Tensor-Completion-Enabled Stealthy False Data Injection Attacks on IoT-Based Smart Grid

Bo Liu, *Member, IEEE*, Yajing Liu, *Member, IEEE*, and Hongyu Wu, *Senior Member, IEEE*

***Abstract*—False data injection (FDI) attacks against power system state estimation through manipulating measurements can result in economic losses and grid operating security issues. FDI attacks are stealthy to the traditional bad data detector. However, existing FDI construction methods fail to consider the stealthiness of attacks against machine-learning (ML) detectors. Since the historical measurement patterns are generally utilized by ML detectors, we apply the tensor completion (TC) technique in the FDI construction to manipulate compromised measurements matching the historical measurement patterns. We propose a novel convex TC-based FDI (TC-FDI) attack algorithm that 1) minimizes the nuclear norm of the compromised measurement tensor to make the compromised measurements consistent with the historical ones and 2) maximizes the L1-norm of the incremental voltage to ensure a sufficient negative impact on the power system operation. Further, the reactance perturbation strategy (RPS) is utilized to detect the TC-FDI attacks by breaking the spatial and temporal correlation of the compromised measurements. Numerical results on the IEEE 14-bus system show the stealthiness of the proposed attacks to the statistic-based detectors and ML detectors. The efficacy of the RPS in detecting TC-FDI attacks is also demonstrated.**

***Index Terms*—False data injection (FDI), machine learning (ML), reactance perturbation strategy (RPS), state estimation (SE), tensor completion (TC).**

I. Introduction

THE SMART grid is experiencing a significant transformation as advanced Internet of Things (IoT) technologies become integrated in electricity facilities. Existing SCADA communication standards, such as the IEEE C37.118 and IEC-61850 frameworks, are known to have insufficient security features (e.g., lack of encryption, etc.) [1]. Due to vulnerabilities in IoT devices and communication protocols, cyberattacks pose a threat to normal control and operation of the smart grid. The state-of-the-art smart grid research has identified the power system applications vulnerable to cyberattacks, including state estimation (SE), wide-area damping control, and automatic generation control. False data injection (FDI) attack is one of the most dangerous cyberattacks against the SE in the smart grids, which results in the system operator's incorrect voltage estimation [2]. The attack manipulates the output of SE by targeting IoT devices, such as PMUs and smart meters. As multiple operational applications use the voltage estimated by the SE in the operator's control room, the consequences of FDI attacks may include economic loss, unstable system states, and even voltage collapse [3].

Reactance perturbation strategy (RPS) has been utilized to detect FDI attacks. The RPS frequently and actively changes the transmission line reactance using the D-FACTS devices to invalidate the attacker's knowledge of the power system. Multiple attack detection effectiveness metrics have been proposed, and operation methods are accordingly proposed to improve the RPS performance. In the simplified dc model, the rank of the composite matrix is widely used to measure the detection effectiveness [4]. Lakshminarayana and Yau [5] used the smallest principal angle of the Jacobian matrices before and after RPS as the detection effectiveness metric, and investigated the relationship between the attack detection effectiveness and the associated cost. In the alternating current (AC) power system model, Liu et al. [6] derived explicit approximations of measurement residuals to quantify the effectiveness and hiddenness of RPS. It adopted the sensitivity analysis around the optimum point and derived explicit approximations of residuals, and further jointly optimized the detection effectiveness and hiddenness. The placement of D-FACTS devices in RPS was studied in [7] and [8]. Liu and Wu [7] proposed an optimal placement that uses the minimum number of D-FACTS devices to achieve the maximum rank of the composite matrix. Liu and Wu [8] proposed a graph-based placement method, which simultaneously maximizes the rank of the composite matrix and eliminates unprotected buses.

Since the transmission line reactance changes affect the parameters, such as the power transfer capacity, voltages, and generation outputs, the grid frequency might not be maintained. Zhang and Deng [9] analyzed the impact of line reactance changes on frequency stability, in which an analytical relationship between the frequency stability and perturbation parameters is derived based on the theory of eigenvalue sensitivity. Zhang et al. [10] investigated the impact of line reactance changes on small-signal stability considering the system dynamics and presented a sufficient condition for maintaining the stability of the power system with RPS. Zhang et al. [11] proposed a novel RPS framework

Manuscript received 15 May 2024; accepted 16 June 2024. Date of publication 19 June 2024; date of current version 7 November 2024. This work was supported in part by the U.S. National Science Foundation under Grant 2146156, and in part by the United States Office of Naval Research under Grant N00014-23-1-2777. *(Corresponding author: Hongyu Wu.)*

Bo Liu is with the School of Engineering and Applied Sciences, Washington State University Tri-Cities, Richland, WA 99354 USA (e-mail: bo.liu1@wsu.edu).

Yajing Liu, deceased, was with the Department of Mathematics, Colorado State University, Fort Collins, CO 80523 USA.

Hongyu Wu is with the Mike Wiegers Department of Electrical and Computer Engineering, Kansas State University, Manhattan, KS 66506 USA (e-mail: hongyuwu@ksu.edu).

Digital Object Identifier 10.1109/JIOT.2024.3416839

that explicitly considers system voltage stability by using continuation power flow and voltage stability indices. The limitation of RPS was discussed in [12]. In addition, a novel parameter-estimate-first (PEF)-FDI attack was proposed to remain stealthy to RPS, in which the power network parameter estimation (NPE) is conducted first and then FDI attacks are constructed using the estimated parameters [13].

Machine-learning (ML) methods have been extensively applied to detect FDI attacks as a classification problem. ML detectors have high detection capability and require no extra defense costs, compared with the traditional defense methods using protected meters [14]. Supervised ML-based binary classifiers were presented to check the distance between normal and compromised measurements [2]. Ozay et al. [15] applied multiple supervised methods, including perceptron, k-nearest neighbor (k-NN), support vector machine (SVM), and sparse logistic regression (SLR) to detect FDI attacks. Esmalifalak et al. [16] first applied dimension reduction to the measurements and then utilized distributed SVM to classify the compromised measurements. Sakhnini et al. [17] tested three classification techniques using different heuristic feature selection techniques and concluded that the SVM and the k-NN algorithms overperform artificial neural networks in detecting FDI attacks. Semisupervised learning methods were also applied to detect FDI attacks, and the information obtained from the unlabeled test samples was used for the learning models. The basic idea is to cluster the normal and compromised measurements into distinct regions in the feature spaces. Esmalifalak et al. [16] proposed a Gaussian abnormal detector (GAD) to detect the deviation in measurements, and the outliers were identified as FDI attacks. However, traditional FDI (TFDI) attacks do not consider the pattern of the historical measurements in the attack construction. Since the historical measurements are learned by the ML detectors, ML detectors effectively detect the TFDI attacks that are significantly different from the pattern of the historical measurements.

To the best knowledge of the authors, the only work considering the spatial and temporal limitations in FDI attack construction is [18]. Du et al. [18] presented a single mixed-integer linear programming (MILP) model for high-stealth FDI attacks that aim to overload a set of lines. The attack model minimizes the distance between the compromised measurements and the center of the normal historical measurements. Consequently, the attack (the compromised measurement) is spatially well concealed among normal measurements. In this case, the attack cannot be recognized as an outlier and remains stealthy to advanced anomaly detection methods.

This article is motivated to resolve this drawback of the TFDI attacks by proposing novel FDI attack algorithms that utilize the tensor completion (TC) technique [19], [20]. We propose a TC-based FDI (TC-FDI) attack algorithm, which minimizes the nuclear norm of the historical measurement tensor and maximizes the L1-norm of the incremental voltage. The minimized nuclear norm enables the compromised measurements to follow the patterns of the historical measurements, and the maximized L1-norm aims to ensure a sufficient negative impact. In addition, the proposed attack takes the attack equation of TFDI as a constraint to ensure the spatial relationship of the compromised measurements for remaining stealthy to the Chi-square detector.

Different from [18], the proposed TC-FDI attack neither utilizes the objective function to force the compromised measurements close to the center of normal data nor utilizes constraints to keep the compromised measurements inside the boundary of the normal data. TC-FDI attacks take advantage of the TC technique to resolve the drawback of the TFDI. Since the TC technique can learn the spatial and temporal correlation of normal historical measurements in the tensor, the proposed attack utilizes the TC technique to fill in the compromised measurements. Thus, the attacks remain stealthy to anomaly detection methods.

The contributions of this article are summarized as follows.

1) We propose a defense–attack framework consisting of a hybrid defense model and novel FDI attack algorithms. The hybrid defense framework is composed of a statistic-based attack detector and ML-based attack detectors. To the best of our knowledge, the proposed framework is the first of its kind in constructing stealthy attacks to a hybrid defense model.
2) We present a novel TC-FDI attack algorithm in the AC power system model. TC-FDI attacks account for the patterns of the historical measurements and ensure the spatial relationship of the compromised measurements. The uniqueness of the attack lies in its strategic balance: minimizing the nuclear norm while maximizing the L1-norm, resulting in a significant impact that is challenging to detect. The key mathematical advancement is the introduction of an attacker preference vector to convexify the nonconvex problem.
3) We apply the RPS to detect the proposed TC-FDI attacks by actively perturbing system configuration using distributed flexible AC transmission system (D-FACTS) devices. Further, we use the analysis to demonstrate that the RPS can break the temporal and spatial correlation of compromised measurement by the TC-FDI attacks.

The remainder of this article is organized as follows. We provide preliminaries and related work in Section II. In Section III, we propose the TC-FDI attack algorithm in the AC power system model. In Section IV, we show how the RPS can be used to detect the TC-FDI attacks. Case studies are conducted in Section V, and this work is concluded in Section VI.

II. Preliminaries

In this section, we provide background knowledge of tensor, TC, SE, FDI attacks, and the ML-based attack detectors as preliminaries for the follow-up sections.

A. Notation

Variables frequently used are summarized in Table I, where boldfaced lowercase letters stand for vectors, and uppercase letters stand for matrices and tensors. From the attacker's perspective, subscript 0 denotes variables before attacks. For

TABLE I
NOMENCLATURE

Symbol	Definition
$\mathbf{x}$	System state vector
$\boldsymbol{a}$	FDI attack vector
$\mathbf{z}$	Measurement vector
$\mathbf{Z}_0$	Historical measurement tensor
$\mathbf{Z}_a$	Compromised measurement tensor
$\mathbf{H}$	DC measurement matrix in state estimation
r_{ij}	Susceptance of line i–j (between bus i and j)
n	Total number of system buses
m	Total number of measurements
idx^t	Index vector of time instants
idx^{bus}	Index vector of buses

example, $\mathbf{z}_0$ and $\mathbf{z}_a$ stand for uncompromised and compromised measurement vectors, respectively. From the defender's perspective, subscript 0 denotes variables before RPSs. For example, $\mathbf{H}_0$ represents the original measurement matrix before an RPS, and $\mathbf{H}_t$ stands for the one after implementation of an RPS at time t. In addition, variables preceded by Δ represent changes in the variables. For example, $\Delta\mathbf{x}$ and $\Delta\mathbf{z}$ represent the malicious incremental voltage and malicious incremental measurement injected by the attacker, respectively.

