Constrained-Differential-Evolution-Based Stealthy Sparse Cyber-Attack and Countermeasure in an AC Smart Grid

Kang-Di Lu and Zheng-Guang Wu

***Abstract*—As the next-generation power grids, smart grids are integrated with advanced information and communication technology (ICT) to make the grid more efficient and stable than conventional power systems. Given the mounting cyber-attack threats, these critical ICT systems create great security issues for smart grids. Additionally, the clever attackers have the ability to not only access and monitor the smart grid, but also hack it by launching well-established cyber-attacks. Thus, this article is devoted to understanding the potential stealthy cyber-attack and its countermeasure. First, this article proposes a stealthy sparse cyber-attack model in an ac smart grid by considering both the residual test-based detector and the interval-state-estimation-based detector, which is not considered in previous studies. The design model is formulated as a constrained optimization problem by minimizing the number of contaminated meters, where the characteristics of two types of detector are considered simultaneously as the constraints for the first time. A constrained differential evolution (CDE) is proposed as the solver because the optimization problem is NP-hard. Then, a generalized-cumulative-sum-based detector is developed to detect the proposed cyber-attacks, where a fractional-order state transition matrix is originally introduced into the estimator to describe the dynamics of the power system. Numerical studies illustrate the feasibility of CDE-based stealthy sparse cyber-attacks and the effectiveness of the proposed countermeasure.**

***Index Terms*—Constrained differential evolution (CDE), false data injection attack (FDIA), generalized cumulative sum, smart grid security, stealthy sparse cyber-attack.**

I. Introduction

SMART grids are integrated with monitoring, sensing, communication, and advanced technologies, making them vulnerable to various cyber-attacks [1]. The goal of attackers is to use various attack techniques to threaten economic health or cause power outages and even blackouts. For example, such a cyber-attack occurred on the Ukrainian power system on December 23, 2015, which caused a power blackout and blue affected approximately 200 000 people [2]. The successful Ukraine attack has shown that attackers can access and monitor the smart grid. Furthermore, the attackers are able to launch the well-established cyber-attacks by hacking components or manipulating the network communication. Thus, it is helpful for the operation to gain an in-depth understanding of cyber-attacks by designing attacks and countermeasures under different conditions.

In the cyber-attack of the smart grid domain, existing studies can be classified into two categories [3]. The first category is designing various cyber-attacks with different attacking aims from the perspective of attackers, false data injection attack (FDIA) [4], overloading attack [5], and resonance attack [6], to name a few. By hacking the measurement equipment, these cyber-attacks were successfully launched under different conditions. As one of the typical malicious cyber-attacks, FDIA can be viewed as the most challenging attack because attackers can design well-established attack vectors to circumvent the conventional bad data detector (BDD) widely used in existing power systems. Most of the existing FDIA models are launched in a confined setting on the assumption that the power system states to the measurements are based on dc power flow models, whereas most state estimators in real-world smart grids are based on nonlinear ac power flow models. Using dc-based attack models may have a higher risk of introducing errors to trigger the existing BDD because ac state estimators have inherent strengths and more powerful robustness ability than dc-based versions. Moreover, as illustrated in [7], the ac-based attack model needs a more sophisticated attacker than the dc version because of complex nonlinear characteristics. Therefore, designing a cyber-attack in ac form is still significant for cybersecurity practitioners and other stakeholders to further understand the smart grid security problem.

Regarding the efforts of attackers, attackers prefer to hack as few measurements as possible to establish sparse cyber-attacks with the least effort [8]. High-sparsity attacks decrease the detection probability of the detector. Most of the existing techniques (e.g., matrix transformation [4], linear transformation-based approach [9], and interior point method [10]) have successfully obtained sparse FDIAs in dc form. However, these techniques cannot be directly employed to establish sparse cyber-attacks in

Manuscript received August 14, 2021; revised November 4, 2021; accepted November 17, 2021. Date of publication November 22, 2021; date of current version May 6, 2022. This work was supported in part by the National Natural Science Foundation of China under Grant U1966202. Paper no. TII-21-3553. *(Corresponding author: Zheng-Guang Wu.)*

The authors are with the National Laboratory of Industrial Control Technology, Institute of Cyber-Systems and Control, Zhejiang University, Hangzhou 310027, China (e-mail: kangdilu789@zju.edu.cn; nashwzhg@zju.edu.cn).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TII.2021.3129487.

Digital Object Identifier 10.1109/TII.2021.3129487

the ac model. In the optimization domain, the characteristics of the sparse stealthy attack optimization problem are nonconvex and NP-hard. On the other hand, as a popular evolutionary algorithm, differential evolution (DE) is free of restrictions on problem characteristics, easily performed to solve various real-life problems, and not sensitive to the initial solution [11]. Because of these advantages, DE can be viewed as a potential method to solve the sparse cyber-attack optimization problem with nonconvex and NP-hard characteristics.

The second category of the existing works concentrates on detecting cyber-attacks from the perspective of defenders. Traditionally, the BDD method is used to detect bad data caused by random noise or faults, but it cannot identify stealth FDIAs [4]. Recently, to detect FDIAs, various interval state estimation (ISE)-based detectors have been proposed by considering the uncertainties of power systems to detect cyber-attacks in smart grids [3], [12], [13]. The vital idea behind ISE-based detectors is based on the interval state values by considering various uncertainties. Considering that the attackers may be advanced to the system or detector, the attack could bypass ISE-based methods by considering the interval characteristics to design stealthy cyber-attacks. In addition, for a timely and reliable response to FDIAs, some online detectors according to the quickest detection theory have been presented. In [14] and [15], two cumulative sum (CUSUM)-based detectors were presented to identify FDIA, where conventional least squares were used for state estimation. More recently, in [16] and [17], two additional CUSUM-based methods were presented to identify FDIA with forecasting-aided state estimations in the dc model. It is noted that these CUSUM-based detectors are focused on detecting FDIAs in dc form. As a consequence, it is worth to investigate the performance of the CUSUM-based detector in detecting attacks in the case of ac-based stealthy FDIA.

The main contributions of this article lie in three aspects as follows.

1) A novel stealthy sparse cyber-attack model based on an ac smart grid is originally presented. First, obtain the behaviors of the power network by performing ac optimal power flow (OPF). Then, to construct a stealthy cyber-attack, the designed attack model considers the characteristics of both the residual test-based detector and the ISE detector. Finally, designing an optimal sparse cyber-attack is formulated as a constrained optimization problem by minimizing the number of contaminated meters to make specific lines overload, where the characteristics of these two types of detectors are considered simultaneously as the constraints for the first time.
2) Constrained differential evolution (CDE) is introduced to solve the constrained optimization problem for launching the stealthy sparse cyber-attack, in which an initialized coding mechanism is proposed to effectively describe the attack vectors. With this initialized coding mechanism, the sparsity of attack vectors is expected to be ensured and effectively optimized by the proposed CDE.
3) An improved CUSUM-based detection scheme is proposed for detecting stealthy FDIA in an ac smart grid, in which a fractional-order state transition matrix is introduced into an iterative weighted least squares (IWLS) estimator to forecast the state values for describing the high dynamics of ac power systems. Additionally, the proposed detector has the ability to estimate the attack variables for attack mitigation and system recovery.

II. Related Work

A. Related Works on Construction of FDIA in Smart Grids

Recently, considerable efforts have been made to construct various FDIAs in smart grids. Liu *et al.* [4] used matrix transformation to design optimal sparse FDIA based on the dc model. To cause the maximum damage for smart grids, a linear-transformation-based approach was presented to identify the optimal meter to be contaminated [9]. Che *et al.* [18] investigated the FDIA on simultaneous damage to several branches by launching a purposeful branch outage sequence to impose significant damages to the grid. To investigate the impacts of FDIA on electricity markets, the interior point method and robustness analysis were used to construct the attack vectors [10]. To reduce system information, a zero-parameter-information FDIA model is presented in [19].

In practice, the state estimation models of smart grids are ac models. DC-based attack models introduce a large residual on ac state estimations. To design more realistic stealthy cyber-attacks, various FDIA models on ac grids were investigated. In [3] and [13], the attack vectors designed based on the ac model and operation scenarios were considered to make specific lines overload. Based on [3], the dynamic FDIA model was constructed by considering the reality of dynamically time-evolving power systems [12]. Zhao *et al.* [20] proposed a generalized FDIA framework against the ac state estimator, where the prefect knowledge of system information was relaxed. In [21], a class of blind FDIA based on the geometric approach was presented without using the grid topology and transmission-line admittances. However, the above ac-based attack models neglect the variants of state values during the design process, which can be easily detected by ISE-based detectors [3], [12], [13]. Although sparse FDIA [3], [13], dynamic FDIA [12], generalized FDIA [20], and blind FDIA [21] have been constructed in ac models, such models are not valid for systems equipped with ISE detectors. Thus, to design stealthier cyber-attacks, this article considers the characteristics of residual test-based detection and ISE detection schemes simultaneously. In addition, although most methods can be used to solve the linear L_0-norm problem to launch sparse cyber-attacks in dc models, these methods cannot be directly employed to solve the L_0-norm problem in ac models. To solve this problem, Wang *et al.* [3], [12] relaxed the L_0-norm minimization to L_1-norm minimization to design sparse attacks in ac form. However, L_1-norm optimization cannot capture vector sparsity. To briefly summarize, Table I lists several of the relevant papers on FDIA construction with corresponding advantages and disadvantages.

TABLE I
BRIEF SUMMARY OF THE PROS AND CONS OF FDIA CONSTRUCTION

Ref.	Pros	Cons
[4]	Vulnerability of existing bad measurement is proved.	(1) These attacks are designed and constructed based on dc model. (2) May introduce large residual in ac model. (3) These solvers used to find attack vectors cannot be directly employed to establish sparse cyber-attack in ac model.
[9]	Identify the optimal meter set to cause the maximum damage.	
[10]	The impacts of FDIA on electricity markets are investigated.	
[18]	Investigate the FDIA on damages several branches.	
[19]	Design attacks without any information of the branch parameters.	
[3], [12], [13]	The attack vectors designed based on ac model and operation scenario or dynamic characteristic are considered.	(1) The sparse optimization problem is nonconvex and NP-hard. (2) L1-norm optimization problem cannot capture vector sparsity. (3) There are not valid for systems equipped with ISE detectors.
[20], [21]	The attack models designed based on the ac model and system information is reduced.	(1) Some characteristics, e.g., dynamic and operation scenario are ignored. (2) These models cannot bypass ISE detector.

B. Related Works on Detection of FDIA in Smart Grids

Because of the severe threat of FDIAs, significant achievements have been made in resisting FDIAs. Generally, these methods can be classified into two categories: physical-based and data-dependent-based methods.

As a physical-based method, phasor measurement units (PMUs) are advanced devices based on the GPS and synchronize highly precise phasor measurements. Yang *et al.* [22] presented an effective greedy algorithm for optimal PMU placement to protect specific sensors against FDIAs. Bi and Zhang [23] suggested optimal PMU locations achieved by mixed-integer linear programming by considering covert topological information. The demerit of PMU-based defending methods is that the operators spend additional investment costs because PMUs are expensive devices. Another disadvantage is that PMUs use GPS, which may be spoofed [27].

In the second category, various data-dependent models are used to detect the FDIA. For example, a convolutional neural network (CNN) was used as the classifier to extract power flow correlation features for detecting the attacks and corresponding locations [24]. In [25], the FDIA detection problem was formulated as a partially observable Markov decision process problem, and reinforcement learning (RL) was used as the tool for timely and reliable detection. Similarly, an ensemble of extreme learning machines (EnELM) was proposed to detect anomaly states caused by FDIAs [26]. These methods do not require system models and parameters and have good scalability. However, these methods need to collect training datasets, and no clear knowledge exists to set hyperparameters in complex models, such as CNN [24].

Additionally, to detect the established FDIA, three ISE-based detectors were proposed by considering the uncertainties related to power systems [3], [12], [13]. In [3], a deep-learning-based ISE (DL-ISE) detector was used to determine the intervals to detect the cyber-attacks. In [12], a system-uncertainty-based ISE (SU-ISE) detector was suggested to detect attacks by solving network parameter perturbations and electric load uncertainties with kernel quantile regression to approximate the variation bounds. Furthermore, a robust ISE (R-ISE) detector was proposed by considering system perturbations and forecasting uncertainties with a parametric Gaussian distribution to determine the possible intervals [13].

To briefly summarize, Table II lists several of the relevant papers of FDIA detection with corresponding advantages and disadvantages. Additionally, Musleh *et al.* [1] summarized the detection algorithms for FIDA in smart grids. Interested readers can refer to [1] for more details.

III. STEALTHY SPARSE CYBER-ATTACK MODEL BASED ON CDE

To successfully launch cyber-attacks, attackers should design the attack strategy, which needs to satisfy the underlying system model to evade the detector used in the dispatch center [28]. Specifically, the attack model constructed according to the simplified dc model may cause a perceptible residual in ac state estimation [29]. In addition to bypassing the residual test detector, other advanced detectors, e.g., ISE detectors, may be considered by attackers to launch stealthier cyber-attacks through the advanced ability of the attackers. Meanwhile, attackers would like to focus their efforts on contaminating as few measurements as possible to reduce the risk of detection. Hence, most attackers consider sparse attack strategies [8], [12]. As a consequence, this article originally proposes a novel stealthy sparse cyber-attack model in an ac smart grid to evade a residual test-based detector and an advanced ISE detector.

A. Establishing Stealthy Sparse Cyber-Attack Model

We assume that the attacker has the ability to know the topology and the parameters of the entire network. In addition, the attacker is assumed to have the capability to perform OPF. Under these assumptions, we can establish a two-stage stealthy sparse cyber-attack model. The first stage is the OPF operation to approximately obtain the measurement values as follows:

$$(P_{it}^*, Q_{it}^*, P_{ijt}^*, Q_{ijt}^*) = \arg\min \sum_{k\in\Omega_G} (f_{1\,k}(P_{Gkt}) + f_{2\,k}(Q_{Gkt})) \quad (1)$$

$$\text{s.t. } E(V_{it}, \theta_{it}, P_{Gkt}, Q_{Gkt}) = 0 \quad (2)$$

$$F(V_{it}, \theta_{it}, P_{Gkt}, Q_{Gkt}) < 0 \quad (3)$$

where P_{it}^* and Q_{it}^* represent the optimal active power injections at the ith bus under the tth scenario, respectively. $f_{1\,k}(P_{GKt})$ and $f_{2\,k}(Q_{GKt})$ represent the cost function of the kth active and reactive power generators, and Ω_G represents the index of all of the generators. $E(\cdot)$ and $F(\cdot)$ represent the equality constraints and inequality constraints, respectively. V_{it} and θ_{it} represent the voltage magnitude and phase angle, respectively.

In the second stage, the fitness function is formulated as a constrained optimization problem to design well-established

TABLE II
BRIEF SUMMARY OF THE PROS AND CONS OF FDIA DETECTION

Category	Method	Pros	Cons
Physical-based methods	Effective greedy algorithm [22] Mixed-integer linear programming [23]	PMUs are advanced devices based on GPS and synchronize highly precise phasor measurements.	(1) Spend additional investment costs because PMUs are the expensive devices. (2) PMUs use GPS which may be spoofed.
Data-dependent-based methods	CNN [24] RL [25] EnELMs [26]	(1) Do not require system models and parameters (2) Have good scalability.	(1) Need to collect training datasets. (2) No clear knowledge exists to set hyperparameters in complex models.
	DL-ISE [3] SU-ISE [12] R-ISE [13]	(1) Less investment is required. (2) No thresholds are determined. (3) Consider various uncertainties.	The vulnerability of ISE-based detectors is not given.

attack vectors by minimizing the contaminated measurements as follows:

$$\text{Fitness function}: \min ||z_t^a - h(x_t^a)||_0 \tag{4}$$

$$\text{s.t. } P_{it}^* + P_{it}^a = \sum_{j\in\Omega_B} V_{it}^a V_{jt}^a (G_{ij}\cos\theta_{ijt}^a + B_{ij}\sin\theta_{ijt}^a) \tag{5}$$

$$P_{ijt}^* + P_{ijt}^a = -(V_{it}^a)^2 G_{ij} + V_{it}^a V_{jt}^a (G_{ij}\cos\theta_{ijt}^a + B_{ij}\sin\theta_{ijt}^a) \tag{6}$$

$$Q_{it}^* + Q_{it}^a = \sum_{j\in\Omega_B} V_{it}^a V_{jt}^a (G_{ij}\sin\theta_{ijt}^a - B_{ij}\cos\theta_{ijt}^a) \tag{7}$$

$$Q_{ijt}^* + Q_{ijt}^a = (V_{it}^a)^2 B_{ij} + V_{it}^a V_{jt}^a (G_{ij}\sin\theta_{ijt}^a - B_{ij}\theta_{ijt}^a) \tag{8}$$

$$V_i^{\min} \le V_{it}^a \le V_i^{\max} \tag{9}$$

$$P_{Gk}^{\min} \le P_{kt}^* + P_{kt}^a \le P_{GK}^{\max} \tag{10}$$

$$Q_{GK}^{\min} \le Q_{kt}^* + Q_{kt}^a \le Q_{GK}^{\max} \tag{11}$$

$$\sqrt{(P_{lt}^* + P_{lt}^a)^2 + (Q_{lt}^* + Q_{lt}^a)^2} \ge S_l^{\max} \tag{12}$$

$$V_{ISE,it}^{\min} \le V_{it}^a \le V_{ISE,it}^{\max} \tag{13}$$

$$\theta_{ISE,it}^{\min} \le \theta_{it}^a \le \theta_{ISE,it}^{\max} \tag{14}$$

$$x_t^a = \{V_{it}^a, V_{jt}^a, \theta_{it}^a, \theta_{jt}^a\} \tag{15}$$

$$U_t^{a,\min} \le U_t^a = \{P_{it}^a, P_{ijt}^a, Q_{it}^a, Q_{ijt}^a\} \le U_t^{a,\max} \tag{16}$$

where $P_{it}^a, P_{ijt}^a, Q_{it}^a$, and Q_{ijt}^a represent the incremental values of measurements of power injections and power flows designed by the attackers [3]. θ_{ij} denotes the phase angle difference between buses i and j. x_t^a represents the attacked state vector including attacked voltage magnitudes V_{it}^a and V_{jt}^a and attacked phase angles θ_{it}^a and θ_{jt}^a. z_t is the measurement, including P_i, P_{ij}, Q_i, and Q_{ij}. Ω_B represents the set of buses. $h(\cdot)$ represents the vector functions (5)–(8) mapping the state vector to attacked measurements. Moreover, G_{ij} and B_{ij} represent real and imaginary parts of the admittance matrix, respectively. P_{Gk} and Q_{Gk} are the kth active and reactive power generators, respectively, whereas the superscripts min and max indicate the corresponding power capacity limits. $S_l^{\max}$ is the lth branch's power limits, where l represents the transmission line. U_t^a is the decision variable optimized by the attackers, and $U_t^{a,\min}$ and $U_t^{a,\max}$ are the lower and upper bounds of U_t^a, respectively. $V_{\text{ISE},it}^{\min}, V_{\text{ISE},it}^{\max}, \theta_{\text{ISE},it}^{\min}$, and $\theta_{\text{ISE},it}^{\max}$ are the lower and upper bounds of the voltage magnitude and phase angle obtained by ISE.

Considering the tth scenario, the attackers collect the network topology, bus loads, and generation to perform the OPF in the first stage with the aim of obtaining all of the measurements. Then, to launch attack, attackers inject incremental values in power injections and line flows to overload the lines and contaminate the state vectors. By selecting the transmission lines, the attackers can overload a single line or multiple lines. If the incremental values meet (5)–(8), the traditional detectors based on the residual value fail to find the abnormal value. In addition, the well-designed attack vector can bypass the ISE detector if the attackers consider (13) and (14).

For the ISE detector, different methods can be used to determine the interval. For example, Wang *et al.* [3] used deep learning to forecast electric load forecasting to obtain the interval states. In [13], a novel interval state forecasting method is given by considering system and forecasting uncertainties. Here, we use the following ISE detector:

$$V_{\text{ISE},it}^{a,\min} = V_{it} - \tau_v, V_{\text{ISE},it}^{a,\min} = V_{it} + \tau_v$$
$$\theta_{\text{ISE},it}^{a,\min} = \theta_{it} - \tau_\theta, V_{\text{ISE},it}^{a,\min} = \theta_{it} + \tau_\theta \tag{17}$$

where τ_v and τ_θ are adjustable parameters to determine the width of the state variables. V_{it} and θ_{it} are obtained by the OPF at time t as the mean values. Through (17), the attackers avoid using complicated techniques to determine the interval and only with two parameters to be tuned, which is convenient for the attackers.

Remark 1: The proposed attack model in (4)–(16) is based on the assumption that the attacker is omnipotent and has all-encompassing knowledge of network information. To extend the attack model with incomplete network information, we can add some constraints. More specifically, in the first stage, the boundary constraint should be satisfied given in (18), and the fitness function should be changed to the local version given in (19)

$$x_{dt}^{\Omega_D} = x_{dt}^0 \tag{18}$$

$$\min ||z_t^{\Omega_A} - h^{\Omega_A}(x_t^a)||_0 \tag{19}$$

where Ω_D represents the boundary connecting the attacking and nonattacking regions, Ω_A represents the attacking region, and x_{dt}^0 represents the initialized state values of buses at the boundary.

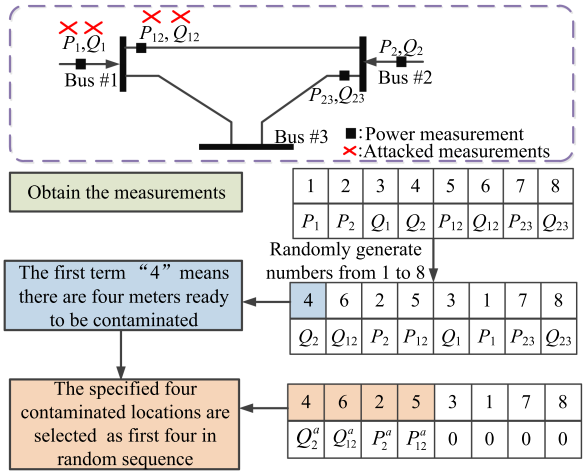

Fig. 1. Example of the initialized coding mechanism in SFDE-IM.

B. Launching Attack Based on CDE

The proposed stealthy sparse attack model is given in (4)–(16). In essence, the optimization problem in (4)–(16) can be viewed as the constrained single-objective optimization problem. Thus, CDE is suitable to solve the considered problem. Here, we select DE with the superiority of feasible solution constraint handling technique (SFDE) [11] as the tool to handle the optimization problem. Before the application of SFDE, an initialized coding mechanism is proposed in the original SFDE (called SFDE-IM) to better describe the attack vector. The coding mechanism's detailed process is given in Fig. 1. We provide the detailed steps of the proposed SFDE-IM to achieve the attack strategy as follows.

Input: The SFDE-IM parameters include the dimension of the decision variable (D), number of population (NP), mutation factor (F), crossover rate (CR), and maximum number of fitness function evaluations ($FES_{\max}$). The network information of the IEEE bus system includes grid topology, bus loads, line parameters, and the generator cost function.

Output: Number of contaminated meters (i.e., the fitness function) and corresponding locations.

Step 1: Generate an initial population PD_g shown in (20) with the initialized coding mechanism in Fig. 1, which represents different attack strategies

$$PD_g = \{U_{1,g}, U_{2,g}, \ldots, U_{NP,g}\} \tag{20}$$

where g is the current generation, and $U_{i,g} = (u_{i,1,g}, \ldots, u_{i,D,g})$ represents the ith individual in PD_g. Set $g = 1$.

Step 2: Calculate the fitness value and constraint violation of each individual in PD_g according to the fitness function and constraints in (4)–(16). The constraint violation υ can be calculated as follows:

$$\upsilon_i(X) = \frac{\sum_{i=1}^{\kappa} \lambda_i (G_i(X))}{\sum_{i=1}^{\kappa} \lambda_i}$$

$$G_i(X) = \begin{cases} \max[\psi_i(X), 0], & i = 1, \ldots, p \\ \max[\varphi_i(X) - \delta, 0], & i = p+1, \ldots, \kappa \end{cases} \tag{21}$$

where υ is the overall constraint violation of the infeasible solution weighted mean of all constraints. λ_i is set as $1G_{\max,i}$, where $G_{\max,i}$ is the maximum value of $G_i(X)$. p is the number of inequality constraints and $\kappa - p$ is the number of equality constraints.

Step 3: Generate the mutated population $WD_g = \{W_{1,g}, W_{2,g}, \ldots, W_{NP,g}\}$ by performing mutation operation. Here, the "DE/rand/1" is used as follows:

$$W_{i,g} = U_{r_1,t} + F(U_{r_2,t} - U_{r_3,t}) \tag{22}$$

where r_1, r_2, and r_3 represent the distinct integers randomly selected from $[1, NP]$.

Step 4: Generate the trial population $YD_g = \{Y_{1,g}, Y_{2,g}, \ldots, Y_{NP,g}\}$ by performing crossover operation. Binomial crossover is employed as follows:

$$y_{i,j,g} = \begin{cases} w_{i,j,g}, & \text{if } j = j_{\text{rand}} \text{ or } \text{rand}_j(0,1) \le CR \\ u_{i,j,g}, & \text{otherwise} \end{cases} \tag{23}$$

where j_{rand} denotes a randomly chosen integer in $[1, D]$.

Step 5: Calculate the fitness value and constraint violation of each trial population in WD_g.

Step 6: Compare U_i in PD_g with W_i in WD_g and select the better individual into the next-generation population PD_{g+1} in terms of the superiority of the feasible solution constraint handling technique (SF). In SF, U_i is viewed as better than W_i when: 1) U_i is feasible, but W_i is infeasible; 2) U_i and W_i are feasible, but U_i achieves a smaller fitness value; and 3) U_i and W_i are infeasible, but U_i achieves a better overall constraint violation.

Step 7: Set $g = g + 1$.

Step 8: Obtain the number of contaminated meters and corresponding locations when $EFS_{\max}$ is satisfied; otherwise, go to Step 2.

IV. CUSUM-Based Detection Mechanism

In this section, the proposed detection mechanism is given. Suppose that the attackers are initially inactive and start to launch attacks at an unknown time τ. The system can be described as follows:

$$\mathbf{z}_t = h(\mathbf{x}_t) + \omega_t, \qquad t \le \tau \tag{24}$$

$$\mathbf{z}_t = h(\mathbf{x}_t) + \mathbf{a}_t + \omega_t, \; t > \tau \tag{25}$$

where $\mathbf{z}_t$ and $\mathbf{a}_t$ represent the measurements and the injected attacks, respectively. $\omega_t \sim N(0, \sigma_w^2 \mathbf{I}_K)$ are supposed to be independent additive white Gaussian random processes, where $\mathbf{I}_K$ represents a $K \times K$ identity matrix.

Then, the hypothesis test of the attack detection problem can be expressed as follows:

$$H_0 : \mathbf{z}_t = h(\mathbf{x}_t) + \omega_t \qquad \forall t$$

$$H_1 : \mathbf{z}_t = \begin{cases} h(\mathbf{x}_t) + \omega_t, & t \le \tau \\ h(\mathbf{x}_t) + \mathbf{a}_t + \omega_t, & t > \tau \end{cases} \tag{26}$$

where the null hypothesis H_0 represents measurements without attacks. The alternative hypothesis H_1 represents measurements with FDIA. In particular, we use the following definition to

describe the worst-case detection delay [30]:

$$J(T) = \sup_{\tau \geq 1} E_\tau[(T-\tau)|T \geq \tau] \tag{27}$$

where T represents the stopping detection time of a detection scheme. The optimization problem can be further described as follows:

$$\inf_T J(T) = \text{s.t. } E_\infty[T] \geq \alpha \tag{28}$$

where α represents a predetermined lower bound of $E_\infty[T]$. Here, we denote the two probability density functions of measurements given in (24) and (25) as $p^0(\mathbf{z}_t|\mathbf{x}_t)$ and $p^f(\mathbf{z}_t|\mathbf{x}_t, \mathbf{a}_t)$, respectively. The optimal solution to (28) can be found by the CUSUM test [17]

$$T^f = \inf\left\{ m \in \mathbb{N} : \max_{1\leq j\leq m} \sum_{t=j}^{m} \log \frac{p^f(\mathbf{z}_t|\mathbf{x}_t, \mathbf{a}_t)}{p^0(\mathbf{z}_t|\mathbf{x}_t)} \geq h^f \right\} \tag{29}$$

where h^f represents the test threshold. As suggested in [17], the generalized likelihood ratio method is used to replace the unknown quantities with related estimates. Two different state estimates under null and alternative hypotheses need to be obtained according to corresponding measurement models. To this end, two parallel state estimators are used simultaneously. Considering that the power system involves high dynamics in the ac model, using the traditional IWLS estimator to forecast the state values is inconvenient. Thus, fractional-order theory is introduced into IWLS to describe the state transition matrix.

Here, the state transition matrix $\mathbf{A_t}$ is supposed to be diagonal, which is expressed as follows:

$$\mathbf{A_t} = \begin{bmatrix} \Theta_t & 0 \\ 0 & \Lambda_t \end{bmatrix} \tag{30}$$

where Θ_t and Λ_t denote the voltage angles and voltage magnitudes, respectively.

As shown in [31], the fractional-order discrete nonlinear system is described as follows:

$$\begin{aligned} \nabla^\alpha \mathbf{x}_t &= \mathbf{f}_{t-1}(\mathbf{x}_{t-1}) + \omega_{t-1} \\ \mathbf{x}_t &= \nabla^\alpha \mathbf{x}_t - \sum_{j=1}^{t} (-1)^j \gamma_j \mathbf{x}_{t-j} \\ \mathbf{z}_t &= \mathbf{h}_t(\mathbf{x}_t) + \mathbf{v}_t \end{aligned} \tag{31}$$

with

$$\begin{aligned} \nabla^\alpha &= [\nabla^{\alpha_1}, \ldots, \nabla^{\alpha_n}] \\ \gamma_j &= \text{diag}\left[\binom{\alpha_1}{j}, \ldots, \binom{\alpha_n}{j}\right] \end{aligned} \tag{32}$$

where ∇ is the nabla operator defined as follows:

$$\begin{aligned} \nabla^\alpha f(t) &= \sum_{j=0}^{t} (-1)^j \binom{\alpha}{j} f(k-j) \\ \binom{\alpha}{j} &= \frac{\alpha(\alpha-1)\cdots(\alpha-j+1)}{j!}. \end{aligned} \tag{33}$$

By introducing A_t, (32) can be rewritten as

$$\mathbf{x}_k + \sum_{j=1}^{t} (-1)^j \gamma_j \mathbf{x}_{t-j} = \mathbf{A}_t \mathbf{x}_{t-1}. \tag{34}$$

Denote $\mathbf{x}_t + \sum_{j=1}^{t} (-1)^j \gamma_j \mathbf{x}_{t-j}$ as $\mathbf{y}_t$; then, for the previous T_t state, (34) can be expressed as

$$\mathbf{Y}_k^{T_t} = (\mathbf{X}_t^{T_t-1})^T \mathbf{F}_t \tag{35}$$

where $Y_k^{T_t} = [y_t, y_{t-1}, \ldots, y_{t-T_t+1}]^T$ and $X_k^{T_t-1} = [x_{k-1}, x_{k-2}, \ldots, x_{k-T_t}]^T$. Finally, $\mathbf{A_t}$ can be obtained as

$$\mathbf{A}_t = (\mathbf{X}_t^{T_t-1}(\mathbf{X}_t^{Tt-1})^T)^{-1} \mathbf{X}_t^{Tt-1} \mathbf{Y}_t^{Tt}. \tag{36}$$

Based on the fractional-order state transition matrix, two parallel state predictions are given as follows:

$$\begin{cases} \hat{\mathbf{x}}_{t|t-1}^0 = \mathbf{A}_t \hat{\mathbf{x}}_{t-1|t-1}^0 \\ \hat{\mathbf{x}}_{t|t-1}^f = \mathbf{A}_t \hat{\mathbf{x}}_{t-1|t-1}^f \end{cases} \tag{37}$$

where $\hat{\mathbf{x}}_{t|t}^0$ and $\hat{\mathbf{x}}_{t|t}^f$ represent the state estimates at time t for null and alternative hypotheses, respectively. $\hat{\mathbf{x}}_{t-1|t-1}^0$ and $\hat{\mathbf{x}}_{t-1|t-1}^f$ are estimated by IWLS [32]. According to the generalized CUSUM test, the stopping time can be calculated as follows [16]:

$$T^f = \inf\left\{ m \in \mathbb{N} : \underbrace{\max_{1\leq j\leq m} \sum_{t=j}^{m} \beta_t}_{g_m^f} \geq h^f \right\} \tag{38}$$

where β_t is the generalized log-likelihood ratio and can be expressed as follows:

$$\beta_t = \sup_{S_t^f} \log \frac{\sup_{|\mathrm{a}_{k,t}|\geq\eta, k\in S_t^f} p^f(\mathbf{z}_t|\hat{\mathbf{x}}_{t|t-1}^f, \mathbf{a}_t)}{p^0(\mathbf{z}_t|\hat{\mathbf{x}}_{t|t-1}^0)} \tag{39}$$

where S_t^f is the set of contaminated measurements. $\mathbf{a}_\mathrm{t}$ is the attack vector, and $\mathrm{a}_{k,t}$ is the kth element in $\mathbf{a}_\mathrm{t}$. Due to $\mathbf{w}_t \sim N(\mathbf{0}, \sigma_w^2 \mathbf{I}_K)$, the normal measurement model and the attacked measurement model are $\mathbf{z}_t \sim N(h(\mathbf{x}_t), \sigma_w^2 \mathbf{I}_K)$ and $\mathbf{z}_t \sim N(h(\mathbf{x}_t) + \mathbf{a}_t, \sigma_w^2 \mathbf{I}_K)$, respectively. Then, $p^0(\mathbf{z}_t|\hat{\mathbf{x}}_{t|t-1}^0)$ can be written as

$$\begin{cases} p^0(\mathbf{z}_t|\hat{\mathbf{x}}_{t|t-1}^0) = \frac{1}{\sqrt{2\pi}\sigma_w} \exp(\Phi_0) \\ \Phi_0 = \frac{-(\mathbf{z}_t - h(\hat{\mathbf{x}}_{t|t-1}^0))^T (\mathbf{z}_t - h(\hat{\mathbf{x}}_{t|t-1}^0))}{2\sigma_w{}^2} \end{cases}. \tag{40}$$

Similarly, $p^f(\mathbf{z}_t|\hat{\mathbf{x}}_{t|t-1}^f, \mathbf{a}_t)$ is expressed as

$$\begin{cases} p^f(\mathbf{z}_t|\hat{\mathbf{x}}_{t|t-1}^f, \mathbf{a}_t) = \frac{1}{\sqrt{2\pi}\sigma_w} \exp(\Phi_f) \\ \Phi_f = \frac{-(\mathbf{z}_t - h(\hat{\mathbf{x}}_{t|t-1}^f) - \mathbf{a}_t)^T (\mathbf{z}_t - h(\hat{\mathbf{x}}_{t|t-1}^f) - \mathbf{a}_t)}{2\sigma_w{}^2} \end{cases}. \tag{41}$$

Upon substituting (40) and (41) into (39), β_t is obtained as

$$\beta_t = \sup_{S_t^f} \log \frac{\sup_{|\mathrm{a}_{k,t}|\geq\eta, k\in S_t^f} \exp\{\Phi_f\}}{\exp\{\Phi_0\}}. \tag{42}$$

Because $\mathrm{a}_{k,t} = 0$ when the set of meters $\{k \notin S_t^f\}$ and calculating the supremum of quantity is equivalent to calculating the

infimum of the negative of the quantity, β_t can be obtained as in (43) based on (42)

$$\beta_t = \frac{1}{2\sigma_w^2}\left(\sum_{k=1}^{K}\left(z_{k,t}-\mathbf{H}_{k,t}^T\hat{\mathbf{x}}_{t|t-1}^0\right)^2 - \inf_{S_t^f}\left\{\sum_{k\in S_t^f}\inf_{|\mathrm{a}_{k,t}|\geq\eta}\left(z_{k,t}-\mathbf{H}_{k,t}^T\hat{\mathbf{x}}_{t|t-1}^f-\mathrm{a}_{k,t}\right)^2+\sum_{k\notin S_t^f}\left(z_{k,t}-\mathbf{H}_{k,t}^T\hat{\mathbf{x}}_{t|t-1}^f\right)^2\right\}\right)$$

$$=\frac{1}{2\sigma_w^2}\sum_{k=1}^{K}\left(\left(z_{k,t}-\mathbf{H}_{k,t}^T\hat{\mathbf{x}}_{t|t-1}^0\right)^2-\left(z_{k,t}-\mathbf{H}_{k,t}^T\hat{\mathbf{x}}_{t|t-1}^f-\hat{\mathbf{a}}_{k,t}\right)^2\right) \tag{43}$$

where $\mathbf{H}_{k,t}$ is the kth row of $\mathbf{H}_t$. Moreover, the Jacobian matrix $\mathbf{H}_t$ can be expressed as

$$\mathbf{H}_t=\begin{bmatrix}\frac{\partial V_i}{\partial\theta} & \frac{\partial P_i}{\partial\theta} & \frac{\partial Q_i}{\partial\theta} & \frac{\partial P_{ij}}{\partial\theta} & \frac{\partial Q_{ij}}{\partial\theta}\\ \frac{\partial V_i}{\partial V} & \frac{\partial P_i}{\partial V} & \frac{\partial Q_i}{\partial V} & \frac{\partial P_{ij}}{\partial V} & \frac{\partial Q_{ij}}{\partial V}\end{bmatrix}^T. \tag{44}$$

Then, maximum likelihood estimate (MLE) of $\mathrm{a}_{k,t}$ is calculated as follows:

$$\hat{\mathrm{a}}_{k,t}=\underset{|\mathrm{a}_{k,t}|\geq\eta,k\in S_t^f}{\operatorname{argmin}}\left(e_{k,t}-\mathrm{a}_{k,t}\right)^2 \tag{45}$$

where $e_{k,t}=z_{k,t}-\mathbf{H}_{k,t}^T\hat{\mathbf{x}}_{t|t-1}^f$. We have $\frac{\partial\hat{\mathbf{a}}_{k,t}}{\partial\mathrm{a}_{k,t}}=-2(e_{k,t}-\mathrm{a}_{k,t})=0$ if $\mathrm{a}_{k,t}=e_{k,t}$. Then

$$\hat{\mathrm{a}}_{k,t}=\begin{cases}e_{k,t}, & \text{if } |e_{k,t}|\geq\eta, k\in S_t^f\\ \eta, & \text{if } 0\leq e_{k,t}<\eta, k\in S_t^f\\ -\eta, & \text{if } -\eta<e_{k,t}<0, k\in S_t^f\\ 0, & \text{if } k\notin S_t^f\end{cases}. \tag{46}$$

Similarly, MLE of S_t^f can be calculated as follows:

$$\hat{S}_t^f=\underset{S_t^f\subset\{1,\ldots,K\}}{\operatorname{argmin}}\sum_{k\in S_t^f}\left(e_{k,t}-\hat{\mathrm{a}}_{k,t}\right)^2+\sum_{k\notin S_t^f}e_{k,t}^2$$

$$=\left\{k:|e_{k,t}|>\frac{\eta}{2},k=1,\ldots,K\right\}. \tag{47}$$

Thus, combining (46) and (47), $\hat{\mathrm{a}}_{k,t}$ is rewritten as

$$\hat{\mathrm{a}}_{k,t}=\begin{cases}e_{k,t}, & \text{if } |e_{k,t}|\geq\eta\\ \eta, & \text{if } \frac{\eta}{2}<e_{k,t}<\eta\\ -\eta, & \text{if } -\eta<e_{k,t}<-\frac{\eta}{2}\\ 0, & \text{else}\end{cases} \tag{48}$$

where η is the scale of security attentions and K is the number of meters.

Finally, according to (38), decision statistic g_m^f at time t can be updated as

$$g_t^f=\left(g_{t-1}^f+\beta_t\right)^+ \tag{49}$$

where g_0^f is set as 0 and $(\cdot)^+=\max(\cdot,0)$.

Fig. 2 provides the framework of the proposed CDE-based stealthy sparse cyber-attack and its countermeasure.

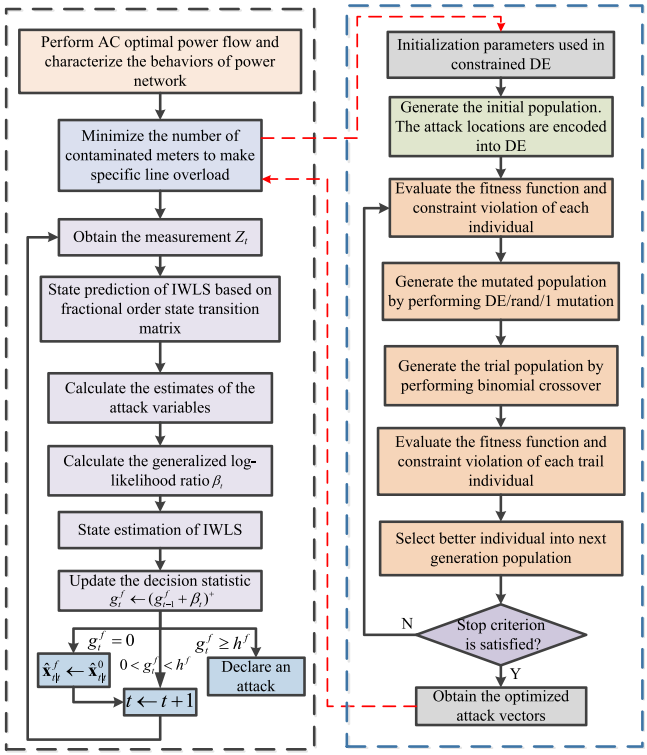

Fig. 2. Framework of the proposed CDE-based stealthy sparse cyber-attack and its countermeasure.

TABLE III
MEASUREMENTS FOR DIFFERENT IEEE SYSTEMS

Test system	14-bus	30-bus	118-bus
Number of lines	20	41	186
Number of states	27	59	235
Number of injection measurements	14	30	78
Number of flow measurements	34	46	222
Number of decision variables	50	78	302
Redundancy	1.85	1.32	1.28

V. SIMULATION RESULTS

This section is devoted to illustrating the efficiency of DE-based stealthy sparse cyber-attack and CUSUM-based detection mechanism by using three IEEE systems, i.e., IEEE 14-bus, 30-bus, and 118-bus systems. If $g_t^f=0$ for any time t, the change-point estimate is updated to time t, and IWLS estimates for the alternative hypothesis are updated by $\hat{\mathbf{x}}_{t|t}^f=\hat{\mathbf{x}}_{t|t}^0$.

A. Investigations on Stealthy Sparse Cyber-Attack

The line parameters and network topologies of the three considered systems are taken from MATPOWER [33]. The detailed measurements are given in Table III. In addition, two additional meters are used to obtain the voltage magnitude and phase angle for each considered system. The meter placements of all test systems are from [34], which are fully observable. After obtaining measurements, we can determine the dimensions of the decision variable in the CDE algorithm. For example, the meters of the IEEE 14-bus system contain 14 injection measurements, 34 flow measurements, one voltage magnitude, and one phase angle, i.e., the dimension is 50 for the decision

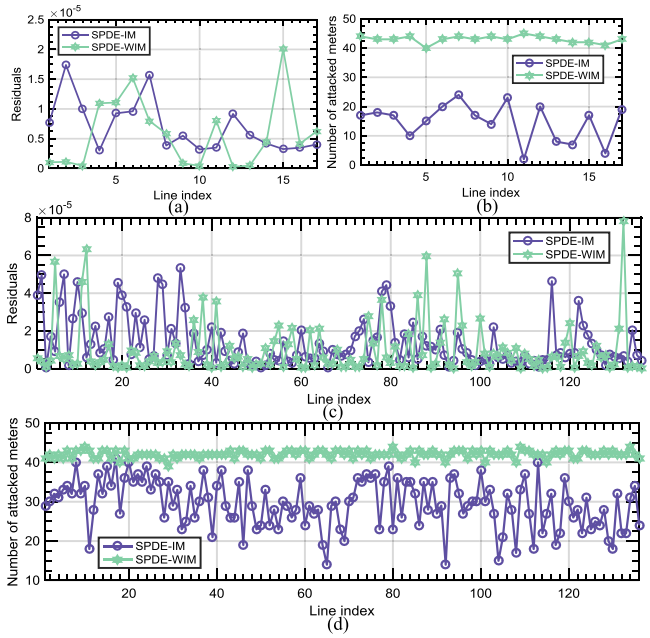

Fig. 3. Attack strategies on the IEEE 14-bus system obtained by SPED-IM and SPED-WIM. (a) Residues after the attack on a single line. (b) Number of attacked meters on a single line. (c) Residues after the attack on two lines. (d) Number of attacked meters on two lines.

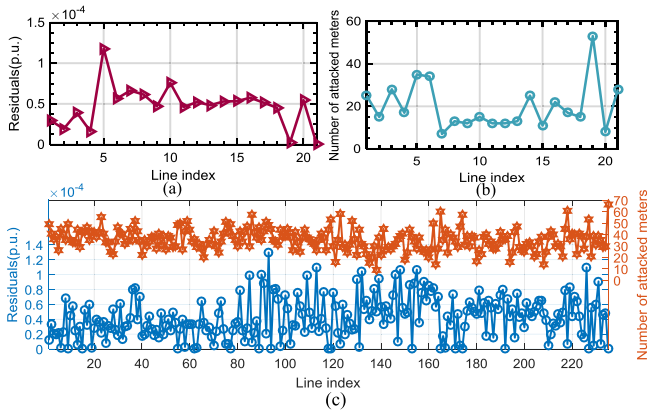

Fig. 4. Residues after the attack and number of attacked meters on the IEEE 30-bus system by SPED-IM. (a) Attack on a single line. (b) Attack on two lines.

variable in CDE. To launch the stealthy sparse cyber-attack, we first perform OPF and then solve the fitness function based on (4)–(16). The adjustable parameters of SPDE-IM include mutation factor (F), crossover rate (CR), number of population (NP), and maximum number of function evaluation ($FES_{\max}$) setting as 0.7, 0.9, 200, and 200 000, respectively. All of the simulations are performed based on MATLAB 2018a on a PC with an Intel Core i7 CPU @ 2.5 GHz and a RAM of 8.00 GB.

To illustrate the feasibility of the proposed stealthy sparse cyber-attack model based on SPDE-IM, a series of simulations are considered. The attack strategy is launched to overload a single line and two lines on different systems. Figs. 3 and 4 provide the residuals and number of contaminated meters obtained by SFDE-IM for the IEEE 14-bus and IEEE 30-bus systems on attacking a single line and multiple lines. As seen

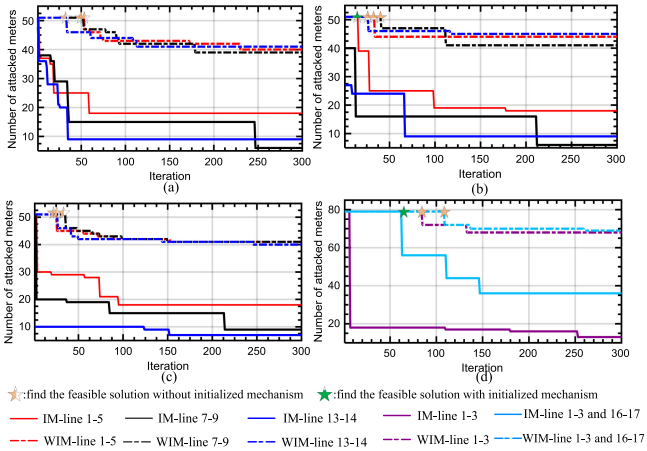

Fig. 5. Convergence curves under different cases. (a) SFDE-IM and SFDE-WIM for the IEEE 14-bus system. (b) SPDE-IM and SPDE-WIM for the IEEE 14-bus system. (c) EnDE-IM and EnDE-WIM for the IEEE 14-bus system. (d) SFDE-IM and SFDE-WIM for the IEEE 30-bus system.

in Fig. 3, the residuals are all lower than 2.5e-5 and 8e-5 per unit for launching the attacks on a single line and two lines on the IEEE 14-bus system, respectively. The residuals are all lower than 1.5e-4 per unit and 1.4e-4 per unit for attacking the IEEE 30-bus system presented in Fig. 4. These results imply that redundant measurements cannot contribute to detecting the proposed cyber-attack. In addition, Fig. 3 also shows the residuals and number of contaminated meters obtained by SPDE without an initialized coding mechanism (SFDE-WIM). As seen in Fig. 3(b) and (d), attack strategies are more or less varied with aiming at different lines. Although the SFDE-WIM attack strategies can bypass the residual error detection, SFDE-IM achieves sparser results on attacking the same line, indicating that SFDE-IM-based strategies have a lower attack effect than SFDE-WIM.

To further demonstrate the efficiency of IM in CDE, in addition to SFDE-IM, self-adaptive-penalty-based DE (SPDE) and ensembles of SFDE and SPED (EnDE) are considered by incorporating IM, denoted as SPDE-IM and EnDE-IM, respectively. The versions without IM, denoted as SPDE-WIM and EnDE-WIM, are used as the competitors. The NP is set as 200, 200, and 100 for SFDE, SPDE, and EnDE, respectively. The $FES_{\max}$ is set as 300 000 for all three algorithms, and other adjustable parameters are recommended by Biswas *et al.* [11]. Fig. 5(a)–(c) shows the obtained convergence characteristics on attacking three different lines, i.e., line 1-5, line 7-9, and line 13-14 in the IEEE 14-bus system. It can be seen that the performance of the algorithms with IM version is highly appreciated because it achieves a better rate of convergence and better fitness values in less time than those by WIM versions. Furthermore, for the IEEE 30-bus system, in addition to attacking a single line, attacking two lines, i.e., line 1-3 and line 16-17, is given in Fig. 5(d). From Fig. 5(d), the same conclusion can be drawn that the proposed IM is helpful to search for a better solution. Nonetheless, the aim of this simulation is not to illustrate the superiority of any algorithm over the other but to note the fact

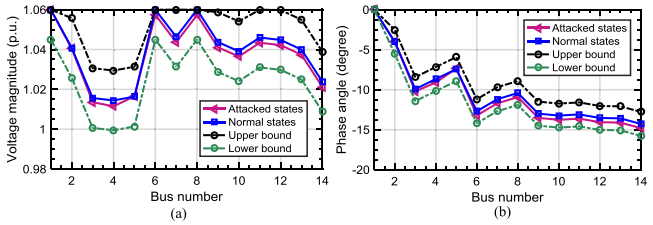

Fig. 6. Stealthy attacks on line 2-5 of the IEEE 14-bus system against an ISE detector. (a) Voltage magnitude estimates. (b) Phase angle estimates.

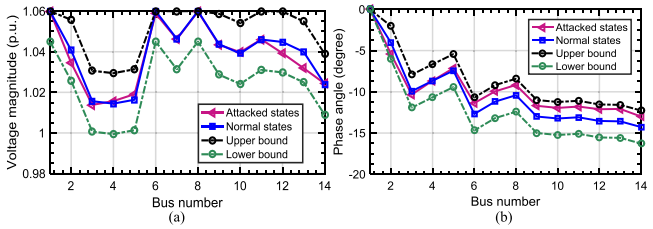

Fig. 7. Stealthy attacks on line 1-2 and line 3-4 of the IEEE 14-bus system against an ISE detector. (a) Voltage magnitude estimates. (b) Phase angle estimates.

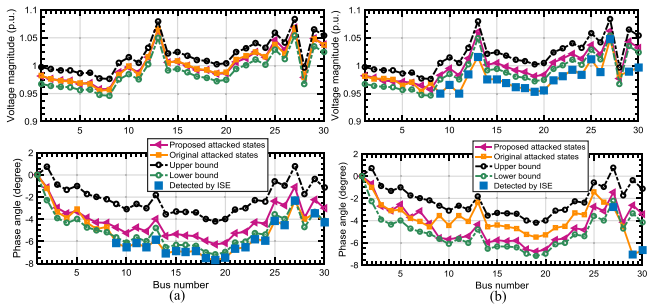

Fig. 8. Stealthy attacks on the IEEE 30-bus system. (a) Attack on line 1-2. (b) Attack on line 2-6 and line 8-28.

that the proposed IM can be incorporated into various algorithms to launch the attack.

To show the stealthy attacks against an ISE detector, we take the attack on single line (i.e., line 4-5) and multiple lines (i.e., line 1-2 and line 3-4) as examples with the corresponding results presented in Figs. 6 and 7, respectively. Clearly, all of the attacked states stay in the acceptable interval, and thus, this stealthy attack can bypass an ISE detector. In Figs. 8 and 9, we also show the original attack strategies (i.e., the attack model in [3]) for comparison. Fig. 8 provides an example of the compared results of the proposed attack strategy and the original one for the IEEE 30-bus system to overload a single line and multiple lines. The two attacks designed to overload line 1-3 on the IEEE 118-bus system are depicted in Fig. 9. Figs. 8 and 9 clearly show that the original attacked states are out of a determined ISE detector, whereas the proposed attacks successfully bypass the ISE detector to overload the lines. This indicates that a well-designed attack strategy can bypass the ISE detector and the traditional residual test.

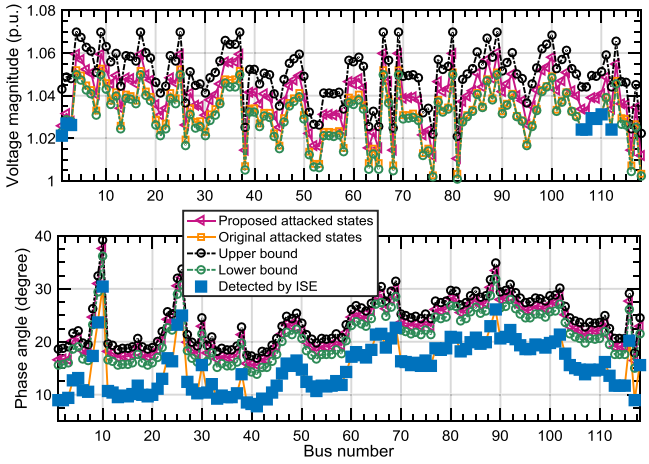

Fig. 9. Stealthy attacks on lines of the IEEE 118-bus system.

B. Investigations on CUSUM-Based Detection Mechanism

In this subsection, we test the effectiveness of the CUSUM-based detection mechanism. There are two key parameters, i.e., γ and h^f, in the CUSUM-based detector. High thresholds will obtain a small false alarm rate but might cause larger detection delays. Here, η and h^f are selected as 0.001 and 10 000 by trial and error, respectively. The cyber-attack is assumed to be launched at $\tau = 25$.

To test the superiority of the proposed CUSUM-based detector, chi-square distribution test (χ^2-test), largest normalized residual (LNR), a sample ISE (S-ISE) detector, DL-ISE detector [3], SU-ISE detector [12], and R-ISE detector [13] are used to detect stealthy sparse cyber-attacks. To ensure a fair comparison, we consider the same attack vectors based on the proposed method to attack the system. Then, the current system is integrated by using the proposed detector and other compared detectors to detect the proposed cyber-attacks. Table IV provides several results. Table IV shows that the LNR and χ^2-test fail to recognize the proposed attacks because these two are residual-based detectors. Table IV also shows that the four different ISE-based detectors, i.e., S-ISE, DL-ISE, SU-ISE, and R-ISE, cannot find abnormal values under considering attack cases. This can be explained by the attack strategy, which considers the ISE detection mechanism to launch the cyber-attack. In contrast, the proposed CUSUM-based detector can effectively detect attacks in all attack cases because it does not depend on residual and state interval. Additionally, Fig. 10 checks all single-line and two-line attack on the IEEE 14-bus system. Except for the attack on line 12-13, all attacks can be detected by the proposed method, whose values of g_t are all higher than h_f. In practice, the attack on line 12-13 can be detected with five sample delays, because h_f can be cumulative with the attack. Fig. 10 provides the comparison results of h_f and g_t on the IEEE 30-bus system under attacks on single line and two lines. Clearly, all of the values of g_t at $t = 25$ are larger than h_f, which means that the proposed detection mechanism can recognize the attacks in a timely manner. Comparing Fig. 10(a) with Fig. 10(b) [or comparing Fig. 11(a) with Fig. 11(b)], the minimum g_t of the two-line

TABLE IV
COMPARISON RESULTS OF DETECTING STEALTHY SPARSE ATTACKS

Attack case	Proposed detector	S-ISE	R-ISE [13]	DL-ISE [3]	SU-ISE [12]	χ^2-test	LNR
Attack in Fig.6	Successful	Fail	Fail	Fail	Fail	Fail	Fail
Attack in Fig.7	Successful	Fail	Fail	Fail	Fail	Fail	Fail
Attack in Fig.8(a)	Successful	Fail	Fail	Fail	Fail	Fail	Fail
Attack in Fig.8(b)	Successful	Fail	Fail	Fail	Fail	Fail	Fail
Attack in Fig.9	Successful	Fail	Fail	Fail	Fail	Fail	Fail

"Successful (Fail)": the corresponding method can (cannot) recognize the proposed attack strategy.

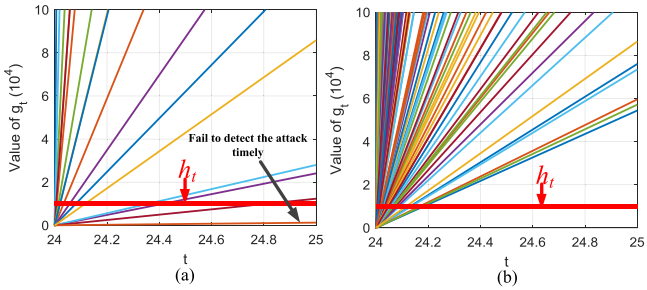

Fig. 10. Values of g_t of attack on the IEEE 14-bus system. (a) Single line. (b) Two lines.

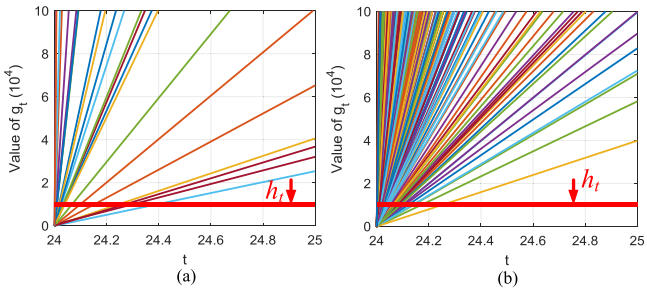

Fig. 11. Values of g_t of attack on the IEEE 30-bus system. (a) Single line. (b) Two lines.

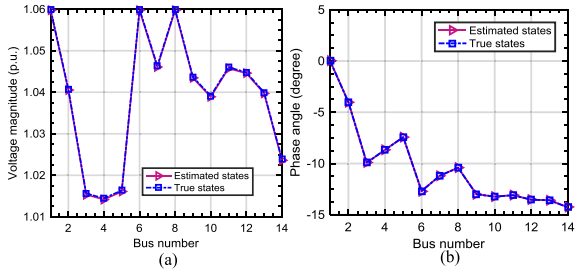

Fig. 12. Recovery of the IEEE 14-bus system under attack line 2-5. (a) Voltage magnitude estimates. (b) Phase angle estimates.

attack is larger than that of the single-line attack. Intuitively, attacks on two lines are easier to detect than single-line attack.

In the CUSUM-based detector, the magnitude of the injected maliciousness can be obtained by (46), which is critical for system recovery. Fig. 12 provides the results of the system recovery under the attack on line 7-8 when the proposed CUSUM-based detector successfully detects cyber-attacks at attack time. The system is seen to recover compared with the nonrecovered state values given in Fig. 6 in the case of the proposed FDIA.

Additionally, the performance of the proposed detector is evaluated on dc-based FDIA. Here, the IEEE 14-bus and IEEE

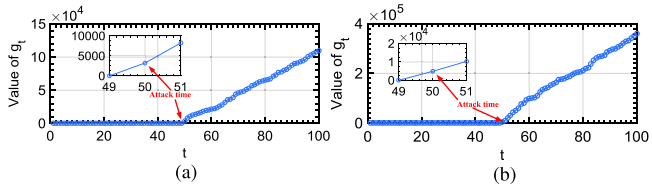

Fig. 13. Sample responses of the proposed CUSUM-based detector on the IEEE 14-bus system. (a) Random FDIA. (b) Stealthy FDIA.

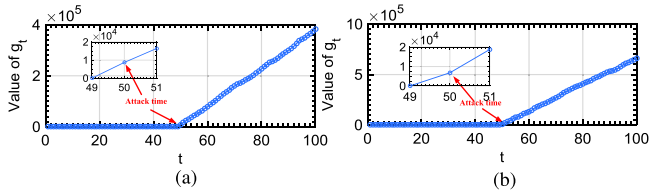

Fig. 14. Sample responses of the proposed CUSUM-based detector on the IEEE 57-bus system. (a) Random FDIA. (b) Stealthy FDIA.

57-bus systems are used as examples. Two cases are considered for each power system. One is attacked by random FDIA, and the other is attacked by stealthy FDIA. The detailed parameters are taken from [16] and [35]. Figs. 13 and 14 present the sample responses of the proposed CUSUM-based detector on the IEEE 14-bus system and the IEEE 57-bus system, respectively. Figs. 13 and 14 show that the decision statistic abruptly changes when the attack is launched, implying that the proposed CUSUM-based detector is valid in detecting dc-based FDIA.

VI. CONCLUSION

In this article, an innovative stealthy sparse cyber-attack model was proposed. In the designed attack model, the characteristics of the residual test-based detector and the ISE detector were considered to ensure that the attack can bypass these detectors. In addition, CDE was used as the search engine to construct the optimal sparse cyber-attack by minimizing the number of contaminated meters to make specific line overload. According to the unique characteristic of designing attack, an initialized coding mechanism was proposed to describe the problem. The effectiveness of the initialized coding mechanism was illustrated by three different CDE algorithms. Then, a novel countermeasure was developed to detect the proposed attacks. In this countermeasure, generalized CUSUM was used to detect the attack, where a fractional-order state transition matrix was introduced into IWLS to describe the dynamics of the power system to forecast the state value. The validations and benefits of the CDE-based stealthy sparse cyber-attack method and the CUSUM-based detector were illustrated on three IEEE bus

systems. The achieved results indicated potential behavior of attackers and highlighted the importance of the defense mechanism for smart grids against stealthy sparse FDIA.

