IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 6 July 2024, accepted 22 July 2024, date of publication 2 August 2024, date of current version 2 September 2024.

Digital Object Identifier 10.1109/ACCESS.2024.3437426

RESEARCH ARTICLE

Countering AC Load Redistribution Attacks in Smart Grids: The Role of Moving Target Defense in a Defense-Attack Game

BO LIU[1], (Member, IEEE), HONGYU WU[2], (Senior Member, IEEE), AND HANG ZHANG[3], (Member, IEEE)

[1]School of Engineering and Applied Sciences, Washington State University Tri-Cities, Richland, WA 99354, USA
[2]Mike Wiegers Department of Electrical and Computer Engineering, Kansas State University, Manhattan, KS 66506, USA
[3]Department of Information Engineering, Henan University of Science and Technology, Luoyang, Henan 471003, China

Corresponding author: Hongyu Wu (hongyuwu@ksu.edu)

This work was supported in part by U.S. National Science Foundation under Grant 2146156, and in part by United States Office of Naval Research under Grant N00014-23-1-2777.

ABSTRACT Load redistribution attacks (LRAs) are a type of false data injection attack that disrupts the normal operation of the power grid by redistributing load. While most LRAs in the literature are based on the DC model, this paper proposes an LRA in the AC model using incomplete network information. To defend against the proposed LRA, the paper proposes using Moving Target Defense (MTD) to actively invalidate the attackers' knowledge. A zero-sum defense-attack game is formulated between MTD and LRA to select an MTD operating range optimally, considering the trade-off between attack detection effectiveness and the extra operation cost. The paper defines a new payoff function as an expected incremental operation cost, consisting of the defense cost, attack cost, and attack mitigation capability. A Nash Equilibrium of the game provides optimal strategies for selecting the MTD operating range. Simulation results on the modified IEEE 14-bus system demonstrate the effectiveness of MTD in detecting the proposed LRA. The paper shows that MTD not only detects ongoing LRAs but also prevents the construction of such attacks by using the proposed game theoretical framework. The proposed approach highlights the role of MTD in enhancing the cybersecurity of power grids against LRAs.

INDEX TERMS AC load redistribution attacks, moving target defense, zero-sum game, optimal strategy.

I. INTRODUCTION

False data injection (FDI) attacks are a type of low-probability, high-consequence cyberattacks against power systems [1]. FDI attacks manipulate the measurements in the Supervisory Control And Data Acquisition (SCADA) system to mislead system operators into obtaining incorrect state estimation. Load redistribution attacks (LRAs) are a highly structured FDI attacks that restrictively manipulate bus injection measurements to increase generation costs or trigger load shedding. Yuan et al. formulated immediate and delayed LRAs based on bi-level optimization [2] and also provided a quantitative analysis of the LRA consequence on power system operations [3]. Liu and Li proposed a stealthy local load redistribution attack using incomplete network information [4] Zhang et al. proposed a novel LRA model aiming to cause voltage violations in the distribution system [5]. In [6], a DC LRA was proposed against the power systems, considering the presence of insider threats. A security resource allocation game is formulated, in which the information leakage of the system operator's defense strategy by the insider to the external attacker is considered. The optimal strategies of both the system operator and attacker can be calculated to maximize their own payoffs. Su et al. developed a defense strategy for the optimal allocation of limited defensive resources to safeguard power systems against LRA [7]. A trilevel optimization problem is formulated, in which chance constraint is used to capture the

The associate editor coordinating the review of this manuscript and approving it for publication was Hao Wang.

possible variations in the attacker's actions. However, most LRA models are constructed in the DC model, and LRAs aiming to trigger load shedding in the AC system is still missing in the literature. Therefore, establishing an AC-LRA model aiming to increase operation costs through involuntary load shedding based on incomplete network information is necessary to quantify the attack consequence, whereby the interaction between such attacks and defense mechanisms can be further studied.

Multiple defense methods have been proposed to detect, identify, and mitigate FDI attacks, using protected sensors, Phasor Measurement Unit (PMU), and machine learning techniques. Since FDI attacks require the attacker's knowledge about the system measurements, one natural approach is to strategically select and protect critical measurements using protected sensors. Bi and Zhang proposed the optimal protection problem as a variant Steiner tree problem in a graph, which protects the state variables using the minimum number of protected sensors [8]. PMUs are also used to detect FDI attacks due to their ability to provide measurement redundancy. Pei et al. first protected the most vulnerable buses, and then proposed a greedy algorithm to deploy other PMUs [9]. However, these two methods require expensive hardware devices to improve the cybersecurity of the power system. Machine learning methods have been used to detect FDI attacks, in which the normal and compromised measurements are clustered into distinct regions in the feature spaces. Esmalifalak et al. applied a support vector machine (SVM) to classify the normal and compromised measurements after the principal component analysis dimension reduction [10]. Sakhnini et al. applied SVM, the k-nearest neighbor algorithm (KNN), and the artificial neural network (ANN) to detect FDI attacks [11]. However, the ML-based algorithms are vulnerable to specifically designed FDI attacks, which has been verified in recent studies [12], [13], [14].

Moving target defense (MTD) is a proactive defense mechanism in computer engineering, that changes the system configuration to reduce the attack surface and increase the cost of attacks. MTD has been applied in the physical layer of the power system by using distributed flexible AC transmission system (D-FACTS) devices to change the impedance of transmission lines. Originally, D-FACTS devices modify the impedance of transmission lines to manage the power flow and reduce the generation costs. In MTD, these installed D-FACTS devices are utilized to change the line impedance to invalidate the attacker's knowledge of the configuration.

Multiple attack detection effectiveness metrics have been proposed, and MTD operation methods are accordingly proposed to improve the performance of MTD. In the simplified DC model, the rank of the composite matrix is widely used to measure the detection effectiveness [15]. Lakshminarayana and Yau used the smallest principal angle of the Jacobian matrices before and after MTD as the detection effectiveness metric, and investigated the relationship between the effectiveness of MTD and the associated cost [16]. In the AC power system model, Liu et al. derived explicit approximations of measurement residuals to quantify the effectiveness and hiddenness of MTD [17]. It adopted the sensitivity analysis around the optimum point and derived explicit approximations of residuals, and further designed explicit residual-based MTD to jointly optimize the detection effectiveness and hiddenness.

In the literature, some works examined the interaction between MTD and cyber-physical attacks in power systems via game theory. Lakshminarayana et al. investigated the interaction between coordinated cyber-physical attacks (CCPA) and MTD in a DC model to solve the placement of D-FACTS devices [18]. In the game, the attacker's action is to select transmission lines to maliciously disconnect, while the defender's action is to select transmission lines to install D-FACTS devices and detect attacks [18]. The Nash equilibrium solution identifies the lines that are most likely to be maliciously disconnected by the attacker. Based on this Nash Equilibrium solution, Yu and Li proposed an algorithm to place D-FACTS devices by taking these lines as protected transmission lines [19].

However, these two works focus on the placement of D-FACTS devices in MTD, rather than the operation of D-FACTS devices. To operate MTD, a system operator (defender) needs to preset the operating range of D-FACTS devices, known as the MTD magnitude, based on various factors, including the physical capability of D-FACTS devices. MTD magnitude influences MTD detection performance in noisy conditions. A small MTD magnitude can degrade the attack detection capability [20], while a large MTD magnitude increases the system operation cost [21] and the gear cost of D-FACTS devices [22]. The selection of a proper MTD magnitude is crucial to strike a meaningful balance between detection capability and defense cost. However, the selection of MTD magnitude remains an unresolved issue for system operators in the literature. To the best of our knowledge, there is little work in the literature that has examined the intricate interaction between MTD operation and LRA attacks using a full AC model.