B. Tensor and Tensor Completion

A tensor is a multidimensional array, whose order is the number of dimensions. Let $\mathbf{M} \in \mathbb{R}^{I_1 \times I_2 \times I_3}$ be a third-order tensor with elements $\mathbf{M}(i, j, t)$, where $i \in \{1, 2, \ldots, I_1\}, j \in \{1, 2, \ldots, I_2\}$, and $t \in \{1, 2, \ldots, I_3\}$. Slabs are 2-D sections of a tensor that is defined by fixing one index. For a third-order tensor, there are three types of slabs: 1) horizontal slabs $\mathbf{M}(i, :, :)$; 2) vertical slabs $\mathbf{M}(:, j, :)$; and 3) frontal slabs $\mathbf{M}(:, :, t)$. Let $\mathbf{M}_{(i)}$ denote the mode-i matricization of $\mathbf{M}$. Specifically, the unfold operation along the ith mode on a third-order tensor $\mathbf{M}$ is defined as $\mathbf{M}_{(i)} \in \mathbb{R}^{I_j \times I_t}$, where $i, j, t \in \{1, 2, 3\}$ and $i \neq t, j \neq t, i \neq j$.

TC is a tool for recovering missing or unobserved entries in tensors based on the low-rank property. TC has been used in image/video inpainting [20], computer vision [19], ML [21], and the SE in distribution power systems [22]. TC can learn the spatial and temporal correlation of available entries in the tensor. The TC problem can be modeled as a convex optimization problem by minimizing the nuclear norm [20]

$$\min_{\mathbf{M}} \sum_{i=1}^{3} a_i \left\| \mathbf{M}_{(i)} \right\|_* \quad \text{s.t. } \mathbf{M}_\Omega = \mathbf{T}_\Omega \tag{1}$$

where $\mathbf{M}$ is the third-order tensor to be recovered, and $\mathbf{T}$ is the observation tensor, Ω is the set of known elements in $\mathbf{T}$, and $\sum_{i=1}^{3} a_i \|\mathbf{M}_{(i)}\|_*$ is the tensor trace norm of a third-order tensor, defined in [20], with $\sum_{i=1}^{3} a_i = 1$ and $a_i \geq 0$. Note that the nuclear norm operator sums the singular values of a given matrix to approximate the rank of the matrix, which is the tightest convex envelope for the rank of the matrix [20].

C. FDI Attack Against Power System State Estimation

An FDI attack manipulates SCADA measurements to mislead the system operator's estimated voltage states by injecting an attack vector $\mathbf{a}$, i.e., $\mathbf{z}_a = \mathbf{z}_0 + \mathbf{a}$. The FDI attack vector is delicately constructed to remain stealthy to the Chi-square detector in SE. In the AC-FDI attack, if an FDI attack vector $\mathbf{a}$ can be calculated by (3), the estimation residual remains the same before and after the FDI attack, i.e., $\gamma_a = ||(\mathbf{z}_0 + \mathbf{a}) - h(\mathbf{x} + \Delta\mathbf{x})||_2 = ||\mathbf{z}_0 - h(\mathbf{x})||_2$ [23]

$$\mathbf{a} = \mathbf{h}(\mathbf{x} + \Delta\mathbf{x}) - \mathbf{h}(\mathbf{x}). \tag{2}$$

D. Statistic-Based Bad Data Detectors

The Chi-square detector is a widely used bad data detector (BDD) to detect the bad data in measurements. BDD calculates the score $\gamma = \sum_{i=1}^{m} [(z_i - h_i(\widehat{x}))^2/\sigma_i^2]$, where z_i is the ith measurement, $h_i(\widehat{x})$is the ith estimated measurement, and σ_i^2 is the variance of the error in z_i. If $\gamma < \gamma_{th}$ holds where $\gamma_{th} = \chi^2_{(m-n),\alpha}$ is the threshold to ensure BDD has a false alarm rate at $1 - \alpha$, it infers that the system is free of bad data.

The cumulative sum (CUSUM) detector, introduced by Page [24], is a statistical technique used for the detection of shifts or changes in a process or system over time. Assume that the stream is initially Gaussian distributed $N(\mu, \sigma^2)$, let S_i denote the high CUSUM value to detect a positive anomaly, and T_i denote the low CUSUM value to detect a negative anomaly. S_i and T_i can be updated by $S_i = \max(0, S_{i-1} + [(x_i - \mu)/\sigma] - k)$ and $T_i = \max(0, T_{i-1} - [(x_i - \mu)/\sigma] - k)$ with $S_0 = 0$ and $T_0 = 0$, where x_i is the ith stream data. A change can then be detected if $S_i > h$ or $T_i > h$. Note that the bias k and the threshold h are control parameters, which need to be chosen according to the application.

The largest normalized residual (LNR) detector is one of the most widely used tools to identify the bad data, after the bad data is detected. In the LNR detector, each residue $r_i = z_i - h_i(\widehat{\mathbf{x}})$ is normalized with the diagonal elements of the residual covariance matrix $\boldsymbol{\Omega}$ by (3). Then, the largest normalized residue is compared with a threshold value

$$r_i^N = \frac{r_i}{\Omega_{ii}} \tag{3}$$

where r_i^N is the normalized residue of the ith measurement, $\Omega_{ii} = (1/\mathbf{W}_{ii}) - \mathbf{H}_i(\widehat{\mathbf{x}})\mathbf{G}_i$, $\mathbf{G} = [\mathbf{H}^T(\widehat{\mathbf{x}})\mathbf{W}\mathbf{H}^T(\widehat{\mathbf{x}})]^{-1}\mathbf{H}^T(\widehat{\mathbf{x}})$, $\mathbf{H}_i$ is the ith row of Jacobian matrix $\mathbf{H}$, $\mathbf{W}$ is a diagonal covariance matrix $\mathbf{W} = \text{diag}(\sigma_1^{-2}, \sigma_2^{-2}, \ldots, \sigma_m^{-2})$, and σ_i^2 is the variance of the error in the ith measurement z_i.

E. Machine-Learning FDI Detectors

ML methods have been applied to detect FDI attacks based on the fact that normal data and compromised data (due to attacks) tend to be separated in a certain projected space. In this article, multiple ML-based detectors are applied to evaluate the stealthiness of the proposed attack, including k-NN, SLR, SVM, and GAD. Here, we briefly introduce the SVM detector [16] since it supports the visualization of the attack detection. The visualization can help highlight the

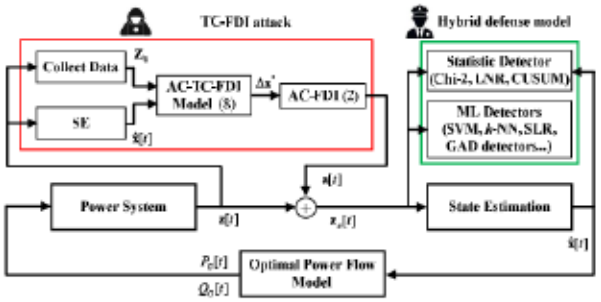


Fig. 1. Framework of TC-FDI attack against the hybrid defense model.

characteristics of the proposed TC-FDI attacks in the simulation. A principal component analysis (PCA) is first applied to project the measurement data to a low-dimensional space. The dimension reduction overcomes the challenge brought by the high-dimensionality and redundancy of measurement data in practical power systems, and it is also beneficial for visualization. Then, the supervised classification method SVM is proposed to detect stealthy FDI attacks [15], [16].

k-NN is widely used for classification problems as a nonparametric supervised learning method. The k refers to the number of closest neighbors to a given point, which serves as the basis for predicting its label. SLR, a popular technique for binary classification problems, extends the basic logistic regression model by allowing for polynomial terms in the input variables, making it capable of capturing nonlinear relationships between the predictors and the response. The GAD is one density-based anomaly detection method, which builds a boundary around the training data and sets a threshold on the estimated density. It is assumed that the training data are normally distributed. GAD uses Gaussian density function to estimate the probability of data points, and a threshold is selected to identify the abnormal data.

III. Tensor-Completion-Based FDI Attack

In this section, we present a defense–attack framework for the TC-FDI attacks against a hybrid defense model. We first define the capability and knowledge of the attacker in TC-FDI attacks and then propose the mathematical model of TC-FDI attacks in the AC power system model.

A. Defense–Attack Framework for TC-FDI Attacks

We present a defense–attack framework consisting of a hybrid defense model and a TC-FDI attacker in Fig. 1.

The hybrid defense model is proposed to detect FDI attacks using both statistic-based attack detectors and ML-based detectors. The TC-FDI attacker utilizes the TC technique to maintain the attack stealthiness to the hybrid defense model and ensure a sufficient negative impact on the system operation.

We propose the TC-FDI attack algorithm in Algorithm 1. The input of the algorithm is 1) the attacked buses $\text{idx}_a^{\text{bus}}$ for maliciously manipulating their voltage; 2) the length of time steps for eavesdropping SCADA measurements; and 3) the system configuration (line impedance and system topology). In

Algorithm 1 TC-FDI Attack Algorithm

Input: Length of the historical measurement T, attacked buses
Output: Compromised measurements $\mathbf{z}_a$
1: **Initialization:** A null historical measurement tensor $\mathbf{Z}_0 = \varnothing$
2: **while** (the number of frontal slab of $Z_0 < T$) // Construct $\mathbf{Z}_0$
3: Eavesdrop SCADA measurements $\mathbf{z}_t$ at time t
4: Append $vec2mat(\mathbf{z}_i)$ to tensor $\mathbf{Z}_0$ as the last frontal slab
5: Wait for next SCADA measurements at time $t+1$
6: **end while**
7: Apply AC SE to estimate the voltage $\widehat{\mathbf{x}}_T$ at time t
8: Calculate Jacobian matrix $\mathbf{H}(\widehat{\mathbf{x}}_T)$ to linearize the AC-FDI model
9: Run TC-FDI model (14) to calculate $\Delta\mathbf{x}^*$
10: Calculate the compromised measurement $\mathbf{z}_a$ according to (5)
11: **return** $\mathbf{z}_a$

the first step of Algorithm 1, the attacker constructs a historical measurement tensor $\mathbf{Z}_0$. Specifically, the attacker constructs a third-order tensor $\mathbf{Z}_0 \in \mathbb{R}^{I\times J\times T}$ that collects the SCADA measurements for T time instants. The tensor takes the form of MEASUREMENT×BUS×TIME. The element $\mathbf{Z}_0(i,j,t)$ represents the measurement i for Bus j eavesdropped at time t. The measurement type in the TC-FDI attacks could include active and reactive power injection, active and reactive power flow, and voltage magnitudes in the AC model. Since the number of transmission lines attached to each bus is different, it is challenging to formulate a tensor that integrates the power flow of all lines. Since at least one transmission line can be assigned to each bus, we can integrate the power flow of one transmission line associated with each bus into the tensor, as shown in Fig. 2.

