Learning-Based Stealthy Load Redistribution Attacks for Market Price Manipulation in Smart Grids

Adnan Anwar
Deakin Cyber Research and Innovation Centre
Deakin University, Melbourne, Australia
adnan.anwar@deakin.edu.au

Abdun Mahmood
Dept.of Computer Science & Information Technology
La Trobe University, Melbourne, Australia
a.mahmood@latrobe.edu.au

***Abstract*—False data injection (FDI) and, in particular, Load Redistribution (LR) attacks pose severe threats to state estimation and market pricing in smart grids. We propose a fully data-driven LR construction methodology that (i) estimates injection shift factors from noisy, partially corrupted SCADA measurements using robust matrix decomposition and least squares estimation, and (ii) demonstrates how stealthy LR attacks can be constructed as an attack model that maximises weighted line flow perturbations while preserving power balance and load manipulation limits. Experiments on IEEE benchmark systems validate that (a) the proposed shift-factor estimator effectively handles Gaussian noise, sparse errors and missing values, and (b) the LR attacks remain undetected by Bad Data Detectors (BDDs) while producing significant locational marginal price (LMP) perturbations.**

***Index Terms*—Cyber-physical systems, SCADA, Load Redistribution attack, False Data Injection, Shift factor estimation.**

I. Introduction

Data integrity attacks against state estimation modules can stealthily mislead grid operation and electricity markets. Load redistribution (LR) attacks, a subclass of false data injection (FDI) attacks, manipulate measured loads under a zero-net-injection constraint with small load deviations to produce virtual congestion that changes line flows and, consequently, alters Locational Marginal Prices (LMPs) [1]. Such stealthy LR attacks depend critically on accurate knowledge of shift factors. Multiple studies have explored profit-driven FDIAs on electricity markets [2], and a recent comprehensive review underscores that such attacks pose serious risks to market stability [3]. Meanwhile, newer LR-attack variants with enhanced stealth (e.g., multi-line high-stealth attacks) continue to emerge [4]. Shift Factors (SF) quantify how an incremental injection at a bus changes flow on each transmission element. By modifying load perturbations with specific SF patterns, an attacker can deliberately modify power flows on targeted branches, thereby inducing congestion that directly influences LMP calculations.

LMP-based energy pricing systems are deployed in many electricity markets (e.g., ERCOT, NYISO, PJM in the U.S., Australia [5], New Zealand, and Singapore [6], [7]). Typically, LMP data and related market information are published online [8], [9], for example, hourly real-time and day-ahead LMPs for PJM are openly accessible [10], and California ISO provides load and price data via OASIS [11]. Over 60% of the U.S. energy market operates under LMP-based mechanisms [12]. This data availability, combined with market coupling to physical congestion, creates attractive leverage for a cyber-adversary whose objectives are to destabilise the grid or to extract economic gain via stealthy LR attacks that affect LMP outcomes.

Prior work often assumes attackers know network topology and branch impedances so they can compute shift factors explicitly [13], [14], [15]. In practice, detailed power system models and line parameters are strictly protected in an energy system control centre. Recent studies instead observe that an intelligent adversary can bypass the need for the grid models by learning the mapping from injections to line flows directly from measurement data by passively eavesdropping on sensor streams for some time [16], [1].

Interestingly, a naive attempt by the attacker to learn shift factors via least-squares estimation (LSE) is brittle in realistic settings. LSE requires sufficiently rich, complete, and clean measurements. Missing entries (due to packet drops or device unavailability) and sparse gross errors (sensor fault or occasional outages) break the Gaussian and complete-data assumptions and can cause the regression to be ill-conditioned or rank-deficient. In contrast, modern robust low-rank and sparse recovery methods (e.g., matrix completion, robust principal component analysis, and structured sparse regression) explicitly estimate the measurement matrix even during the presence of sparse gross errors or missing entries. These techniques can recover the underlying measurement subspace. Consequently, an attacker equipped with robust estimation tools can reconstruct effective shift-factor (or their projection onto the measurement subspace) from eavesdropped data and use those estimates to construct stealthy LR attacks that remain undetected by Bad Data Detectors (BDDs). This paper investigates the research question: *Can an attacker construct stealthy LR attacks by estimating shift factors from measurements without the need for prior topology/admittance knowledge, even in the presence of missing values and sparse errors?*. Our contributions are:

1) Develop a robust, ***measurement-based shift factor estimation method*** that tolerates Gaussian noise, sparse gross errors and missing values using a low-rank and sparse matrix decomposition technique.
2) Propose an ***LR attack construction strategy*** based on Weighted Power-Flow LR (WPF-LR) to induce virtual congestion via optimised load redistribution.

979-8-3315-8138-1

3) Validate ***experimentally*** using IEEE benchmark test systems showing stealthiness against BDD and significant LMP perturbations.

The paper is organized as follows. Section II outlines the LR attack model and shift-factor formulation. Section III describes the proposed measurement-based estimation framework, and Section IV details the WPF-LR attack strategy. Section V presents experimental results, followed by concluding remarks.

II. Load Redistribution (LR) Attack

The LR attack is a realistic subclass of False Data Injection (FDI) attacks in which the adversary manipulates only load measurements and possibly a few power flow sensors without altering generation data [13], [14], [15]. To maintain system power balance, total load changes must sum to zero, and each load deviation must remain within a small fraction of its nominal value to avoid detection. Formally,

$$\sum_{i}^{N_L} \Delta \mathbf{P}_{l_i} = 0, \tag{1}$$

$$-\varepsilon \mathbf{P}_{l_i} \leq \Delta \mathbf{P} l_i \leq \varepsilon \mathbf{P}_{l_i}, \tag{2}$$

$$\Delta \mathbf{F} = \mathbf{H}^{SF} \Delta \mathbf{P}_l, \tag{3}$$

where $\mathbf{H}^{SF}$ is the shift-factor matrix linking load injections to line-flow changes. In a typical attack model, successful LR attacks require access to load data and $\mathbf{H}^{SF}$, which is difficult to obtain, as sensitive power system information is protected in a secure database system within the control centre.

The shift factor represents the linear sensitivity of a line's power flow to a bus-level injection change [17], [18], [19]. It is essential for LMP computation [20] and enables line flows to be expressed directly in terms of bus injections [21], [22], [23]. For a unit power injection at bus i and an equal withdrawal at the reference bus, the shift factor on line k is

$$\mathbf{H}^{SF}_{k-i} = \frac{\Delta \mathbf{F}^i_k}{\Delta \mathbf{P}_i}. \tag{4}$$

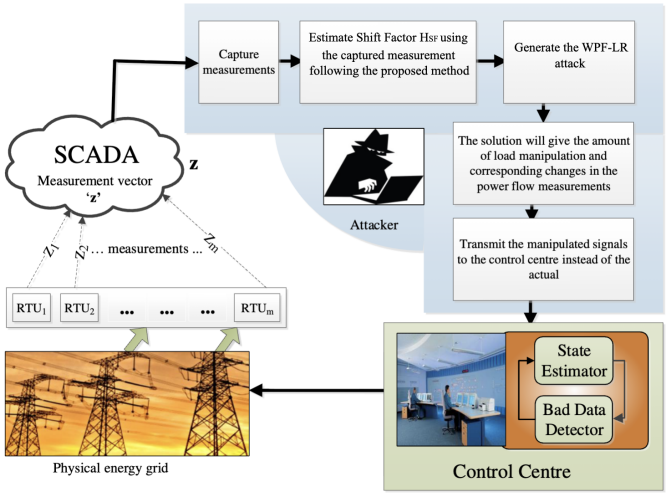

Fig. 1. Construction strategy of WPF-LR attack

III. Proposed Method of Estimating Shift Factor using Measurement Data in a Noisy Environment

The proposed method comprises two steps: (1) data-driven estimation of shift factors from time-series measurements, and (2) robust estimation via low-rank sparse decomposition to recover the measurement subspace for attack construction.

