CHALMERS
UNIVERSITY OF TECHNOLOGY

Trade-offs in Data-Driven False Data Injection Attacks Against the Power Grid

Citation for the original published paper (version of record):
Lakshminarayana, S., Wen, F., Yau, D. (2018). Trade-offs in Data-Driven False Data Injection Attacks Against the Power Grid. ICASSP, IEEE International Conference on Acoustics, Speech and Signal Processing - Proceedings, 2018-April: 2022-2026.
http://dx.doi.org/10.1109/ICASSP.2018.8461493

(article starts on next page)

Trade-offs in Data-Driven False Data Injection Attacks Against the Power Grid

Subhash Lakshminarayana* ‡, Fuxi Wen† ‡ and David K.Y. Yau *§

* Advanced Digital Sciences Center, Illinois at Singapore, Singapore 138682
† Department of Electrical Engineering, Chalmers University of Technology, Sweden 412 96
§ Singapore University of Technology and Design, Singapore 487372
Email: *subhash.l@adsc.com.sg, † fuxi@chalmers.se, ‡ david_yau@sutd.edu.sg

***Abstract*—We address the problem of constructing false data injection (FDI) attacks that can bypass the bad data detector (BDD) of a power grid. The attacker is assumed to have access to only power flow measurement data traces (collected over a limited period of time) and no other prior knowledge about the grid. Existing related algorithms are formulated under the assumption that the attacker has access to measurements collected over a long (asymptotically infinite) time period, which may not be realistic. We show that these approaches do not perform well when the attacker has a limited number of data samples only. We design an enhanced algorithm to construct FDI attack vectors in the face of limited measurements that can nevertheless bypass the BDD with high probability. Furthermore, we characterize an important trade-off between the attack's BDD-bypass probability and its sparsity, which affects the spatial extent of the attack that must be achieved. Extensive simulations using data traces collected from the MATPOWER simulator and benchmark IEEE bus systems validate our findings.**

***Index Terms*—Data-driven FDI attack, bad data detection, BDD-bypass probability, sparsity of attack vector.**

I. Introduction

Information and communication technologies (ICTs) play a key role in reducing costs and improving the quality of service in critical infrastructures such as the power grid. However, they also make the infrastructures vulnerable to cyber attacks, which may cause widespread damage as witnessed in a recent attack against the Ukraine power grid [1]. Hence, it is critical to assess the vulnerabilities of ICT-enabled critical infrastructures and devise ways to protect them.

In this work, we study the problem of constructing false data injection (FDI) attacks against state estimation (SE) in a power grid from an attacker's perspective. It has been shown [2] that if the attacker obtains detailed knowledge of the power grid topology and transmission line reactance values – i.e., the system's *measurement matrix* – then he can construct FDI attacks that bypass the grid's bad data detector (BDD). Subsequent research [4], [5] has shown that an attacker can learn the power grid's measurement matrix [4], or learn the structure of its column space by estimating the basis vectors [5] from accessed measurement data (i.e., nodal power injections and line power flows) only. The focus of our work is on constructing these *data-driven* FDI attacks.

Prior work on designing data-driven BDD-bypass attacks [4], [5] has only studied the setting of a long measurement period encompassing (asymptotically infinitely) many samples. However, for practical purposes, it is important to understand these attacks under a limited measurement time window. The reasons include (i) active topology control [6] or renewable energy integration [7] that leads to an inherently dynamic operating environment, thereby rendering measurements outdated and irrelevant after some time; and (ii) an attacker's desire or need (e.g., due to limited resources or limited exploitation time windows) to launch the attack quickly. Our experiments show that FDI attacks constructed by the existing algorithms [4], [5] do not perform well (in terms of the BDD-bypass probability) when applied in a limited measurement period setting.