Assume the attacker collects measurements for T time instants, and then launches attack. In order to utilize the TC technique, the attacker constructs the compromised measurement tensor $\mathbf{Z}_a$ based on the vector-form equation $\mathbf{z}_a = \mathbf{z}_0 + \mathbf{a}$ which we introduced in Section II-D. The following equations hold:

$$\begin{aligned}\mathbf{Z}_a(:,:,\text{idx}_a^t) &= \mathbf{Z}_0(:,:,\text{idx}_a^t) + \mathbf{A}\\ \mathbf{Z}_a(:,:,\text{idx}_0^t) &= \mathbf{Z}_0(:,:,\text{idx}_0^t)\end{aligned} \tag{4}$$

where $\text{idx}_a^t = \{T\}$ and $\text{idx}_0^t = \{1, 2, \ldots, T-1\}$; $\mathbf{A}$ is the matrix form of $\mathbf{a}$, and $\mathbf{a}$ is the malicious measurements injected by the attacker whose value is determined by the malicious incremental voltage $\Delta\mathbf{x}$ according to (2).

The compromised tensor $\mathbf{Z}_a$ and its frontal slab $\mathbf{Z}_a(:,:,\text{idx}_a^t)$ are shown in Fig. 2, where it is assumed that the attacker aims to compromise the voltage of Buses 3 and 4 ($\text{idx}_a^{\text{bus}} = \{3,4\}$) at time T ($\text{idx}_a^t = \{T\}$) in the IEEE 14-bus system. Four transmission lines are connected to Bus 2, and any one of these lines is selected as the power flow measurement to construct the tensor. For example, we can take the power flow of Line 2-5 for Bus 2, Line 3-2 for Bus 3, and Line 4-3 for Bus 4 to construct the tensor. The measurements related to the attacked buses (Buses 3 and 4) and their neighbors (Buses 2, 5, 7, and 9) need to be compromised, according to the construction rule of FDI attacks (3) in [23]. Note that idx_a and idx_0 are the index vectors of compromised and uncompromised measurements in the frontal slab, respectively. In Fig. 2, the compromised measurements, highlighted in red, are the missing values from the attacker's perspective.

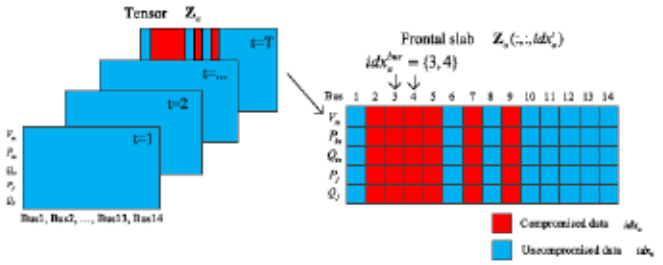


Fig. 2. Compromised tensor and its frontal slab at T time instant.

If an attack modifies the voltage of Buses 3 and 4 without considering the historical measurement pattern, it is likely that the compromised measurements can be outliers. In this case, the attack can be easily detected by ML detectors. Since the TC technique can learn the spatial and temporal correlation of normal historical measurements in the tensor, the proposed attack utilizes the TC technique to fill in the compromised measurements. Consequently, the completed compromised measurements (the red area) can avoid significant distinct from the pattern of historical measurements.

In the second step of Algorithm 1, the attacker utilizes the TC-FDI models proposed in the following section to determine the optimal incremental voltage state $\Delta\mathbf{x}^*$. Note that the attacker needs to estimate voltage at time T before the TC-FDI attacks. In the transmission system, the SE redundant factor is usually around 2.5. It is likely that the voltage magnitude, active power injection, and reactive power injection of some buses have not been measured. Therefore, estimated measurements by the SE also assist in filling the missing entries in the defined tensor.

In the last step of the TC-FDI attack, the attacker can use the TFDI model to calculate the malicious measurements at time T using the optimal malicious incremental voltage determined by the TC-FDI model. The compromised measurements in the TC-FDI attack at time T can be expressed as follows:

$$\mathbf{z}_a^T = \mathbf{z}_0^T + h\big(\widehat{\mathbf{x}}_T + \Delta\mathbf{x}^*\big) - h\big(\widehat{\mathbf{x}}_T\big). \tag{5}$$

The estimation residual after the attack is the same as the estimation residual before the attack in the noiseless condition, as shown in (8). Thus, the estimation residual of the attack is less than the threshold, indicating stealthy to the Chi-square detector

$$\begin{aligned}\gamma_a &= \left\|\mathbf{z}_a - h\big(\widehat{\mathbf{x}} + \Delta\mathbf{x}^*\big)\right\|_2 \\ &= \left\|\mathbf{z}_0 + h\big(\widehat{\mathbf{x}} + \Delta\mathbf{x}^*\big) - h\big(\widehat{\mathbf{x}}\big) - h\big(\widehat{\mathbf{x}} + \Delta\mathbf{x}^*\big)\right\|_2 \\ &= \left\|\mathbf{z}_0 - h\big(\widehat{\mathbf{x}}\big)\right\|_2 < \gamma_{th}.\end{aligned} \tag{6}$$

Since the SE residual after the attack is the same as the estimation residual before the attack, there is no difference between the averaged residual of normal measurements and the averaged residual of compromised measurements. Since the CUSUM detector is designed to detect the shift of averaged estimation residual, the TC-FDI attacks are stealthy to the CUSUM detector. Since each of the compromised measurements follows Kirchhoff's circuit laws and power injection balance, the compromised measurements should not be identified as bad data by the LNR detector. In our case studies, we will evaluate the stealiness of TC-FDI attacks against the Chi-squared detector, LNR detector, and CUSUM detector in noisy conditions.

B. TC-FDI Attack Mathematical Model

In TFDI attacks, there is a tradeoff in selecting the value of $\Delta\mathbf{x}$. From the perspective of attack consequences, the FDI attacks with large $\Delta\mathbf{x}$ lead to a sufficiently large negative impact on the power system operation, whereas the FDI attacks with small $\Delta\mathbf{x}$ may have a trivial negative impact. From the perspective of attack detection, FDI attacks with large $\Delta\mathbf{x}$ value are more likely to be detected by the ML-based detectors than those with small $\Delta\mathbf{x}$. Thus, it is necessary to balance the tradeoff to select an optimal incremental voltage value that maintains a sufficient impact on the power system operation while remaining stealthy to the ML-based detectors.

This article proposes a novel TC-FDI attack to calculate an optimal malicious incremental voltage, which accounts for the historical measurement pattern with sufficient impact on the power system operation. The TC-FDI attack is proposed in (7), which minimizes the nuclear norm of the compromised measurement tensor and maximizes the L1-norm of the malicious incremental voltage angle

$$\min_{\mathbf{Z}^a_{(1)},\mathbf{Z}^a_{(2)},\mathbf{Z}^a_{(3)},\Delta\mathbf{x}} \sum_{i=1}^{3}\alpha_i\left\|\mathbf{Z}^a_{(i)}\right\|_* - \lambda\|\Delta\mathbf{x}\|_1 \tag{7}$$

$$\text{s.t. } \mathbf{a} = h\big(\widehat{\mathbf{x}}_T + \Delta\mathbf{x}\big) - h\big(\widehat{\mathbf{x}}_T\big) \tag{7.1}$$

$$\text{vec}\Big(\mathbf{Z}^a_{(i)}\big(\text{idx}^i_a\big)\Big) = \text{vec}\Big(\mathbf{Z}^0_{(i)}\big(\text{idx}^i_a\big)\Big) + \mathbf{a}\ \ i = 1, 2, 3 \tag{7.2}$$

$$\text{vec}\Big(\mathbf{Z}^a_{(i)}\big(\text{idx}^i_0\big)\Big) = \text{vec}\Big(\mathbf{Z}^0_{(i)}\big(\text{idx}^i_0\big)\Big)\ \ i = 1, 2, 3 \tag{7.3}$$

$$\Delta\mathbf{x}(j) = \mathbf{0}\quad j \in \text{idx}^{\text{bus}}_0 \tag{7.4}$$

$$\Delta\mathbf{x}_{lb}(j) \le \Delta\mathbf{x}(j) \le \Delta\mathbf{x}_{ub}(j)\quad j \in \text{idx}^{\text{bus}}_a \tag{7.5}$$

where the decision variable $\Delta\mathbf{x}$ is composed of the incremental voltage magnitude and incremental voltage angle; α_i is the weight in the nuclear norm for the ith mode of tensor, and this article sets $\alpha_i = 1/3$; λ is the positive weight parameter; $\text{idx}^{\text{bus}}_0$ and $\text{idx}^{\text{bus}}_a$ are the index of buses free of attack and the index of attacked buses, respectively; $\text{idx}^i_a \in \mathbb{R}^m$ and $\text{idx}^i_0 \in \mathbb{R}^{I\times J\times T-m}$ are the index vector of compromised and uncompromised measurements in the ith mode of tensor $\mathbf{Z}^a_{(i)}$, respectively. *vec* is a vectorization operator that converts selected entities in a matrix into a vector. For example, $\text{vec}(\mathbf{Z}^a_{(i)}(\text{idx}^i_a))$ is a vector consisting of the entities in the matrix $\mathbf{Z}^a_{(i)}$ selected by idx^i_a, and the dimension of $\text{vec}(\mathbf{Z}^a_{(i)}(\text{idx}^i_a))$ is the same as the dimension of idx^i_a, i.e., $\text{vec}(\mathbf{Z}^a_{(i)}(\text{idx}^i_a)) \in \mathbb{R}^{|\text{idx}^i_a|}$. Note that we replace the voltage state $\mathbf{x}_T$ with the attacker's estimated state $\widehat{\mathbf{x}}_T$, as the true state $\mathbf{x}_T$ is unknown.

