Proceedings Paper:
Wen, F. and Liu, W. (2018) An efficient data-driven false data injection attack in smart grids. In: 2018 IEEE 23rd International Conference on Digital Signal Processing (DSP). IEEE 23rd International Conference on Digital Signal Processing (DSP), 19-21 Nov 2018, Shanghai, China. IEEE. ISBN: 978-1-5386-6812-2. ISSN: 1546-1874. EISSN: 2165-3577.

https://doi.org/10.1109/icdsp.2018.8631857

An Efficient Data-Driven False Data Injection Attack in Smart Grids

Fuxi Wen
Department of Electrical Engineering
Chalmers University of Technology
Göteborg, Sweden
Email: fuxi@chalmers.se

Wei Liu
Department of Electronic & Electrical Engineering
University of Sheffield
Sheffield, United Kingdom
Email: w.liu@sheffield.ac.uk

***Abstract*—Data-driven false data injection attack is one of the emerging techniques in smart grids, provided that the adversary can monitor the meter readings. The basic idea is constructing attack vectors from the estimated signal subspace, without knowing system measurement matrix. However, its stealthy performance is significantly influenced by the accuracy of the estimated subspace. Furthermore, it is computationally demanding, because full-size singular value decomposition (SVD) is required for model order selection. In this paper, we propose a truncated SVD based computationally efficient attacking scheme using only the first dominant eigenvector. Both experiment and simulation results are provided to evaluate the performance of the proposed scheme. Compared with the standard false data injection techniques with known measurement matrix, similar stealthy performance is achieved with a reasonable computational complexity.**

***Index Terms*—Data-driven false data injection attack, smart grid, subspace method, bad data detector**

I. Introduction

Information and communication systems are widely used in power grids. However, they have convenient entry points for malicious attackers and are vulnerable to cyber-attacks. Although it is possible to compromise the control center directly, in practice, existing security measures make it unlikely [1], and it is more realistic to assume that the attackers have access to the field devices, and the associated supervisory control and data acquisition (SCADA) communication channels, because they are geographically scattered over a large area, and lack adequate protection features. Here we focus on the false data injection (FDI) attacks against direct current (DC) linear state estimation in power grids [2]–[4]. In general, attacks on the measurements can be detected by bad data detector (BDD). But a well designed FDI attack vector that lies in the subspace spanned by measurement matrix can remain stealthy to the BDD [5]. The basic idea is to learn the measurement matrix or estimate its subspace structure from the meter readings. Using such vulnerabilities, crafting stealthy data-driven FDI attacks from the measurement data are shown in [6] and [7].

Principal component analysis (PCA) and independent component analysis (ICA) [7]–[9] are two widely used projection methods for subspace based data-driven stealthy attacks. Recently, low rank matrix recovery techniques [10], [11] are consolidated to launch such an attack from incomplete measurements [12], [13]. Another interesting extension is considering alternating current nonlinear state estimation [14]–[16]. Here we focus on PCA based data-driven FDI attacks against DC linear state estimation. The basic idea of PCA is to find a set of principal components such that the projected measurements retain most information about original measurements. However, one limitation of the existing PCA based data-driven FDI attacks is determining the pseudorank [7], [17], which is defined as the rank of the noiseless data matrix and depends on the number of measurements and the correlation of the system states [18]. Full-size singular value decomposition (SVD) is required to estimate pseudorank. Therefore, the computational complexity is high, especially for large scale systems. Furthermore, for the existing data-driven techniques, performance degradation occurs if the nominated and actual pseudorank are mismatched. Besides the pseudorank, the error of the estimated eigenvectors are also critical, which are inversely proportional to the eigenvalues [19]. In general, larger errors will cause larger residuals, and therefore increase the probability of being detected by BDD.

To overcome these drawbacks, we propose a computationally efficient implementation scheme for data-driven FDI attack , where only the first principal component is utilized to construct the attack, and pseudorank estimation and full-size SVD are not required, which leads to significant reduction in computational complexity. Furthermore, compared with the standard FDI attack, which assumes that the measurement matrix is known, similar stealthy performance is achieved for the proposed data-driven scheme. Even though the proposed technique is introduced for power grids, the key idea can be applied to other linear cyber-physical systems.