In this paper, we analyze the problem of finding BDD-bypassing attack based on data obtained in a limited time window and identify guiding principles for the solution in this context. We make two important contributions. *First*, we propose an enhanced algorithm to construct FDI attacks in the face of limited measurements that can nevertheless bypass the BDD with high probability. The algorithm is designed based on the following key observation. With limited data samples, it is important to recognize that some of the basis vectors spanning the column space of the measurement matrix can be estimated more accurately than the others, and accordingly focus on the critical (i.e., well estimated) basis vectors in crafting the attack. Specifically, the attack has a high probability of bypassing the BDD if it is restricted to a lower-dimensional subspace that is spanned by the critical basis vectors only. Otherwise, the inaccurately estimated basis vectors may mislead the attack vector to a subspace that is different from the intended one, thereby risking detection by the BDD.

Second, we characterize an important trade-off between the FDI attack's BDD-bypass probability and the number of power meters in the grid that the attacker has to compromise in achieving the attack. Naturally, a resource-constrained attacker may wish to minimize the number of the meters that must be compromised, or equivalently find a sparsest attack vector in

‡ These authors have contributed equally to this work.

This work was supported by the National Research Foundation (NRF), Prime Minister's Office, Singapore, under its National Cybersecurity R&D Programme (Award No. NRF2014NCR-NCR001-31) and administered by the National Cybersecurity R&D Directorate.

the execution [8], [9]. Clearly, maximizing the sparsity of the attack vector is best achieved if we have an unconstrained choice of this vector over the full estimated column space of the measurement matrix. Hence, the attacker faces a fundamental tradeoff. On the one hand, as we observed, restricting the attack vector to a lower-dimensional subspace (spanned by the accurately estimated basis vectors) will enhance the BDD-bypass probability under limited measurements; i.e., the restriction makes the attack efficient temporally. On the other hand, this restriction may reduce the sparsity of the optimized attack vector, thus making it less efficient spatially. To understand the tradeoffs between the conflcting objectives, we compute the sparsest attack vector while constraining it to subspaces of varying lower dimensions of the full estimated column space.

We illustrate the fundamental trade-off by performing extensive simulations using benchmark IEEE bus systems.The results show that the attacker can significantly enhance the BDD-bypass probability using our proposed approach. Moreover, there exists an attacker-friendly operating regime in which the sparsity of the attack vector can be significantly increased by tolerating a small reduction in the BDD-bypass probability. Our results provide important understanding about the design of FDI attacks by a temporal and/or spatial resource-limited attacker against power systems.

II. System Model

We consider a power grid that is characterized by a set of buses $\mathcal{N} = \{1, 2, \ldots, N\}$ and transmission lines $\mathcal{L} = \{1, 2, \ldots, L\}$. The grid is assumed to operate in a time slotted manner indexed by $t = 1, 2, \ldots, T$. To model power flows within the grid, we adopt the direct current (dc) power flow model [10]. Under this model, the system state corresponds to the nodal voltage phase angles, which we denote by $\boldsymbol{\theta}[t] = [\theta_1[t], \ldots, \theta_N[t]]^T$; i.e., $\theta_i[t],\ i \in \mathcal{N}$ is the voltage phase angle at bus i during the time slot t. We assume that $\boldsymbol{\theta}[t]$ is a random vector whose covariance matrix is given by $\boldsymbol{\Sigma}_\theta$.[1] We denote the reactance of transmission line l by x_l. We let $\mathbf{D} \in \mathbb{R}^{L\times L}$ denote a diagonal matrix with its diagonal entries given by $\frac{1}{x_l}, l = 1, \ldots, L$. Furthermore, we denote the bus-branch incidence matrix by $\mathbf{A} \in \mathbb{R}^{N\times L}$, which specifies the connectivity between different buses in the grid [10]. We assume that within the considered time interval T, the power grid topology and the line reactances are unchanged.