Constraint (7.1) is the traditional AC-FDI model. Constraints (7.2) and (7.3) define the 1st mode, 2nd mode, and 3rd mode of the tensor under attack $\mathbf{Z}^a_{(i)}$. Specifically, idx^i_a in (7.2) identifies all entities in the mode i of the tensor $\mathbf{Z}^a_{(i)}$ to be compromised. $\text{vec}(\mathbf{Z}^a_{(i)}(\text{idx}^i_a))$ is a vector of the compromised measurements, which are equal to the sum of the vector of original measurements $\text{vec}(\mathbf{Z}^0_{(i)}(\text{idx}^i_a))$ and the

attack injection $\mathbf{a}$. In (7.3), idx_0^i identifies all entities in $\mathbf{Z}_{(i)}^a$ free of attacks. $\text{vec}(\mathbf{Z}_{(i)}^a(\text{idx}_0^i))$ is a vector of the measurements free of attack, which is equal to the original measurements $\text{vec}(\mathbf{Z}_{(i)}^0(\text{idx}_0^i))$. Constraint (7.4) ensures that the voltage of the uncompromised buses in $\text{idx}_0^{\text{bus}}$ remains unchanged. In (7.5), lower bound $\Delta\mathbf{x}_{lb}$ and upper bound $\Delta\mathbf{x}_{ub}$ are introduced to allow but limit the malicious incremental voltage for the attacked buses. We want to highlight that $\Delta\mathbf{x} = 0$ is a feasible solution, but it is not the optimal solution since the objective function aims to maximize the $\|\Delta\mathbf{x}\|_1$.

However, it is challenging to solve the TC-FDI attack in (7) due to the nonlinear constraints. To address this issue, we apply the first-order Taylor series expression on $\mathbf{h}(\cdot)$ to linearize the relationship between the measurements and states, i.e., $\mathbf{h}(\mathbf{x}_T + \Delta\mathbf{x}) = \mathbf{h}(\mathbf{x}_T) + \mathbf{H}(\mathbf{x}_T)\Delta\mathbf{x}$, where $\mathbf{H}(\mathbf{x}_T) = \partial\mathbf{h}(\mathbf{x})/\partial\mathbf{x}|_{\mathbf{x}=\mathbf{x}_T}$ is the Jacobian matrix of $\mathbf{h}(\mathbf{x})$ at $\mathbf{x} = \mathbf{x}_T$. Note that since the Jacobian matrix is also needed to estimate the voltage in the traditional AC-FDI attacks, the calculation of the Jacobian matrix is not an extra burden for the TC-FDI attack.

In addition, since the objective function is a sum of a convex function and a concave function, the optimization formulation (7) is a nonconvex optimization problem. We transform the concave term to a plane $p'\Delta\mathbf{x}$. Specifically, we convexify the problem by introducing an attacker preference vector $p \in \mathbb{R}^n$. The entries in p reflect the attacker's intention for each bus in the system. The attacker can set the entries of p as 1, -1, and 0 to decrease, increase, and retain the voltage, respectively. Multiple open-source packages can be used to solve the following convex problem (7), such as CVX [25] and CVXPY [26]:

$$\begin{aligned}&\min_{\mathbf{Z}_{(1)}^a,\mathbf{Z}_{(2)}^a,\mathbf{Z}_{(3)}^a,\Delta\mathbf{x}} \sum_{i=1}^{3}\alpha_i\left\|\mathbf{Z}_{(i)}^a\right\|_* + \lambda p'\Delta\mathbf{x}\\ &\text{s.t. } \mathbf{a} = \mathbf{H}(\widehat{\mathbf{x}}_T)\Delta\mathbf{x}\\ &\quad (7.2)-(7.5).\end{aligned} \tag{8}$$

In summary, there are two main steps in constructing TC-FDI attacks. In the first step, the attacker solves the convex TC completion optimization model (8) to determine the optimal injected voltage $\Delta\mathbf{x}^*$, in which linearization is employed to make the problem solvable. In the second step, the attacker constructs the compromise measurements using $\Delta\mathbf{x}^*$ according to (5), in which the nonlinear relation $h(x)$ is used to accurately calculate the compromised measurement.

IV. Detection of TC-FDI Attacks Using RPS

A. RPS Model

Since the proposed TC-FDI attacks are designed to be stealthy to both the statistic-based detectors and the ML-based detectors, it is necessary to provide extra defense for the power systems. We propose to apply the RPS in the physical layer of power systems to detect TC-FDI attacks, as shown in Fig. 3. This work adopts the graph-based placement method [8] to determine the allocation of D-FACTS devices in RPS, which ensures the maximum attack detection effectiveness with a limited number of D-FACTS devices.

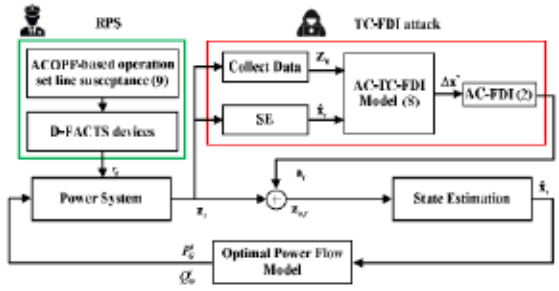


Fig. 3. Framework of RPS applied to detect TC-FDI attacks.

According to the smart wire company, D-FACTS devices use SHA-256, one of the most secure hashing algorithms, to ensure the cryptographic integrity of all messages [27], such that the system operator can securely send the setpoints to D-FACTS devices. In addition, RPS updates the impedances of the lines, leaving a limited attack window for the attacker, who applies data-driven methods [28] to learn the system configuration by collecting SCADA measurements. Thus, the attacker does not have access to the impedances of all lines equipped with D-FACTS devices, which is widely adopted in RPS work.

The system operator is responsible for operating RPS (determine the setpoints of D-FACTS devices) based on load conditions. This work proposes an operation model (9) to modify the impedance of the transmission lines equipped with D-FACTS devices with two benefits. First, the controllable line impedance enables system operators to control power flow, which can be used to reduce the generation costs and system losses. Second, the varying system configuration introduced by RPS can prevent attackers from knowing the true system configuration and thus contributes to detecting FDI attacks. Thus, we apply an ACOPF model considering D-FACTS devices as an RPS operation method to achieve these two benefits simultaneously. In the ACOPF model considering D-FACTS devices, the reactance of transmission lines equipped with D-FACTS devices is introduced as decision variables in the traditional ACOPF. The objective of the ACOPF model is to minimize the weighted sum of the generation costs and system losses, formulated as follows:

$$\min_{\mathbf{X}} \cos\ t(\mathbf{X}) + \kappa\,\text{loss}(\mathbf{X}) \tag{9}$$

$$\text{s.t. } g_P(\theta, \mathbf{V}, \mathbf{P}_\mathbf{g}, \mathbf{r}) = 0 \tag{9.1}$$

$$g_Q(\theta, \mathbf{V}, \mathbf{Q}_\mathbf{g}, \mathbf{r}) = 0 \tag{9.2}$$

$$h_f(\theta, \mathbf{V}, \mathbf{r}) \le 0 \tag{9.3}$$

$$h_t(\theta, \mathbf{V}, \mathbf{r}) \le 0 \tag{9.4}$$

$$\theta_0 = \theta_{\text{ref}} \tag{9.5}$$

$$v_i^{\min} \le v_i \le v_i^{\max}, \quad i = 1, \ldots, n_b \tag{9.6}$$

$$p_i^{\min} \le p_i \le p_i^{\max}, \quad i = 1, \ldots, n_g \tag{9.7}$$

$$q_i^{\min} \le q_i \le q_i^{\max}, \quad i = 1, \ldots, n_g \tag{9.8}$$

$$(1-\tau)r_i^0 \le r_i \le (1+\tau)r_i^0, \quad i = 1, \ldots, n_{\text{DF}} \tag{9.9}$$

where the decision variables $\mathbf{X} = [\theta\ \mathbf{V}\ \mathbf{P}_\mathbf{g}\ \mathbf{Q}_\mathbf{g}\ \mathbf{r}]$ are voltage angle, voltage magnitude, generator active generation, generator reactive generation, and the reactance of D-FACTS

lines, respectively; and n_b, n_l, n_g, and n_{DF} are the number of buses, lines, generators, and D-FACTS devices, respectively. $cost(\mathbf{X})$ is generation cost with a quadratic function of active generator generation, and loss($\mathbf{X}$) is system loss. κ is a positive weight parameter. In the proposed ACOPF model, (9.1) and (9.2) are nonlinear equality constraints of the nodal active and reactive power balance, respectively. Constraints (9.3) and (9.4) are nonlinear inequality of line power flow limits corresponding to lines starting from from-end and to-end, respectively. Constraint (9.5) sets the reference for the voltage angle of the slack-bus, and (9.6) is voltage magnitude constraint of each bus. Constraints (9.7) and (9.8) represent the constraints on the active and reactive of power generation. In (9.9), τ in % reflects the physical capacity of D-FACTS devices.

The following sections show that the RPS is able to break both the temporal and spatial correlation of compromised measurement in TC-FDI attacks. The sensitivities of the estimation residual against reactance changes are derived in [6], which provides a pathway to design a more effective RPS specific to TC-FDI attacks. However, designing RPS specific to TC-FDI attacks is beyond the scope of this work and will be investigated in our future work.

B. Impact of RPS on Temporal Correlation in TC-FDI

One objective of the proposed TC-FDI models is to minimize the nuclear norm of the compromised measurement tensor. In the dc noiseless condition, the compromised measurement tensor $\mathbf{Z}_a$ can be constructed by defining its frontal slab as follows:

$$\mathbf{Z}_a(:,:,t) = \begin{cases} \mathbf{L}\mathrm{diag}\left(\mathbf{H}_0\mathbf{x}_t^0\right)\mathbf{S} & (t < T) \\ \mathbf{L}\mathrm{diag}\left(\mathbf{H}_0\left(\mathbf{x}_t^0 + \Delta\mathbf{x}\right)\right)\mathbf{S} & (t = T) \end{cases} \tag{10}$$

where diag(.) is a diagonal matrix operator, $\mathbf{H}_0$ is the original measurement matrix without RPS, and $\mathbf{L}$ and $\mathbf{S}$ are constant matrices that perform elementary column or row operations for converting $\mathrm{diag}(\mathbf{H}_0\mathbf{x}_t^0)$ to the tensor $\mathbf{Z}_a$ based on the definition of $\mathbf{Z}_a$. The superscript of $\mathbf{x}_t^0$ indicates that the voltage is free of RPS.

