Wang *et al.*
Protection and Control of Modern Power Systems (2023) 8:55
https://doi.org/10.1186/s41601-023-00332-8

Protection and Control of Modern Power Systems

ORIGINAL RESEARCH

Open Access

A tri-level programming-based frequency regulation market equilibrium under cyber attacks

Ying Wang[1], Chunyu Chen[2*], Sen Zhang[3], Yilong Liu[4], Chongxin Huang[5] and Yuxin Du[6]

Abstract

Owing to their flexibility and rapid response, grid-connected distributed energy resources (DERs) are wielding growing influence in frequency regulation markets (FRMs). Nevertheless, compared with conventional large-scale generators, small-scale DERs are usually weakly shielded by cyber security measures. This offers attackers the opportunity of disrupting the clearing and settlement of FRMs by manipulating the bid information of DERs. In this paper, the frequency regulation market equilibrium is studied considering the dynamic gaming between attackers and defenders, both of which need the knowledge of FRMs for their interventions. Specifically, a tri-level programming model characterizing the attacker–defender–operator (ADO) interdiction problem in FRMs is developed and then analyzed using a column and constraint generation algorithm, thereby achieving market equilibrium representing the defender's best response to the attacker. The defense strategy in the market equilibrium can attenuate the negative influence of cyber attacks upon the FRMs to the maximum extent. Finally, based on the operating rules of the California Independent System Operator, the FRM process considering the ADO interdiction is simulated and the numerical equilibrium results are presented.

Keywords Cyber attack, Frequency regulation market, Defender–attacker–operator interdiction, Tri-level programming

1 Introduction

Distributed energy resources (DERs) such as small-scale wind and solar power were once deemed exogenous disturbances because of their intermittent generation. Nevertheless, when integrating with microgrids or virtual power plants (VPPs), DERs gradually become frequency regulation service providers by collectively offering their respective capacities. Energy aggregation attenuates the fluctuation of individual DERs via a smoothing effect, thereby assisting DERs to provide controllable reserves similar to large-scale thermal and hydropower plants. Energy aggregation also enhances the bargaining power of DERs, transforming DERs from price takers to price makers. Although DERs-based frequency regulation has benefits such as reduced regulation costs and improved performance owing to the economy and quick response of DERs, the security risks of DERs' participation in frequency regulation markets (FRMs) cannot be ignored. The bottom-level DERs are susceptible to cyber attacks because of their comparatively weak security measures. Attack propagation may finally collapse the energy aggregators designated as vulnerable FRM participants. Attackers can manipulate the bid information

*Correspondence:
Chunyu Chen
chunyuchen@cumt.edu.cn
[1] Southeast University, Nanjing, China
[2] China University of Mining and Technology, Xuzhou, China
[3] State Grid Jiangsu Electric Power Company Ltd. Research Institute, Nanjing, China
[4] KTH Royal Institute of Technology, Stockholm, Sweden
[5] Nanjing University of Posts and Telecommunications, Nanjing, China
[6] Xuzhou University of Technology, Xuzhou, China

of vulnerable participants, thereby disrupting FRM processes for the attackers' benefit.

Since ancillary services play essential roles in reliable energy provision on a real-time basis, FRMs usually have more stringent requirements for FRM quality, e.g., all participating resources should demonstrate the ability to meet the control, telemetry, and minimum capacity requirements [1]. To reach the minimum threshold, spatially segregated DERs can integrate with VPPs to elevate collective capacity [2], and aggregators of VPPs then participate in FRMs on behalf of DERs. DERs in the same locality can form microgrids, and the corresponding aggregators will represent DERs to participate in FRMs [3]. As a result, researchers study the bidding behaviors of aggregators extensively. As for the battery energy storage (BES) aggregator, studies have proposed optimal bidding policies based on different market settings and BES characteristics. Although BES aggregators mainly target the provision of actual regulation by behaving as price takers [4], new BES aggregators begin to secure more operational profits by actively submitting bid prices [5]. Considering battery lifespan degradation, some studies also incorporate battery aging cost into the bidding strategies [6]. There is also research investigating real-time control policy to optimize the battery regulation response [7], whereas in [8], a BES optimal operation for both frequency regulation and energy arbitrage is considered and the optimization methodology for sizing and operating BES in distribution networks is developed. As well as pure BES, the bid of combined renewable energy and BES also attracts the attention of researchers in [9–13]. In [14], they investigate an aggregator controlling a fleet of electric vehicles (EVs) and energy storage (ES), and determine the optimal size of the aggregator's bids. By considering the uncertain energy and frequency regulation prices, the conditional value-at-risk method is employed to model the FRM risk, and a stochastic mixed integer linear programming model is established to obtain the optimal bids.