REFERENCES

[1] A. S. Musleh, G. Chen, and Z. Y. Dong, "A survey on the detection algorithms for false data injection attacks in smart grids," *IEEE Trans. Smart Grid*, vol. 11, no. 3, pp. 2218–2234, May 2020.

[2] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 Ukraine blackout: Implications for false data injection attacks," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3317–3318, Jul. 2017.

[3] H. Wang *et al.*, "Deep learning-based interval state estimation of AC smart grids against sparse cyber attacks," *IEEE Trans. Ind. Informat.*, vol. 14, no. 11, pp. 4766–4778, Nov. 2018.

[4] 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. 1–33, 2011.

[5] Y. Tan, Y. Li, Y. Cao, and M. Shahidehpour, "Cyber-attack on overloading multiple lines: A bilevel mixed-integer linear programming model," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 1534–1536, Mar. 2018.

[6] Y. Wu, Z. Wei, J. Weng, X. Li, and R. H. Deng, "Resonance attacks on load frequency control of smart grids," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 4490–4502, Sep. 2018.

[7] 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.

[8] J. Hao, R. J. Piechocki, D. Kaleshi, W. H. Chin, and Z. Fan, "Sparse malicious false data injection attacks and defense mechanisms in smart grids," *IEEE Trans. Ind. Informat.*, vol. 11, no. 5, pp. 1–12, Oct. 2015.

[9] 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.

[10] M. R. Mengis and A. Tajer, "Data injection attacks on electricity markets by limited adversaries: Worst-case robustness," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 5710–5720, Nov. 2018.

[11] P. P. Biswas, P. N. Suganthan, R. Mallipeddi, and G. A. Amaratunga, "Optimal power flow solutions using differential evolution algorithm integrated with effective constraint handling techniques," *Eng. Appl. Artif. Intell.*, vol. 68, pp. 81–100, 2018.

[12] H. Wang *et al.*, "Dynamic data injection attack detection of cyber physical power systems with uncertainties," *IEEE Trans. Ind. Informat.*, vol. 15, no. 10, pp. 5505–5518, Oct. 2019.

[13] H. Wang, X. Wen, S. Huang, B. Zhou, Q. Wu, and N. Liu, "Generalized attack separation scheme in cyber physical smart grid based on robust interval state estimation," *Int. J. Elect. Power Energy Syst.*, vol. 129, 2021, Art. no. 106741.

[14] S. Li, Y. Yılmaz, and X. Wang, "Quickest detection of false data injection attack in wide-area smart grids," *IEEE Trans. Smart Grid*, vol. 6, no. 6, pp. 2725–2735, Nov. 2015.

[15] Y. Huang, J. Tang, Y. Cheng, H. Li, K. A. Campbell, and Z. Han, "Real-time detection of false data injection in smart grid networks: An adaptive CUSUM method and analysis," *IEEE Syst. J.*, vol. 10, no. 2, pp. 532–543, Jun. 2016.

[16] M. N. Kurt, Y. Yılmaz, and X. Wang, "Distributed quickest detection of cyber-attacks in smart grid," *IEEE Trans. Inf. Forensics Secur.*, vol. 13, no. 8, pp. 2015–2030, Aug. 2018.

[17] M. N. Kurt, Y. Yilmaz, and X. Wang, "Real-time detection of hybrid and stealthy cyber-attacks in smart grid," *IEEE Trans. Inf. Forensics Secur.*, vol. 14, no. 2, pp. 498–513, Feb. 2019.

[18] L. Che, X. Liu, Z. Li, and Y. Wen, "False data injection attacks induced sequential outages in power systems," *IEEE Trans. Power Syst.*, vol. 34, no. 2, pp. 1513–1523, Mar. 2019.

[19] Z. Zhang, R. Deng, D. K. Y. Yau, and P. Chen, "Zero-parameter-information data integrity attacks and countermeasures in IoT-based smart grid," *IEEE Internet of Things J.*, vol. 8, no. 8, pp. 6608–6623, Apr. 2021.

[20] J. Zhao, L. Mili, and M. Wang, "A generalized false data injection attacks against power system nonlinear state estimator and countermeasures," *IEEE Trans. Power Syst.*, vol. 33, no. 5, pp. 4868–4877, Sep. 2018.

[21] W.-L. Chin, C.-H. Lee, and T. Jiang, "Blind false data attacks against AC state estimation based on geometric approach in smart grid communications," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 6298–6306, Nov. 2018.

[22] Q. Yang, D. An, R. Min, W. Yu, X. Yang, and W. Zhao, "On optimal PMU placement-based defense against data integrity attacks in smart grid," *IEEE Trans. Inf. Forensics Secur.*, vol. 12, no. 7, pp. 1735–1750, Jul. 2017.

[23] S. Bi and Y. J. Zhang, "Using covert topological information for defense against malicious attacks on DC state estimation," *IEEE J. Sel. Areas Commun.*, vol. 32, no. 7, pp. 1471–1485, Jul. 2014.

[24] S. Wang, S. Bi, and Y.-J. A. Zhang, "Locational detection of the false data injection attack in a smart grid: A multilabel classification approach," *IEEE Internet of Things J.*, vol. 7, no. 9, pp. 8218–8227, Sep. 2020.

[25] M. N. Kurt, O. Ogundijo, C. Li, and X. Wang, "Online cyber-attack detection in smart grid: A reinforcement learning approach," *IEEE Trans. Smart Grid*, vol. 10, no. 5, pp. 5174–5185, Sep. 2019.

[26] T. Wu *et al.*, "Extreme learning machine-based state reconstruction for automatic attack filtering in cyber physical power system," *IEEE Trans. Ind. Informat.*, vol. 17, no. 3, pp. 1892–1904, Mar. 2021.

[27] S. Pal, B. Sikdar, and J. H. Chow, "Classification and detection of PMU data manipulation attacks using transmission line parameters," *IEEE Trans. Smart Grid*, vol. 9, no. 5, pp. 5057–5066, Sep. 2018.

[28] R. Deng, G. Xiao, and R. Lu, "Defending against false data injection attacks on power system state estimation," *IEEE Trans. Ind. Inform.*, vol. 13, no. 1, pp. 198–207, Feb. 2017.

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

[30] T. Zhou, K. Xiahou, L. L. Zhang, and Q. H. Wu, "Real-time detection of cyber-physical false data injection attacks on power systems," *IEEE Trans. Ind. Informat.*, vol. 17, no. 10, pp. 6810–6819, Oct. 2021.

[31] T. Liu, S. Cheng, Y. Wei, A. Li, and Y. Wang, "Fractional central difference Kalman filter with unknown prior information," *Signal Process.*, vol. 154, pp. 294–303, 2019.

[32] A. Abur and A. G. Exposito, *Power System State Estimation: Theory and Implementation*. Boca Raton, FL, USA: CRC Press, 2004.

[33] R. D. Zimmerman, C. E. Murillo-Sánchez, 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.

[34] J. Zhao, M. Netto, and L. Mili, "A robust iterated extended Kalman filter for power system dynamic state estimation," *IEEE Trans. Power Syst.*, vol. 32, no. 4, pp. 3205–3216, Jul. 2017.

[35] M. N. Kurt, Y. Yilmaz, and X. Wang, "Real-time nonparametric anomaly detection in high-dimensional settings," *IEEE Trans. Pattern Anal. Mach. Intell.*, vol. 43, no. 7, pp. 2463–2479, Jul. 2021.

Kang-Di Lu received the B.S. degree in electrical engineering and its automation from Wenzhou University, Wenzhou, China, in 2016, and the M.S. degree in control science and engineering from Donghua University, Shanghai, China, in 2019. He is currently working toward the Ph.D. degree in control science and engineering with Zhejiang University, Hangzhou, China.

His current research interests include evolutionary computation and smart grid security.

Zheng-Guang Wu was born in 1982. He received the B.S. and M.S. degrees in mathematics from Zhejiang Normal University, Jinhua, China, in 2004 and 2007, respectively, and the Ph.D. degree in control science and engineering from Zhejiang University, Hangzhou, China, in 2011.

He has authored or coauthored more than 100 papers in refereed international journals. His current research interests include hybrid systems, smart grid, and cyber-physical systems.

Dr. Wu was named a Highly Cited Researcher (Clarivate Analytics). He is an Invited Reviewer for *Mathematical Reviews*. He is an Associate Editor/Editorial Board Member for some international journals, such as IEEE TRANSACTIONS ON SYSTEMS, MAN AND CYBERNETICS: SYSTEMS, *Journal of the Franklin Institute*, *International Journal of Control, Automation, and Systems*, IEEE ACCESS, and *International Journal of Sensors, Wireless Communications and Control*. He is also a member of the Conference Editorial Board of the IEEE Control Systems Society.