In this paper, we provide a novel perspective on the complex interplay between MTD and FDI attacks that has not been explored previously. Specifically, we formulate a unique defense-attack game between MTD and LRAs to address the trade-off in selecting the MTD magnitude with a full AC model. Unlike existing literature that either switches the D-FACTS placements [18] or suggests a fixed MTD magnitude [15], [16], [20], [21], [23], [24], [25], [26], [27], we propose a more realistic and mixed strategy in which the MTD magnitude changes over time based on a pre-designed probability. Additionally, we investigate the detection effectiveness of MTDs in detecting AC-LRA, a highly structured FDI attack. Since both the LRAs and MTD affect the system operation cost, we integrate both the attack detection effectiveness and system operation cost into the

payoff function. The proposed D-A game can assist system operators in optimally selecting MTD magnitudes to reduce the system operation cost, including the defense cost and attack consequence, while considering the attacker's actions. Furthermore, while previous research on MTDs in power systems has focused primarily on assessing their effectiveness in detecting attacks, little attention has been given to their potential role in preventing attacks by varying the system's attack surface. As such, we believe it is essential to investigate the prevention function of MTDs against LRAs and explore their full potential for mitigating the impact of these attacks on the system.

The contributions of this paper are summarized as follows:

- We propose a novel approach for formulating a defense-attack game between MTD and LRAs. We define a new payoff function as the expected incremental system operation cost, which includes both the generation cost and the load-shedding cost. By solving the Nash Equilibrium, we obtain optimal strategies for defenders and attackers, respectively, to select the MTD magnitude and LRA attack magnitude. Moreover, we suggest that defenders ought to update the MTD magnitude based on load conditions.
- Through the proposed D-A game theoretical framework, we have shown that the MTD not only detects ongoing LRAs in the power system but also effectively prevents the successful construction of highly structured attacks. The feature of ''prevention'' is often overlooked in the literature related to MTD applications in the power system. As a result, we introduce a novel MTD effectiveness metric to quantitatively measure the prevention and detection benefits of MTD against LRAs in the game. By changing the attack surfaces and preventing potential attacks, MTD can play a crucial role in improving the security of power systems.

The rest of this paper is organized as follows. Preliminaries of MTD are presented in Section II. A novel AC-LRA is proposed in Section III. A D-A game between MTD and LRAs is formulated in Section V. Case studies are conducted, and the results are analyzed in Section V. Conclusions are drawn in Section VI.

II. MTD PRELIMINARIES

A. MTD PLANNING METHODS

There are multiple MTD planning methods, i.e., the placement methods of D-FACTS devices, to determine the location of D-FACTS devices in MTD, including arbitrary placement [23], full placement [26], spanning-tree placement [27], max-rank placement [21], hidden MTD placement [24], [25], and graph-based placement [20]. It has been proved that MTD planning determines the effectiveness of MTD attack detection in DC noiseless conditions in the following two ways. First, the rank of the composite matrix, an MTD detection metric, is determined by the number of loops in G_A, if there exists no loop in G_B:

$$r(\mathbf{M}) = l - lp \tag{1}$$

where G_A and G_B are the graphs composed of lines equipped with and without D-FACTS devices, respectively, l is the number of transmission lines in the system, and lp is the number of loops in G_B. Second, improper MTD planning will result in unprotected buses, such that FDI attacks against these buses are undetected by the MTD. Thus, the existence of unprotected buses caused by the MTD planning degrades the MTD detection effectiveness [20].

The approach taken in this paper involves using graph-based placement to effectively detect LRAs. By adopting this method, we are able to ensure that the composite matrix achieves its maximum rank while also eliminating unprotected buses with only a limited number of D-FACTS devices. Additionally, the use of graph-based placement allows for maximum detection effectiveness in the DC noiseless condition, regardless of the D-FACTS operation setpoints.

B. MTD-ENABLED ATTACK DETECTION AND ATTACK PREVENTION

In previous research on MTD, the Attack Detection Probability (ADP), which is the ratio of the number of detected attacks to the total number of launched attacks, has been widely used as an indicator of MTD's detection effectiveness. Constructing an LRA requires solving an optimization problem [3], [4], [5], which presents a challenge for attackers when the MTD is in place. Specifically, incorrect line parameters could render the optimization problem infeasible, preventing attackers from successfully generating and launching LRAs. In this paper, we see the failure of the attacker's optimization problem as a benefit of the MTD's *attack prevention* capabilities. Conversely, if an attack is successfully generated by solving the attacker's optimization problem under the MTD, but the estimation residual of the attack in the BDD system exceeds the estimation threshold, we view this as a benefit of the MTD's *attack detection* capabilities.

The existing MTD detection effectiveness metrics (e.g., ADP) fail to consider the MTD attack prevention capability. Therefore, we propose a novel MTD effectiveness, i.e., attack mitigation probability (AMP), to simultaneously measure the MTD attack prevention and detection capability as follows:

$$p = (n_P + n_D)/n_A \tag{2}$$

where n_A is the number of total attacks the attacker intends to launch; n_P is the number of prevented attacks (diverged); n_D is the number of detected launched attacks (converged but detected). Note that $n_A - (n_P + n_D)$ is the number of undetected attacks (converged and stealthy). Thus, $p \leq 1$ holds.

III. PROPOSED AC-LOAD REDISTRIBUTION ATTACK MODEL

We propose an AC-LRA using the incomplete network information from the perspective of the attacker. To account for

the attacker's incomplete network information, we simplify the power system into a sub-system consisting of an attack zone (A zone) and a tie-line zone (T zone). The A zone includes all buses within the attack area and the transmission lines between them. The T zone is composed of all buses neighboring those in the A zone, but not included in the A zone itself. Transmission lines between a bus in the A zone and a bus in the T zone are considered as tie-lines. In our proposed LRA, loads in the T zone are treated as fixed loads, while loads in the A zone are considered dispatchable by adversaries.

We propose an ACOPF-based LRA model, shown in (3), to determine the dispatchable load in the A zone. In the proposed model, complex generation ($\mathbf{S}_G$), voltage magnitude ($\mathbf{v}$), voltage angle ($\boldsymbol{\theta}$), and complex dispatchable load ($\mathbf{S}_D$) are decision variables. Note that traditional LRA attack in the DC system is a bi-level optimization problem, in which the upper-level optimization problem represents the attacker's malicious objective (maximizing the system operation costs), and the lower-level optimization problem simulates the system response (minimizing the system operation costs). However, it is challenging to solve an AC LRA attack modeled by a bi-level optimization problem. To address this, we simplify the bi-level LRA by ignoring the system response (the lower-level optimization problem). Without modeling the system response, the proposed attack cannot effectively maximize the system operation costs. Thus, the proposed model prioritizes the feasibility of the AC LRA over its optimality to ensure the proposed attack is stealthy.

The objective function in (3) is to maximize a weighted sum of the dispatchable loads, with the weight ω being adjustable to the attacker based on the load conditions. The sum of the dispatchable loads is constrained to be close to the total load before attack in (3.12) and (3.13). The objective function in the proposed LRA (3) maximizes a weighted sum of the dispatchable loads. It doesn't aim to achieve the maximum operation costs. Using the weighted sum, the attacker can adjust the weights to find a feasible solution. Without modeling the system response, the proposed attack intends to trigger load shedding; nevertheless, this is not guaranteed.

The proposed AC-LRA follows the constraints of the traditional DC-LRA model. The generator output measurements are not allowed to be compromised by attackers in the LRA. Constraints (3.1)-(3.5) are traditional ACOPF constraints. Constraints (3.6) and (3.7) are voltage angle and magnitude constraints for the buses on the tie-line. These constraints enforce the voltage of the two end buses on tie-lines to be unchanged after the LRA, implying the same flow measurements on the tie-line after attacks. Constraints (3.8) and (3.9) indicate the load in T zone remains unchanged before and after LRA. The nodal load in the attack zone can only be modified in a pre-prescribed range to avoid abnormal alerts in the control room triggered by sudden significant nodal load changes. Thus, nodal active and reactive dispatchable load in A zone is constrained by LRA magnitude a in (3.10) and (3.11), respectively. Unlike the constraint on a constant total load in the traditional DC-LRA model [2], [3], Constraints (3.12) and (3.13) introduce a parameter λ to allow but limit the change of total active and reactive power load in the A zone. This is because the redistribution of load can result in changes in the power loss in the AC model and cause a power imbalance in the A zone. A small λ value (i.e., less than 1%) is therefore suggested in the AC model to avoid infeasibility while keeping the total load after the attack close to that before the attack.

$$\max_{S_G, S_D, v, \theta} \sum_{i \in A} \omega_i p_{d,i}$$

$$s.t.\ \mathbf{S}_{Bus} + \mathbf{S}_D - \mathbf{C}_g \mathbf{S}_G = 0 \tag{3.1}$$

$$\mathbf{S}_D = \mathbf{p}_d + j\mathbf{q}_d \tag{3.2}$$

$$\mathbf{S}_G = \mathbf{p}_g + j\mathbf{q}_g \tag{3.3}$$

$$\mathbf{S}_{Bus} = [\mathbf{v}] \cdot (\mathbf{Y}_{bus} \cdot \mathbf{v})^* \tag{3.4}$$

$$v_i^{\min} \le v_i \le v_i^{\max} \quad i \in A \tag{3.5}$$

$$\theta_i^0 - \beta_\theta \le \theta_i \le \theta_i^0 + \beta_\theta \quad i \in T \tag{3.6}$$

$$v_i^0 - \beta_v \le v_i \le v_i^0 + \beta_v i \in T \tag{3.7}$$

$$p_{d,i} = p_{d,i}^0 \quad i \in T \tag{3.8}$$

$$q_{d,i} = q_{d,i}^0 \quad i \in T \tag{3.9}$$

$$(1-a)p_{d,i}^0 \le p_{d,i} \le (1+a)p_{d,i}^0 \quad i \in A \tag{3.10}$$

$$(1-a)q_{d,i}^0 \le q_{d,i} \le (1+a)q_{d,i}^0 \quad i \in A \tag{3.11}$$

$$(1-\lambda)\sum_{i \in A} p_{d,i}^0 \le \sum_{i \in A} p_{d,i} \le (1+\lambda)\sum_{i \in A} p_{d,i}^0 \quad i \in A \tag{3.12}$$

$$(1-\lambda)\sum_{i \in A} q_{d,i}^0 \le \sum_{i \in A} q_{d,i} \le (1+\lambda)\sum_{i \in A} q_{d,i}^0 \quad i \in A \tag{3.13}$$

where $\mathbf{S}_{Bus}$ is complex bus power injections; $\mathbf{Y}_{bus}$ is the system bus admittance matrix; $[\mathbf{v}]$ is a diagonal matrix with vector $\mathbf{v}$ on the diagonal; the superscript $*$ is complex conjugate operator; $\mathbf{p}_d$ and $\mathbf{q}_d$ are active and reactive load vector; $\mathbf{p}_g$ and $\mathbf{q}_g$ are active and reactive power generation vector; C_g is the generator connection matrix, whose (i, j)th element is 1 if generator j is located at Bus i and 0 otherwise; a is LRA magnitude, indicating the operating range of dispatchable load; β_θ and β_v are the parameters, which are suggested to be a very small number; i and j are the index of buses; active and reactive power generation, active and reactive power load, and voltage with superscript 0 are the measurements before LRA.

The proposed LRA and the ACOPF problem are non-convex and nonlinear optimization problems. Interior-point methods are considered one of the most powerful algorithms for solving large-scale nonlinear optimization problems. It has been proven that interior-point methods are efficient tools for resolving the traditional ACOPF problem [28], [29]. The proposed LRA is modeled based on the ACOPF problem. Therefore, this work solves the proposed

LRA model (3) using the MATLAB Interior Point Solver (MIPS) provided in MATPOWER [30].

The nodal voltages obtained from (3) are used to calculate all malicious measurements in the attack area. Then, the attacker can replace all measurements needed to be compromised in the attack area with calculated malicious measurements. In such a case, the system operator conducts state estimation using the compromised measurements to estimate the voltage and nodal load. Consequently, the compromised load condition will mislead the ACOPF model run by the system operators to generate incorrect generation dispatch and even load curtailment.

IV. DEFENSE-ATTACK GAME BETWEEN MTD AND LRA

This section presents a zero-sum defense-attack game between MTD and LRA. We define the attack and defense models and their respective action strategies, and propose the expected incremental operation cost as the payoff function, which includes MTD defense cost, LRA attack cost, and MTD's attack mitigation capability. We also provide a payoff computation algorithm in this section.

In the defense-attack game between MTD and LRA, the attacker's action is to select the LRA magnitude, and the defender's action is to select the MTD magnitude. A Nash Equilibrium of the defense-attack game can provide the optimal strategy in selecting MTD and LRA magnitudes for the defender and the attacker, respectively.

A. ATTACK MODEL AND STRATEGY

In the game, we use the AC-LRA proposed in the previous section as the attack model. This is because traditional FDI attacks target voltage magnitude or angle, whereas the impact of such attacks on the system's operation cost is unclear. In contrast, the impact of LRA on the system's operation cost is quantifiable.

Before launching an LRA, the attacker must decide the LRA magnitude. LRA magnitude is the value of a in (3.10) and (3.11), indicating the operating range of dispatchable load. For example, if the attacker selects $a = 0.2$, the attacker can compromise the load of Bus i ($p_{d,i}$) among the range $\left[0.8p^0_{d,i},\ 1.2p^0_{d,i}\right]$. In a LRA with a larger LRA magnitude, the attacker can modify dispatchable loads in a wider range, indicating the attacker has a better capability in compromising dispatchable loads.

There is a trade-off in the LRA magnitude selection between attack stealthy and attack consequence. A larger LRA magnitude enables the attacker to modify the load in a wider range, consequently resulting in a larger increase in the system operation cost. However, a larger LRA magnitude makes the attack more likely to be detected by the system operators, therefore failing to increase the system operation cost. From the perspective of the attacker, it is necessary to balance the trade-off in the selection of attack magnitude. Therefore, in the defense-attack game, the attacker's action strategies are the selection of LRA magnitude. Specifically, we set five distinct LRA magnitudes for the attacker, i.e., $\mathrm{A} = \{0.15, 0.2, 0.25, 0.3, 0.35\}$. These are proper magnitudes in constructing LRA, avoiding the compromised measurements being easily detected as an outlier.

B. DEFENSE MODEL AND STRATEGY

In this game, we adopt random MTD (RMTD) [23] as the defense model because it is the most generalized method, and its conclusion can be extended to other MTD operation methods. Other methods such as hidden MTD (HMTD) [15], OPF-based [16], [21], optimization-based [26], and voltage stability constrained operation [31], [32] may bring extra benefits to the system, but these benefits are either unquantifiable or unrelated to system operation costs. For instance, the HMTD method makes the MTD hidden to alert attackers [24], [25], but its benefits are unquantifiable and do not contribute to improving attack detection effectiveness.

The random MTD operation method randomly selects setpoints for each D-FACTS device based on uniform distribution within the given operation range as follows:

$$x \sim U((1-d)x_0, (1+d)x_0) \tag{4}$$

where d is the MTD magnitude that determines the MTD operation range; x is the line reactance modified by D-FACTS devices; and x_0 is the original line reactance.

MTD magnitude is the value of d in (4), indicating the operating range of D-FACTS devices. The defender can adjust the operating range of D-FACTS devices based on the load condition within the physical limits of D-FACTS device. For example, if the defender selects $d = 0.2$, the D-FACTS devices can modify the impedance of i-th line among the range $\left[0.8x^0_i,\ 1.2x^0_i\right]$. In the MTD with a larger MTD magnitude, the defender can modify the impedance of the transmission lines equipped with D-FACTS devices in a larger range, indicating the defender has a better capability in introducing uncertainties to attackers.

The defender should determine the MTD magnitude before implementing the MTD operation (4). There is a trade-off in the selection of MTD magnitudes [8] between the operation cost and attack detection capability. A larger MTD magnitude has a better attack detection capability, but it increases the system's operation costs by introducing more randomness. A smaller MTD magnitude generally causes less system's operation costs. However, a smaller MTD magnitude may result in low attack detection capability, leading to high operation costs caused by undetected LRAs. Therefore, it is crucial to investigate the optimal MTD magnitude selection in the presence of cyberattacks. In the defense-attack game, MTD magnitude d is selected as the defense action strategy in RMTD operation with a fixed graph-based MTD planning as *a priori* [20]. This allows the system operator to adjust the defense strategy based on system conditions. Here, we set five distinct MTD magnitudes, $\mathrm{D} = \{0.15, 0.2, 0.25, 0.3, 0.35\}$, for the defender to choose from. These MTD magnitudes are within the physical limits of D-FACTS devices, which are widely used in MTD work [15], [21], [25], [26], [27]. The

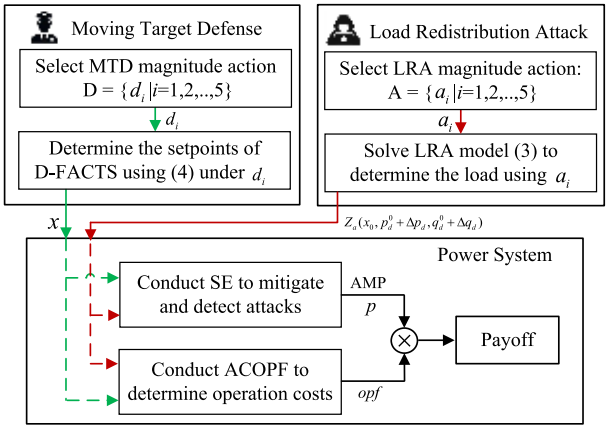

FIGURE 1. The framework of the D-A game between MTD and LRA.

Nash Equilibrium of the game can provide the defender with the optimal MTD magnitude to balance operation cost and attack detection capability.

C. DEFENSE-ATTACK GAME AND PAYOFF FUNCTION

The interaction between MTD and LRA can be simulated through a two-player zero-sum game, where the attacker aims to increase the operation cost while the defender aims to reduce it. We define the payoff function based on the system operation cost. The payoff for the defender is opposite to that of the attacker, meaning the defender's cost is a benefit for the attacker.

Figure 1 shows the framework of the defense-attack game between MTD and LRA. From the defender's perspective, the defender first selects MTD magnitude, i.e., the value of d in (4), and then determines the specific setpoints of D-FACTS devices using (4). From the attacker's perspective, the attacker first selects LRA magnitude, i.e., the value of a in (3), and then determines the load by solving the attack model (3). The power system operator (the defender) uses the D-FACTS setpoints to implement MTD in the system and receives the compromised measurements from the SCADA system injected by the attacker. The system operator then conducts SE under the MTD to determine whether the measurements are compromised or not. AMP value represents the attack mitigation probability of MTD against LRA. Then, the system operator conducts ACOPF using the compromised load to determine the operation costs. In the zero-sum defense-attack game, the defender's and attacker's payoff can be calculated by (7) and (8), respectively. It reflects the increased power system operation costs, which are composed of defense costs (the operating cost of MTD) and attack costs (the consequence of undetected attacks). A Nash Equilibrium of the game provides the defender with the optimal strategies for the MTD magnitude selection, and the attacker with the optimal strategies for the LRA magnitude selection.

Table 1 summarizes the system operation conditions and associated costs for the game. In this paper, the system operation cost is the sum of generation costs and load-shedding costs. Generation cost is a quadratic function of active power generation, and shedding cost is a linear function of active curtailed load. These two costs can be calculated by solving the ACOPF model considering the load shedding (ACOPF-LS) in [33]. We use d_0 and d_i to denote the system without the defense and with the i-th defense action, respectively. Similarly, a_0 and a_i denote the system without attack and with i-th attack action, respectively.

TABLE 1. System operation conditions and costs in the D-A game.

System conditions	Operation cost	Explanation
Without defense and attack	$\text{opf}(d_{0,i}^*, a_0)$	D-FACTS devices are used to minimize the operation cost under a given operation range
Defense deployed without attack	$\text{opf}(d_i, a_0)$	Randomness from MTD increases the operation cost
Defense deployed under attack	$\text{opf}(d_i, a_j)$	Assume LRA is successful, and LRA increases the operation cost

In the D-A game, the base case is the system free of defense and attack. In this condition, the setpoints of D-FACTS devices installed in the system are optimally dispatched by the ACOPF model considering the D-FACTS devices (ACOPF-DF) to minimize the operation cost [33]. Thus, the system in the base case has the lowest operation cost in the D-A game, denoted by $\text{opf}(d_{0,i}^*, a_0)$, where the superscript $*$ indicates the optimal D-FACTS setpoints, and subscript i implies that the operation range of D-FACTS devices in ACOPF-DF is the same as that in defense action d_i.

When MTDs with defense action d_i are deployed in the system free of attacks, RMTD increases the operation cost to $\text{opf}(d_i, a_0)$. When the system is under attack and MTD is deployed in the system, there are two possible situations. If the MTDs with defense action d_i successfully prevent or detect the attack, the impact of the LRA on the operation cost is negligible. Thus, the system operation cost is equal to the cost in the system with the defense action d_i deployed without attacks, i.e., $\text{opf}(d_i, a_0)$. If MTDs with the defense action d_i fail to prevent or detect the attack with action a_j, the system can suffer from the increasing operation cost caused by the attack. Then, we assume that the operation cost is $\text{opf}(d_i, a_j)$.

The payoff of the defender is defined as the expected incremental system operation cost caused by the defense action and attack action. If the LRA with attack action a_j is prevented or detected by the MTD with defense action d_i, the incremental operation cost can be calculated as follows:

$$\text{cost}_D(d_i, a_j) = \text{opf}(d_{0,i}^*, a_0) - \text{opf}(d_i, a_0) \tag{5}$$

If the LRA with attack action a_j successfully passes the MTD with defense action d_i, the incremental operation cost can be calculated as follows:

$$\text{cost}_A(d_i, a_j) = \text{opf}(d_{0,i}^*, a_0) - \text{opf}(d_i, a_j) \tag{6}$$

Here, $\text{cost}_D(d_i, a_j)$ merely reflects the operation cost spent on the defense, denoted as defense cost hereafter, and

$\text{cost}_A(d_i, a_j)$ mainly reflects the damage brought by LRA to the operation cost, denoted as attack cost hereafter. Note that $\text{cost}_A(d_i, a_j)$ also includes the cost spent on the defense, since the impact of MTD on the operation cost is considered in $\text{opf}(d_i, a_j)$.

It is necessary to integrate the capability of MTD to prevent and detect LRAs into the calculation of the incremental operation cost. Assume the attack mitigation probability of MTD with defense action d_i against LRA with attack action a_j is $p(d_i, a_j)$. The paper defines a payoff function as an expected incremental operation cost. Specifically, the payoff of the defender, under the defense action d_i and attack action a_j is defined in (7).

$$u_D(d_i, a_j) = p(d_i, a_j) \times \text{cost}_D(d_i, a_j) + (1 - p(d_i, a_j)) \times \text{cost}_A(d_i, a_j) \quad (7)$$

In the zero-sum game, the payoff of the attacker is the opposite of the defender's payoff:

$$u_A(d_i, a_j) = -u_D(d_i, a_j) \quad (8)$$

The payoff is defined as the expected incremental operation cost, considering the defense cost $\text{cost}_D(d_i, a_j)$, attack cost $\text{cost}_A(d_i, a_j)$, and attack mitigation probability $p(d_i, a_j)$. Note that defense cost, calculated by (5), represents the incremental operation cost caused by MTD when the LRA is detected or prevented. Similarly, the attack cost, calculated by (6), represents the incremental operation cost caused by the stealthy LRA.

The payoff computation of the game is proposed in Algorithm 1. First, we generate N RMTDs to create a pool of defense actions. Using the ACOPF-LS model, we calculate the system operation cost of each RMTD, then take the average of these costs with defense action d_i to obtain the operation cost of the deployed defense $\text{opf}(d_i, a_0)$. Next, we calculate the base operation cost without defense or attack, i.e., $\text{opf}(d^*_{0,i}, a_0)$, using the ACOPF-DF model and dispatching D-FACTS devices to only minimize the operation cost [33]. We use Line 9 of Algorithm 1 to calculate the defense cost under each defense action. To compute the attack cost, we construct and launch LRAs on each RMTD in the pool of defense actions. The average of the system operation costs under all successful LRAs is considered as $\text{opf}(d_i, a_j)$.

Algorithm 1 computes the payoff for the defender and attacker based on their respective actions in the game. The Nash Equilibrium of the game provides the optimal solution for the defender's choice of defense actions and the attacker's choice of attack actions. This equilibrium yields the defender's optimal probabilities for selecting each defense action and the attacker's optimal probabilities for selecting each attack action.

Algorithm 1 Payoff Computation in the Proposed Game

Input: Defense action set $\text{D} = \{d_1, d_2, d_3, d_4, d_5\}$
Attack action set $\text{A} = \{a_1, a_2, a_3, a_4, a_5\}$

Output: Payoff $u_D(\text{D}, \text{A})$ and $u_A(\text{D}, \text{A})$

1: **Initialization:** Suppose the graph-based D-FACTS placement
2: Generate N RMTDs in each defense actions d_i
3: **for** each defense action d_i
4: **for** k-th RMTD in defense action d_i
5: Run ACOPF-LS to get $\text{opf}(k, d_i, a_0)$
6: **end for**
7: Calculate $\text{opf}(d_i, a_0) = \sum_{k \in d_i} \text{opf}(k, d_i, a_0)/N$
8: Run ACOPF-DF to get $\text{opf}(d^*_{0,i}, a_0)$
9: Calculate defense cost $\text{cost}_D(d_i, a_j)$ according to (5)
10: **end for**
11: **for** each defense action d_i
12: **for** each attack action a_j
13: **for** k-th RMTD in defense action d_i
14: Construct and launch LRA
15: SE and BDD using k-th RMTD to detect attack
16: **if** MTD fails to prevent and detect LRA
17: Run ACOPF-LS to get $\text{opf}(k, d_i, a_j)$
18: **end if**
19: **end for**
20: Calculate AMP $\text{p}(d_i, a_j)$ according to (2)
21: Calculate $\text{opf}(d_i, a_j)$ using $\text{opf}(k, d_i, a_j)$
22: Calculate attack cost $\text{cost}_A(d_i, a_j)$ according to (6)
23: Calculate $u_D(d_i, a_j)$ and $u_A(d_i, a_j)$ according to (7) and (8)
24: **end for**
25: **end for**
26: **return** $u_D(\text{D}, \text{A})$ and $u_A(\text{D}, \text{A})$

V. NUMERICAL RESULTS

A. TEST SYSTEM AND SIMULATION SETTING

We simulate the D-A game in the modified IEEE 14-bus system under both light and heavy load conditions. For each defense action, we generate 100 RMTDs as a defense pool. For each attack action, one LRA is constructed and launched on each MTD in the defense pool. Therefore, there are 100 attack and defense simulations for each pair of defense and attack actions, and there are 2,500 attack and defense simulations in total to calculate the payoff in the defense-attack game considering five attack actions and five defense actions. The Nash equilibria point of the proposed game can be calculated by the enumeration technology [34]. The graph-based MTD planning installs D-FACTS devices on Line {1, 3, 4, 8, 10, 11, 12, 13, 17, 18} in the IEEE 14-bus modified system. In a noisy condition, the measurement noise is assumed to be Gaussian distributed with zero mean and the standard deviation as 1% of the actual measurement.

B. TEST SYSTEM AND SIMULATION SETTING

In this section, we construct and evaluate LRAs in the IEEE 14-bus modified system under light and heavy load conditions, respectively, when there is no defense algorithm deployed in the system. Assume that the attacker selects Buses 9, 10, 11, and 14 as the attack area, as shown in Fig. 2. We adopt $\beta_\theta = 0.01\%$, $\beta_v = 0.01\%$, and $\lambda = 0.1\%$ in the LRA model. We set the load shedding cost 10^6 \$/MWh and use the default quadratic generation cost in the MATPOWER [35]. Under the heavy load condition, the

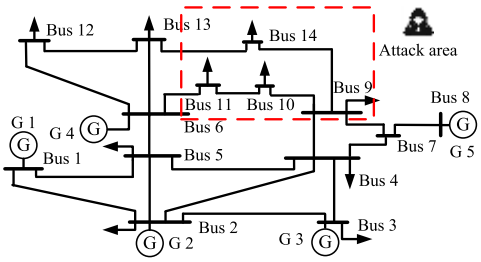

FIGURE 2. Attack area in the IEEE 14-bus system.

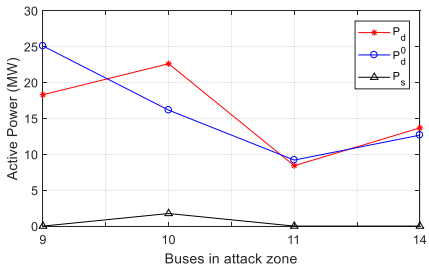

FIGURE 3. System operation condition before and after the LRA.

load values at Buses 1 to 14 is given as 10.1, 18.4, 80.1, 40.6, 9.2, 9.5, 8.8, 10.1, 25.1, 16.2, 9.2, 8.7, 11.5, 12.7. Under the light load condition, each nodal load is half of that under the heavy load condition. The power flow limits of all lines are given as 135.1, 68.8, 57.1, 52.8, 39.3, 9.6, 58.1, 29.2, 18.1, 34.8, 19.3, 11.7, 23.5, 18.2, 36.1, 13.9, 7.9, 7.1, 5, 8.7 MW following the order of transmission lines in MATPOWER. Specifically, the power flow limits for Line 9-14, Line 9-10, and Line 10-11 in the attack zone are 7.9 MW, 13.9 MW, and 7.1 MW, respectively.

When an LRA with $a = 0.4$ is launched on the IEEE 14-bus system under the heavy load condition, the nodal active power load in the attack area before the LRA (P_d^0) and after the LRA (P_d), and load curtailment (P_s) in the attack area are demonstrated in Fig. 3. It is observed that redistributed loads vary in the range constrained by LRA magnitude to avoid abnormal alerts. Due to the total load constraints, the load on Buses 9 and 11 decreases while that on Buses 10 and 14 increases. Specifically, the total active load in the attack zone before and after the attack is 63.08 MW and 63.02 MW, respectively. Under the redistributed load, the traditional ACOPF fails to converge, and the ACOPF-LS model curtails 1.75 MW load on Bus 10. This is because the LRA increases the load of Bus 10 from 16.15 MW to 22.61 MW, which is beyond the line flow limit of Lines 10-11 and 9-10.

We study the impact of the LRA magnitude on the operation cost under the heavy load condition. When the LRA magnitude is increased from 0 to 0.4, the system operation conditions after the attacks are summarized in Table 2, including the total active load in the attack area (P_d), the total reactive load in the attack area (Q_d), the generation cost of the system (GC), the load shedding cost (LC) and the system operation cost (OC). Without MTD deployed, OC under

TABLE 2. System operation conditions under different LRA magnitudes at the heavy load.

a	0	0.1	0.2	0.3	0.4
P_d(MW)	63.08	63.07	63.05	63.03	63.01
Q_d(MVar)	6.31	6.27	6.23	6.18	6.13
GC ($)	8490.69	8490.70	8490.76	8487.72	8422.74
LC ($)	0.00	0.00	0.00	136732.74	1751600.05
OC($)	8490.69	8490.70	8490.76	145220.46	1760022.80

TABLE 3. System operation conditions under different LRA magnitudes at the light load.

a	0	0.1	0.2	0.3	0.4
P_d(MW)	31.54	31.54	31.53	31.53	31.52
Q_d(MVar)	3.15	3.14	3.13	3.12	3.11
GC ($)	3467.34	3467.34	3467.34	3467.35	3467.35
LC ($)	0.00	0.00	0.00	0.00	0.00
OC($)	3467.34	3467.34	3467.34	3467.35	3467.35

attack can be denoted by opf(d_0, a_j), and it is equal to the sum of GC and LC. Note that the system operation condition under zero LRA magnitude refers to the condition free from attacks. Firstly, as seen the active and reactive total loads under attack are slightly different from those free of attack, which indicates the total load constraints (3.12) and (3.13) are satisfied. Secondly, it can be seen from the LC that the LRA doesn't trigger the load curtailment until the LRA magnitude is larger than 0.2. As the LRA magnitude increases, the amount of load curtailment increases. A larger attack magnitude gives the attacker more ability to redistribute the load, which in turn increases the effectiveness of LRAs in driving up system operation costs through load curtailments.

In addition, we evaluate the LRA's performance under light load conditions, as shown in Table 3, and find that even the largest LRA magnitude (i.e., $a = 0.4$) fails to trigger load curtailment. This occurs because the post-attack line power flow is far below the line flow limit, which allows generators to supply nodal loads within the attack zone. The above results demonstrate the validity of the proposed LRA model.

C. DETECTION OF LRA UNDER MTD IN THE GAME

In this subsection, we evaluate the effectiveness of the MTD methods in preventing and detecting the proposed LRA. Specifically, we calculate the AMP of MTD for each pair of defense and attack actions in the IEEE 14-bus system under light and heavy load conditions, respectively. Note that the i-th attack action refers to the i-th LRA magnitude in attack action set A = {0.15, 0.2, 0.25, 0.3, 0.35}. Similarly, the i-th defense action refers to the i-th MTD magnitude in set D.

Figures 4(a) and 4(b) demonstrate, respectively, the number of prevented attacks n_P and the number of detected attacks n_D under each pair of defense and attack actions in the IEEE 14-bus system under the heavy load condition. From the perspective of the defender, MTDs with a larger MTD magnitude can prevent more LRAs, and are more likely to detect

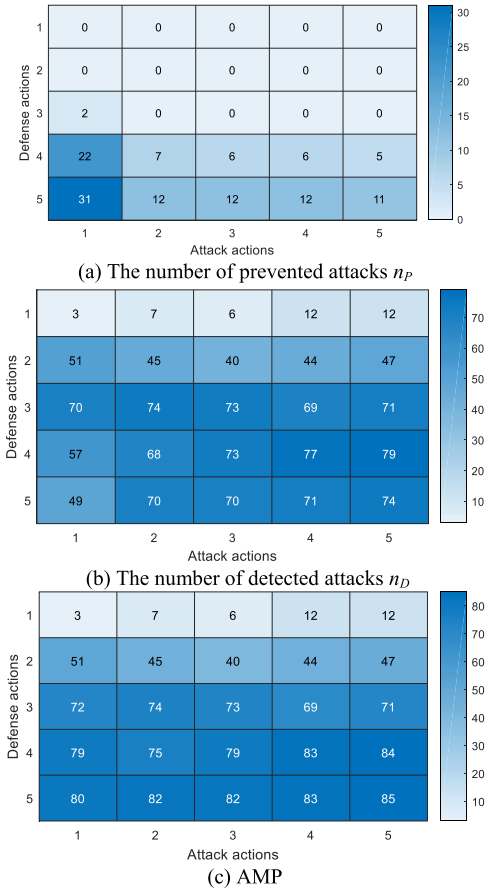

FIGURE 4. Performance of MTD in mitigating attacks at the heavy load.

TABLE 4. Defense costs versus defense actions.

Cost	d_1	d_2	d_3	d_4	d_5
opf(d_0, a_0)	8488.10	8486.43	8485.37	8484.74	8484.29
opf(d_i, a_0)	8505.44	8506.22	8506.86	8509.44	8511.27
$\text{cost}_D(d_i, a_j)$	-17.34	-19.79	-21.49	-24.70	-26.97

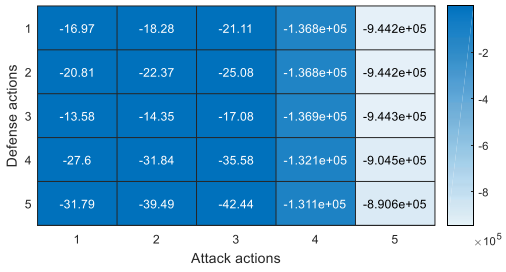

FIGURE 5. Attack cost under the heavy load condition in the IEEE 14-bus system.

attacks. From the attacker's standpoint, LRAs with smaller magnitudes are more likely to be prevented, but LRAs with large magnitudes are more likely to be detected. The AMP under each pair of the defense and attack actions, calculated by (2), is shown in Fig. 4(c). AMP greatly increases with an increase in MTD magnitude, suggesting setting the MTD magnitude greater than defense action 3 for achieving a high AMP.

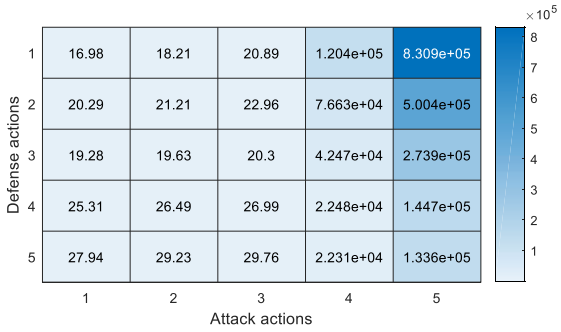

FIGURE 6. The payoff of the attacker in the IEEE 14-bus system under the heavy load condition.

TABLE 5. Nash Equilibrium under heavy load condition.

Action	1	2	3	4	5	Payoff
Defender	0	0	0	0	1	-133611
Attacker	0	0	0	0	1	133611

D. THE DEFENSE AND ATTACK COSTS IN THE GAME

In this subsection, we calculate the defense cost cost_D and attack cost cost_A in the game. Table 4 summarizes the operation cost with and without the MTD defense, and defense cost. The ACOPF-DF model optimally dispatches the set-points of D-FACTS devices such that a larger operation range can further reduce opf(d_0, a_0). But, the randomness in the RMTD causes more extra operation cost such that a larger operation range can further increase opf(d_i, a_0). Therefore, MTDs with a larger magnitude result in a higher defense cost. Note that the defense cost is unrelated to the attack actions, as it is assumed that attacks are successfully prevented or detected in the calculation of defense cost.