A. Data-driven estimation of shift factors

Measurement data can also be used to estimate the shift factors [18], [19], [17]. Let us consider the power injection at node i for time instant t and $t+\Delta t$ (where Δt is very small) are $\mathbf{P}_i(t)$ and $\mathbf{P}_i(t+\Delta t)$. Hence, the difference of power injection becomes $\Delta \mathbf{P}_i(t)$. Due to this change of injection, the power flow in line k varies $\Delta \mathbf{F}^i_k$. According to the definition of shift factor ($\mathbf{H}^{SF}_{k-i}$), we can write [23], [18], [19], [17]:

$$\mathbf{H}^{SF}_{k-i} = \frac{\Delta \mathbf{F}^i_k(t)}{\Delta \mathbf{P}_i(t)} \tag{5}$$

As $\Delta \mathbf{P}_i(t) = \mathbf{P}_i(t+\Delta t) - \mathbf{P}_i(t)$, the difference of power injection $\Delta \mathbf{P}_i(t)$ can be calculated from $\mathbf{P}_i(t)$ and $\mathbf{P}_i(t+\Delta t)$ which are directly obtained from measurements [18]. However, $\mathbf{F}^i_k(t)$ or $\Delta \mathbf{F}^i_k(t)$ is not directly measurable from sensor data [18], [19], [17]. Rather, the total change of power flow ($\Delta \mathbf{F}_k(t)$) in line k due to all injection variations can be obtained from the measurements, which can be expressed simply $\Delta \mathbf{F}_k(t) = \mathbf{F}_k(t+\Delta t) - \mathbf{F}_k(t)$. Theoretically, total change of power flow ($\Delta \mathbf{F}_k(t)$) in line k can be written as below [18], [19], [17]:

$$\Delta \mathbf{F}_k(t) \approx \Delta \mathbf{F}^1_k(t) + ... + \Delta \mathbf{F}^i_k(t) + ... + \Delta \mathbf{F}^N_k(t) \tag{6}$$

Based on Eq. (5), the above relationship can be rewritten as:

$$\Delta \mathbf{F}_k(t) \approx \Delta \mathbf{P}_1(t)\mathbf{H}^{SF}_{k-1} + ... + \Delta \mathbf{P}_i(t)\mathbf{H}^{SF}_{k-i} + ... + \Delta \mathbf{P}_N(t)\mathbf{H}^{SF}_{k-N} \tag{7}$$

Now, consider $t = 1 \ ... \ T$ number of instances which produce the following relationship [18], [19], [17]:

$$\Delta \mathbf{F}_k \approx \Delta \mathbf{P} \mathbf{H}^{SF}_k \tag{8}$$

where, following [24], $\mathbf{H}^{SF}_k$ can be obtained using the below equation:

$$\mathbf{H}^{SF}_k = (\Delta \mathbf{P})^+ \Delta \mathbf{F}_k \tag{9}$$

where $(\Delta \mathbf{P})^+$ is the Moore-Penrose pseudo-inverse of $\Delta \mathbf{P}$ [24]. In the above model, measurement noises are ignored. In the presence of the Gaussian noise, Eq. (8) can be written as:

$$\Delta \mathbf{F}_k \approx \Delta \mathbf{P} \mathbf{H}^{SF}_k + \mathbf{e} \tag{10}$$

where, $\Delta \mathbf{P} \in \mathbb{R}^{T \times N}$, $\Delta \mathbf{F}_k \in \mathbb{R}^N$ and $\mathbf{H}^{SF}_k \in \mathbb{R}^N$. The equations in (10) is overdetermined [18] as $T > N$. Therefore, the least-square error (LSE) estimation of the problem defined in Eq (10) is obtained as below [18], [19], [17]:

$$\hat{\mathbf{H}}^{SF}_k = (\Delta \mathbf{P}^T \Delta \mathbf{P})^{-1} \Delta \mathbf{P} \Delta \mathbf{F}_k \tag{11}$$