In contrast to aggregators, FRM operators aim to minimize the regulation cost on the condition that participants (including the aggregators) satisfy all market rules. Taking the American FRMs rules as an example, prior to FERC Order 755, cleared participants received no compensation for performing regulation. Fast-ramping aggregators tend to bear a more gratuitous burden of regulation than conventional units, thus discouraging quality resources from contributing to the regulation process. Therefore, Order 755 requires fair compensation for the frequency regulation service [15]. In recent years, various markets also propose different clearing strategies considering new FRM rules. In [16], researchers design a performance ratio that quantifies the relative effectiveness of generators and flexible demand resources in frequency regulation. Clearing processes considering response rates are studied. Reference [17] proposes an integrated dynamic market mechanism that combines the real-time and frequency regulation markets. Market players including renewable generators and flexible consumers can negotiate electricity prices using the most recent information on the available wind power and quality of grid frequency.

Instead of exploring new bidding or clearing strategies, this paper investigates how possible cyber attacks affect FRM processes including the clearing and the settlement results. It is known that the degree of security and operational reliability is usually positively correlated with the size of resources. The smaller the size of resources is, the lower the protection level is, and vice versa. DERs are usually of small capacity and equipped with comparatively weaker protection measures, and hence they are more likely to suffer cyber attacks. It is difficult for attackers to compromise strongly protected large-scale generators like thermal or hydro units. Attackers may infiltrate DERs via various vulnerability points like unauthorized access to DER controllers and penetration through the facility network [18]. Through attack propagation in the aggregator network, the upper-level aggregators may also suffer cyber security threats. Attackers can manipulate the bid information of these vulnerable aggregators to disrupt the market processes, i.e., the clearing and settlement.

Attackers can also exploit financial arbitrage opportunities through cyber attacks. Reference [19] analyzes how attackers can manipulate locational marginal prices (LMPs) in the electricity market by injecting malicious data into critical parameters. Unlike many attack models that neglect the characteristics of LMPs, reference [20] develops a new cyber attack strategy that not only bypasses bad data detection during state estimation but also conceals the compromised LMPs as normal LMPs to evade detection by market operators. Besides electricity markets, researchers have considered cyber attacks against various applications. Reference [21] proposes a load redistribution attack model using DC state estimation in which attackers have limited access to network topology and information. In [22], a new attack model using AC state estimation is studied. This takes into account both the cost of the attacker and the attack influence. As for the detection, reference [23] proposes a novel data-driven FDIA framework and designs an unsupervised detection scheme to detect the stealthy FDIA, whereas [24] constructs a novel method that employs graph theory principles for identifying false data injection attacks (FDIAs) on AC state estimation.

An attacker usually has no physical asset (the generating units), and hence, he or she chooses to collude with proxy participants and action so that the proxy participants can increase their compensation in the settlement. In this situation, the proxy participants are the stakeholders on behalf of the attacker. This profit-oriented attack strategy will fundamentally change the settlement results, diverging the compensation from the expected value for other non-proxy participants. To reverse this undesired compensation deviation and maintain the compensation at a reasonable level, the defender could alter specific market parameters, e.g., the bidding data of the defensive unit. In summary, both the attacker and defender exert influence on the FRM (clearing) model to reach their specific attack and defense objectives. In return, the attacker and the defender form an interdependency relationship by exchanging information during the clearing process. In this paper, a tri-level programming model is used to characterize the aforementioned interaction among the defender, the attacker, and the FRM. The upper-level attacker's model formulates the optimal compensation for the stakeholders. The middle-level defender's model formulates the minimal compensation deviation, and the lower-level market model formulates the minimal regulation cost in the clearing process. The attacker and the defender form a noncooperative game relationship in the tri-level hierarchy, and the independent system operator desires to obtain a market equilibrium where each player selects the best response to the opponent's strategies. By linearizing the three-level model and using the column and constraint generation (C&CG) algorithm, the FRM equilibrium is assessed under the attacker-and-defender game.

The main contributions of this paper are:

- Considering the vulnerabilities of DER aggregators that participate in FRMs along with conventional units, a new cyber attack scenario that targets the FRM is researched and the FRM equilibrium in attacker-and-defender game scenarios is studied. The proposed FRM equilibrium evaluation mechanism can offer better insights and quantitative information on how the FRM clearing results evolve during advanced attacker-and-defender interplay. Also, the proposed strategy has great applicability in the equilibrium evaluation of other market-oriented cyber attacks.
- By formulating a novel attacker-and-defender Stackelberg game, where both players interact and impact each other's decisions in the FRM, it analyzes the effect of having a profit-driven attacker and a balance-focused defender simultaneously operating in the FRM.
- By linearizing the attacker-and-defender Stackelberg game model and reformulating it into an equivalent bi-level optimization model, the C&CG algorithm is used to solve the bottom-level sub-problem and top-level master problem in an iterative manner, thus achieving market equilibria more efficiently.