The RPS frequently changes the susceptance of the lines equipped with D-FACTS devices according to (9). As the $\mathbf{H}$ matrix in the SE contains the information of line parameters, the $\mathbf{H}$ matrix under RPS is time-variant. Assume that $\mathbf{H}_t$ is the measurement matrix under the RPS at time instant t. In RPS, it is reasonable to assume that the attacker utilizes $\mathbf{H}_0$ to construct the TC-FDI attacks for the following reasons. First, the attacker may not detect the existence of RPS deployed in the field. Second, the attacker can fail to obtain or estimate accurate knowledge of the current system configuration due to the narrow attack window under RPS. Therefore, the frontal slab of the compromised measurement tensor constructed by the TC-FDI attack under the RPS can be expressed as follows:

$$\mathbf{Z}_a^{\mathrm{MTD}}(:,:,t) = \begin{cases} \mathbf{L}\mathrm{diag}((\mathbf{H}_0 + \Delta\mathbf{H}_t)\mathbf{x}_t)\mathbf{S} & (t < T) \\ \mathbf{L}\mathrm{diag}((\mathbf{H}_0 + \Delta\mathbf{H}_t)\mathbf{x}_t + \mathbf{H}_0\Delta\mathbf{x})\mathbf{S} & (t = T). \end{cases} \tag{11}$$

Comparing $\mathbf{Z}_a^{\mathrm{MTD}}$ and $\mathbf{Z}_a$, the RPS breaks the temporal correlation of the measurements in the TC-FDI attacks in the following two aspects. First, when the system is free of attacks ($t < T$), RPS influences the temporal correlations of historical measurements, since the changes in the system configuration $\Delta\mathbf{H}_t$ can cause nodal voltage changes and the measurement changes at each time instant. Second, when the system is under the attacks ($t = T$), RPS makes the injected measurement $\mathbf{H}_0\Delta\mathbf{x}$ inconsistent with previous measurements under different system configurations $\mathbf{H}_0 + \Delta\mathbf{H}_t$. Therefore, the optimal solution of TC-FDI attack is also impacted by $\Delta\mathbf{H}_t$ introduced by RPS.

C. Impact of RPS on Spatial Correlation in TC-FDI

The TC-FDI model takes the FDI model (7.1) as constraint such that the compromised measurements can satisfy the spatial correlation, i.e., the subject to the physical law of the power system. RPS can break the spatial correlation of the compromised measurements. Under the RPS, the compromised measurements in the TC-FDI attack at time T in a noiseless condition can be expressed as $\mathbf{z}_a^T = \mathbf{H}_T\mathbf{x}_T + \mathbf{H}_0\Delta\mathbf{x}^*$. According to (3), the estimation residual in the defender's SE is zero, i.e., $\gamma_{\mathrm{MTD}} = 0$, if and only if $\mathbf{H}_0\Delta\mathbf{x}^* \in \mathrm{col}(\mathbf{H}_T)$. As $\mathbf{H}_0 \neq \mathbf{H}_T$, the estimation residual is likely larger than zero, indicating the detection of TC-FDI attacks. Specifically, the estimation residual of the TC-FDI attack under the RPS can be expressed in (14). This is because the attacker uses incorrect system configuration to construct the attack vector, which violates the physical law of the power system. Therefore, the RPS can break the spatial correlation of the compromised measurement vector in TC-FDI attacks

$$\begin{aligned} \gamma_{\mathrm{MTD}} &= \left\| (\mathbf{H}_T\mathbf{x}_T + \mathbf{H}_0\Delta\mathbf{x}) - \mathbf{H}_T\left(\mathbf{H}_T^T\mathbf{H}_T\right)^{-1}\mathbf{H}_T^T(\mathbf{H}_T\mathbf{x}_T + \mathbf{H}_0\Delta\mathbf{x}) \right\| \\ &= \left\| \left(I - \mathbf{H}_T\left(\mathbf{H}_T^T\mathbf{H}_T\right)^{-1}\mathbf{H}_T^T\right)\mathbf{H}_0\Delta\mathbf{x} \right\|. \end{aligned} \tag{12}$$

D. TC-FDI Attack With Parameter-Estimate-First Strategy

If TC-FDI attackers detect that RPS is deployed in the system, the attackers would know that inaccurate line impedance used in the TC-FDI attack construction can cause the attack detected by RPS. Inspired by [13], we further enhance the TC-FDI attacks with a PEF strategy in the context of RPS. PEF strategy estimates the impedance of unknown lines related to attack buses, and then the attacker constructs TC-FDI attacks using the estimated impedance. Specifically, the PEF strategy uses SCADA measurements of single or multiple sampling instants to estimate the line impedance by solving a weighted least-square NPE in

$$\min_{\widehat{\mathbf{x}},\widehat{\mathbf{p}}} \sum_{t=1}^{N} (\mathbf{z}_t - \mathbf{h}(\widehat{\mathbf{x}},\widehat{\mathbf{p}}))^T\mathbf{W}(\mathbf{z}_t - \mathbf{h}(\widehat{\mathbf{x}},\widehat{\mathbf{p}})) \tag{13}$$

where $\mathbf{z}_t$ is the SCADA measurement sampled at instant t, N is the number of measurement vectors, $\widehat{\mathbf{x}}$ is the bus voltage state vector, $\widehat{\mathbf{p}}$ is the line impedance state vector, $\mathbf{W}$ is a diagonal covariance matrix $\mathbf{W} = \mathrm{diag}(\sigma_1^{-2}, \sigma_2^{-2}, \ldots, \sigma_m^{-2})$, and σ_i^2 is the variance of the error in the ith measurement.

Hereafter, we use the PEF-TC-FDI attack to refer to the TC-FDI attack with the PEF strategy. In the PEF-TC-FDI attack,

the attacker first estimates the impedance of unknown lines $\widehat{\mathbf{p}}$ related to attacked buses by (13), calculates the incremental voltage $\Delta\mathbf{x}^*$ by (8), and then constructs TC-FDI attacks by (14) using $\widehat{\mathbf{p}}$ and $\Delta\mathbf{x}^*$

$$\mathbf{z}_a = \mathbf{z}_0 + h\big(\widehat{\mathbf{x}}_T + \Delta\mathbf{x}^*, \widehat{\mathbf{p}}\big) - h\big(\widehat{\mathbf{x}}_T, \widehat{\mathbf{p}}\big). \tag{14}$$

Compared with TC-FDI attacks, PEF-TC-FDI attacks have an extra parameter estimation step. However, the PEF strategy, in fact, weakens the attacker's knowledge of the power system, making TC-FDI attacks more realistic. In the case study, we will evaluate the stealthiness of PEF-TC-FDI attacks against RPS.

V. Numerical Results

A. Test Systems and Simulation Setting

We first evaluate the performance of the TC-FDI attacks against ML detectors and statistic-based detectors, and then evaluate the detection effectiveness of the RPS against the TC-FDI attacks.

An hourly load profile of ERCOT [29] is adopted and scaled. Historical voltage states and measurements in the training and testing data set are generated by MATPOWER [30]. The measurements include active and reactive power injection, active and reactive power flow, and voltage magnitude. We adopt a 2.5 redundancy factor (i.e., a ratio between the numbers of measurements and system states) to guarantee the observability of the system in AC-SE [31], [32]. The measurement noise is assumed to be Gaussian distributed with zero mean and the standard deviation as 1% of the actual measurement. The proposed TC-FDI attacks are modeled and solved by the CVX package [25]. The ML detectors are trained and tested using Sklearn package [33].

We constructs tensors using the active power injection, reactive power injection, and voltage magnitude measurements. The historical measurement tensor contains the measurements of 50 time instants. Specifically, the tensor size is $3\times14\times50$. In TFDI attacks, we use TFDI attack magnitude (AM) μ to measure the range of incremental voltage as $\Delta\mathbf{x} \in [(1-\mu)\mathbf{x}, (1+\mu)\mathbf{x}]$. A larger AM reflects a larger selection range of $\Delta\mathbf{x}$, but not necessarily a larger absolute value of $\Delta\mathbf{x}$. We use attack detection probability (ADP), which is defined as the ratio of the number of detected attacks to the total number of launched attacks, to evaluate the stealthiness of FDI attacks against ML detectors. A lower ADP value indicates a more stealthy FDI attack.

B. Comparison Between TFDI and TC-FDI Attacks

We compare the performance of the TFDI attacks and TC-FDI attacks against the SVM detector [16]. The SVM detector supports the visualization in the attack detection process and highlights the advantages of TC-FDI attacks. First, we collect the SCADA measurements of 600 time instants as the normal data free of attacks. The attacker continuously launches TC-FDI from the 300th time instant to the 500th time instant with $\lambda = 5$, aiming to increase the voltage angle of Buses 2, 4, and 5. For the comparison, we also generate 200 TFDI attacks from the 300th time instant to the 500th time instant

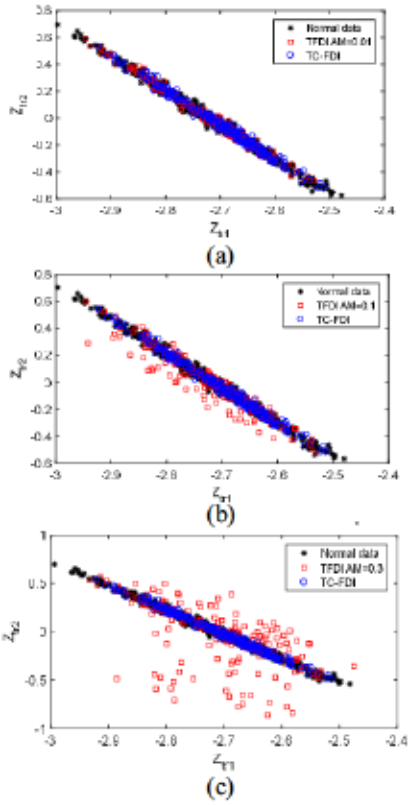


Fig. 4. Comparison of TFDI and TC-FDI attacks against SVM detector from the 300th to 500th time instant. (a) TFDI attack with AM = 0.01. (b) TFDI attack with AM = 0.1. (c) TFDI attack with AM = 0.3.

using AM = 0.01, AM = 0.1, and AM = 0.3, respectively. In each TFDI attack, the voltage angles of Buses 2, 4, and 5 are compromised by randomly generated incremental values within the AM. In total, we generate 200 TC-FDI attacks and 600 TFDI attacks.