State Estimation & Bad Data Detection: The system state $\boldsymbol{\theta}[t]$ is monitored using sensors deployed at the buses and transmission lines. These sensors measure respectively the nodal power injections and the forward/reverse line power flows. Under the dc power flow model, these measurements, which we denote by $\boldsymbol{z}[t] \in \mathbb{R}^M$ (where M denotes the number of measurements), are related to the system state $\boldsymbol{\theta}[t] \in \mathbb{R}^N$ as

$$\boldsymbol{z}[t] = \mathbf{H}\boldsymbol{\theta}[t] + \mathbf{n}[t], \quad t = 1, 2, \cdots, T, \tag{1}$$

[1]In Section V, we perform simulations to show the application of the proposed algorithm to system states that are derived from real-world load data traces.

where $\mathbf{H} \in \mathbb{R}^{M\times N}$ is the measurement matrix and $\mathbf{n}[t]$ is the sensor measurement noise. The noise is assumed to be zero-mean Gaussian with covariance matrix $\sigma^2\mathbf{I}_M$ (where $\mathbf{I}_M$ denotes an identity matrix of size $M \times M$), and independent of the system state $\boldsymbol{\theta}[t]$. It is also assumed to be i.i.d. across the time slots. The measurement matrix $\mathbf{H}$ is given by $\mathbf{H} = [\mathbf{D}\mathbf{A}^T; -\mathbf{D}\mathbf{A}^T; \mathbf{A}\mathbf{D}\mathbf{A}^T]$ ($[\mathbf{A}; \mathbf{B}]$ denotes the row concatenation of matrices $\mathbf{A}$ and $\mathbf{B}$). The estimate of the system state, denoted by $\widehat{\boldsymbol{\theta}}[t]$, is recovered from the measurement vector $\boldsymbol{z}[t]$ using a maximum-likelihood (ML) technique [11]: $\widehat{\boldsymbol{\theta}}[t] = \left(\mathbf{H}^T\mathbf{W}\mathbf{H}\right)^{-1}\mathbf{H}^T\mathbf{W}\boldsymbol{z}[t]$, where $\mathbf{W}$ is a diagonal weighting matrix whose elements are reciprocals of the variances of the sensor measurement noise.

The BDD check for possible measurement inconsistencies in $\mathbf{z}[t]$ works by comparing the residual, defined as $r[t] = \|\boldsymbol{z}[t] - \mathbf{H}\widehat{\boldsymbol{\theta}}[t]\|$, against a pre-defined threshold τ. It raises an alarm if $r[t] \geq \tau$. The threshold τ is selected to ensure a certain false-positive (FP) rate.

Attacker Model: We consider an attacker who can eavesdrop on the measurement data communicated between the field devices and the control center by exploiting vulnerabilities in the communication system. However, the attacker is assumed to be unaware of the semantics of the accessed data. Furthermore, the attacker has no other information about the grid (e.g., its topology or bus system).

The attacker's objective is to craft FDI attacks against the state estimation. Denote the attack vector by $\mathbf{a}[t] \in \mathbb{R}^M$, the sensor measurements under attack by $\mathbf{z}_a[t]$, where $\mathbf{z}_a[t] = \mathbf{z}[t] + \mathbf{a}[t]$, and the BDD residual under attack by $r_a[t]$. It has been shown [2] that for an attack of the form $\mathbf{a}[t] = \mathbf{H}\mathbf{c}[t]$, the residual value remains unchanged under the attack, i.e., $r_a[t] = r[t]$. Hence, the BDD's detection probability for such attacks is no greater than the FP rate. We will henceforth refer to these attacks as *undetectable* attacks.

III. Existing Algorithm and the Drawbacks

In this section, we review an existing approach [5] for constructing undetectable data-driven FDI attacks, which is particularly relevant to our work, and point out its drawbacks.

A. Algorithm Description

Note that designing an undetectable attack is equivalent to finding a non-zero vector in $Col(\mathbf{H})$, or equivalently, a linear combination of the basis vectors that span $Col(\mathbf{H})$. The attacker must estimate the basis vectors using the noisy measurement data $\mathbf{z}[t],\ t = 1, \ldots, T$. This problem is well studied in the signal processing literature [12], and has been used to guide the construction of data-driven FDI attacks [5].