The remainder of the paper is organized as follows: Sect. 2 gives the basis of profit-oriented cyber attacks in FRMs, while Sect. 3 presents the mechanism of FRM-oriented cyber attacks via vulnerable aggregators. Section 4 describes the strategy of calculating the FRM equilibrium in a non-cooperative game between the defender and the attacker. Section 5 gives the case studies and Sect. 6 draws the conclusions.

2 Profit-oriented cyber attack in frequency regulation market

This section presents a theoretical background of profit-oriented cyber attacks in FRMs. Specifically, it explains in detail the feasibility of compromising the energy aggregator and illustrates the complete attack process of obtaining lucrative compensation for the attacker.

2.1 Cyber security threats of distributed energy resources and energy aggregators

The large-scale integration of DERs transforms the utility-centric structure into a multi-aggregator network. Inspired by the architecture in [18], a DER architecture is categorized into four levels as shown in Fig. 1.

Level 1 represents a collection of individual DER devices and the corresponding controllers, while level 2 mainly contains utility communication systems exchanging

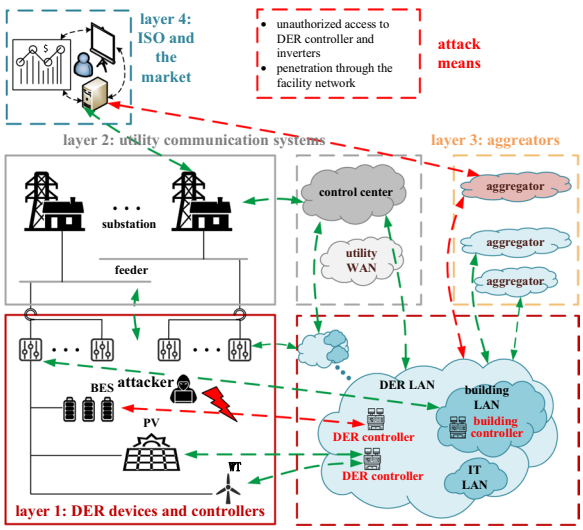

Fig. 1 DER architecture considering cyber attacks

control commands and data with DER devices. Level 3 is the collection of aggregators integrated with multiple DERs, where aggregators represent DERs to participate in the FRM and other markets. Level 4 is the ISO supervising markets and operation of power systems. Such DER architecture is susceptible to cyber attacks. For instance, attackers may infiltrate the DER network in level 1 by exploiting protocol bugs. The attack can then propagate in the architecture if there is insufficient deployment of firewalls, security gateways, and other measures. The attacker eventually collapses the aggregator in level 3, which is entirely subject to the whim of the attacker when bidding in the FRM in level 4.

2.2 Profit-making attack measures in the frequency regulation market

For brevity, those aggregators that suffer the cyber security threats in Fig. 1 are designated as vulnerable aggregators. When corrupted by attackers, vulnerable aggregators will submit compromised offer prices, thus disrupting the clearing and settlement results for the benefit of stakeholders, who represent attackers, in securing payments for providing frequency regulation services. A simple merit order model is used to show that attackers can enhance payments by elevating the offer prices of vulnerable units. Figure 2 shows the clearing process of a simplified FRM.

As seen, the market operator ranks four market participants based on ascending offer prices, and the clearing price is equal to the offer price of the marginal participant, i.e., the most expensive participant that is required to meet the inelastic reserve demand. When the offer price of the vulnerable aggregator (participant 1) is manipulated from to $O^{c}_{1,co}$, a clearing price difference Δp^{c}_{cl} between the intact and compromised clearing prices occurs. The positive Δp^{c}_{cl} will increase the compensation for the stakeholder (participant 2) by $\Delta p^{c}_{cl} r^{c}_{2}$. Obviously, price manipulation of the vulnerable aggregator will disrupt the original market equilibrium by changing the order of clearing and the expected compensation. Specifically, the expected compensation is studied in this paper. This refers to the expected regulation capacity payment the cleared participant can obtain. Although the attacker targets compensation increase of stakeholders, it also causes deviations in the expected compensation for other participants. In response, defenders try to restore equilibrium by reducing compensation deviations. In this paper, it assumes that the defender uses attack vs defense drills to evaluate the market equilibrium in the most severely adversarial situation where the attacker and defender form a non-cooperative game relationship. It occurs when the attacker turns to an insider lurking in the DER architecture with complete information. The attacker desires to maximize the stakeholder's compensation (by manipulating vulnerable aggregators), while the defender hopes to minimize the expected compensation deviation (by dispatching defensive participants). Since both implementations are dependent upon a market clearing and interplay reciprocally, the defender should reassess the market equilibrium where both players achieve the best responses to their opponent.