The estimation error residual will be as follows:

$$\hat{\mathbf{r}} = \Delta \mathbf{F}_k - \Delta \mathbf{P} \hat{\mathbf{H}}^{SF}_k \tag{12}$$

Hence, the sum of squared error (SSE) will become:

$$SSE = \hat{\mathbf{r}}^T \hat{\mathbf{r}} \tag{13}$$

B. Robust Estimation under Missing Values and Gross Errors

The LSE estimator in (11) is sensitive to missing entries and sparse gross errors. To obtain reliable shift factors in such conditions we first recover a clean measurement matrix by separating a low-rank physical component from sparse corruptions. Model the observed (corrupted) measurements as

$$\tilde{\mathbf{P}} = \mathbf{P} + \mathbf{E}, \tag{14}$$

where $\mathbf{P}$ denotes the true (low-rank) measurement and $\mathbf{E}$ contains sparse gross errors and missing-value indicators. The robust convex matrix recovery becomes [25], [26]:

$$\min_{\mathbf{P},\mathbf{E}} \ \|\mathbf{P}\|_* + \lambda\|\mathbf{E}\|_1 \quad \text{s.t.} \quad \tilde{\mathbf{P}} = \mathbf{P} + \mathbf{E}, \tag{15}$$

where $\|\cdot\|_*$ is the nuclear norm, $\|\cdot\|_1$ the elementwise l_1 norm, and $\lambda > 0$ balances rank and sparsity. Problem (15) admits efficient solvers; here we use an Accelerated Proximal Gradient (APG) method that iteratively minimises a separable quadratic approximation of the objective and thresholds singular values and entries to recover $\mathbf{P}$ and $\mathbf{E}$ [26], [27].

After obtaining the cleaned injection differences from $\mathbf{P}$, the SF for line k is estimated by LSE applied to the denoised data. This two-step procedure produces SF that remain accurate in the presence of missing values and sparse corruptions, and hence are suitable for subsequent LR-attack construction.

IV. Proposed LR Attack using Estimated Shift Factors

Unlike prior studies that assume an attacker knows the network model [13], [14], [15], we consider an adversary learns shift factors from data and then constructs LR attacks using those estimates. The data-driven SF estimation described above is robust against noise, missing data, and sparse errors.

A. Weighted Power-Flow LR Attack (WPF-LR)

The WPF-LR attack aims to create *virtual congestion* by manipulating load measurements so that the operator's state estimation for selected lines is heavily loaded or overloaded, resulting in non-optimal redispatch and LMP changes. Let the true and attacked load vectors be $\mathbf{P}_l$ and $\mathbf{P}_l^a$, with deviation $\Delta\mathbf{P}_l = \mathbf{P}_l^a - \mathbf{P}_l$. Under the linearised model the resulting line-flow change is

$$\Delta\mathbf{F} = \mathbf{H}^{SF}\,\Delta\mathbf{P}_l, \tag{16}$$

where signs indicate direction and magnitudes indicate flow variation. Using a weighting vector $\mathbf{w}$ to prioritise target branches, the attacker maximises the (weighted) apparent flow change subject to power balance and (individual) load limits:

$$\max_{\mathbf{P}_l^a} \ \mathbf{w}^\top\left|\Delta\mathbf{F}\right| \quad \text{s.t.} \quad \Delta\mathbf{F} = \mathbf{H}^{SF}(\mathbf{P}_l^a - \mathbf{P}_l). \tag{17}$$

