An Adaptive Moving-Target Defense Strategy for Dynamic Nonlinear Power Systems

Mohammadpourfard, Mostafa; Shefaei, Alireza; Weng, Yang

DOI
10.1109/TII.2024.3522771

Publication date
2025

Document Version
Final published version

Published in
IEEE Transactions on Industrial Informatics

An Adaptive Moving-Target Defense Strategy for Dynamic Nonlinear Power Systems

Mostafa Mohammadpourfard, *Senior Member, IEEE*, Alireza Shefaei, and Yang Weng, *Senior Member, IEEE*

***Abstract*—Existing attack prevention strategies in smart grid including firewalls, encryption, and access controls, face the challenge of static configurations prone to exploitation. Unlike traditional mechanisms, moving-target defense (MTD), by dynamically altering system parameters, introduces a layer of unpredictability, making it a potent tool against cyber-attacks, including false data injection attacks (FDIA) and zero-day exploits. While MTD has demonstrated efficacy in dc systems by complicating attackers' efforts, its application to ac systems introduces new complexities. AC systems' nonlinearity and vulnerability to topology changes challenge traditional MTD methods, especially in ensuring convergence and adapting to dynamic topologies during emergencies. Such methods, though innovative, fall short in real-world applications where topology changes can render such methods ineffective. Recognizing these limitations, our work introduces a data-driven moving-target defense (DD-MTD) strategy that employs Kullback–Leibler divergence and the Kolmogorov–Smirnov test. Our method quantifies the impact of system perturbations to improve FDIA detection while ensuring changes adhere to operational and cost constraints, a critical factor during contingencies. Our approach, leveraging piecewise linear approximation and mixed-integer linear programming, addresses convergence and adaptability issues, offering a robust defense for ac systems. Simulations on IEEE 14 and 118-bus systems demonstrate that our DD-MTD method enhances detection rates and efficiency, outperforming existing state-of-the-art MTD strategies.**

***Index Terms*—AC power systems, cybersecurity, false data injection attacks, moving target defense, protection.**

I. Introduction

SMART grid technology has revolutionized the electrical utility sector, improving efficiency, reliability, and sustainability in electricity distribution. This shift results from the incorporation of advanced metering and analytics, backed by information and communication technologies. However, these interconnected systems also introduce new cyber-vulnerabilities, which threaten the integrity and functionality of the grid through data manipulation or false communication of commands [1]. A notable example is the extensive power outage in Venezuela in March 2019, which caused prolonged disruptions that caused widespread traffic chaos and the breakdown of essential services such as healthcare and education [2]. Among the numerous types of attacks identified, false data injection attacks (FDIAs) [3], which could launch unobservable attacks against state estimates (SE), have garnered significant interest. In such scenarios, attackers manipulate measurement data, causing discrepancies between estimated and actual states. This can lead to substantial disruptions, including power outages, and financial losses [4], [5].

The moving-target defense (MTD) strategy, positioned within the prevention layer of the defense-in-depth cybersecurity approach, enhances grid security against FDIAs by dynamically altering system configurations. This proactive method obscures potential attack vectors, prevents the exploitation of static vulnerabilities, and reduces the overall attack surface. Integrating MTD enhances power systems' cybersecurity, complicating attackers' efforts to breach defenses and forming a solid foundation for comprehensive security measures. Unlike traditional prevention mechanisms, such as static firewalls or encryption, which offer fixed protection layers, MTD introduces variability and unpredictability into the system's configuration. This approach not only counters existing threats but also proactively defends against new ones, providing a robust defense against a wide range of cyber risks. MTD employs distributed flexible ac transmission system (D-FACTS) devices to dynamically alter transmission line reactances, creating uncertainty and complexity that thwart FDIAs. The success of MTD is bolstered by the capabilities of D-FACTS devices, which allow for active impedance injection. These devices are cost-effective, easy to deploy, and adaptable, making them increasingly popular for power flow management in power grids [6], [7], [8], [9], [10].

A. Related Work

Literature review on MTD in the context of smart grids reveals several notable studies, highlighting the evolution and integration of various strategies to enhance grid security. A dual-focused approach on security and cost optimization is explored in [11], where the authors propose a strategy for deploying D-FACTS devices. This strategy not only counters cyber-physical

Received 11 June 2024; revised 4 October 2024; accepted 12 December 2024. Date of publication 24 February 2025; date of current version 21 April 2025. This work was supported by U.S.-Israel Energy Center managed by the Israel-U.S. Binational Industrial Research and Development (BIRD) Foundation. Paper no. TII-24-2895. *(Corresponding author: Yang Weng.)*

Mostafa Mohammadpourfard is with National Wind Institute, Texas Tech University, Lubbock, TX 79409 USA.

Alireza Shefaei is with the Delft University of Technology, 2628 Delft, The Netherlands.

Yang Weng is with Arizona State University, Tempe, AZ 85281 USA (e-mail: yang.weng@asu.edu).

Digital Object Identifier 10.1109/TII.2024.3522771

attacks but also aims at optimizing generation costs, marking a significant advancement in MTD applications for smart grids. This work is foundational in demonstrating how economic considerations can be integrated with security measures. Building on this, Lakshminarayana et al. [12] presented an MTD strategy using D-FACTS devices to counter cyber-physical attacks by optimally adjusting grid reactances. This study focuses on strategic placement and cost minimization through a zero-sum game, further refining the cost-benefit analysis introduced in earlier works. The combination of strategic placement and cost optimization highlights a critical progression in enhancing the efficiency of MTD deployments.

Wang et al. [13] introduced a multistage MTD that enhances FDIA detection by combining security-oriented and economy-oriented schemes. This approach, optimized through a greedy algorithm, represents a significant step toward balancing security with economic efficiency, a theme consistent with the findings of [11] and [12]. An innovative integration of meter coding with MTD is presented in [14], aimed at enhancing the detection of stealthy FDIA. This method underscores the importance of combining different defensive techniques to address sophisticated attack vectors, aligning with the multifaceted approach seen in previous studies. A robust MTD for power systems in noisy environments, guaranteeing worst-case detection of FDIA, is proposed in [15]. By theoretically analyzing the minimal principal angle between Jacobian subspaces, this work highlights the necessity of ensuring detection robustness under varying conditions, building upon the robust optimization strategies discussed in earlier research.

The research in [16] utilizes MTD to uncover covert Stuxnet-like attacks, meticulously crafted to exploit system vulnerabilities. This study underscores the necessity of MTD in identifying sophisticated cyber threats tailored to the system's specific configurations, complementing the findings of [14] on stealthy attack detection. A hidden MTD method is proposed in [17], capable of evading attacker detection while being effective against parameter confirming-first FDIA. This work delves into the tradeoffs between maintaining stealthiness and ensuring defense completeness, offering insights into the complexities of implementing MTD strategies, and expanding on the stealth and efficiency aspects discussed in [16]. Liu and Wu [18] enhanced the MTD strategy by proposing efficient D-FACTS device placement algorithms to optimize MTD effectiveness and system loss balance. This study complements earlier works by focusing on practical deployment strategies, ensuring that MTD can be effectively integrated into existing infrastructure.

Zhang et al. [19] explored the optimization of MTD, offering a heuristic algorithm for efficient D-FACTS deployment and proving that coordinated perturbation schemes enhance FDI detection. This research highlights the ongoing refinement of optimization techniques to improve MTD efficacy. Liu and Wu [20] presented an enhanced hidden MTD strategy, focusing on optimal D-FACTS device planning and operation to achieve stealth and efficiency in detecting FDIA. This aligns with the broader theme of integrating advanced planning and operational strategies into MTD frameworks. Zhang et al. [21] advanced MTD by establishing key conditions for effective MTD, developing an algorithm to optimize D-FACTS device deployment, proposing cost-reduction strategies, and analyzing the impact on system dynamics. Lakshminarayana and Yau [22] refined MTD strategies by formulating effective reactance perturbations and analyzing the operational costs, thereby balancing MTD's effectiveness with cost.