Then, we calculate the attack cost $\text{cost}_A(d_i, a_j)$, as shown in Fig. 5. It is observed that the attack cost is very low when the LRA magnitude is low (less than 4), because the LRA fails to trigger the load curtailment. In this case, the attack cost is mainly caused by the extra operation cost due to the MTD, i.e., the defense cost. When the LRA magnitude is more than 3, the LRAs start to trigger the load curtailment, and a larger LRA magnitude results in a higher operation cost, which is consistent with the attack performance in Table 2.

The simulation results suggest the attacker adopts a high LRA magnitude to maximize the attack cost. We also calculate the attack cost when the system operates under the light load condition. As LRAs fail to trigger the load curtailment, the attack cost under the light load condition is similar to its defense cost, as shown in Table 3. Therefore, under the light load condition, we neglect the attack cost and directly present the payoff in the next section.

E. NASH EQUILIBRIUM OF THE GAME

In the IEEE 14-bus system under the heavy load condition, we calculate the attacker's payoff, which is shown in Fig. 6. It is shown that the payoff increases with the increase of LRA magnitude under the same MTD magnitude. This is because

FIGURE 7. The payoff of the attacker in the IEEE 14-bus system under the light load condition.

TABLE 6. Nash Equilibrium under the light load condition.

Action	1	2	3	4	5	Payoff
Defender	1	0	0	0	0	-0.25
Attacker	0	0	0	0	1	0.25

the cost of load shedding increases with the LRA magnitude, but the AMP under the same MTD magnitude doesn't obviously increase with LRA magnitude. When LRAs with low magnitudes fail to trigger the load curtailment (attack action less than 4), the payoff is mainly determined by the defense cost such that the payoff slightly increases with the increase of MTD magnitude. When LRAs with large magnitude trigger the load curtailment, payoff obviously decreases with the increase of MTD magnitude under the same LRA magnitude. This is determined by two facts in the game. First, the payoff is mainly determined by the attack cost since the defense cost is rather small compared with the damage by LRA. Second, MTD with a larger magnitude has better attack mitigation capability against LRA, which can effectively reduce the impact of attack cost.

Nash Equilibrium in Table 5 suggests attackers adopt the largest LRA magnitude (attack action 5) to maximize its payoff, as a larger LRA magnitude increases its benefit regardless of defense actions adopted by the defender. The Nash Equilibrium also suggests defenders adopt the largest MTD magnitude (defense action 5) to minimize its payoff. A large MTD magnitude can enhance the attack mitigation capability, which is effective in reducing the payoff.

In the IEEE 14-bus system under the light load condition, the payoff of the attacker is shown in Fig. 7. It is seen that payoff almost remains the same under the same MTD magnitude with different LRA magnitudes. This is because LRAs fail to cause the load shedding under the light load condition with limited LRA magnitude. Therefore, the payoff is mainly composed of the operation cost spent on defense. As shown in Table 6, Nash Equilibrium suggests that defenders adopt the lowest MTD magnitude to reduce the defense cost, and attackers adopt the largest LRA magnitude to have the most negative impact on the grid operation.

We further simulate the D-A game in the IEEE 118-bus system under light and heavy load conditions, respectively.

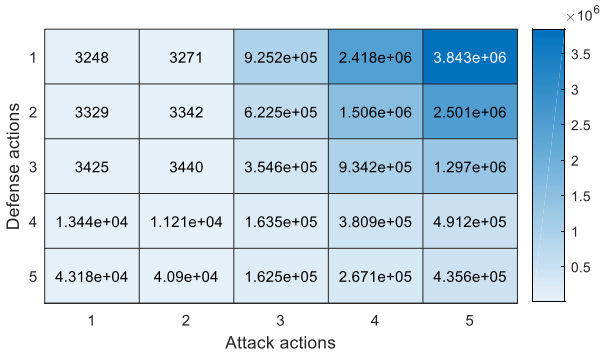

FIGURE 8. The payoff of the attacker in the IEEE 118-bus system under the heavy load condition.

TABLE 7. Nash equilibrium under heavy load condition.

Action	1	2	3	4	5	Payoff
Defender	0	0	0	0	1	-435600
Attacker	0	0	0	0	1	435600

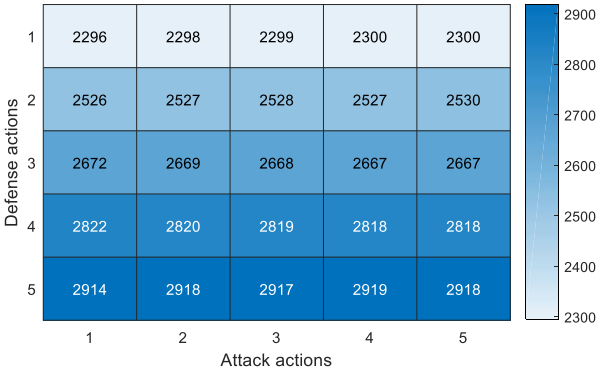

FIGURE 9. The payoff of the attacker in the IEEE 118-bus system under the light load condition.

From the defender's perspective, the graph-based MTD planning solution in the IEEE 118-bus system can be found in [20]. From attacker's perspective, it is assumed that the attacker selects Buses 43, 44, and 45 as the attack area, and Buses 34, 46, and 49 are buses on the tie-lines.

The payoff of the attacker and the Nash Equilibrium under the heavy load condition are shown in Fig. 8 and Table 7, respectively. As shown in Fig. 8, the attacker's payoff significantly increases under a given defense action when LRA magnitude is more than attack action two due to the load curtailment triggered by the LRA. Similar to the case in the IEEE 14-bus system, the payoff decreases with the increase of the defense action due to the attack prevention and detection when the load curtailment occurs in attack actions 3-5. It is interesting to observe that attacker's payoff significantly increases when the defense action increases from 3 to 4 under attack actions 1 and 2. A larger MTD magnitude leads to a higher payoff under the same LRA magnitude because certain RMTDs in the defense pool can drive the system to operate in more stressful conditions under heavy load condition. Consequently, LRAs with low magnitude can cause

TABLE 8. Nash Equilibrium under light load condition.

Action	1	2	3	4	5	Payoff
Defender	1	0	0	0	0	-2300.0
Attacker	0	0	0	0	1	2300.0

load curtailment in large-magnitude MTDs. This is an inherent drawback of RMTDs. The Nash Equilibrium in Table 7 suggests the attackers adopt the largest attack magnitude to maximize the attacker's payoff, while defenders adopt the largest defense action to minimize the defender's payoff.

Under the light load condition, the payoff of the attacker and the Nash Equilibrium are shown in Fig. 9 and Table 8, respectively. The attacker's payoff slightly increases with the defense action due to the increasing defense cost. As the LRAs fail to cause load shedding in any attack action under the light load condition, the payoff under a given defense action nearly remains the same. The Nash Equilibrium recommends that the attackers adopt the largest attack magnitude and the defenders should adopt the lowest defense magnitude.