In the SVM detector, the PCA dimension reduction is first applied to 1000 measurement vectors, including 600 historical measurement vectors, 200 compromised measurement vectors by the TC-FDI attack, and 200 compromised measurement vectors by the TFDI attack. For the visualization, 68-D measurement data is reduced to two principal components with more than 99% of the signal variance retained. We demonstrate the 2-D plot of 1000 measurement data in Fig. 4, where the AM of 200 TFDI attacks is 0.01, 0.1, and 0.3 in Fig. 4(a)–(c), respectively. In Fig. 4(a), both TC-FDI attack data points and TFDI attack data points overlap with the historical data. It is necessary to mention that the SVM detector identifies outliers far from the cluster of the historical measurements in the 2-D plot as the detected compromised data [16]. As the data points of TC-FDI and the TFDI attacks remain inside of the cluster of the historical measurements, these attacks are stealthy to the SVM detector. In Fig. 4(b) and (c), more TFDI attacks become outliers and are detected by the SVM detector with the increase of AM. It is interesting to observe that some attacks with large AM are also located inside the historical data area in Fig. 4(c). This is because the attacks with large AM could inject a small incremental voltage due to the definition of AM.

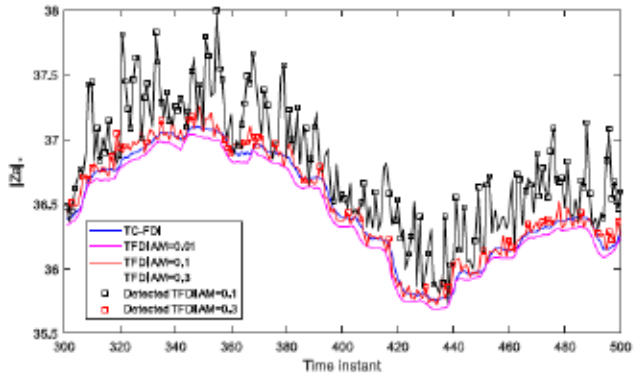


Fig. 5. Nuclear norm of TFDI and TC-FDI attacks.

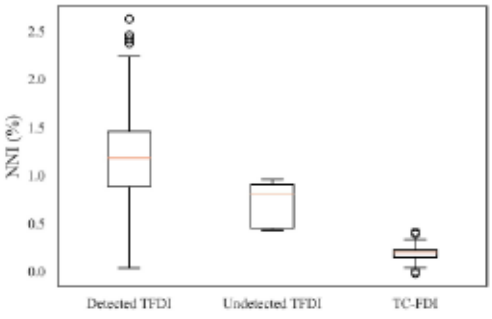
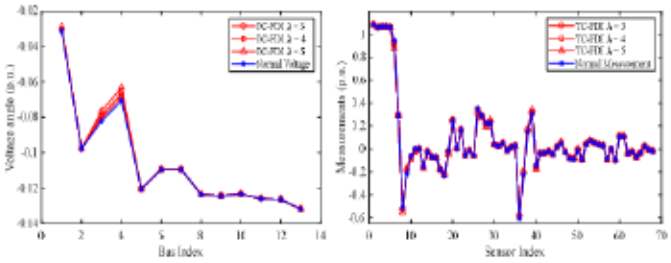


Fig. 6. NNI values of TFDI attacks and TC-FDI attacks.



(a) (b)

Fig. 7. TC-FDI attack under different weights in a single time instant. (a) Compromised voltage. (b) Compromised measurements.

We demonstrate the importance of the nuclear norm in the attack construction against the SVM detector. The nuclear norm of the compromised measurement tensor in TC-FDI attacks and TFDI attacks with different AMs from the 300th to 500th time instant are shown in Fig. 5. We mark all attacks detected by the SVM detector by square. Note that the proposed TC-FDI attacks and TFDI attacks with 0.01 AM are not detected by the SVM detector, and thus we only highlight the detected TFDI attacks with 0.1 and 0.3 AMs. As 0.01 AM is very small, the nuclear norm value of TFDI attacks with 0.01 AM is very close to the nuclear norm of the historical tensor without attacks. It is seen that a larger AM results in a higher nuclear norm value, indicating a low temporal correlation between the compromised measurements and historical measurements. Most detected TFDI attacks have relatively high nuclear norm values, while most undetected TFDI attacks have relatively low nuclear norm values. Therefore, the drawbacks of TFDI attacks are summarized as follows: 1) there is no guide for selecting the incremental voltage, and a random selection of the incremental voltage could compromise the historical measurement pattern; 2) TFDI attacks with small incremental voltage can be stealthy to the SVM detector, but they also have a low negative impact on the system; and 3) TFDI attacks with large incremental voltage can be detected by the SVM detector. In contrast, the TC-FDI attacks remain stealthy to the SVM detector by considering the temporal correlation of the historical measurements.

We demonstrate the relationship between the tensor nuclear norm and attack detection. The SVM detector is used to detect 100 TFDI attacks and 100 TC-FDI attacks. Then, we calculate the tensor nuclear norm increase (NNI) of detected TFDI attacks, undetected TFDI attacks, and TC-FDI attacks, respectively. For a given attack, its NNI is defined as $k = [(\|\mathbf{Z}_a\|_* - \|\mathbf{Z}_0\|_*)/(\|\mathbf{Z}_0\|_*)]$, where $\|\mathbf{Z}_0\|_*$ is the nuclear norm of historical measurements free of attack and $\|\mathbf{Z}_a\|_*$ is that of historical measurements under the attack. For example, an attack with NNI k indicates that the attack will increase $\|\mathbf{Z}_0\|_*$ by $k\%$. Fig. 6 shows the boxplot of NNI values of detected TFDI attacks, undetected TFDI attacks, and TC-FDI attacks. The boxplot shows that stealthy attacks generally have low nuclear norm values. The proposed TC-FDI attacks have very low NNI values. Even though an attack with a low nuclear norm value does not guarantee its stealthiness to ML detectors, the attack with a lower nuclear norm is more likely to remain stealthy to ML detectors.

C. Impact of Weights on the Performance of TC-FDI Attacks

We evaluate the impact of weights λ in the objective function of TC-FDI attacks on the performance of TC-FDI attacks. It is assumed that the attacker launches TC-FDI attacks with λ weights 3, 4, and 5, respectively, in the 300th time instant, aiming at increasing the voltage angle of Buses 2, 4, and 5. The compromised measurements received by the system operator and the compromised voltage angle estimated by the system operator are shown in Fig. 7.

In Fig. 7, we show the normal measurement and compromised measurement under TC-FDI attacks in a single time instant. In Fig. 7(a), it is seen that the compromised voltage angles of Buses 2, 4, and 5 are larger than the normal voltage of these three buses. A larger λ weight results in a larger $\|\Delta\mathbf{x}\|_1$. In Fig. 7(b), all measurements related to the attacked buses (Buses 2, 4, and 5) are compromised by the attacks. Note that the TC-FDI attacks do not yield a distinct change of measurement values, which contributes to the stealthiness of the proposed attack against ML detectors.

D. TC-FDI Attacks Against Statistic-Based BDD

We evaluate the stealthiness of TC-FDI attacks against Chi-squared, LNR and CUSUM detectors in the IEEE 14-bus system. For each detector, 400 normal measurements are used to calculate the false positive rate and 400 TC-FDI attacks are generated to calculate the ADP.

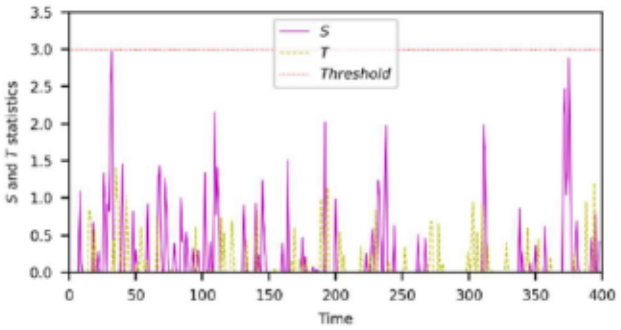


Fig. 8. S and T in the CUSUM detector.

TABLE II
ADP OF TC-FDI ATTACKS AGAINST STATISTIC-BASED BDDS

Detector	Chi-square	LNR	CUSUM
Normal	1.25%	1.50%	0%
TC-FDI	1.25%	1.25%	0%

We apply the CUSUM detector in Python package [34]. It is assumed that the CUSUM detector receives normal measurements from the 1st time instant to the 200th time instant, and TC-FDI attacks continually compromise the measurements from the 201st time instant to the 400th time instant. When the system is free of attacks, bias k and threshold h are selected to ensure no false alert. Specifically, we set bias k to 1.02 and threshold h to 3, indicating 3 standard deviations above the average CUSUM error summation under normal conditions. When the system is under attacks from the 201st time instant to the 400th time instant, it is seen that S and T do not trigger any alert in Fig. 8. Since the residual of TC-FDI attacks is the same as that of the normal measurements, there is no mean shift for the residual.

We summarize the performance of three statistic-based BDDs in Table II. Due to the space limit, the residual and LNR of normal and compromised measurements in Chi-square and LNR detectors are not shown. It is seen that the ADP of TC-FDI attack against each detector is similar to the false-positive rate. It indicates the stealthiness of TC-FDI attacks against statistic-based BDDs.

E. TC-FDI Attacks Against ML Detectors

This section evaluates the stealthiness of TC-FDI attacks against four different detectors, including SVM, k-NN detector [15], SLR detector [15], and GAD [16]. The training set includes the uncompromised measurement vectors of 500 time instants and the compromised measurement vectors of 500 time instants under the TFDI attacks. The testing set includes 100 uncompromised measurement vectors and 500 compromised measurement vectors. Specifically, in the testing set, we generate 100 TC-FDI attacks with $\lambda = 4$, 100 TC-FDI attacks with $\lambda = 5$, 100 TFDI attacks with 0.05 AM, 100 TFDI attacks with 0.1 AM, and 100 TFDI attacks with 0.2 AM. The AM in TFDI and weight λin TC-FDI are selected in a way such that their average $\|\Delta\mathbf{x}\|_1$ are comparable, as shown in 3rd row of Table III.