Finally, the authors in [23] and [24] introduced innovative methods to enhance MTD strategies. Liu et al. [23] employed meter coding to encode sensor outputs with an invertible matrix, enabling detection of stealthy FDIAs without significantly impacting the physical operation of the power system. It introduces variability in data representation, aligning with MTD's goal of thwarting attacks through dynamic system changes. Huang et al. [24] used pseudorandom sequences as watermarks to encrypt and decrypt transmitted data, distinguishing between legitimate and tampered data. By introducing dynamic changes in data patterns, it complements MTD strategies by enhancing data transmission security and integrity.

B. Contributions

The literature underscores MTD's role in reducing smart grid cyber vulnerabilities, primarily focusing on dc systems without considering the dynamic changes in system configurations or contingencies [11], [12], [13], [14], [15], [17], [18], [19], [21], [22]. However, ac power systems, crucial for modern electricity grids, and characterized by complex, nonlinear equations, present significant challenges for analysis and optimization. The "dynamic" aspect highlights the evolving nature of power systems, particularly smart grids, which experience changes in topology due to contingencies. MTD must adapt to these variations to maintain an effective defense. Recent studies have begun to address ac model's nonlinear challenges, but these approaches lack confirmed optimality and often disregard contingency impacts, highlighting areas for future exploration[23], [25]. Traditional optimization-based MTD methods, like particle swarm optimization [25], are often sensitive to initial conditions and require careful tuning of parameters to achieve optimal performance. This sensitivity can lead to variability in performance and challenges in ensuring consistent convergence across different system states and contingencies.

To address this limitations, this article presents a data-driven moving-target defense (DD-MTD) optimized for dynamic ac power systems, utilizing Kullback–Leibler divergence (KLD) to enhance the distinction in reactance distributions for improved FDIA detection. Alongside, the Kolmogorov–Smirnov (KS) test ensures operational compliance, balancing enhanced security with cost control. To address ac systems' nonlinearities, we employ mixed-integer linear programming (MILP) combined with piecewise linear approximation and the big-M method, effectively overcoming nonconvexity challenges for optimal strategy execution. This effectively resolves nonconvexity issues, enabling optimal strategy implementation [26], [27], [28], [29]. The proposed method leverages real-time data to continuously update its understanding of the system's current state. The KLD metric inherently accounts for changes in the system's configuration incorporating the system's dynamic nature into the proposed

MTD strategy, ensuring adaptability to topology changes. This integration ensures that the perturbations introduced by MTD are statistically significant and adhere to operational constraints, enhancing the detection of FDIAs without compromising system stability. By maximizing KLD, our method increases the divergence between the original and perturbed system states, making it more difficult for attackers to predict and execute successful attacks. The Kolmogorov–Smirnov Test (KS) test ensures that these perturbations remain within acceptable operational limits, maintaining the system's reliability and stability. The main contributions of this article are as follows.

1) Unlike many existing methods, our approach does not assume any specific network topology or ac–dc system parameters. This allows our MTD strategy to be applied broadly and adaptively across different grid configurations. This is while past methods primarily focused on dc models and recent ac models lacked proven optimality.
2) Our approach uniquely integrates KLD maximization and KS test compliance to balance the tradeoffs between security enhancement and operational viability. This dual optimization not only improves the detection rates of FDIAs but also ensures that the system's operational integrity is not compromised, addressing a critical challenge in existing MTD applications.
3) Transforming the optimization challenge into an MILP model through piecewise linear approximation and the big-M method guarantees global optimality, making the MTD approach more practical for real-world applications. It effectively tackles the nonconvexity issues of ac power systems. In addition, our strategy integrates $n-1$ contingency management into the MTD framework, significantly boosting power system resilience. This integration marks a significant improvement over previous MTD approaches that tend to overlook the vital role of contingencies.

The rest of this article is organized as follows. Section II provides an overview of the system modeling and highlights the importance of MTD in mitigating cyber threats. Section III details our proposed DD-MTD approach. Section IV presents simulation results. Finally, Section V concludes this article.

II. System Modeling and Background

A. AC State Estimation and FDIA

This article explores the use of the ac power system model for analysis, whereas the majority of preceding investigations into MTD predominantly utilize the dc model. For the SE, the commonly employed technique is the least squares method. We examine a power grid described by a collection $\mathcal{N}=\{1,\ldots,N\}$ of buses and $\mathcal{L}=\{1,\ldots,L\}$ of branches. The nonlinear measurement equation characterizing the system is often denoted as [30]: $\boldsymbol{z}=\boldsymbol{h}(\boldsymbol{x})+\boldsymbol{e}$, where, the symbol $\boldsymbol{z}$ represents the measurement vector, and $\boldsymbol{h}(\cdot)$ indicates the nonlinear measurement equation. The state variable $\boldsymbol{x}$ includes voltage amplitude and phase at each bus, with $\boldsymbol{e}$ representing measurement errors. $\boldsymbol{h}(\boldsymbol{x})$ is defined as

$$\boldsymbol{h}(\boldsymbol{x})=\begin{bmatrix} f_{ij}^{p} & f_{ij}^{q} & p_i & q_i & V_i \end{bmatrix}^T \quad i=1,2,\ldots,N \quad \forall j\in\mathcal{K}_i \tag{1}$$

where V_i denotes voltage amplitude at bus i, and $\mathcal{K}_i$ is the set of connected buses to bus i, f_{ij}^{p} indicates active power flow from bus i to bus j, f_{ij}^{q} represents reactive power flow from bus i to bus j, p_i is active power injection at bus i, q_i signifies reactive power injection at bus i. The outcome of the SE process involves determining the value $\hat{\boldsymbol{x}}$, which minimizes the following objective function based on the provided measurements denoted by $\boldsymbol{z}$, $J(\boldsymbol{x})=[\boldsymbol{z}-\boldsymbol{h}(\boldsymbol{x})]^T\boldsymbol{R}^{-1}[\boldsymbol{z}-\boldsymbol{h}(\boldsymbol{x})]$, where $\boldsymbol{R}$ is the measurement error covariance matrix.

To detect anomalous meter measurements, SE typically uses a bad data detection (BDD) mechanism, based on the ℓ_2-norm estimation residual $|\boldsymbol{r}|=|\boldsymbol{z}-\boldsymbol{h}(\hat{\boldsymbol{x}})|\geq\tau$. Here, τ is a predefined threshold. Measurements are classified as unreliable if $|\boldsymbol{r}|$ is greater than or equal to τ, and valid if less. However, in FDIAs, an adversary can bypass BDD and produce an inaccurate system state $\hat{\boldsymbol{x}}_a=\hat{\boldsymbol{x}}+\boldsymbol{c}$ by introducing manipulated measurements $\boldsymbol{z}_a=\boldsymbol{z}+\boldsymbol{a}$, where $\boldsymbol{a}=\boldsymbol{h}(\hat{\boldsymbol{x}}+\boldsymbol{c})-\boldsymbol{h}(\hat{\boldsymbol{x}})$ is the attack vector and $\boldsymbol{c}$ is the error introduced in the system's estimates $\hat{\boldsymbol{x}}$ [30].