The remainder of this paper is organized as follows. In Section II, some preliminaries are provided. In Section III, we present the proposed stealthy data-driven FDI scheme. Experiment and numerical results are provided to demonstrate the effectiveness of the proposed algorithm in Section IV. Finally, conclusions are drawn in Section V.

Notation: Transpose and inverse operators are denoted as $(\cdot)^T$ and $[\cdot]^{-1}$, respectively. We use $\mathbf{I}_m$ to represent the identity matrix of size m. Moreover, the blackboard bold letter $\mathbb{R}$ denotes the set of real numbers, $\text{rank}(\cdot)$ and $\text{col}(\cdot)$ denote the rank and column space of a matrix. $\mathcal{R}(\mathbf{A})$ is the space spanned by $\mathbf{A}$. The ℓ_2-norm is denoted as $\|\cdot\|_2$.

II. Preliminaries

The set of nodes in power grids is denoted by $\mathcal{N} = \{1, 2, \ldots, n\}$. The voltage phase angle at node i during time slot t is denoted by $x_i[t],\ i \in \mathcal{N}$, which corresponds to the system state at time t for a DC power flow model. The system state is monitored using sensors deployed at the nodes as well as the transmission lines, which measure the power injections and the forward and reverse power flows, respectively. These measurements are collected at the fusion center. Under the DC power flow model, the measurements at the t-th sampling instance $\boldsymbol{z}[t] \in \mathbb{R}^m$ are related to the system state $\boldsymbol{x}[t] \in \mathbb{R}^n$ in a linear fashion [20], given by

$$\boldsymbol{z}[t] = \mathbf{H}\boldsymbol{x}[t] + \boldsymbol{e}[t], \quad t = 1, 2, \cdots, k. \tag{1}$$

where $\mathbf{H} = \begin{bmatrix}\mathbf{h}_1 & \mathbf{h}_2 & \cdots & \mathbf{h}_n\end{bmatrix} \in \mathbb{R}^{m\times n}$ is the system measurement matrix and $\boldsymbol{e}[t]$ is the sensor measurement noise, which is assumed to be white Gaussian and independent of the system state $\boldsymbol{x}[t]$. At each time slot t, one convenient way to estimate the system state $\hat{\boldsymbol{x}}[t]$ from measurement vector $\boldsymbol{z}[t]$ is using the least squares estimation method, and the closed-form solution is given by

$$\hat{\boldsymbol{x}}[t] = \left(\mathbf{H}^T\mathbf{H}\right)^{-1}\mathbf{H}^T\boldsymbol{z}[t]. \tag{2}$$

After state estimation, BDD checks for possible measurement inconsistencies by comparing the residual

$$r[t] = \left\|\boldsymbol{z}[t] - \mathbf{H}\hat{\boldsymbol{x}}[t]\right\|_2, \tag{3}$$

against a pre-defined threshold τ, and an alarm is raised if $r[t] \geq \tau$. Threshold τ is selected to maintain a certain false-positive rate. We consider a strong attacker model who has read and write access to the sensor measurements. The objective of the attacker is to construct FDI attack vectors that can bypass BDD. Note that designing a stealthy attack is equivalent to finding a nonzero vector in col($\mathbf{H}$) [7]. Therefore, it can be constructed from the basis of $\mathcal{R}(\mathbf{H})$ without knowing system measurement matrix. The basis is obtained by applying SVD on the estimated sample covariance matrix.

A. Existing Data-Driven FDI Scheme

The data-driven approach proposed in [7] is based on the subspace of the covariance matrix of $\boldsymbol{z}[t]$. Because the noise is additive white Gaussian, the covariance matrix of $\boldsymbol{z}[t]$ can be described as

$$\boldsymbol{\Sigma}_z = \mathbf{H}\boldsymbol{\Sigma}_x\mathbf{H}^T + \sigma^2\mathbf{I}_m = \boldsymbol{\Phi} + \sigma^2\mathbf{I}_m, \tag{4}$$

where $\boldsymbol{\Sigma}_x$ denotes the sample covariance matrix of the states and noise power σ^2 is unknown. Assuming that the system measurement matrix $\mathbf{H}$ is of full column rank and states covariance matrix $\boldsymbol{\Sigma}_x$ is non-singular, the pseudorank of $\boldsymbol{\Phi}$ is n.

Applying SVD to $\boldsymbol{\Sigma}_z$, we have

$$\boldsymbol{\Sigma}_z = \mathbf{U}\boldsymbol{\Lambda}\mathbf{V}^T, \tag{5}$$

where $\boldsymbol{\Lambda} = \text{diag}\left\{\lambda_1 \quad \lambda_2 \quad \cdots \quad \lambda_m\right\}$ is a diagonal matrix, with its entries being the eigenvalues of $\boldsymbol{\Sigma}_z$ in descending order, and

$$\mathbf{U} = \begin{bmatrix}\boldsymbol{u}_1 & \boldsymbol{u}_2 & \cdots & \boldsymbol{u}_m\end{bmatrix}, \tag{6}$$

are the corresponding eigenvectors.

Since $\lambda_{n+1} = \lambda_{n+2} = \cdots = \lambda_m = \sigma^2$, the first n largest eigenvalues $\lambda_1, \lambda_2, \cdots, \lambda_n$ are referred to as the dominant eigenvalues. After obtaining all the eigenvalues, the information theoretic criteria (ITC) can be used for pesudorank estimation, which is one of the widely used techniques [17]. Let $\mathbf{U}_s = \begin{bmatrix}\boldsymbol{u}_1 & \boldsymbol{u}_2 & \cdots & \boldsymbol{u}_n\end{bmatrix}$ contain the first n columns of $\mathbf{U}$; then

$$\mathbf{H}\boldsymbol{\Sigma}_x\mathbf{H}^T = \mathbf{U}_s\boldsymbol{\Lambda}_s\mathbf{U}_s^T \tag{7}$$

where

$$\boldsymbol{\Lambda}_s = \text{diag}\left\{\lambda_1 - \sigma^2 \quad \lambda_2 - \sigma^2 \quad \cdots \quad \lambda_n - \sigma^2\right\}. \tag{8}$$

Since $\mathbf{H}$ and $\mathbf{U}_s$ have independent columns, and meanwhile $\boldsymbol{\Sigma}_x$ and $\boldsymbol{\Lambda}_s$ are nonsingular, $\mathbf{U}_s$ forms a basis of $\mathcal{R}(\mathbf{H})$ as well as $\mathcal{R}(\mathbf{H}\boldsymbol{\Sigma}_x\mathbf{H}^T)$. The relationship between $\mathbf{U}_s$ and $\mathbf{H}$ is given by

$$\mathbf{U}_s = \mathbf{H}\mathbf{Q}, \tag{9}$$

where $\mathbf{Q} = \begin{bmatrix}\boldsymbol{q}_1 & \boldsymbol{q}_2 & \cdots & \boldsymbol{q}_n\end{bmatrix} \in \mathbb{R}^{n\times n}$ is a invertible matrix and $\boldsymbol{u}_1 = \mathbf{H}\boldsymbol{q}_1$. This is the theoretical foundations for data-driven FDI techniques. Generate a non-zero vector $\mathbf{c}[t] \in \mathbb{R}^{n\times 1}$, either random or deterministic. Then, the attack vector $\mathbf{a}[t]$ is constructed by [7],

$$\mathbf{a}[t] = \mathbf{U}_s\mathbf{c}[t]. \tag{10}$$

III. The Proposed Data-Driven FDI Scheme

Comparing with the existing data-driven scheme, the proposed scheme have two main advantages.

1) First of all, the error of the estimated eigenvectors $\mathbf{U}_s$ are inversely proportional to the eigenvalues [19]. Since a larger error will cause larger residuals and increase the probability to be detected by BDD, for the proposed data-driven FDI scheme, only the first dominant eigenvector is used to construct the attack vector.
2) An additional advantage is that pseudorank estimation is not required in the proposed scheme. Instead of full-size SVD, a reduced version of the SVD is sufficient, such as the thin, compact and truncated SVDs. They are faster and have a lower storage requirement.

For the proposed data-driven FDI scheme, the attack vector or false data is constructed as

$$\mathbf{a}[t] = c[t]\mathbf{u}_1, \tag{11}$$

where $c[t]$ is either a deterministic or random number, and $\mathbf{u}_1$ denotes the first column of the estimated signal subspace $\mathbf{U}_s$.

Compromised measurement $\mathbf{z}_a[t]$ is obtained by injecting $\mathbf{a}[t]$ into the original measurements [5],

$$\mathbf{z}_a[t] = \mathbf{H}\mathbf{x}[t] + \mathbf{e}[t] + \mathbf{a}[t]. \tag{12}$$

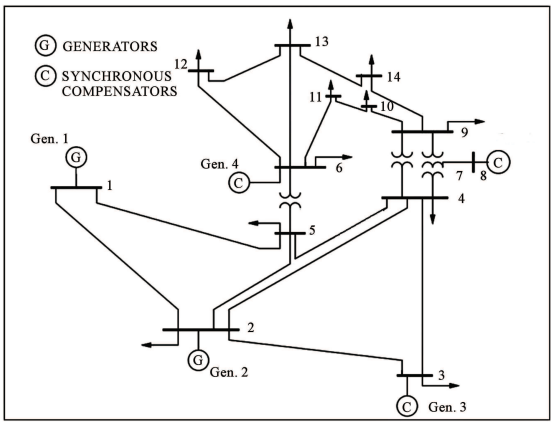

Fig. 1. A circuit diagram of the IEEE 14-bus test system [21].

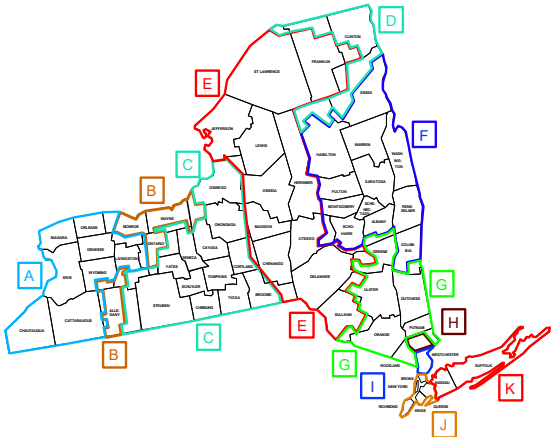

Fig. 2. Region index of NYISO

After state estimation, we have

$$\boldsymbol{z}_a[t] - \mathbf{H}\hat{\boldsymbol{x}}[t] = \boldsymbol{\Pi}^{\perp}\big(\mathbf{e}[t] + \mathbf{a}[t]\big). \tag{13}$$

where

$$\boldsymbol{\Pi}^{\perp} = \mathbf{I} - \mathbf{H}\left(\mathbf{H}^T\mathbf{H}\right)^{-1}\mathbf{H}^T. \tag{14}$$

Let $r_a[t]$ be the residual contributed by $\mathbf{a}[t]$, which is given by

$$r_a[t] = \left\|\boldsymbol{\Pi}^{\perp}\mathbf{a}[t]\right\|_2 = \left\|c[t]\boldsymbol{\Pi}^{\perp}\mathbf{u}_1\right\|_2, \tag{15}$$

and substituting $\mathbf{u}_1 = \mathbf{H}\mathbf{q}_1$ into (15), where $\mathbf{q}_1$ is a non-zero column vector, we have

$$r_a[t] = \left\|c[t]\boldsymbol{\Pi}^{\perp}\mathbf{H}\mathbf{q}_1\right\|_2. \tag{16}$$

Since

$$\boldsymbol{\Pi}^{\perp}\mathbf{H} = 0 \text{ and } r_a[t] = \mathbf{0}, \tag{17}$$

the proposed data-driven FDI scheme using the first dominant eigenvector is stealthy and can bypass BDD.

IV. Case Studies

A. Experiment Results

As shown in Fig. 1, the IEEE 14-bus system with 11 load buses is chosen as the test system. The software toolbox MATPOWER [21] is utilized to generate the measurements. Real power load data on January 02, 2016 from New York Independent System Operator (NYISO) is fed into the IEEE 14-bus system. Sampling interval is 5 minutes. NYISO consists of 11 regions and is marked from A to K in Fig. 2. The following procedures are utilized to estimate system states using load patterns from NYISO:

- Link the buses of the IEEE 14-bus system to regions of NYISO as follows:

$$\begin{bmatrix} 2 & 3 & 4 & 5 & 6 & 9 & 10 & 11 & 12 & 13 & 14 \\ F & C & I & B & G & K & E & H & J & D & A \end{bmatrix},$$

  where the row is the bus number of the IEEE 14-bus system and the second row represents the NYISO region index in Fig. 2.
- Normalize the load data collected from NYISO accordingly, the DC power flow model is considered [5]. For each set of the power loads, optimal power flow (OPF) is used to extract the system states.
- White Gaussian noise with amplitude 0.1 is added to the raw measurements. All the results are obtained over 5000 independent trials.

Fig. 3 shows the BDD bypassing probability versus observation time for different probability of false alarm p_{FA} ratios. Noise amplitude is 0.1 and $\|\mathbf{a}\|_2 = 100$. As shown in Fig. 3, a similar performance is achieved for the proposed data-driven FDI scheme without knowing the measurement matrix as compared to benchmark [5]. However, performance deterioration occurs for the proposed approach if only a few measurements are available, since the estimated signal subspace is erroneous with a limited number of measurements, which generates a larger residual and increases the probability of being detected by BDD.

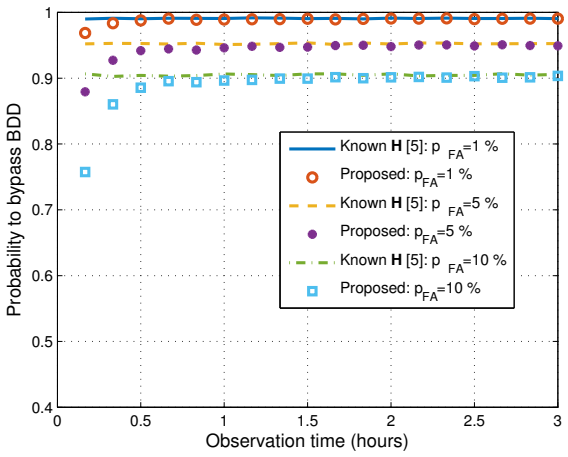

Fig. 3. Probability to bypass BDD versus observation time for different probability of false alarm ratios. Sampling interval is 5 minutes.

B. Simulation Results

First, we consider the effects of the number of columns used to construct FDI attacks. The proposed approach is compared

with benchmark [5], which assumes that the measurement matrix $\mathbf{H}$ is known. The noise amplitude is 1, $\|\mathbf{a}\|_2 = 200$ and $p_{FA} = 0.01$. As shown in Fig. 4, using more columns will reduce the probability to bypass BDD. The results are consistent with the observations in [19], which shows that the error of the estimated eigenvectors are inversely proportional to the eigenvalues. A larger error will cause larger residuals. Therefore, for a given number of measurements, using more eigenvectors will increase the probability of being detected by BDD. It is better to using a smaller number of columns to obtain a higher BDD bypassing probability, especially when the number of measurements or observation time is limited. This is one of the motivations of using only the first dominant eigenvector to construct FDI attacks.

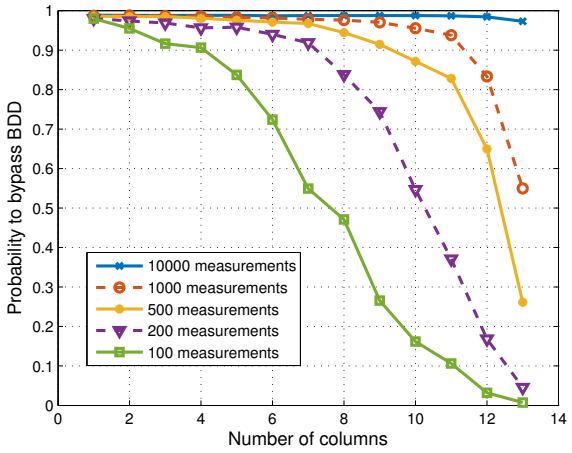

Fig. 4. Probability to bypass BDD versus number of columns used to construct FDI attacks.

In the second test, the proposed scheme is compared with the data-driven scheme in [7] and benchmark [5], which assumes that the measurement matrix is known. The noise amplitude is 1, attacking strength $\|\mathbf{a}\|_2 = 100$, and probability of false alarm $p_{FA} = 0.01$. As shown in Fig. 5, the proposed scheme outperforms [7] and is close to the benchmark, even with a limited number of measurements. On the other hand, for [7], a large number of measurements are required to achieve a reasonable BDD bypassing probability. Furthermore, even more measurements are required if the measurements are highly correlated, which is common in real applications.

In the last test, we evaluate the effects of attacking strength $\|\mathbf{a}\|_2$. Noise amplitude is 1 and $p_{FA} = 0.01$. As shown in Fig. 6, accuracy of the estimated signal subspace is critical for the data-driven techniques. The allowed attacking strength is affected by the accuracy of the estimated signal subspace. This is a limitation of the data-driven schemes, when compared with benchmark [5].

V. Conclusion

The emerging data-driven FDI attack in power grids has been studied. A truncated SVD based computationally efficient data-driven FDI attacking scheme was proposed using only the first dominant eigenvector of the measurement covariance matrix. As a result, the pseudorank or model order information is not required. Furthermore, trade-offs between the attacking strength and accuracy of the estimated signal subspace were investigated. Although the work has been presented from an attacker's points of view, the insight provided by the proposed scheme is also helpful for system operators. Furthermore, the key idea of the proposed scheme can be applied to other cyber-physical systems with a similar linear model.

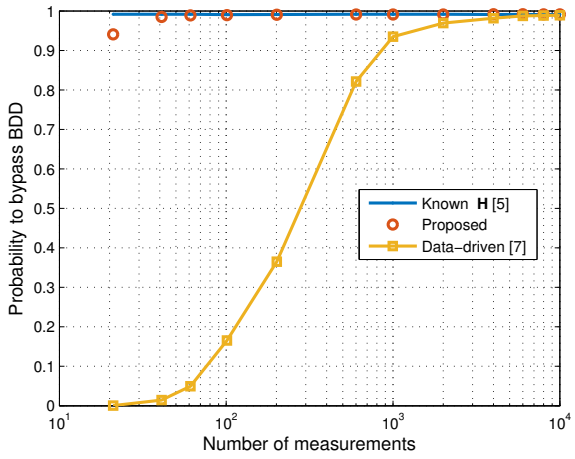

Fig. 5. Probability to bypass BDD versus number of measurements.

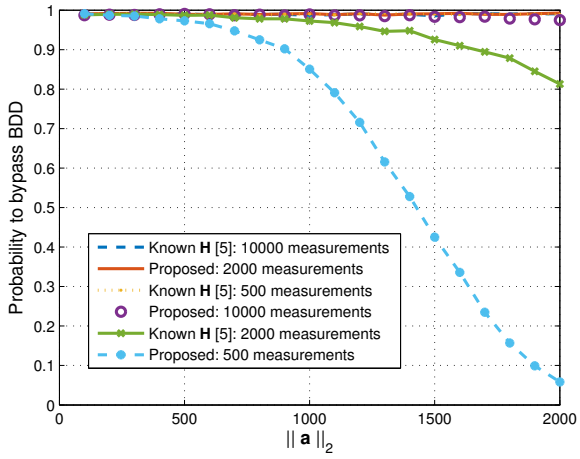

Fig. 6. Probability to bypass BDD versus attacking strength.

Acknowledgment

This work is partially supported by Science and Technology Innovation Project of Shaanxi Province (Grant No. 2016KTZDGY04-01), Natural Science Foundation of Education Department of Shaanxi Province, China (No.17JK0711) and Research Program of Xi'an Science and Technology Bureau No.2017084CG/RC047 (XAYD001).