TABLE III
ADP OF ML DETECTORS AGAINST TFDI AND TC-FDI ATTACKS

Attack	TFDI			TC-FDI	
Weight	0.05	0.10	0.20	4.0	5.0
$\|\Delta\mathbf{x}\|_1$	0.008	0.017	0.033	0.008	0.015
SVM	0.55	0.80	0.90	0.04	0.10
SLR	0.51	0.76	0.85	0.02	0.08
KNN	0.50	0.79	0.84	0.06	0.15
GAD	0.13	0.43	0.68	0.09	0.09

For the k-NN detector, k value is optimized by searching $k = \{1, 2, \ldots, \sqrt{M^{\mathrm{Tr}}}\}$, where M^{Tr} is the number of training samples. Specifically, under each k value, we conduct fivefold cross-validation in the training data set, and the optimal k value is selected which has the highest average F1 scores. The SLR detector is solved using the Newton-CG solver and the penalization parameter of the SLR is optimized by searching in the interval [0.01, 1] based on fivefold cross-validation. The maximum number of iterations is chosen as 1000. In GAD, the compromised measurements in the training data set are subsampled according to the principle of anomaly detection (few abnormal data), such that the ratio of abnormal data to normal data is 0.1. Since the PCA is applied on the measurements, the assumption of independence for the historical measurements holds for the Gaussian distributed features. The training data set is used to create a multivariate Gaussian distribution model and the crossing validation data set is used to select the best threshold. Finally, the SVM detector with Gaussian kernel is applied to detect FDI attacks, since the data set is not linearly separable.

The ADP of four detectors against TFDI and TC-FDI attacks is summarized in Table III. First, we can observe that TC-FDI with $\lambda = 4$ and TFDI with 0.05 AM have the same average $\|\Delta\mathbf{x}\|_1$, and TC-FDI with $\lambda = 5$ and TFDI with 0.1 AM have similar average $\|\Delta\mathbf{x}\|_1$. It is seen that all detectors are able to detect the TFDI attacks. Specifically, the ADP of the detectors increases with the increase of AMs. For the TFDI attacks with 0.1 AM, the ADP of most detectors is around 80%. For the TC-FDI attacks, the ADP of the detectors slightly increases with the attack weight. For the TC-FDI attacks with $\lambda = 4$, the ADP of most detectors is below 6%. For the TC-FDI attacks with $\lambda = 5$, the ADP of most detectors is below 10%, and the ADP of KNN is 15%. From the results in Table III, the TC-FDI attacks are highly stealthy FDI attacks to traditional ML detectors.

F. Detection of TC-FDI Attacks Using RPS

This section assesses the detection effectiveness of the RPS against the proposed TC-FDI attacks in the IEEE 14-bus system. The graph-based planning method installs nine D-FACTS devices on the transmission lines indexed by {1, 3, 4, 8, 10, 12, 13, 17, 18} [8]. RPS utilizes the ACOPF-based operation method (9) to generate the setpoints of all D-FACTS devices. Since the attacker does not know the actual line reactance dispatched by RPS, it is assumed that the attacker uses the original line impedance without the RPS to continually launch TC-FDI attacks.

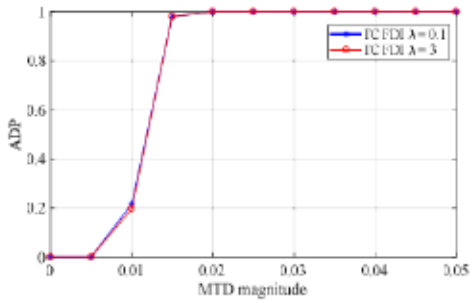


Fig. 9. ADP of RPS against TC-FDI attacks under different RPS magnitudes.

We generate RPS operation points (D-FACTS setpoints) using eight different RPS magnitudes η from 0.005 to 0.05 with an incremental of 0.005 to study the impact of RPS magnitude on the detection effectiveness. Under each RPS magnitude, the attack constructs 50 TC-FDI attacks using weights $\lambda = 0.1$ and $\lambda = 3$, respectively. The ADP of RPS is shown in Fig. 9. It is seen that the ADP of RPS increases with the RPS magnitude. When the RPS magnitude is larger than 0.02, the RPS method is able to detect all TC-FDI attacks. This is because a larger RPS magnitude has a larger capability to increase the estimation residual. When the attack weight increases, the ADP remains the same under different RPS weights. This is because the ADP is mainly determined by the placement of D-FACTS devices under the given RPS magnitude, which is consistent with the characteristics of RPS in [8]. It is necessary to note that the incremental angle of the TC-FDI attack is very small under the weight $\lambda = 0.1$. Therefore, the simulation results suggest that the RPS under the graph-based placement with a large RPS magnitude is effective in detecting TC-FDI attacks.

G. Detection of PEF-TC-FDI Attacks Using RPS

This section evaluates the detection effectiveness of the RPS against the PEF-TC-FDI attacks. In PEF-TC-FDI attacks, it is assumed that the attacker has no prior knowledge of line parameters of all transmission lines connected to attacked buses and uses the NPE (13) to estimate the line parameters. We use root mean-square error (RMSE) to measure the accuracy of the line parameter estimation.

Consistent with the TC-FDI attacks in previous sections, PEF-TC-FDI attacks compromise the voltage of three buses (Buses 2, 4, and 5) in the IEEE 14-bus system. There are 10 transmission lines connected to three attacked buses, five neighbor buses, and 35 measurements related to these eight buses and ten lines. For each transmission line, there are three line parameters. According to the standard π branch model, a single transmission line i–j has three line parameters, i.e., series admittance $g_{ij} + jb_{ij}$ and charging susceptance jy_{ij}. Therefore, there are 30 unknown line parameters for these ten lines. This means that the NPE needs to estimate 16 voltage states (eight buses) and 30 line parameter states (10 lines) using 35 measurements. In this case, the system is not observable. To simplify the problem, we further assumed that the attacker knows the charging susceptance of all lines and only needs to estimate the series admittance $g_{ij} + jb_{ij}$ of ten lines.

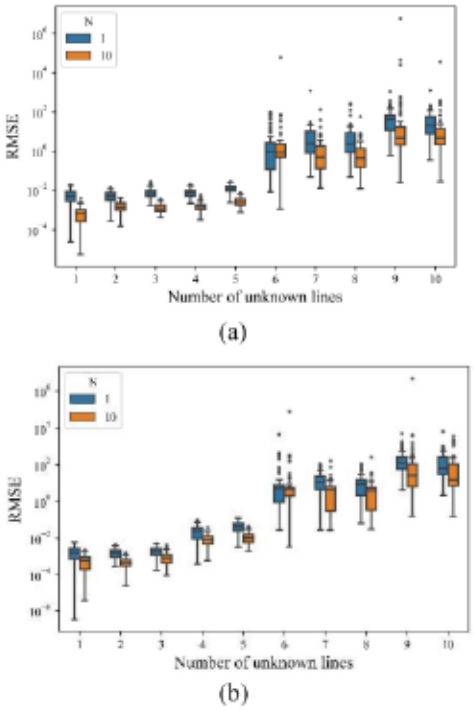


Fig. 10. Boxplot of RMSE of estimated series admittance. (a) RMSE of estimated g. (b) RMSE of estimated b.

First, we evaluate the performance of NPE under different numbers of measurement vectors and different numbers of unknown lines. For the number of measurement vectors, we consider the following two cases: 1) using measurements sampled in a single instant ($N = 1$) and 2) using measurements sampled in 10 instants ($N = 10$). When the number of unknown lines increases from 1 to 10, we conduct NPE 100 times under different noises. The boxplots for the RMSE of the estimated g and estimated b are shown in Fig. 10(a) and (b), respectively. It is seen that the number of unknown lines greatly impacts the accuracy of the estimated parameters. When there are more than five unknown lines in NPE, the accuracy of the estimated parameters is greatly reduced. This is because the system becomes unobservable in the NPE due to the increased number of states. In addition, more measurement vectors contribute to improving the estimation accuracy. It suggests PEF-TC-FDI attackers use more measurement vectors to get more accurate estimated line parameters.

Second, we evaluate the detection effectiveness of the RPS against the PEF-TC-FDI attacks. We construct four PEF-TC-FDI attack scenarios, as shown in Table IV, in which the number of attack buses is different. In each attack scenario, we construct 100 PEF-TC-FDI attacks using the estimated line parameters by NPE under $N = 10$. Table IV summarizes the attack scenario, NPE performance, and ADP of the RPS. It is seen that PEF-TC-FDI attacks with a single attack bus are stealthy to RPS due to accurate estimated line parameters. However, RPS can effectively detect PEF-TC-FDI attacks that compromise multiple buses.

In summary, the stealthiness of PEF-TC-FDI attacks against RPS is significantly impacted by the accuracy of the line

TABLE IV
DETECTION OF PEF-TC-FDI ATTACKS USING RPS

Scenario	1	2	3	4
# Attack buses	1	1	2	3
Attack buses	{2}	{5}	{2,4}	{2,4,5}
# Unknown lines	4	5	8	10
Median RMSE g	0.002	0.016	3.870	4.410
Median RMSE b	0.009	0.165	24.583	18.110
ADP	0	0.01	0.93	1.00

parameter estimation, which is determined by the number of unknown lines. More attacked buses lead to more line parameters being estimated, thus degrading the stealthiness of PEF-TC-FDI attacks. Note that TC-FDI attacks are designed to remain stealthy to ML detectors in this work, and thus, TC-FDI attacks generally compromise the voltage of multiple buses to make the compromised measurements consistent with the temporal correlation of historical measurements. Thus, RPS is able to detect PEF-TC-FDI attacks that compromise multiple buses.

From the defender's perspective, it is necessary to increase the frequency of RPS in order to reduce the number of measurement vectors collected by the attacker. A smaller N value contributes to reducing the accuracy of line parameter estimation and improving the detection capability to detect PEF-FDI attacks. In order to effectively detect PEF-FDI attacks, it is necessary to combine RPS with other detection methods, such as meter protection [35] and meter coding [36]. These joint methods can protect the buses with single transmission lines from PEF-FDI attacks.