B. Moving Target Defence

MTD strategies alter key parameters like line reactance x_{ij} within a specified range $[x_{\min},x_{\max}]$ across a network with buses N and branches L. This change in reactance impacts the branch susceptance b_{ij} is defined as the negative of the imaginary part of the branch admittance y_{ij}, which is calculated from the complex impedance as $-\frac{x_{ij}}{r_{ij}^2+x_{ij}^2}$, affecting ac SE $\boldsymbol{z}_{\text{MTD}}=\boldsymbol{h}_{\text{MTD}}(\boldsymbol{x}_{\text{MTD}})+\boldsymbol{e}$, where $\boldsymbol{z}_{\text{MTD}}$ is the measurement vector under MTD, $\boldsymbol{h}_{\text{MTD}}$ represents the nonlinear measurement function considering the altered reactances. Note that the susceptance b_{ij} is negative for inductive reactance and positive for capacitive reactance. The new state vector $\boldsymbol{x}_{\text{MTD}}$ includes the altered reactances. The objective function for SE under MTD becomes $J_{\text{MTD}}(\boldsymbol{x}_{\text{MTD}})=[\boldsymbol{z}_{\text{MTD}}-\boldsymbol{h}_{\text{MTD}}(\boldsymbol{x}_{\text{MTD}})]^T\boldsymbol{R}^{-1}[\boldsymbol{z}_{\text{MTD}}-\boldsymbol{h}_{\text{MTD}}(\boldsymbol{x}_{\text{MTD}})]$. The BDD mechanism in the context of MTD must account for the varying reactances. The residual under MTD, denoted as $\boldsymbol{r}_{\text{MTD}}$, is calculated as $\|\boldsymbol{r}_{\text{MTD}}\|=\|\ \boldsymbol{z}_{\text{MTD}}-\boldsymbol{h}_{\text{MTD}}(\widehat{\boldsymbol{x}}_{\text{MTD}})\|$. MTD execution can increase the detection residual $\boldsymbol{r}_{\text{MTD}}$ compared to the original $\boldsymbol{r}$, improving attack detection effectiveness. While MTD hampers attackers and bolsters grid resilience, it also incurs extra generation costs due to line reactance adjustments, formulated as: $C_{\text{MTD},t'}=\frac{C_{\text{OPF},t'}-C_{\text{OPF},t}}{C_{\text{OPF},t}}$, where $C_{\text{MTD},t'}$, is defined as the relative change in optimal power flow (OPF) cost due to MTD at time t', with $C_{\text{OPF},t'}$ being the operational cost after MTD and $C_{\text{OPF},t}$ being the operational cost before MTD.

C. Optimization of Cost-Benefit MTD Strategy

The cost-benefit MTD strategy optimizes the power grid's operational parameters, like generator outputs and line reactances, to enhance cybersecurity without compromising efficiency or increasing costs. It seeks to minimize operational expenses within MTD constraints by adjusting reactances, thus hindering potential cyberattacks. The optimization framework is as follows [6]:

$$\underset{g'_{t'},x'_{t'}}{\text{minimize}} \quad \sum_{i\in N} C_i(G'_{i,t'}) \tag{2a}$$

$$\text{subject to} \quad \gamma(h_t, h_{\text{MTD},t'}) \geq \gamma_{\text{th}} \tag{2b}$$

$$g'_{t'} - l_{t'} = B'_{t'}\theta'_{t'} \tag{2c}$$

$$-f^{\max} \leq f'_{t'} \leq f^{\max} \tag{2d}$$

$$g^{\min} \leq g'_{t'} \leq g^{\max} \tag{2e}$$

$$x^{\min} \leq x'_{t'} \leq x^{\max} \tag{2f}$$

where $C_i(G'_{i,t'})$ denotes the cost associated with power generation adjustments at bus i, considering the MTD-induced changes. $G'_{i,t'}$ represents the power generation at bus i at time t'. Constraint (2b) ensures that the MTD effectively detects attacks by requiring a significant change in the system's behavior. This change is measured by the smallest principal angle, γ, between the subspaces spanned by the columns of the pre-MTD and post-MTD Jacobian matrices, h_t and $h_{\text{MTD},t'}$, respectively. The singular value decompositions of these matrices are represented as $h_t = u_t\Sigma_t v_t^T$ and $h_{\text{MTD},t'} = u_{\text{MTD},t'}\Sigma_{\text{MTD},t'}v_{\text{MTD},t'}^T$, respectively. The smallest principal angle γ is calculated as

$$\gamma(h_t, h_{\text{MTD},t'}) = \min(\arccos(\sigma_1), \arccos(\sigma_2), \ldots, \arccos(\sigma_n)) \geq \gamma_{\text{th}} \tag{3}$$

where σ_i are the singular values of the matrix $v_t^T v_{\text{MTD},t'}$ and γ_{th} is a predefined threshold. The constraint ensures that this smallest principal angle γ meets or exceeds the threshold γ_{th}, indicating a significant change in the system's behavior due to the MTD. Constraint (2c) requires that the power grid maintains a balanced flow of energy at each node. The power injected into a node (from generation, $g'_{t'}$, and any changes due to the MTD, $\Delta g_{t'}$) must equal the power flowing out of that node (to meet demand, $l_{t'}$). This balance is crucial for maintaining the stability and overall power balance of the grid. The relationship between these parameters is defined by the susceptance matrix $B'_{t'}$, which is calculated as $B'_{t'} = AD'_{t'}A^\top$, where A is the branch-bus incidence matrix and $D'_{t'}$ is a diagonal matrix of the reciprocal of link reactances after the MTD is implemented. The phase angles at all buses after the MTD is implemented are represented by $\theta'_{t'}$. Equation (2d) regulates transmission line power flow, not surpassing the maximal allowable limit. Equation (2e) ensures power generated post-MTD at time t' stays within minimum and maximum bounds. Equation (2f) keeps line reactance within D-FACTS devices' feasible ranges. We have adapted constraint (2b) from the dc context to effectively handle the nonlinearities of ac systems.

III. Proposed DD-MTD

The proposed DD-MTD, Algorithm 1, designed for the intricate dynamics of nonconvex ac power systems, utilizes KLD to enhance FDIA detection markedly. By adopting KLD, our approach maximizes the discrepancy between the probability distributions of the original and modified system states. This maximization not only disrupts attackers' predictive models but also provides a quantifiable metric to gauge the efficacy of the MTD deployment. Simultaneously, the implementation of the KS test in our model serves as a safeguard, ensuring that the alterations in system parameters induced by MTD do not deviate excessively from operational norms. This incorporation is a conscious effort to maintain this balance. We have transformed the nonlinear optimization challenge of ac systems into a manageable MILP framework by applying piecewise linear approximation and the big-M method, effectively addressing nonconvexity and facilitating optimal strategy deployment [26], [27], [28], [29]. Our methodology excels at managing contingencies, providing adaptability and robustness in the dynamic smart grid environment.

As aforementioned, the algorithm starts by loading the system model, defining parameters such as buses, branches, and measurement vectors, and initializing thresholds for KLD and KS tests. It iteratively optimizes reactance settings within a predefined range by updating branch susceptance, recalculating the measurement function, computing the optimization function, and performing linearized KLD and KS tests to ensure operational norms are maintained. The OPF is calculated, and reactance adjustments are confirmed if they pass the KS test. The algorithm selects the optimal reactance settings that minimize operational costs while satisfying both KLD and KS test criteria. We have validated this approach through extensive simulations, demonstrating its ability to achieve both cost minimization and improved FDIA detection under diverse operating conditions. In the following sections, we outline our methods and describe how we linearize the model for optimal solutions.

A. Kullback–Leibler Distance

The KLD between two discrete probability distributions P and Q on the same space $\mathcal{X}$ is defined as

$$D_{\text{KL}}(P \parallel Q) = \sum_{x\in\mathcal{X}} P(x)\log\left(\frac{P(x)}{Q(x)}\right) \tag{4}$$

where $P(x)$ and $Q(x)$ are the probabilities of event x under distributions P and Q, respectively. KLD measures MTD's impact by comparing reactance changes, enhancing security by complicating attackers' predictions.

B. Two-Sample KS Test

The KS test compares data distributions of two vectors, denoted as $\mathbf{D1} = \{d1_1, d1_2, \ldots, d1_n\}$ and $\mathbf{D2} = \{d2_1, d2_2, \ldots, d2_n\}$. The KS test evaluates whether MTD changes to system parameters like line reactances stay statistically consistent, ensuring cost-effectiveness for real-world application. The null hypothesis posits that both data vectors come from the same

Algorithm 1: Data-Driven Moving Target Defense.

Require: AC system model with buses N, branches L
Ensure:I mproved FDIA detection and cost efficiency
Load system model, define N, L, $\boldsymbol{z}$
Initialize thresholds, and reactance range $\boldsymbol{X}_{\text{range}}$
function OptimizeMTD$\boldsymbol{z}$, $\boldsymbol{X}_{\text{range}}$
  for each reactance x_{ij} in $\boldsymbol{X}_{\text{range}}$ **do**
    Update susceptance b_{ij}
    Recalculate $\boldsymbol{h}(\boldsymbol{x})$ (1)
    Compute Optimization Function (6)
    Compute Linearized KLD (7)
    Perform Linearized KS-test (8)
    Calculate OPF (10)
    if KS-test passes **then**
      Confirm reactance adjustment
    else
      Revert to previous settings
    end if
    Evaluate cost
  end for
  return optimized reactance settings
end Function
$\boldsymbol{x}_{\text{opt}} \leftarrow$ OptimizeMTD($\boldsymbol{z}$, $\boldsymbol{X}_{\text{range}}$)
Apply $\boldsymbol{x}_{\text{opt}}$ to system model
return updated system state, detection rates, costs

distribution. The KS test distance denotes the largest absolute difference observed between the cumulative distribution functions (CDFs) of $\mathbf{D}_1$ and $\mathbf{D}_2$. For a given sample $\mathbf{Y} = y_1, y_2, \ldots, y_m$, its CDF can be expressed as [30] $F_{Y,m}(y) = \frac{\#i:y_i \leqslant y}{m}$, where $\#i : y_i \leqslant y$ is the total count of items in the set that meet the condition $y_i \leqslant y$ for all i. When comparing two sets with n and m samples, the KS statistic is as follows:

$$D_{n,m} = \sup_{-\infty<s<\infty} |F_{S1,n}(s) - F_{S2,m}(s)| \tag{5}$$

where the null hypothesis is rejected at the α significance level if the maximal distance, $\sup_s$, between the empirical distribution functions $F_{S1,n}$ and $F_{S2,m}$ meets the specified condition $D_{n,m} > c(\alpha) \times \sqrt{\frac{n+m}{n\times m}}$, where $c(\alpha) = \sqrt{-\frac{1}{2} \times \ln \alpha}$ and n and m represent the first and second sample sizes, respectively. Lower α values strengthen confidence in hypothesis testing. A P_Value at or below the significance level suggests significant deviation, rejecting the null hypothesis, while a higher P_Value indicates the sample conforms, supporting the null hypothesis. The P_Value is derived from the Kolmogorov distribution, which assesses the KS statistic under the null hypothesis: P_Value $= 1 - 2\sum_{k=1}^{\infty}(-1)^{k-1}\exp(-2k^2D^2)$.

C. Data-Driven MTD Model

The optimization problem for finding the new reactance vector is formulated as

$$\max_{x\in\mathcal{X}} \quad D_{\text{KL}}\left(P \parallel Q\right) \tag{6a}$$

$$\text{s.t.} \quad D_{n,m} = 0. \tag{6b}$$

Our method aims to optimize grid security by minimizing the divergence between the original Q and new reactance P distributions within the same probability space, while ensuring the variance changes meet the criteria set by the KS test. The proposed method in combination with (2) becomes where the DD-MTD's objective can be weighted and added to optimization problem (2) or treated as a second goal in a multiobjective framework with the first objective from problem (2):

$$\max_{g'_{t'},x'_{t'}} \quad -\sum_{i\in N} C_i(G'_{i,t'}) + D_{\text{KL}}\left(P(x'_{t'}) \parallel Q(x'_{t'})\right) \tag{7a}$$

$$\text{s.t.} \quad \max\{|P(x'_{t'}) - Q(x'_{t'})|\} = 0 \tag{7b}$$

$$(2a)-(2f). \tag{7c}$$

D. Linearization of Optimization Model

To ensure global optimality by handling the nonconvexity from the nonlinear objective function and constraints, we apply a piecewise linear approximation to the KLD metric represented as $f_2(x) = x\log(x)$ over interval $[a, b]$. This involves dividing the function into m segments, requiring m positive variables λ and $m-1$ binary variables z. The value of $f_2(x)$ at each segment's start point b_i is $f_2(b_i)$. This allows substituting the nonlinear term with an optimized linear approximation in the problem

$$\max_{x'_{t'},\lambda_i,z_i} \quad \sum_{i=1}^{m} \lambda_i f_2(b_i) \tag{8a}$$

$$\text{s.t.} \quad \sum_{i=1}^{m-1} z_i = 1 \tag{8b}$$

$$\lambda_1 \leq z_1 \tag{8c}$$

$$\lambda_i \leq z_i + z_{i-1}, \qquad i = 2, \ldots, m-1 \tag{8d}$$

$$\lambda_m \leq z_{m-1} \tag{8e}$$

$$\sum_{i=1}^{m} \lambda_i = 1 \tag{8f}$$

$$x = \sum_{i=1}^{m} \lambda_i b_i \tag{8g}$$

$$\lambda_i \geq 0 \qquad i = 1, \ldots, m \tag{8h}$$

$$z_i \in \{0, 1\} \qquad i = 1, \ldots, m-1. \tag{8i}$$

The first condition ensures only one z is set to 1, with the rest at 0. The following conditions specify that λ_i and λ_{i+1} are the only nonzero λs, representing adjacent segments to x'. In addition, $\lambda_i = \Lambda$ and $\lambda_{i+1} = 1 - \Lambda$ align with the approximation f_a in the objective function, enabling an MILP approach for optimality in approximating the nonlinear component of our DD-MTD. The piecewise linear approximation, illustrated in Fig. 1, uses $m = 6$ sampling points along the function domain. By introducing a continuous variable λ for each breakpoint and employing 5 binary variables z to denote intervals between breakpoints (with $z_1, z_5 = 0$ for domain edges), the function f_2 is approximated.

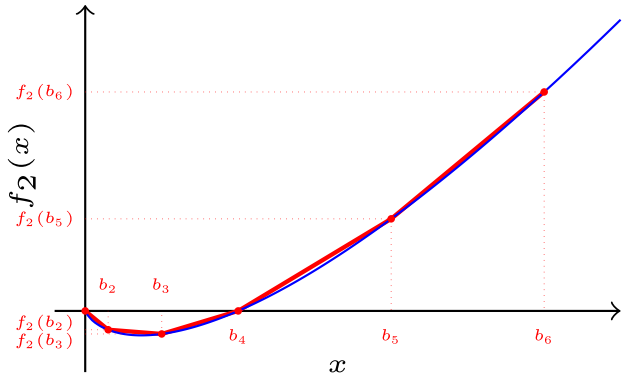

Fig. 1. Piecewise linear approximation of $f_2(x) = x\log(x)$.

This approximation, as shown in Fig. 1, closely matches the original $x\log(x)$ function, allowing for accurate modeling with minimal computational effort.

Evaluating a function value within its domain involves three steps: first, identifying the two adjacent nonzero λs; second, determining their values by solving constraints (8f) and (8g); and finally, calculating the function value using (8a). Another challenge to achieving a global optimum is the nonlinearity from statistical hypothesis testing constraints. Introducing a constant M ensures that $P(x)$ and $Q(x)$ do not exceed M in any feasible solution, with binary variable y^{KS} defined through

$$P(x) - Q(x) \le My^{\text{KS}} \tag{9a}$$

$$Q(x) - P(x) \le M(1 - y^{\text{KS}}). \tag{9b}$$

Then, the following constraints enforce $0 = \max\{P(x), Q(x)\}$:

$$0 \ge P(x) \tag{10a}$$

$$0 \ge Q(x) \tag{10b}$$

$$0 \le P(x) + M(1 - y^{\text{KS}}) \tag{10c}$$

$$0 \le Q(x) + My^{\text{KS}}. \tag{10d}$$

By substituting these constraints with the test's constraint, our optimization problem transitions to a MILP model. This approach effectively addresses the nonlinear SE challenges of ac power systems, enabling optimal reactance adjustments with DD-MTD—an outcome not previously attained, as highlighted in studies like [25].

E. Linearized AC OPF

MTD solutions in complex, nonlinear power systems can stress operational and voltage stability, impacting transformer capacity and transmission attributes under peak or stressed conditions [18], [31]. To ensure MTD modifications are both secure and cost-effective, this study uses a linearized AC optimal power flow (ACOPF) model, combining techniques like segment-wise linear estimation and Taylor expansions, to develop defensive strategies that are viable in normal and high-stress scenarios. This optimized ACOPF approach focuses on minimizing total generation costs (TGC), ensuring operational integrity during regular and contingency conditions [32]

$$\min \text{TGC} = \sum_{i \in N} \left(C_i^{\mathbb{N}} G_i^{\mathbb{N}} + C_i^{\mathbb{C}} G_i^{\mathbb{C}} \right) \tag{11}$$

where TGC is the total generation cost. Here, $C_i^{\mathbb{N}}$ and $C_i^{\mathbb{C}}$ represent the generation costs for the ith generator under normal and critical conditions, respectively, and $G_i^{\mathbb{N}}$ and $G_i^{\mathbb{C}}$ are the corresponding generation outputs. The optimization minimizes generation costs across both normal and critical conditions with specific constraints to ensure efficient operation. For normal operating conditions, the constraints are as follows:

$$p_{Gi,\min}^{\mathbb{N}} \le p_{Gi}^{\mathbb{N}} \le p_{Gi,\max}^{\mathbb{N}} \tag{12}$$

$$q_{Gi,\min}^{\mathbb{N}} \le q_{Gi}^{\mathbb{N}} \le q_{Gi,\max}^{\mathbb{N}} \tag{13}$$

$$V_{i,\min}^{\mathbb{N}} \le V_i^{\mathbb{N}} \le V_{i,\max}^{\mathbb{N}} \tag{14}$$

$$(f_{ij}^{p,\mathbb{N}})^2 + (f_{ij}^{q,\mathbb{N}})^2 \le (s_{l,\max}^{\mathbb{N}})^2 \tag{15}$$

$$\sum_{i \in N} p_{Gi}^{\mathbb{N}} + \sum_{ij \in \kappa} f_{ij}^{p,\mathbb{N}} = p_{Di} \tag{16}$$

$$\sum_{i \in N} q_{Gi}^{\mathbb{N}} + \sum_{ij \in \kappa} f_{ij}^{q,\mathbb{N}} = q_{Di} \tag{17}$$

where $p_{Gi,\min}^{\mathbb{N}}$, $p_{Gi}^{\mathbb{N}}$, and $p_{Gi,\max}^{\mathbb{N}}$ denote the minimum, actual, and maximum active power generation under normal conditions, respectively, and $q_{Gi,\min}^{\mathbb{N}}$, $q_{Gi}^{\mathbb{N}}$, and $q_{Gi,\max}^{\mathbb{N}}$ are the reactive power limits. Similarly, $V_{i,\min}^{\mathbb{N}}$ and $V_{i,\max}^{\mathbb{N}}$ are the voltage limits for the ith bus, $f_{ij}^{p,\mathbb{N}}$ and $f_{ij}^{q,\mathbb{N}}$ are the real and reactive power flows between bus i and j, and $s_{l,\max}^{\mathbb{N}}$ denotes the thermal limit of the transmission line. Here, κ represents the set of transmission lines, and p_{Di} and q_{Di} are the active and reactive power demands at bus i. Constraints (12)–(15) set operational limits, while constraints (16) and (17) ensure power balance. Constraint (15) uses a segment-wise linear approximation as detailed in [33]. For stressed conditions, the constraints are as follows:

$$p_{Gi}^{\mathbb{C}} = \Gamma_{Gi}(p_{Gi}^{\mathbb{N}} + \Delta p_{Gi,\text{inc}}^{\mathbb{C}} - \Delta p_{Gi,\text{dec}}^{\mathbb{C}}) \tag{18}$$

$$\Gamma_{Gi} q_{Gi,\min}^{\mathbb{C}} \le q_{Gi}^{\mathbb{C}} \le \Gamma_{Gi} q_{Gi,\max}^{\mathbb{C}} \tag{19}$$

$$V_{i,\min}^{\mathbb{C}} \le V_i^{\mathbb{C}} \le V_{i,\max}^{\mathbb{C}} \tag{20}$$

$$(\Gamma_l f_{ij}^{p,\mathbb{C}})^2 + (\Gamma_l f_{ij}^{q,\mathbb{C}})^2 \le (\Gamma_l s_{l,\max}^{\mathbb{C}})^2 \tag{21}$$

$$\sum_{i \in N} p_{Gi}^{\mathbb{C}} + \sum_{ij \in \kappa} \Gamma_l f_{ij}^{p,\mathbb{C}} = (1 + \rho) p_{Di} \tag{22}$$

$$\sum_{i \in N} q_{Gi}^{\mathbb{C}} + \sum_{ij \in \kappa} \Gamma_l f_{ij}^{q,\mathbb{C}} = (1 + \rho) q_{Di} \tag{23}$$

$$|p_{Gi}^{\mathbb{N}} - p_{Gi}^{\mathbb{C}}| \le \Delta T_{Gi} \tag{24}$$

where Γ_{Gi} and Γ_l are binary parameters representing the operational status under stress, $\Delta p_{Gi,\text{inc}}^{\mathbb{C}}$ and $\Delta p_{Gi,\text{dec}}^{\mathbb{C}}$ represent incremental and decremental active power adjustments, and ρ is a parameter introducing additional load stress. Finally, ΔT_{Gi}

denotes the allowable thermal output change for generator i under stressed conditions.

The proposed method effectively manages contingencies in dynamic and nonlinear power systems through several key features. Its nonparametric nature allows it to adapt to various scenarios without specific assumptions about network topology or the need for retraining. Incorporating an $n-1$ contingency management framework within the MTD strategy ensures system stability even if individual components fail. By dynamically altering system configurations based on real-time data, the method maintains continuous security and stability. The use of KLD enhances the detection of FDIA by maximizing the divergence between the original and perturbed system states, while the KS test keeps changes within operational norms, balancing security, and cost-effectiveness. To address the nonconvex nature of ac power systems, the optimization problem is formulated using MILP with piecewise linear approximation and the big-M method, ensuring optimal and computationally feasible solutions for real-time applications. The method's lack of a training phase enhances its adaptability and ease of deployment.

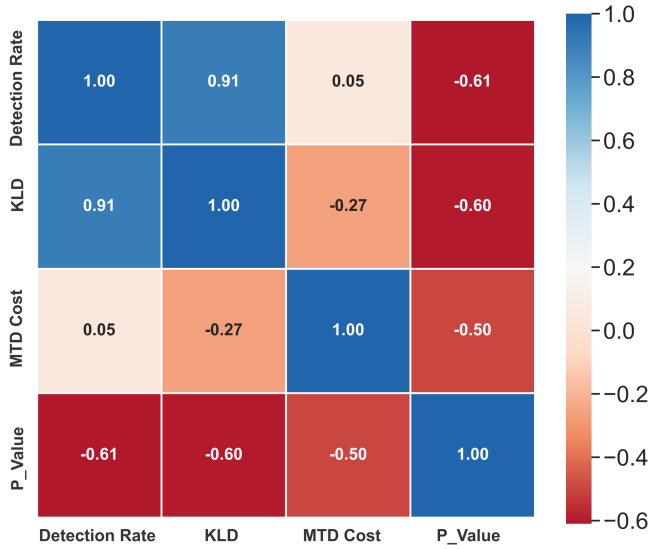

Fig. 2. Correlation Heatmap for 14-bus.

IV. Simulation Results

This section outlines the outcomes from simulations performed on IEEE 14 and 118-bus systems. For these simulations, it is hypothesized that D-FACTS devices are deployed on randomly chosen branches like [6]. To assess the proposed MTD's efficacy, we designed two simulation scenarios: Case I tests it in a stable network, while Case II evaluates its performance under topological changes. In addition, a comparative analysis with existing MTD strategies [6], [25] illustrates our method's advantages. To ensure robust scalability and applicability across diverse operational conditions, our method incorporates a comprehensive normalization procedure to address the potential for imbalance when combining generation cost and the KLD.

A. Case I: Without Contingency

Fig. 2 presents the correlation heatmap for the IEEE 14-bus system, which provides a visual representation of the relationships between four key variables: detection rate, KLD, MTD Cost, and P_Value.

1) *Detection rate and KLD:* A strong positive correlation is observed, indicating that an increase in the divergence between the probability distributions of the original and perturbed reactance is associated with improved capabilities to detect FDIA. This finding underscores the effectiveness of maximizing KLD to bolster detection rates.
2) *Detection rate and MTD cost:* The correlation approaches zero, suggesting minimal impact of detection rate improvements on the operational cost. This observation underscores the method's effectiveness in boosting security cost-efficiently. This means, we observed that while higher KLD values generally lead to improved detection rates, the correlation between detection rate and MTD Cost approaches zero. This counterintuitive result stems from our optimized cost-benefit balance, where significant detection improvements are achieved without proportionally high costs. This highlights the efficiency of our data-driven approach, which leverages advanced statistical measures and real-time data to adaptively enhance detection capabilities while minimizing operational and implementation costs.
3) *Detection Rate and P_Value:* A negative correlation reveals that lower P_Values, which denote higher statistical significance in reactance changes, are linked to better detection rates. This relationship emphasizes the proposed method's resilience against sophisticated adversaries in nonlinear ac systems.
4) *KLD and MTD Cost:* The weak negative correlation observed suggests that heightened security, achieved through significant distribution divergence (high KLD values), does not necessarily incur proportional increases in cost. This insight is crucial for developing cost-effective security strategies.
5) *KLD and P_Value:* The negative correlation between these metrics indicates that statistically significant deviations in system parameters, as reflected by lower P_Values, correlate with higher KLD values. This alignment validates the strategy of leveraging KLD to identify optimal vectors for system parameter perturbation.
6) *MTD Cost and P_Value:* A correlation of -0.5 indicates that aligning the reactance vector closely with the base distribution, verified by the KS test, does not notably raise MTD strategy costs. This outcome underscores the KS test's effectiveness in balancing security improvements with cost constraints.

In summary, the heatmap analysis suggests that the proposed DD-MTD is effectively increasing the detection rate without necessarily escalating the costs for complex nonlinear ac systems. This demonstrates our method's flexibility and ability to

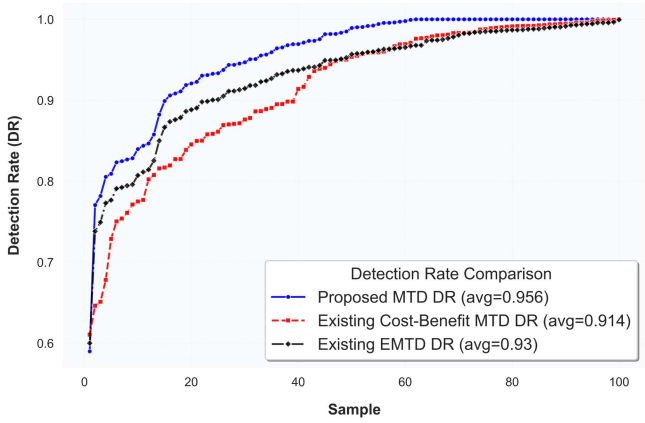

Fig. 3. Detection rate (DR)-14 bus.

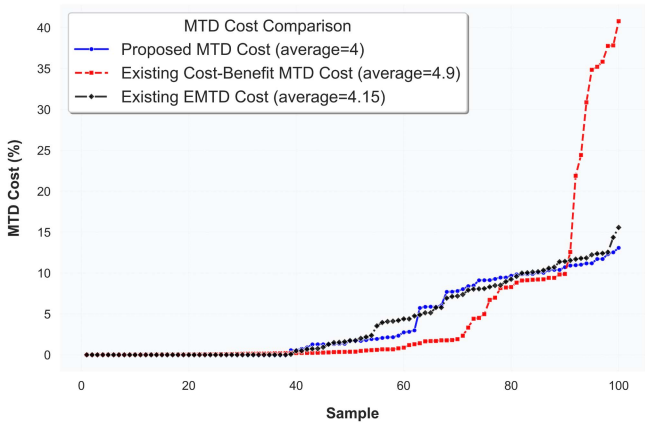

Fig. 4. MTD cost-14 bus.

TABLE I
DETECTION RATE AND MTD COST-14 BUS

Method	Detection rate	MTD cost (%)
Proposed method	0.956	4
Cost-benefit	0.914	4.9
EMTD	0.93	4.15

work based on data without being limited to specific network topologies or assumptions. Fig. 3 shows the detection rate comparison between the DD-MTD and an existing cost-benefit (dc) and also extended MTD (EMTD)(ac) strategies [6], [25] over a series of samples for an IEEE 14-bus system. The plot indicates that the proposed data-driven MTD method not only achieves a high detection rate but also surpasses the existing methods.

Fig. 4 presents a cost comparison of MTD implementations, contrasting our data-driven approach with existing methods on an IEEE 14-bus system. The comparison reveals that the proposed DD-MTD method sustains a lower operational cost. Cost reduction is crucial due to the complexity of nonlinear ac power flow models, which usually make implementing cybersecurity measures like MTD challenging. The results for IEEE 14-bus system are summarized in Table I. Results show our strategy

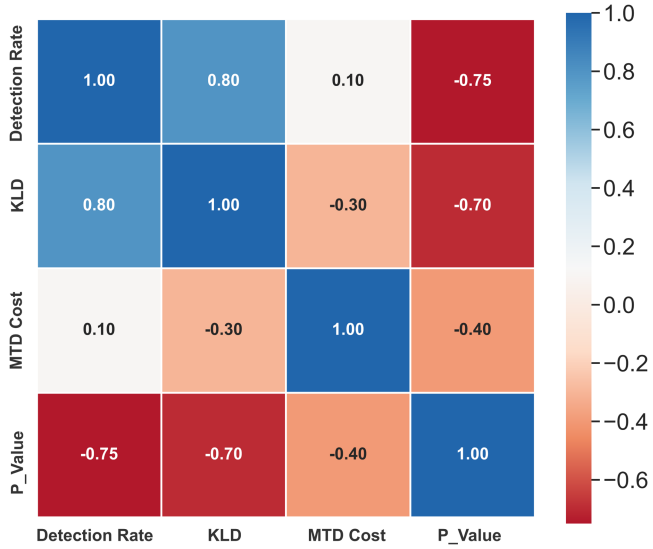

Fig. 5. Correlation Heatmap for 118 bus.

outperforms current methods, delivering enhanced security and cost-efficiency in ac systems. This dual advantage positions it as an appealing choice for utilities aiming to boost grid security affordably.

Fig. 5 presents the correlation heatmap for the IEEE 118-bus system. The heatmap indicates that the detection rate and KLD exhibit a strong positive correlation of 0.80, demonstrating that an increase in the KLD positively influences the detection rate. This link is vital, indicating that greater divergence in reactance distribution, quantified by KLD, enhances anomaly detection in the system. The heatmap indicates a minimal 0.10 correlation between detection rate and MTD cost, suggesting that enhancing detection does not significantly raise costs, highlighting DD-MTD's cost-effective scalability in larger networks. The P_Value's negative correlations with both the detection rate -0.75 and KLD -0.70 affirm that the statistical significance of the changes in the system's parameters is a contributing factor to both the detection effectiveness and the divergence of reactance distribution. A lower P_Value indicates better detection, improving MTD's threat countermeasures. The -0.40 correlation between MTD Cost and P_Value shows that substantial reactance adjustments minimally affect MTD costs.

The DD-MTD method shows exceptional scalability and effectiveness in enhancing ac power systems' cybersecurity, evidenced by a consistent positive correlation between detection rate and KLD across different system sizes, from IEEE 14-bus to IEEE 118-bus. In addition, the moderate negative correlation between MTD Cost and P_Value across these systems underscores the method's cost-efficiency, illustrating its capability to improve security without significant cost increases, which is crucial for its practical application in power systems. In Figs. 6 and 7, the proposed MTD method is evaluated against existing approaches for the IEEE 118-bus system. Table II succinctly compares detection rates and MTD costs, highlighting the benefits of the proposed data-driven technique. The analysis highlights the

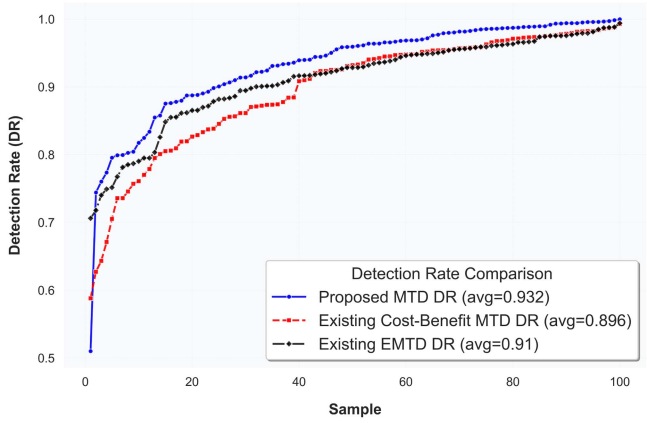

Fig. 6. Detection rate (DR)-118 bus.

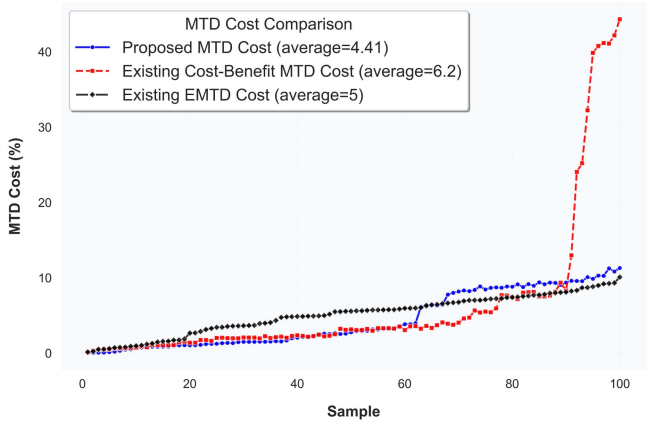

Fig. 7. MTD cost-118 bus.

TABLE II
DETECTION RATE AND MTD COST-118 BUS

Method	Detection rate	MTD cost (%)
Proposed method	0.932	4.41
Cost-benefit	0.896	6.20
EMTD	0.91	5

method's success in combining high detection rates with lower MTD costs, showcasing efficient resource optimization suitable for extensive and intricate power systems.

B. Case II: With Contingency

In this scenario, we assess the resilience of the proposed method in handling topology changes through simulated line outages in both IEEE 14-bus (branch 2–5) and IEEE 118-bus (branch 75–77) test systems. In the realm of power systems, contingencies are a vital consideration, given their capacity to introduce significant volatility and necessitate immediate recalibrations of operational constraints. Such scenarios present a formidable challenge to the robustness and adaptability of MTD methodologies. The effect of contingencies on MTD strategies is profound, as they force a re-evaluation of the balance between system stability and cybersecurity. The proposed MTD method is designed to be dynamic, with an inherent flexibility that allows it to manage the nonlinearities introduced by contingencies as shown by consistent high convergence rates in both the 14 and 118 bus systems, affirming its adaptability to unforeseen changes.

TABLE III
DETECTION RATE AND MTD COST-14 BUS (UNDER CONTINGENCY)

Method	Detection rate	MTD cost (%)	Convergence rate
Proposed method	0.92	4.5	1
Cost-benefit	0.84	6.5	1
EMTD	0.87	5.9	0.95

TABLE IV
DETECTION RATE AND MTD COST-118 BUS (UNDER CONTINGENCY)

Method	Detection rate	MTD cost (%)	Convergence rate
Proposed method	0.906	5.2	1
Cost- benefit	0.81	8.2	1
EMTD	0.84	7.1	0.93

As shown in Table III, under contingency conditions, the proposed MTD method surpasses both cost-benefit and EMTD in detection rate and cost for the 14-bus system, with a perfect convergence rate 1 indicating robust performance despite complexities induced by contingencies. In contrast, the EMTD method, while showing a respectable detection rate of 0.87, falls short in terms of convergence, with a rate of 0.95. This suggests that the EMTD's constraints may not be fully compatible with the nonlinear conditions imposed by the contingency, hindering its ability to reach an optimal solution in some cases. The cost-benefit method shows the highest cost and lowest detection rate, indicating it may be less equipped to handle the heightened stress of a contingency. Table IV presents the results for 118-bus system. As it is clear, the proposed method continues to demonstrate superior performance with a 0.906 detection rate and a manageable increase in MTD cost to 5.2%, maintaining a perfect convergence rate. This underscores the proposed method's scalability and adaptability, affirming its effectiveness in larger, more complex networks. While the EMTD method's performance drops in the 118-bus system, with a lower convergence rate of 0.93 compared to the 14-bus system. This further underlines the difficulty EMTD faces under the compounded nonlinearity of larger systems during contingencies.

V. CONCLUSION

This article introduces a data-driven MTD strategy for enhancing cybersecurity in dynamic nonlinear smart grids, addressing both the detection efficacy and operational cost-efficiency. Our proposed method, distinguished by its utilization of KLD and the KS test, maximizes the divergence in line reactance while ensuring the changes remain within a reasonable cost spectrum. A key contribution of our work lies in its mathematical rigor, particularly in handling the nonlinearities of ac

power systems. By applying a piecewise linear approximation to the KLD function and incorporating KS test constraints, we transform a complex optimization problem into a tractable MILP model. This strategic linearization not only facilitates the practical application of the method but also ensures its computational efficiency and optimality in real-world scenarios. Morover, simulation results on IEEE 14-bus and 118-bus systems exhibit the method's superiority, outperforming existing MTD strategies in terms of detection rates while maintaining lower operational costs. Postcontingency simulation results demonstrate the outstanding performance of the proposed MTD method, which consistently achieves high detection rates and effectively controls costs, outperforming other MTD approaches.

References

[1] A. Shefaei, M. Mohammadpourfard, B. Mohammadi-ivatloo, and Y. Weng, "Revealing a new vulnerability of distributed state estimation: A data integrity attack and an unsupervised detection algorithm," *IEEE Trans. Control Netw. Syst.*, vol. 9, no. 2, pp. 706–718, Jun. 2022.

[2] K. Aygul, M. Mohammadpourfard, M. Kesici, F. Kucuktezcan, and I. Genc, "Benchmark of machine learning algorithms on transient stability prediction in renewable rich power grids under cyber-attacks," *Internet Things*, vol. 25, 2024, Art. no. 101012.

[3] T.S. Sreeram and S. Krishna, "Graph-based assessment of vulnerability to false data injection attacks in distribution networks," *IEEE Trans. Power Syst.*, vol. 39, no. 2, pp. 4510–4520, Mar. 2024.

[4] M. Tajdinian, M. Mohammadpourfard, Y. Weng, and I. Genc, "Preserving microgrid sustainability through robust islanding detection scheme ensuring cyber-situational awareness," *Sustain. Cities Soc.*, vol. 96, 2023, Art. no. 104592.

[5] M. Mohammadpourfard, F. Ghanaatpishe, Y. Weng, I. Genc, and M. T. Sandikkaya, "Real-time detection of cyber-attacks in modern power grids with uncertainty using deep learning," in *Proc. Int. Conf. Smart Energy Syst. Technol.*, 2022, pp. 1–6.

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

[7] M. Cui and J. Wang, "Deeply hidden moving-target-defense for cybersecure unbalanced distribution systems considering voltage stability," *IEEE Trans. Power Syst.*, vol. 36, no. 3, pp. 1961–1972, May 2021.

[8] 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.

[9] C. Liu, J. Wu, C. Long, and D. Kundur, "Reactance perturbation for detecting and identifying FDI attacks in power system state estimation," *IEEE J. Sel. Topics Signal Process.*, vol. 12, no. 4, pp. 763–776, 2018.

[10] Z. Zhang, R. Deng, D. K. Y. Yau, P. Cheng, and J. Chen, "Analysis of moving target defense against false data injection attacks on power grid," *IEEE Trans. Inf. Forensics Secur.*, vol. 15, pp. 2320–2335, 2020.

[11] Z. Zhang, Y. Tian, R. Deng, and J. Ma, "A double-benefit moving target defense against cyber–physical attacks in smart grid," *IEEE Internet Things J.*, vol. 9, no. 18, pp. 17912–17925, Sep. 2022.

[12] S. Lakshminarayana, E. V. Belmega, and H. V. Poor, "Moving-target defense against cyber-physical attacks in power grids via game theory," *IEEE Trans. Smart Grid*, vol. 12, no. 6, pp. 5244–5257, Nov. 2021.

[13] J. Wang, J. Tian, Y. Liu, D. Yang, and T. Liu, "MMTD: Multistage moving target defense for security-enhanced D-FACTS operation," *IEEE Internet Things J.*, vol. 10, no. 14, pp. 12234–12247, Jul. 2023.

[14] 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.

[15] W. Xu, I. M. Jaimoukha, and F. Teng, "Robust moving target defence against false data injection attacks in power grids," *IEEE Trans. Inf. Forensics Secur.*, vol. 18, pp. 29–40, Sep. 2023.

[16] J. Tian, R. Tan, X. Guan, Z. Xu, and T. Liu, "Moving target defense approach to detecting Stuxnet-like attacks," *IEEE Trans. Smart Grid*, vol. 11, no. 1, pp. 291–300, Jan. 2020.

[17] 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.

[18] 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.

[19] Z. Zhang, R. Deng, P. Cheng, and M.-Y. Chow, "Strategic protection against FDI attacks with moving target defense in power grids," *IEEE Trans. Control Netw. Syst.*, vol. 9, no. 1, pp. 245–256, Mar. 2022.

[20] B. Liu and H. Wu, "Optimal planning and operation of hidden moving target defense for maximal detection effectiveness," *IEEE Trans. Smart Grid*, vol. 12, no. 5, pp. 4447–4459, Sep. 2021.

[21] Z. Zhang, R. Deng, D. K. Y. Yau, P. Cheng, and M.-Y. Chow, "Security enhancement of power system state estimation with an effective and low-cost moving target defense," *IEEE Trans. Syst., Man, Cybern. Syst.*, vol. 53, no. 5, pp. 3066–3081, May 2023.

[22] S. Lakshminarayana and D. K. Yau, "Cost-benefit analysis of moving-target defense in power grids," in *Proc. Annu. IEEE/IFIP Int. Conf. Dependable Syst. Netw.*, 2018, pp. 139–150.

[23] C. Liu, R. Deng, W. He, H. Liang, and W. Du, "Optimal coding schemes for detecting false data injection attacks in power system state estimation," *IEEE Trans. Smart Grid*, vol. 13, no. 1, pp. 738–749, Jan. 2022.

[24] J. Huang, D. W. Ho, F. Li, W. Yang, and Y. Tang, "Secure remote state estimation against linear man-in-the-middle attacks using watermarking," *Automatica*, vol. 121, 2020, Art. no. 109182.

[25] M. Zhang, X. Fan, R. Lu, C. Shen, and X. Guan, "Extended moving target defense for AC state estimation in smart grids," *IEEE Trans. Smart Grid*, vol. 14, no. 3, pp. 2313–2325, May 2023.

[26] A. Hinneck and D. Pozo, "Optimal transmission switching: Improving solver performance using heuristics," *IEEE Trans. Power Syst.*, vol. 38, no. 4, pp. 3317–3330, Jul. 2023.

[27] Z. Li, W. Wu, X. Tai, and B. Zhang, "A reliability-constrained expansion planning model for mesh distribution networks," *IEEE Trans. Power Syst.*, vol. 36, no. 2, pp. 948–960, Mar. 2021.

[28] M. A. Lejeune and P. Dehghanian, "Optimal power flow models with probabilistic guarantees: A Boolean approach," *IEEE Trans. Power Syst.*, vol. 35, no. 6, pp. 4932–4935, Nov. 2020.

[29] H. Hua et al., "Optimal allocation and sizing of fault current limiters considering transmission switching with an explicit short circuit current formulation," *IEEE Trans. Power Syst.*, vol. 38, no. 2, pp. 1322–1335, Mar. 2023.

[30] M. Mohammadpourfard, Y. Weng, M. Pechenizkiy, M. Tajdinian, and B. Mohammadi-Ivatloo, "Ensuring cybersecurity of smart grid against data integrity attacks under concept drift," *Int. J. Elect. Power Energy Syst.*, vol. 119, 2020, Art. no. 105947.

[31] 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.

[32] M. Sahraei-Ardakani and K. W. Hedman, "A fast LP approach for enhanced utilization of variable impedance based facts devices," *IEEE Trans. Power Syst.*, vol. 31, no. 3, pp. 2204–2213, May 2016.

[33] T. Akbari and M. Tavakoli Bina, "Linear approximated formulation of AC optimal power flow using binary discretisation," *IET Gener., Transmiss. Distrib.*, vol. 10, no. 5, pp. 1117–1123, 2016.