VI. CONCLUSION

This paper introduces a new AC-LRA, based on the ACOPF model, to increase system operation costs by curtailing loads. We then create a zero-sum defense-attack game between MTD and LRA, where MTD magnitude is the defense action and LRA magnitude is the attack action. We define a novel payoff function that considers defense cost, attack cost, and attack mitigation capability, which helps balance the trade-off between operation cost and attack mitigation effectiveness. The Nash Equilibrium of the game provides optimal action strategies for defenders and attackers. We suggest using the lowest MTD magnitude under light load conditions and the largest MTD magnitude under heavy load conditions to minimize the expected incremental operation cost under LRAs. The case studies on modified IEEE 14-bus system reveal the benefits and drawbacks of RMTD against LRAs. RMTDs can prevent and detect LRAs, but also increase system operation costs, especially with larger magnitudes. In some cases, RMTDs can even cause more stressful conditions under heavy load, leading to load curtailment by low-magnitude LRAs. Future work will focus on more advanced MTD operation methods (e.g., HMTD) integrated into the payoff definition.

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

[3] Y. Yuan, Z. Li, and K. Ren, "Quantitative analysis of load redistribution attacks in power systems," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1731–1738, Sep. 2012.

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

[5] H. Zhang, B. Liu, and H. Wu, "Net load redistribution attacks on nodal voltage magnitude estimation in AC distribution networks," in *Proc. IEEE PES Innov. Smart Grid Technol. Eur. (ISGT-Europe)*, Oct. 2020, pp. 46–50.

[6] Z. Liu and L. Wang, "Defense strategy against load redistribution attacks on power systems considering insider threats," *IEEE Trans. Smart Grid*, vol. 12, no. 2, pp. 1529–1540, Mar. 2021.

[7] J. Su, C. Xie, P. Dehghanian, and S. Mehrani, "Optimal defense strategy against load redistribution attacks under attacker's resource uncertainty: A trilevel optimization approach," in *Proc. IEEE PES Grid Edge Technol. Conf. Expo. (Grid Edge)*, Apr. 2023, pp. 1–5.

[8] S. Bi and Y. J. Zhang, "Graphical methods for defense against false-data injection attacks on power system state estimation," *IEEE Trans. Smart Grid*, vol. 5, no. 3, pp. 1216–1227, May 2014.

[9] C. Pei, Y. Xiao, W. Liang, and X. Han, "PMU placement protection against coordinated false data injection attacks in smart grid," *IEEE Trans. Ind. Appl.*, vol. 56, no. 4, pp. 4381–4393, Jul. 2020.

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

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

[12] A. Sayghe, O. M. Anubi, and C. Konstantinou, "Adversarial examples on power systems state estimation," in *Proc. IEEE Power Energy Soc. Innov. Smart Grid Technol. Conf. (ISGT)*, Washington, DC, USA, Feb. 2020, pp. 1–5.

[13] B. Liu, Y. Liu, and H. Wu, "Tensor-completion enabled stealthy false data injection attacks on IoT-based smart grid," *IEEE Internet Things J.*, early access, Jun. 19, 2024, doi: 10.1109/JIOT.2024.3416839.

[14] B. Liu, H. Wu, Q. Yang, H. Zhang, Y. Liu, and Y. Zhang, "Matrix-completion-based false data injection attacks against machine learning detectors," *IEEE Trans. Smart Grid*, vol. 15, no. 2, pp. 2146–2163, Mar. 2024.

[15] 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.

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

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

[18] 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.

[19] J. Yu and Q. Li, "Optimal deployment in moving target defense against coordinated cyber–physical attacks via game theory," *Electronics*, vol. 12, no. 11, p. 2484, May 2023.

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

[21] 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.

[22] C. A. Ordóñez M, A. Gómez-Expósito, M. G. E. Vinasco, and J. M. Maza-Ortega, "Optimal coordinated operation of distributed static series compensators for wide-area network congestion relief," *J. Mod. Power Syst. Clean Energy*, vol. 10, no. 5, pp. 1374–1384, Sep. 2022.

[23] M. A. Rahman, E. Al-Shaer, and R. B. Bobba, "Moving target defense for hardening the security of the power system state estimation," in *Proc. 1st ACM Workshop Moving Target Defense*, Nov. 2014, pp. 59–68.

[24] 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.

[25] Z. Zhang, R. Deng, D. K. Y. Yau, P. Cheng, and J. Chen, "On hiddenness of moving target defense against false data injection attacks on power grid," *ACM Trans. Cyber-Phys. Syst.*, vol. 4, no. 3, pp. 1–29, Jul. 2020.

[26] 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, Aug. 2018.

[27] 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.
[28] G. L. Torres and V. H. Quintana, "An interior-point method for nonlinear optimal power flow using voltage rectangular coordinates," *IEEE Trans. Power Syst.*, vol. 13, no. 4, pp. 1211–1218, Nov. 1998.
[29] G. Torres and M. De Carvalho, "On efficient implementation of interior-point based optimal power flows in rectangular coordinates," in *Proc. IEEE PES Power Syst. Conf. Expo.*, Oct. 2006, pp. 1747–1752.
[30] R. D. Zimmerman, "AC power flows, generalized OPF costs and their derivatives using complex matrix notation," Power Syst. Eng. Res. Center (PSERC), New York, NY, USA, Tech. Rep., 2019.
[31] M. Liu, C. Zhao, Z. Zhang, R. Deng, P. Cheng, and J. Chen, "Converter-based moving target defense against deception attacks in DC microgrids," *IEEE Trans. Smart Grid*, vol. 13, no. 5, pp. 3984–3996, Sep. 2022.
[32] 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.
[33] B. Liu, Q. Yang, H. Zhang, and H. Wu, "An interior-point solver for AC optimal power flow considering variable impedance-based FACTS devices," *IEEE Access*, vol. 9, pp. 154460–154470, 2021.
[34] D. Avis, G. D. Rosenberg, R. Savani, and B. von Stengel, "Enumeration of Nash equilibria for two-player games," *Econ. Theory*, vol. 42, no. 1, pp. 9–37, Jan. 2010.
[35] 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.

BO LIU (Member, IEEE) received the Ph.D. degree from the Mike Wiegers Department of Electrical and Computer Engineering, Kansas State University (K-State), Manhattan, KS, USA, in 2021. From 2022 to 2024, he was a Research Assistant Professor with the Mike Wiegers Department of Electrical and Computer Engineering, K-State. He is currently an Assistant Professor with the School of Engineering and Applied Sciences, Washington State University Tri-Cities, Richland, WA, USA. His current research interests include cyber-physical security of power systems, smart grid technologies, machine learning, and state estimation in smart grids.

HONGYU WU (Senior Member, IEEE) received the B.S. degree in energy and power engineering and the Ph.D. degree in control science and engineering from Xi'an Jiaotong University, Xi'an, China. From 2011 to 2014, he was a Postdoctoral Researcher with the Robert W. Galvin Center for Electricity Innovation, Illinois Institute of Technology, Chicago, IL, USA. He is currently an Associate Professor and a Lucas-Rathbone Professor with the Mike Wiegers Department of Electrical and Computer Engineering, Kansas State University (K-State), Manhattan, KS, USA. Before joining K-State, he was a Research Engineer with the Power Systems Engineering Center, National Renewable Energy Laboratory, Golden, CO, USA. His research interests include cyber-physical security of smart grids, power system planning, operation and energy management, and power grid integration of renewable energy. He is a National Science Foundation (NSF) CAREER Awardee and an NSF EPSCoR Research Fellow. He serves in the IEEE-NERC Security Integration Project Committee and an Associate Editor for IEEE TRANSACTIONS ON SMART GRID and IEEE TRANSACTIONS ON INDUSTRIAL INFORMATICS.

HANG ZHANG (Member, IEEE) received the B.S., M.S., and Ph.D. degrees in electrical and computer engineering from Kansas State University, Manhattan, KS, USA, in 2017, 2018, and 2022, respectively. He is currently an Assistant Professor with the Department of Information Engineering, Henan University of Science and Technology, Henan, China. His research interests include cyber-physical security and resiliency of power systems, machine learning, and renewable energy.