The key idea is to use the covariance matrix of the measurements $\boldsymbol{\Sigma}_z = \mathbb{E}[(\mathbf{z}[t] - \mathbb{E}[\mathbf{z}[t]])(\mathbf{z}[t] - \mathbb{E}[\mathbf{z}[t]])^T]$. From (1), it follows that $\boldsymbol{\Sigma}_z = \mathbf{H}\boldsymbol{\Sigma}_\theta\mathbf{H}^T + \sigma^2\mathbf{I}_M$. Let $\mathbf{U}\boldsymbol{\Lambda}\mathbf{V}^T$ be the SVD of $\boldsymbol{\Sigma}_z$, where $\mathbf{U} = [\mathbf{u}_1, \ldots, \mathbf{u}_M]$, and $\mathbf{V} = [\mathbf{v}_1, \ldots, \mathbf{v}_N]$ are matrices consisting of left and right singular vectors, respectively, and $\boldsymbol{\Lambda}$ is a matrix consisting of the singular values. Note that the rank of the matrix $\mathbf{H}\boldsymbol{\Sigma}_\theta\mathbf{H}^\mathbf{T}$ is N. Thus, the first N columns of $\mathbf{U}$ corresponding to the N largest singular

values must form the basis vectors of $Col(\mathbf{H}\boldsymbol{\Sigma}_\theta\mathbf{H}^T)$. Since, $Col(\mathbf{H}\boldsymbol{\Sigma}_\theta\mathbf{H}^T)$ is equivalent to $Col(\mathbf{H})$, they also form the basis vectors of $Col(\mathbf{H})$ [12]. For convenience, we partition the matrix $\mathbf{U}$ as $\mathbf{U}_s = [\mathbf{u}_1, \ldots, \mathbf{u}_N]$ and $\mathbf{U}_n = [\mathbf{u}_{N+1}, \ldots, \mathbf{u}_M]$, where the columns of $\mathbf{U}_s$ span the $Col(\mathbf{H})$.

We note that the attacker cannot directly execute the procedure stated above since the actual covariance matrix $\boldsymbol{\Sigma}_z$ is unknown. However, it can be estimated using the measurement data. Based on this observation, the procedure to construct data-driven FDI attacks is summarized in Alg.1. (We use the superscript $\widehat{\ }$ to denote estimates of the corresponding quantities).

Algorithm 1 Construction of Data-driven FDI attack

1. Using measurements $\{\mathbf{z}[1], \ldots, \mathbf{z}[T]\}$, compute the sample covariance matrix $\widehat{\boldsymbol{\Sigma}}_{\boldsymbol{z}}$ as
$$\widehat{\boldsymbol{\Sigma}}_{\boldsymbol{z}} = \frac{1}{T-1}\sum_{t=1}^{T}\left(\boldsymbol{z}[t] - \widehat{\boldsymbol{\mu}_z}\right)\left(\boldsymbol{z}[t] - \widehat{\boldsymbol{\mu}_z}\right)^T,$$
where $\widehat{\boldsymbol{\mu}_z}$ denotes the sample mean given by $\widehat{\boldsymbol{\mu}_z} = \frac{1}{T-1}\sum_{t=1}^{T}\boldsymbol{z}[t]$.
2. Perform singular value decomposition (SVD) of $\widehat{\boldsymbol{\Sigma}}_{\boldsymbol{z}}$ as $\widehat{\boldsymbol{\Sigma}}_{\boldsymbol{z}} = \widehat{\mathbf{U}}\widehat{\boldsymbol{\Lambda}}\widehat{\mathbf{V}}^T$.
3. Let $\widehat{\mathbf{U}}_s$ be the first N columns of $\widehat{\mathbf{U}}$. Construct an undetectable FDI attack vector as $\mathbf{a}[t] = \widehat{\mathbf{U}}_s\mathbf{c}[t]$, where $\mathbf{c}[t] \in \mathbb{R}^N$.

B. Drawbacks of Existing Techniques

Note that when the number of measurements sample is large ($T \to \infty$), Step 1 of Alg. 1 produces a *consistent* estimate of Σ_z [13]. Consequently, the estimated basis vectors $\widehat{\mathbf{u}}_i, i = 1, \ldots, N$ are well aligned with the basis vectors of $Col(\mathbf{H})$, and the FDI attacks constructed as in Step 3 can bypass the BDD.

However, when the basis vectors are estimated from a limited number of measurements, the estimated singular vectors are inaccurate. This is illustrated in Fig. 1 for an IEEE-4 bus system. In this figure, we plot $||\delta(\mathbf{u}_i)||_2,\ i = 1, 2, 3$ as a function of the number of measurements T, where $\delta(\boldsymbol{u}_i) = \boldsymbol{u}_i - \widehat{\boldsymbol{u}}_i,\ i = 1, 2, 3$ denotes the estimation accuracy. It can be observed that while the estimates become accurate asymptotically, they are not accurate for a limited number of measurements. Thus, the estimated basis vectors are not aligned with those of the targeted subspace. The estimation inaccuracy directly contributes to the residual, thus making the attacks detectable. The result is formally stated in the following proposition.

Proposition 1. *For a data-driven FDI attack constructed using Algorithm 1 with a limited number of measurement samples, $r_a[t] \neq r[t]$. Hence, it violates the condition for an undetectable attack.*

The proof is omitted here due to lack of space; it can be found in the Appendix of the technical report [14].

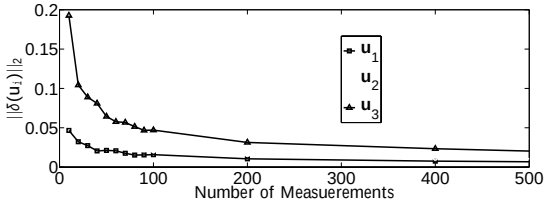


Fig. 1: Accuracy of the estimated singular vectors as a function of the number of measurements for an IEEE 4-bus systems.

IV. Data-driven FDI Attacks with Limited Number of Measurements

In this section, we present an enhanced algorithm for strengthening the attack's BDD-bypass probability when the attacker has access to a limited number of measurements only. Furthermore, we characterize an important trade-off between the attack's BDD-bypass probability and the number of compromised measurements in executing the attack.

A. Accuracy of the Estimated Basis Vectors

The enhanced algorithm is based on the following important observation. From Fig. 1, we note that for a given number of measurement samples $\mathbf{z}[t], t = 1, \ldots, T$, the accuracy of the estimates is in decreasing order of the column index (i.e., the first singular vector is estimated most accurately, followed by the second, etc). The result is generic and holds true for any bus system. It can be explained by a prior result [15] (Lemma 1), which shows that $\delta(\boldsymbol{u}_i)$ can be approximated as

$$\delta(\boldsymbol{u}_i) \approx \lambda_i^{-1}\mathbf{U}_n\mathbf{U}_n^H\mathbf{N}\boldsymbol{v}_i, i = 1, \ldots, N, \tag{2}$$

where $\mathbf{N} = \begin{bmatrix}\mathbf{n}[1] & \mathbf{n}[2] & \cdots & \mathbf{n}[T]\end{bmatrix}$ is a matrix consisting of the noise values. From (3), we note that $\delta(\mathbf{u}_i)$ is inversely proportional to its corresponding singular value λ_i, which implies that the singular vectors corresponding to the large singular values can be estimated more accurately than those corresponding to smaller values. Since the singular values are ordered as $\lambda_1 \geq \lambda_2 \geq \cdots \geq \lambda_N$, the estimation accuracy decreases with the column index.

Note that the attack vector has a high chance of bypassing the BDD if it is restricted to a lower-dimensional subspace of the estimated column space spanned by the accurately estimated basis vectors (since they are well aligned with the corresponding basis vectors of the targeted subspace, i.e., $Col(\mathbf{H})$). Thus, it follows that the attack's BDD-bypass probability is enhanced when it is constructed using only the first few estimated basis vectors. If too many estimated basis vectors are utilized, the attack's BDD-bypass probability will decrease (since their estimation accuracy is low).

B. Trade-offs in Data-Driven FDI Attacks

An important question is: how many estimated basis vectors should the attacker use in the construction of the FDI attack? To answer this question, we quantify the minimum number of compromised measurements required to execute the FDI attack, or equivalently, the sparsity of the resulting attack vector. The number of estimated basis vectors for constructing

the FDI attack must be chosen to balance between the BDD-bypass probability and the attack's sparsity.

The sparsest attack vector that can be constructed by constraining the attack vector to a lower-dimensional subspace of the estimated column space can be cast as the following optimization problem [9]:

$$S_K^* = \min_{\mathbf{c}} \|\widehat{\mathbf{U}}_{s,[1:K]}\mathbf{c}\|_0, \text{ s.t. } ||\mathbf{c}||_\infty \geq \tau, \tag{3}$$

where $\widehat{\mathbf{U}}_{s,[1:K]}$ denotes the matrix with the first $K(\leq N)$ columns of $\widehat{\mathbf{U}}_s$ and $\tau > 0$ is a positive threshold. The objective function of (4) gives the number of non-zero elements in the FDI attack vector while restricting it to within $Col(\widehat{\mathbf{U}}_{s,[1:K]})$. The constraint $||\mathbf{c}||_\infty \geq \tau$ implies that the shift caused by at least one of the elements of $\mathbf{c}$ the must be greater than a threshold. This constraint is important since without it, $\mathbf{c} = \mathbf{0}$ is always a trivial solution to the optimization problem (corresponding to the zero attack). The optimization problem (4) can be solved using an l_1-relaxation based approach. We omit the details here and refer the reader to [9].

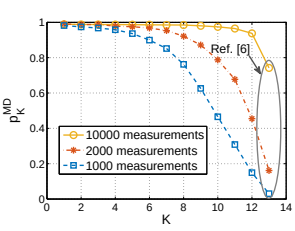
We note that for two integers K_1, K_2 such that $0 \leq K_1 \leq K_2 \leq N$, we have $Col(\widehat{\mathbf{U}}_{s,[1:K_1]}) \subseteq Col(\widehat{\mathbf{U}}_{s,[1:K_2]})$. Thus, we have that $S^*_{K_2} \leq S^*_{K_1}$, or equivalently, a less constrained attacker can find a sparser attack vector than a more constrained one. In the following, we present simulation results to validate this claim and illustrate the entailed trade-offs.

V. Simulation Results

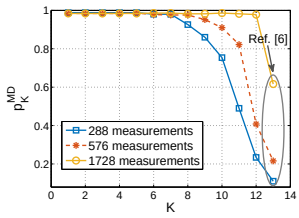
In this section, we present the simulation results. All the simulations are conducted on an IEEE 14-bus system using the MATPOWER simulator [16]. For convenience, throughout this section, we denote the BDD-bypass probability by p_K^{MD}, and the number of compromised measurements by C_K^*, where $C_K^* = M - S_K^*$, when K estimated basis vectors are used to construct the FDI attack.

In Fig. 2, we plot p_K^{MD} as a function of K. The measurement samples used in the estimation of the basis vectors are obtained from (1). The system state is generated using two methods. In Fig. 2a, $\boldsymbol{\theta}[t]$ is assumed to be an i.i.d. Gaussian random vector. In Fig. 2b, we use the load data trace from New York state [17] to generate $\boldsymbol{\theta}[t]$. Specifically, we feed the load data (sampled at intervals of 5 minutes) to the IEEE- 14-bus system and solve the optimal power flow problem to obtain $\boldsymbol{\theta}[t]$. The FDI attack vector is constructed according to Alg. 1 using the measurement samples, and p_K^{MD} is computed by averaging the BDD's detection results over 1000 independent trials. The BDD threshold is adjusted such that the FP rate is set to 0.02.

We make the following observations. First, p_K^{MD} is high when more measurement samples are used in the estimation of the basis vectors. This is expected since the basis vectors can be estimated more accurately with more measurement samples. Second, for a given number of measurements, p_K^{MD} decreases as K is increased. This confirms our hypothesis in Sec. IV. We also observe that the approach proposed in Alg. 1 (ref. [5]) has a low BDD-bypass probability (encircled in the figure)



(a) I.I.D. system states.



(b) System state derived from New York state load-data trace [17].

Fig. 2: BDD-bypass probability versus the number of estimated basis vectors used in the construction of the FDI attack for IEEE 14-bus system.

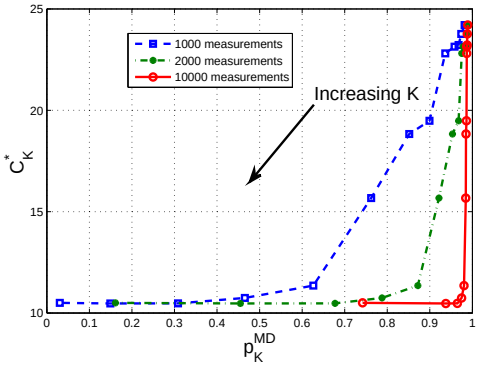


Fig. 3: Trade-off between the number of compromised sensors required to construct sparse FDI attacks and the probability of bypassing the BDD.

using a finite measurement set, and our proposed approach significantly outperforms their algorithm.

Next, we illustrate the trade-off between p_K^{MD} and C_K^* in Fig. 3. The points of the trade-off curve are obtained by varying K. We make the following observations. First, we observe that C_K^* decreases as we increase K. More importantly, we observe that the number of compromised measurements to execute the FDI attack is significantly reduced if the attacker can tolerate a small decrease in the BDD-bypass probability. For instance, with 2000 measurements, C_K^* reduces from 24 to 15 when p_K^{MD} is reduced from 0.98 to 0.87. In practice, the attacker can make use of such trade-off curves to select suitable parameters for the construction of the FDI attack, e.g., based on the resources available to him.

VI. Conclusions

We have studied the construction of data-driven FDI attacks when the attacker has access to only a limited number of measurements. We showed that in this regime, the attacker can enhance the BDD-bypass probability by constraining the attack vector to a lower-dimensional subspace spanned by the accurately estimated basis vectors. We also characterized an important trade-off between the attacker's ability to bypass the BDD and the sparsity the attack vector. Our framework gives practical guidance to a resource-constrained attacker in designing stealthy FDI attacks. In the future, we will analytically characterize the attacker's trade-off and address the defense problem against these attackers.

REFERENCES

[1] "Confirmation of a coordinated attack on the Ukrainian power grid," http://bit.ly/1OmxfnG.

[2] 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.

[3] 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.

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

[5] 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.

[6] D. Divan and H. Johal, "Distributed FACTS; A new concept for realizing grid power flow control," *IEEE Trans. Power Syst.*, vol. 22, no. 6, pp. 2253–2260, Nov 2007.

[7] R. Verzijlbergh, L. De Vries, G. Dijkema, and P. Herder, "Institutional challenges caused by the integration of renewable energy sources in the european electricity sector," *Renewable and Sustainable Energy Reviews*, vol. 75, pp. 660–667, 2017.

[8] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Sparse attack construction and state estimation in the smart grid: Centralized and distributed models," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1306–1318, July 2013.

[9] T. T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 326–333, Jun. 2011.

[10] A. Wood and B. Wollenberg, *Power Generation, Operation, and Control*. A Wiley-Interscience, 1996.

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

[12] H. Krim and M. Viberg, "Two decades of array signal processing research: the parametric approach," *IEEE Signal Processing Magazine*, vol. 13, no. 4, pp. 67–94, Jul. 1996.

[13] T. W. Anderson, *An Introduction to Multivariate Statistical Analysis*, 3rd ed. Wiley, 2003.

[14] "Technical report," https://tinyurl.com/y972t86z.

[15] F. Li, H. Liu, and R. J. Vaccaro, "Performance analysis for DOA estimation algorithms: unification, simplification, and observations," *IEEE Transactions on Aerospace and Electronic Systems*, vol. 29, no. 4, pp. 1170–1184, Oct. 1993.

[16] 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.

[17] "NYISO load data," https://tinyurl.com/kx3h82t.