VI. CONCLUSION

This article proposes novel convex TC-FDI attacks in AC power system model, which balances the tradeoff between the negative attack impact on the system operation and attack stealthiness. Specifically, the objective function of the proposed TC-FDI attack maximizes the L1-norm of the malicious incremental voltage to increase the negative attack impact, and minimizes the nuclear norm of the compromised historical measurement tensor to make the compromised measurements consistent with the historical measurements. The linearized power system model is utilized as constraints to make the proposed attack follow the spatial correlation of the historical measurements. An RPS method is utilized to detect TC-FDI attacks, in which D-FACTS devices are integrated into the ACOPF model. Simulation results compare the performance of TFDI and TC-FDI attacks against four ML detectors and demonstrate the stealthiness of the TC-FDI attacks. Simulation results also verify the effectiveness of RPS in detecting TC-FDI attacks. In our future work, we will use the local information of the attack area to construct TC-FDI attacks, which contributes to reducing the computational time.

REFERENCES

[1] R. Khan, K. McLaughlin, D. Laverty, and S. Sezer, "Analysis of IEEE C37.118 and IEC 61850-90-5 synchrophasor communication frameworks," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, 2016, pp. 1–5.

[2] H. Zhang, B. Liu, and H. Wu, "Smart grid cyber-physical attack and defense: A review," *IEEE Access*, vol. 9, pp. 29641–29659, 2021.

[3] J. Liang, L. Sankar, and O. Kosut, "Vulnerability analysis and consequences of false data injection attack on power system state estimation," *IEEE Trans. Power Syst.*, vol. 31, no. 5, pp. 3864–3872, Sep. 2016.

[4] J. Tian, R. Tan, X. Guan, and T. Liu, "Enhanced hidden moving target defense in smart grids," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2208–2223, Mar. 2019.

[5] S. Lakshminarayana and D. K. Y. Yau, "Cost-benefit analysis of moving-target defense in power grids," *IEEE Trans. Power Syst.*, vol. 36, no. 2, pp. 1152–1163, Mar. 2021.

[6] M. Liu, C. Zhao, Z. Zhang, and R. Deng, "Explicit analysis on effectiveness and hiddenness of moving target defense in AC power systems," *IEEE Trans. Power Syst.*, vol. 37, no. 6, pp. 4732–4746, Nov. 2022.

[7] B. Liu and H. Wu, "Optimal D-FACTS placement in moving target defense against false data injection attacks," *IEEE Trans. Smart Grid*, vol. 11, no. 5, pp. 4345–4357, Sep. 2020.

[8] B. Liu and H. Wu, "Systematic planning of moving target defence for maximising detection effectiveness against false data injection attacks," *IET Cyber-Phys. Syst., Theory Appl.*, vol. 6, no. 3, pp. 151–163, 2021.

[9] Z. Zhang and R. Deng, "Impact analysis of MTD on the frequency stability in smart grid," *IEEE/CAA J. Automatica Sinica*, vol. 10, no. 1, pp. 275–277, Jan. 2023.

[10] B. Wang, J. Song, L. Wan, Y. Tian, X. Wang, and Z. Zhang, "Impact analysis of moving target defense on the small-signal stability in power systems," in *Proc. IEEE 6th Int. Conf. Ind. Cyber Phys. Syst. (ICPS)*, Wuhan, China, 2023, pp. 1–6.

[11] H. Zhang, B. Liu, X. Liu, A. Pahwa, and H. Wu, "Voltage stability constrained moving target defense against net load redistribution attacks," *IEEE Trans. Smart Grid*, vol. 13, no. 5, pp. 3748–3759, Sep. 2022.

[12] B. Li, G. Xiao, R. Lu, R. Deng, and H. Bao, "On feasibility and limitations of detecting false data injection attacks on power grid state estimation using D-FACTS devices," *IEEE Trans. Ind. Informat.*, vol. 16, no. 2, pp. 854–864, Feb. 2020.

[13] C. Liu, Y. Li, H. Zhu, Y. Tang, and W. Du, "Parameter-estimate-first false data injection attacks in AC state estimation deployed with moving target defense," *IEEE Trans. Circuits Syst. I, Reg. Papers*, vol. 71, no. 4, pp. 1842–1851, Apr. 2024.

[14] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: Modeling and countermeasures," *IEEE Trans. Parallel Distrib. Syst.*, vol. 25, no. 3, pp. 717–729, Mar. 2014.

[15] M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Machine learning methods for attack detection in the smart grid," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 27, no. 8, pp. 1773–1786, Aug. 2016.

[16] M. Esmalifalak, L. Liu, N. Nguyen, R. Zheng, and Z. Han, "Detecting stealthy false data injection using machine learning in smart grid," *IEEE Syst. J.*, vol. 11, no. 3, pp. 1644–1652, Sep. 2017.

[17] J. Sakhnini, H. Karimipour, and A. Dehghantanha, "Smart grid cyber attacks detection using supervised learning and heuristic feature selection," in *Proc. IEEE 7th Int. Conf. Smart Energy Grid Eng. (SEGE)*, Aug. 2019, pp. 108–112.

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

[19] D. Goldfarb and Z. Qin, "Robust Low-rank tensor recovery: Models and algorithms," *SIAM J. Matrix Anal. Appl.*, vol 35, no. 1 pp. 225–253, 2014.

[20] J. Liu, P. Musialski, P. Wonka, and J. Ye, "Tensor completion for estimating missing values in visual data," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 35, no. 1, pp. 208–220, Jan. 2013.

[21] M. Signoretto, Q. T. Dinh, L. Lathauwer, and J. A. Suykens, "Learning with tensors: A framework based on convex optimization and spectral regularization," *Mach. Learn.*, vol 94, pp. 303–351, Mar. 2014.

[22] Y. Liu, A. S. Zamzam, and A. Bernstein, "Multi-area distribution system state estimation via distributed tensor completion," Mar. 2022, *arXiv:2203.00260*.

[23] G. Hug and J. A. Giampapa, "Vulnerability assessment of AC state estimation with respect to false data injection cyber-attacks," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1362–1370, Sep. 2012.

[24] E. S. Page, "Continuous inspection schemes," *Biometrika*, vol. 41, nos. 1–2, pp. 100–115, 1954.

[25] M. C. Grant and S. P. Boyd, "Graph Implementations for Nonsmooth Convex Programs," in *Recent Advances in Learning and Control* (Lecture Notes in Control and Information Sciences) V. D. Blondel, S. P. Boyd, and H. Kimura, Eds., London, U.K.: Springer, 2008, pp. 95–110.

[26] S. Diamond and S. Boyd, "CVXPY: A Python-embedded modeling language for convex optimization," *J. Mach. Learn. Res.*, vol. 17, no. 83, pp. 1–5, 2016.

[27] "Smart Wire." Accessed: Dec. 1, 2023. [Online]. Available: https://www.smartwires.com/smartvalve/#720236843

[28] S. Lakshminarayana, A. Kammoun, M. Debbah, and H. V. Poor, "Data-driven false data injection attacks against power grids: A random matrix approach," *IEEE Trans. Smart Grid*, vol. 12, no. 1, pp. 635–646, Jan. 2021.

[29] "Electric Reliability Council of Texas." Accessed: Mar. 1, 2023. [Online]. Available: https://www.ercot.com/

[30] 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 Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, Feb. 2011.

[31] J. Wu, Y. He, and N. Jenkins, "A robust state estimator for medium voltage distribution networks," *IEEE Trans. Power Syst.*, vol. 28, no. 2, pp. 1008–1016, May 2013.

[32] W. Lambrichts and M. Paolone, "Linear recursive state estimation of hybrid and unbalanced AC/DC micro-grids using synchronized measurements," *IEEE Trans. Smart Grid*, vol. 14, no. 1, pp. 54–67, Jan. 2023.

[33] F. Pedregosa et al., "Scikit-learn: Machine learning in Python," *J. Mach. Learn. Res.*, vol. 12, no. 85, pp. 2825–2830, 2011.

[34] V. Khamesi, "ocpdet: A Python package for online changepoint detection in univariate and multivariate data," Preprint, Zenodo. [Online]. Available: https://doi.org/10.5281/zenodo.7632721

[35] C. Liu, H. Liang, T. Chen, J. Wu, and C. Long, "Joint admittance perturbation and meter protection for mitigating stealthy FDI attacks against power system state estimation," in *IEEE Trans. Power Syst.*, vol. 35, no. 2, pp. 1468–1478, Mar. 2020.

[36] C. Liu, Y. Tang, R. Deng, M. Zhou, and W. Du, "Joint meter coding and moving target defense for detecting stealthy false data injection attacks in power system state estimation," *IEEE Trans. Ind. Informat.*, vol. 20, no. 3, pp. 3371–3381, Mar. 2024.

Bo Liu (Member, IEEE) received the Ph.D. degree from the Mike Wiegers Department of Electrical and Computer Engineering, Kansas State University (K-State), Manhattan, KS, USA, in 2021.

He is currently an Assistant Professor with the School of Engineering and Applied Sciences, Washington State University Tri-Cities, Richland, WA, USA. From 2022 to 2024, he was a Research Assistant Professor with the Mike Wiegers Department of Electrical and Computer Engineering, K-State. His current research interests include cyber–physical security of power systems, smart grid technologies, machine learning, and state estimation in smart grids.

Yajing Liu (Member, IEEE) (deceased) received the Ph.D. degree in electrical engineering from Colorado State University, Fort Collins, CO, USA, in 2018.

She was a Research Scientist with Colorado State University. From 2018 to 2021, she worked as a Researcher with the National Renewable Energy Laboratory, Golden, CO, USA. Her research spanned optimization algorithms, matrix and tensor completion, with specific applications in power system state estimation and cyberattack mitigation, as well as the geometries of learning. She made significant contributions to the methodologies employed in this work. Her expertise and dedication will be deeply missed.

Hongyu Wu (Senior Member, IEEE) received the B.S. degree in energy and power engineering and the Ph.D. degree in control science and engineering from Xi'an Jiaotong University, Xi'an, China, in 2003 and 2011, respectively.

He is an Associate Professor and a Lucas-Rathbone Professor with the Mike Wiegers Department of Electrical and Computer Engineering, Kansas State University (K-State), Manhattan, KS, USA. Before joining K-State, he was a Research Engineer with the Power Systems Engineering Center, National Renewable Energy Laboratory, Golden, CO, USA. From 2011 to 2014, he was a Postdoctoral Researcher with the Robert W. Galvin Center for Electricity Innovation, Illinois Institute of Technology, Chicago, IL, USA. His research interests include cyber–physical security of smart grids, power system planning, operation and energy management, and power grid integration of renewable energy.

Dr. Wu is a National Science Foundation (NSF) CAREER Awardee and an NSF EPSCoR Research Fellow. He serves on the IEEE-NERC Security Integration Project Committee and as an Associate Editor for IEEE TRANSACTIONS ON SMART GRID and IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS.