford, S.K. Sarawgi, Decision tree-based online voltage security assessment using PMU measurements. IEEE Trans. Power Syst. **24**(2), 832–839 (2009)

9. P. Gao, M. Wang, J.H. Chow, M. Berger, L.M. Seversky, Matrix completion with columns in union and sums of subspaces, in *2015 Proceedings of the IEEE Global Conference on Signal and Information Processing (GlobalSIP)* (2015), pp. 785–789
10. P. Gao, M. Wang, J.H. Chow, S.G. Ghiocel, B. Fardanesh, G. Stefopoulos, M.P. Razanousky, Identification of successive "unobservable" cyber data attacks in power systems. IEEE Trans. Signal Process. **64**(21), 5557–5570 (2016)
11. P. Gao, M. Wang, S.G. Ghiocel, J.H. Chow, Modeless reconstruction of missing synchrophasor measurements, in *Proceedings of the IEEE PES General Meeting (Selected in Best Papers Sessions)* (2014), pp. 1–5
12. P. Gao, M. Wang, S.G. Ghiocel, J.H. Chow, B. Fardanesh, G. Stefopoulos, Missing data recovery by exploiting low-dimensionality in power system synchrophasor measurements. IEEE Trans. Power Syst. **31**(2), 1006–1013 (2016)
13. P. Gao, R. Wang, M. Wang, J.H. Chow, Low-rank matrix recovery from quantized and erroneous measurements: accuracy-preserved data privatization in power grids, in *Proceedings of the Asilomar Conference on Signals, Systems, and Computers* (2016)
14. E. Ghahremani, I. Kamwa, Dynamic state estimation in power system by applying the extended kalman filter with unknown inputs to phasor measurements. IEEE Trans. Power Syst. **26**(4), 2556–2566 (2011)
15. A.K. Ghosh, D.L. Lubkeman, The classification of power system disturbance waveforms using a neural network approach. IEEE Trans. Power Del. **10**(1), 109–115 (1995)
16. J. Gomez-Vilardebo, D. Gunduz, Smart meter privacy for multiple users in the presence of an alternative energy source. IEEE Trans. Inf. Forensics Secur. **10**(1), 132–141 (2015)
17. A. Hauer, D. Trudnowski, J.G. DeSteese, A perspective on wams analysis tools for tracking of oscillatory dynamics, in *Proceedings of the IEEE Power Engineering Society General Meeting* (2007), pp. 1–10
18. R.A. Horn, C.R. Johnson, *Matrix Analysis* (Cambridge university press, 2012)
19. H. Jiang, J.J. Zhang, D,W. Gao, Fault localization in smart grid using wavelet analysis and unsupervised learning, in *Proceedings of the Asilomar Conference on Signals, Systems and Computers (ASILOMAR)*, 2012, pp. 386–390
20. H. Jiang, J.J. Zhang, W. Gao, Z. Wu, Fault detection, identification, and location in smart grid based on data-driven computational methods. IEEE Trans. Smart Grid **5**(6), 2947–2956 (2014)
21. A. Kaci, I. Kamwa, L.-A. Dessaint, S. Guillon, Synchrophasor data baselining and mining for online monitoring of dynamic security limits. IEEE Trans. Power Syst. **29**(6), 2681–2695 (2014)
22. H. Khurana, R. Bobba, T. Yardley, P. Agarwal, E. Heine, Design principles for power grid cyber-infrastructure authentication protocols, in *Proceedings of the Hawaii International Conference on System Sciences (HICSS)* (2010), pp. 1–10
23. H. Khurana, M. Hadley, N. Lu, D.A. Frincke, Smart-grid security issues. IEEE Secur. Priv. **8**(1), 81–85 (2010)
24. T. Kim, H. Poor, Strategic protection against data injection attacks on power grids. IEEE Trans. Smart Grid **2**(2), 326–333 (2011)
25. O. Kosut, L. Jia, R. Thomas, L. Tong, Malicious data attacks on smart grid state estimation: attack strategies and countermeasures, in *Proceedings of the IEEE International Conference on Smart Grid Communications (SmartGridComm)* (2010), pp. 220–225
26. W. Li, M. Wang, J.H. Chow, Fast event identification through subspace characterization of PMU data in power systems, in *Proceedings of the IEEE Power and Energy Society (PES) General Meeting* (2017), pp. 1-5
27. W. Li, M. Wang, J.H. Chow, Real-time event identification through low-dimensional subspace characterization of high-dimensional synchrophasor data. IEEE Trans. Power Syst. (Early access) (2018)
28. Y.-H. Lin, C.-W. Liu, C.-S. Chen, A new PMU-based fault detection/location technique for transmission lines with consideration of arcing fault discrimination-Part I: Theory and algorithms. IEEE Trans. Power Del. **19**(4), 1587–1593 (2004)

29. G. Liu, J. Quintero, V.M. Venkatasubramanian, Oscillation monitoring system based on wide area synchrophasors in power systems, in *Proceedings of the iREP Symposium-Bulk Power System Dynamics and Control-VII. Revitalizing Operational Reliability* (IEEE, 2007), pp. 1–13
30. L. Liu, M. Esmalifalak, Q. Ding, V.A. Emesih, Z. Han, Detecting false data injection attacks on power grid by sparse optimization. IEEE Trans. Smart Grid **5**(2), 612–621 (2014)
31. Y. Liu, P. Ning, M.K. Reiter, False data injection attacks against state estimation in electric power grids, in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, 2009, pp. 21–32
32. J. Ma, Y. Makarov, C. Miller, T. Nguyen, Use multi-dimensional ellipsoid to monitor dynamic behavior of power systems based on PMU measurement, in *Proceedings of the IEEE Power and Energy Society General Meeting* (2008), pp. 1–8
33. P. McDaniel, S. McLaughlin, Security and privacy challenges in the smart grid. IEEE Secur. Priv. **7**(3), 75–77 (2009)
34. Y. Mo, T.H.-J. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, B. Sinopoli, Cyber-physical security of a smart grid infrastructure. Proc. IEEE **100**(1), 195–209 (2012)
35. North America Synchrophasor Initiative(NASPI), https://www.naspi.org/Badger/content/File/FileService.aspx?fileid=49CC0BEB3E3C36F3BF9C7930E0FFFD1B
36. A. Peterson, Hackers caused a blackout for the first time, researchers say, https://www.washingtonpost.com/news/the-switch/wp/2016/01/05/hackers-caused-a-blackout-for-the-first-time-researchers-say/
37. A. Phadke, J. Thorp, *Synchronized Phasor Measurements and Their Applications* (Springer, 2008)
38. A. Reinhardt, F. Englert, D. Christin, Enhancing user privacy by preprocessing distributed smart meter data, in *Proceedings of the Sustainable Internet and ICT for Sustainability (SustainIT)* (2013), pp. 1–7
39. H. Sandberg, A. Teixeira, K.H. Johansson, On security indices for state estimators in power networks, in *Proceedings of the the First Workshop on Secure Control Systems (SCS)* (2010)
40. H. Sedghi, E. Jonckheere, Statistical structure learning of smart grid for detection of false data injection, in *Proceedings of the IEEE Power and Energy Society General Meeting (PES)* (2013), pp. 1–5
41. A. Silverstein, J.E. Dagle, Successes and challenges for synchrophasor technology: an update from the north american synchrophasor initiative, in *Proceedings of the Hawaii International Conference on System Science (HICSS)* (2012), pp. 2091–2095
42. J.E. Tate, T.J. Overbye, Line outage detection using phasor angle measurements. IEEE Trans. Power Syst. **23**(4), 1644–1652 (2008)
43. G. Valverde, V. Terzija, Unscented Kalman filter for power system dynamic state estimation. IET Gener. Trans. Distrib. **5**(1), 29–37 (2011)
44. M. Wang, J.H. Chow, P. Gao, X. T. Jiang, Y. Xia, S.G. Ghiocel, B. Fardanesh, G. Stefopolous, Y. Kokai, N. Saito, A low-rank matrix approach for the analysis of large amounts of power system synchrophasor data, in *Proceedings of the IEEE Hawaii International Conference on System Sciences (HICSS)* (2015), pp. 2637–2644
45. M. Wang, G. de Mijolla, P. Gao, J. H. Chow, B. Fardanesh, G. Stefopoulos, S. Babaei, A. Ettlinger, D. Iles, D. Tran, Missing data recovery by exploiting low-dimensionality in synchrophasor measurements, in *North American Synchrophasor Initiative meetings*, March 2016
46. S. Wang, L. Cui, J. Que, D.-H. Choi, X. Jiang, S. Cheng, L. Xie, A randomized response model for privacy preserving smart metering. IEEE Trans. Smart Grid **3**(3), 1317–1324 (2012)
47. W. Wang, L. He, P. Markham, H. Qi, Y. Liu, Q.C. Cao, L.M. Tolbert, Multiple event detection and recognition through sparse unmixing for high-resolution situational awareness in power grid. IEEE Trans. Smart Grid **5**(4), 1654–1664 (2014)
48. M. Wu, L. Xie, Online detection of low-quality synchrophasor measurements: a data-driven approach. IEEE Trans. Power Syst. **32**(4), 2817–2827 (2017)
49. L. Xie, Y. Mo, B. Sinopoli, Integrity data attacks in power market operations. IEEE Trans. Smart Grid **2**(4), 659–666 (2011)

50. M. Zhou, V.A. Centeno, J.S. Thorp, A.G. Phadke, An alternative for including phasor measurements in state estimators. IEEE Trans. Power Syst. **21**(4), 1930–1937 (2006)
51. H. Zhu, G.B. Giannakis, Sparse overcomplete representations for efficient identification of power line outages. IEEE Trans. Power Syst. **27**(4), 2215–2224 (2012)