The attack must preserve total demand,

$$\sum_i^{N_L} \mathbf{P}_{l_i}^a - \sum_i^{N_L} \mathbf{P}_{l_i} = 0 \tag{18}$$

and respect load perturbation limits

$$-\varepsilon\,\mathbf{P}_{l_i} \le \Delta\mathbf{P}_{l_i} \le \varepsilon\,\mathbf{P}_{l_i}, \ \forall i, \tag{19}$$

with $0 < \varepsilon \ll 1$. Collecting these constraints yields the complete WPF-LR formulation:

$$\begin{aligned} \max_{\mathbf{P}_l^a} \quad & \mathbf{w}^T\Delta\mathbf{F} \\ s.t., \quad & \Delta\mathbf{F} = \mathbf{H}^{SF}\Delta\mathbf{P}_l \\ & \Delta\mathbf{P}_l = (\mathbf{P}_l^a - \mathbf{P}_l) \\ & \sum_i^{N_L}\mathbf{P}_{l_i}^a - \sum_i^{N_L}\mathbf{P}_{l_i} = 0 \\ & -\varepsilon\mathbf{P}_{l_i} \le \Delta\mathbf{P}_{l_i} \le \varepsilon\mathbf{P}_{l_i} \end{aligned} \tag{20}$$

By selecting $\mathbf{w}$ to emphasise specific lines, the attacker can target branches for virtual congestion.

TABLE I
SSE of SF estimation (SNR: 20–35 dB; 2% sparse errors)

Method	20 dB	25 dB	35 dB
Ideal case	10^{-12}	10^{-12}	10^{-12}
LSE method	15.6540	14.9343	12.3752
Pseudo-inverse	15.7691	14.1704	12.2619
Proposed method	**0.2608**	**0.1641**	**0.1234**

TABLE II
SSE vs. sparse-error rate (Gaussian noise, IEEE 14-bus)

Method	2%	3%	4%	5%
LSE method	12.3752	17.4592	18.2527	19.2938
Pseudo-inverse	12.2619	17.0826	18.3935	19.4300
Proposed method	**0.1234**	**0.1328**	**0.1333**	**0.1444**

V. Experimental Evaluation

We evaluate the proposed methods on the IEEE benchmark system and examine the impact on Bad Data Detection (BDD) and Locational Marginal Prices (LMPs).

A. Test System and Data Preparation

All experiments use the IEEE 14-bus system [28], [29]. Simulation and data generation are performed in MATPOWER [29], [30], [31]. From power-flow solutions, we form time-series measurements and inject Gaussian noise (SNR 20–35 dB) and 1–5% sparse errors (missing values and large-magnitude outliers). Experiments are conducted in MATLAB on a PC with Intel(R) Core i7 @ 3.4 GHz and 16 GB RAM.

B. Estimating Shift Factors from Measurements

For each line k, the goal is to estimate its shift-factor from measured line-flow changes and bus-injection variations collected over T time instants. We compare three approaches: (i) Moore–Penrose pseudo-inverse [24], (ii) standard LSE [18], [17], and (iii) the proposed robust method (Section III). The performance is measured by SSE (13). With Gaussian noise (20–35 dB) and 2% sparse errors, averaged over 100 trials, our

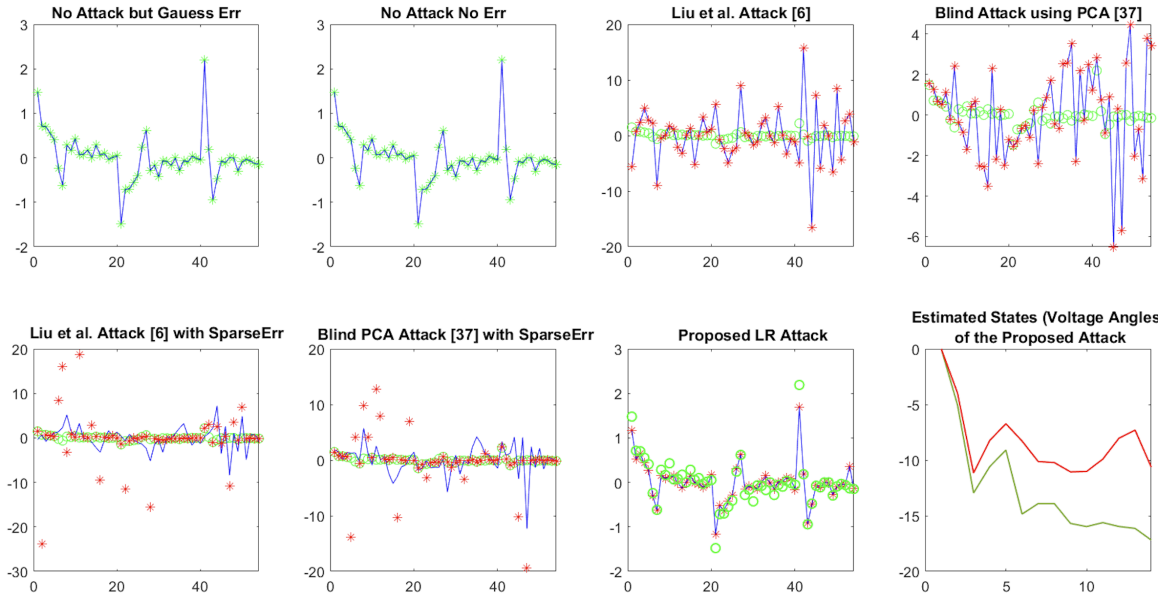

Fig. 2. Comparison of BDD outcomes across attack scenarios (IEEE 14-bus).

TABLE III
IMPACT ON BDD (95% CONFIDENCE INTERVAL)

Scenario	$J(\hat{x})$	Threshold	Decision
No attack, no noise	4.3×10^{-27}	56.94	Not detected
No attack, Gaussian noise	38.94	56.94	Not detected
Random attack	5.2×10^{5}	56.94	Detected
Liu et al. [32]	43.65	56.94	Not detected
Blind PCA [31]	48.25	56.94	Not detected
Liu et al. + sparse errors	1.58×10^{7}	56.94	Detected
Blind PCA + sparse errors	3.28×10^{7}	56.94	Detected
Proposed LR + sparse errors	37.26	56.94	Not detected

method achieves the lowest SSE, approaching the ideal case (Table I). Increasing the sparse-error rate degrades all methods, but the proposed approach remains far more accurate due to its ability to reject bad data (Table II).

C. Impact of WPF-LR on BDD

We evaluate the weighted power-flow LR (WPF-LR) strategy of Section IV-A on the IEEE 14-bus system with 54 measurements (20 lines with bidirectional flow meters and 14 bus injections) and 13 angle states (one slack), giving 41 degrees of freedom (BDD threshold 56.94 at 95% CI). We compare: (i) no-attack (no noise), (ii) no-attack (Gaussian noise), (iii) Random Attack, (iv) and (v) benchmark stealthy FDI attacks using strategies [32], [31], their counterparts under sparse errors in (vi) and (vii), and the proposed LR attack under sparse errors in (viii). Results in Table III and Fig. 2 show that while random and benchmark methods are detected under sparse errors, the proposed LR construction remains stealthy (objective function value < 56.94) in the BDD detector.

We further vary the load limits $\varepsilon \in \{5\%, 10\%, 20\%\}$ and generate 50 random feasible WPF-LR attack instances for each

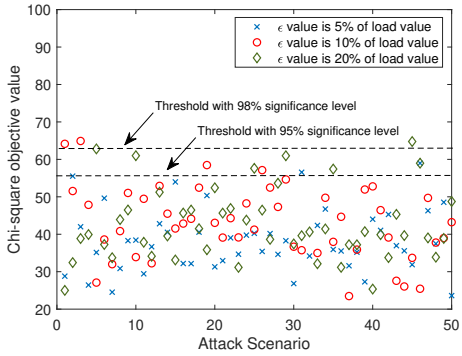

Fig. 3. BDD detection performance vs. ε (no two-bus-only cases).

case. Most attacks remain below the BDD threshold for ε up to 20%, as shown in Fig. 3.

D. Impact of WPF-LR on Energy Pricing

We use line rating limits from [9] for the IEEE 14-bus system. In the base case, no lines are congested and LMPs are uniform. Under a crafted WPF-LR attack, the system operator's state estimator "sees" congestion on targeted line(s) and runs an optimal power flow that redispatches generation. This produces LMP differentials, i.e., buses downstream of the fake congestion experience higher prices. For example, Fig. 4 shows the LMP profile before and after an attack that induces a fake overload on a particular line. In other words, the attacked scenario causes that line's connected buses to face elevated LMPs relative to the base case.

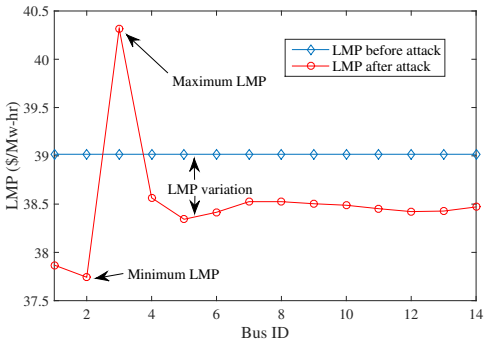

Fig. 4. LMPs before vs. after a WPF-LR attack causing virtual congestion.

VI. Conclusion

This paper presented a data-driven learning framework for constructing stealthy load redistribution (LR) attacks without prior knowledge of system topology or line parameters. A robust two-step method was developed to estimate shift factors directly from noisy SCADA measurements by combining low-rank sparse decomposition with least-squares estimation. The proposed approach effectively handled Gaussian noise, sparse errors, and missing data. The estimated shift factors enable an attacker to craft weighted power-flow LR (WPF-LR) attacks that induce virtual line congestion while respecting load manipulation limits and avoiding detection.

Experimental results on IEEE benchmark systems demonstrated that the constructed LR attacks remain stealthy to conventional bad data detectors and can significantly manipulate LMPs. As LR attacks continue to evolve, future work will investigate real-time detection and mitigation strategies that exploit the temporal and spatial patterns of system state variables to thwart such data-driven attacks.

References

[1] H. T. Reda, A. Anwar, and A. Mahmood, "Comprehensive survey and taxonomies of false data injection attacks in smart grids: attack models, targets, and impacts," *Renewable and Sustainable Energy Reviews*, vol. 163, p. 112423, 2022.

[2] Q. Zhang, F. Li, Q. Shi, K. Tomsovic, J. Sun, and L. Ren, "Profit-oriented false data injection on electricity market: Reviews, analyses, and insights," *IEEE Transactions on Industrial Informatics*, vol. 17, no. 9, pp. 5876–5886, 2021.

[3] G. O. Alsharif, C. Anagnostopoulos, and A. K. Marnerides, "Energy market manipulation via false-data injection attacks: A review," *IEEE Access*, vol. 13, pp. 42 559–42 573, 2025.

[4] M. Du, L. Wang, and Y. Zhou, "High-stealth false data attacks on overloading multiple lines in power systems," *IEEE Transactions on Smart Grid*, vol. 14, no. 2, pp. 1321–1324, 2023.

[5] P. Wild and J. Foster, "A non-technical introduction to the anemmarket model of the australian national electricity market (NEM)," in *Energy Economics and Management Group Working Papers 03, School of Economics, University of Queensland, Australia*, 2010.

[6] "NYISO transmission and dispatch operations manual," *NYISO*, vol. 1999.

[7] "FERC electric rate schedule," *ISO-New England*, vol. 2001.

[8] V. Kekatos, G. B. Giannakis, and R. Baldick, "Online energy price matrix factorization for power grid topology tracking," *IEEE Transactions on Smart Grid*, vol. 7, no. 3, pp. 1239–1248, May 2016.

[9] V. Kekatos, G. Giannakis, and R. Baldick, "Grid topology identification using electricity prices," in *IEEE PES General Meeting*, July 2014.

[10] "PJM dataviewer," https://dataviewer.pjm.com/dataviewer/pages/public/lmp.jsf, accessed: 2016-06-19.