REFERENCES

[1] C.-W. Ten, M. Govindarasu, and C.-C. Liu, "Cybersecurity for electric power control and automation systems," in *IEEE International Conference on Systems, Man and Cybernetics*, 2007.

[2] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos, "False data injection on state estimation in power systemsxattacks, impacts, and defense: A survey," *IEEE Transactions on Industrial Informatics*, vol. 13, no. 2, pp. 411–423, 2017.

[3] H. He and J. Yan, "Cyber-physical attacks and defences in the smart grid: a survey," *IET Cyber-Physical Systems: Theory & Applications*, vol. 1, no. 1, pp. 13–27, 2016.

[4] G. Liang, J. Zhao, F. Luo, S. Weller, and Z. Y. Dong, "A review of false data injection attacks against modern power systems," *IEEE Transactions on Smart Grid*, 2017.

[5] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security*, vol. 14, no. 1, pp. 1–33, May 2011.

[6] X. Li, H. V. Poor, and A. Scaglione, "Blind topology identification for power systems," in *IEEE International Conference on Smart Grid Communications*. IEEE, Oct. 2013.

[7] J. Kim, L. Tong, and R. J. Thomas, "Subspace methods for data attack on state estimation: A data driven approach," *IEEE Transactions on Signal Processing*, vol. 63, no. 5, pp. 1102–1114, Mar. 2015.

[8] Y. Huang, M. Esmalifalak, H. Nguyen, R. Zheng, Z. Han, H. Li, and L. Song, "Bad data injection in smart grid: attack and defense mechanisms," *IEEE Communications Magazine*, vol. 51, no. 1, pp. 27–33, 2013.

[9] Z.-H. Yu and W.-L. Chin, "Blind false data injection attack using PCA approximation method in smart grid," *IEEE Transactions on Smart Grid*, vol. 6, no. 3, pp. 1219–1226, May 2015.

[10] E. J. Candès, X. Li, Y. Ma, and J. Wright, "Robust principal component analysis?" *Journal of the ACM (JACM)*, vol. 58, no. 3, p. 11, 2011.

[11] M. A. Davenport and J. Romberg, "An overview of low-rank matrix recovery from incomplete observations," *IEEE Journal of Selected Topics in Signal Processing*, vol. 10, no. 4, pp. 608–622, 2016.

[12] A. Anwar, A. N. Mahmood, and M. Pickering, "Data-driven stealthy injection attacks on smart grid with incomplete measurements," in *Intelligence and Security Informatics*. Springer, 2016, pp. 180–192.

[13] ——, "Modeling and performance evaluation of stealthy false data injection attacks on smart grid in the presence of corrupted measurements," *Journal of Computer and System Sciences*, May 2016.

[14] C. Konstantinou and M. Maniatakos, "A case study on implementing false data injection attacks against nonlinear state estimation," in *Proceedings of the 2nd ACM Workshop on Cyber-Physical Systems Security and Privacy*. ACM, 2016, pp. 81–92.

[15] G. Chaojun, P. Jirutitijaroen, and M. Motani, "Detecting false data injection attacks in ac state estimation," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2476–2483, 2015.

[16] W.-L. Chin, C.-H. Lee, and T. Jiang, "Blind false data attacks against ac state estimation based on geometric approach in smart grid communications," *IEEE Transactions on Smart Grid*, 2017.

[17] P. Stoica and Y. Selen, "Model-order selection: a review of information criterion rules," *IEEE Signal Processing Magazine*, vol. 21, no. 4, pp. 36–47, Jul. 2004.

[18] S. Kritchman and B. Nadler, "Determining the number of components in a factor model from limited noisy data," *Chemometrics and Intelligent Laboratory Systems*, vol. 94, no. 1, pp. 19–32, 2008.

[19] Z. Xu, "Perturbation analysis for subspace decomposition with applications in subspace-based algorithms," *IEEE Transactions on Signal Processing*, vol. 50, no. 11, pp. 2820–2830, 2002.

[20] A. Abur and A. G. Exposito, *Power system state estimation: theory and implementation*. CRC press, 2004.

[21] R. D. Zimmerman, C. E. Murillo-Sanchez, and R. J. Thomas, "Matpower: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 12–19, Feb. 2011.