[11] "California independent system operator," url: https://goo.gl/ZtC0tS, accessed: 2016-06-19.

[12] M. Sahni, R. Jones, and Y. Cheng, "Beyond the crystal ball: Locational marginal price forecasting and predictive operations in u.s. power markets," *IEEE Power and Energy Magazine*, vol. 10, no. 4, pp. 35–42, July 2012.

[13] Y. Yuan, Z. Li, and K. Ren, "Modeling load redistribution attacks in power systems," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 382–390, June 2011.

[14] X. Liu and Z. Li, "Local load redistribution attacks in power systems with incomplete network information," *IEEE Transactions on Smart Grid*, vol. 5, no. 4, pp. 1665–1676, July 2014.

[15] Y. Yuan, Z. Li, and K. Ren, "Quantitative analysis of load redistribution attacks in power systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1731–1738, 2012.

[16] A. Anwar, A. N. Mahmood, Z. Tari, and A. Kalam, "Measurement-driven blind topology estimation for sparse data injection attack in energy system," *Electric Power Systems Research*, vol. 202, p. 107593, 2022.

[17] Y. C. Chen, A. D. Dominguez-Garcia, and P. W. Sauer, "Generalized injection shift factors and application to estimation of power flow transients," in *North American Power Symposium (NAPS)*, Sept 2014, pp. 1–5.

[18] A. D. D.-G. Y. C Chen. and P. W. Sauer, "Measurement-based estimation of linear sensitivity distribution factors and applications," *IEEE Transactions on Power Systems*, vol. 29, no. 3, pp. 1372–1382, May 2014.

[19] Y. C. Chen, S. V. Dhople, A. D. Dominguez-Garcia, and P. W. Sauer, "Generalized injection shift factors," *IEEE Transactions on Smart Grid*, vol. PP, no. 99, pp. 1–10, 2016.

[20] B. F. Hobbs, C. B. Metzler, and J. S. Pang, "Strategic gaming analysis for electric power systems: an MPEC approach," *IEEE Transactions on Power Systems*, vol. 15, no. 2, pp. 638–645, May 2000.

[21] Y. Fu and Z. Li, "A direct calculation of shift factors under network islanding," *IEEE Transactions on Power Systems*, vol. 30, no. 3, pp. 1550–1551, May 2015.

[22] A. Wood and B. Wollenberg, *Power Generation, Operation, and Control*. Wiley, 2012.

[23] M. Rahmani, A. Kargarian, and G. Hug, "Comprehensive power transfer distribution factor model for large-scale transmission expansion planning," *IET Generation, Transmission Distribution*, vol. 10, no. 12, pp. 2981–2989, 2016.

[24] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Bilevel model for analyzing coordinated cyber-physical attacks on power systems," *IEEE Transactions on Smart Grid*, vol. 7, no. 5, pp. 2260–2272, Sept 2016.

[25] A. Anwar, A. N. Mahmood, and M. Pickering, "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*, vol. 83, no. 1, pp. 58 – 72, 2017.

[26] Z. Lin, M. Chen, and Y. Ma, "Fast convex optimization algorithms for exact recovery of a corrupted low-rank matrix," UIUC Technical Report UILU-ENG-09-2214, Tech. Rep., 2009.

[27] M. C. Zhouchen Lin. and Y. Ma, "The augmented lagrange multiplier method for exact recovery of corrupted low-rank matrices," UIUC Technical Report UILU-ENG-09-2214, Tech. Rep., 2009.

[28] "Power systems test case archive." [Online]. Available: \\https://www.ee.washington.edu/research/pstca

[29] R. Zimmerman, C. Murillo-Sanchez, and R. 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.

[30] M. Esmalifalak, H. Nguyen, R. Zheng, and Z. Han, "Stealth false data injection using independent component analysis in smart grid," in *IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Oct 2011, pp. 244–248.

[31] 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, 2015.

[32] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Trans. Inf. Syst. Secur.*, vol. 14, no. 1, pp. 13:1–13:33, Jun. 2011.