3 Frequency regulation market equilibrium considering cyber attacks against vulnerable aggregators

From Sect. 2, we know the three basic truths about FRMs with aggregators. First, the attacker can infiltrate the DER architecture and compromise vulnerable aggregators. Second, the attacker can manipulate compromised vulnerable aggregators for its own benefit while causing expected compensation deviations. Third, the attacker and defender form a non-cooperative game by interacting through the common market clearing process. The attacker moves before the defender, while the defender moves before the operator, leading to an ADO interdiction problem. Figure 3 gives the general framework of the non-cooperative interplay between the attacker and the defender in the FRM.

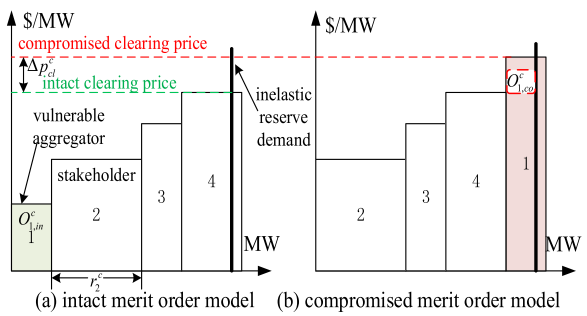

Fig. 2 Clearing process using a merit order market model

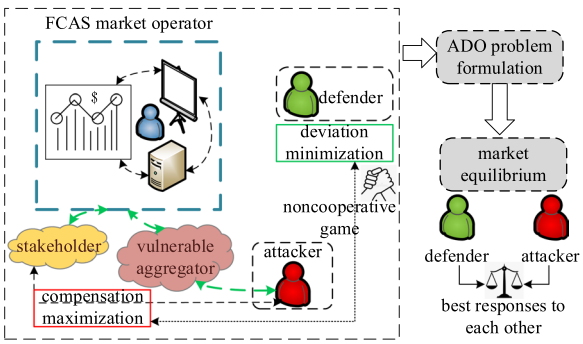

Fig. 3 Non-cooperative interplay between the attacker and the defender in the FRM

In this section, the following two issues are further elucidated:

> Question 1: How to formulate the ADO interdiction problem in the FRM?
> Question 2: How to establish market equilibrium considering the non-cooperative interplay between the defender and the attacker?

3.1 Tri-level programming-based attacker–defender–operator interdiction

Here, a tri-level programming model is used to formulate the attacker–defender–operator interdiction problem. As profit-oriented entities, attackers aim to maximize the capacity compensation of the stakeholders who represent attackers to trade in FRMs. Instead of minimizing attackers' compensation, the primary goal of defenders is to minimize the attack influence on the originally desired market equilibria. The upper-level model characterizes the attacker's objective of compensation maximization for the stakeholder, the middle-level model characterizes the defender's objective of minimization of expected compensation deviations, and the lower-level model describes the market clearing process.

As the game leader, the attacker moves first by manipulating the offer prices of vulnerable aggregators. Then the defender evaluates the defense's goal under the given attack strategies. Finally, under the given attack and defensive strategies, the operator model completes the clearing process which passes the clearing results to the defender and the attacker to evaluate their respective objectives. Figure 4 demonstrates the above tri-level game hierarchy. In the following, the tri-level model is expanded from the lower to the upper levels.

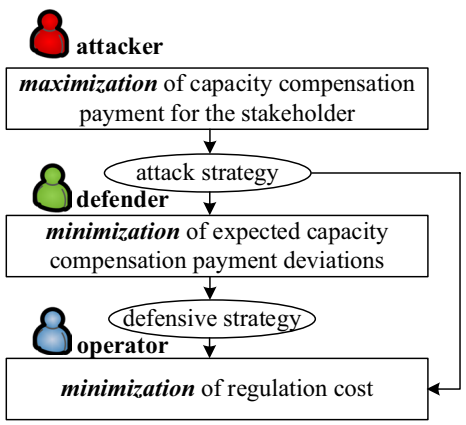

Fig. 4 Tri-level game hierarchy of the non-cooperative interplay among the attacker, defender, and operator

3.2 Attacker model: increase of capacity compensation payment for the stakeholder

As mentioned in Sect. 2, the attacker manipulates the offer prices of vulnerable aggregators to increase the capacity compensation payment for the stakeholder. Specifically, the payment maximization model is used to characterize the attack problem, as:

$$\max_{O_j^{\mathrm{C}},O_j^{\mathrm{M}},j\in\mathcal{N}_{\mathrm{v}}} \sum\nolimits_{j\in\mathcal{N}_{\mathrm{a}}} p_{\mathrm{cl}}^{\mathrm{C}} r_j^{\mathrm{C}} \tag{1}$$

where $\mathcal{N}_v$ represents the set of vulnerable aggregators. The offer prices of vulnerable aggregators should be within certain limits, i.e.:

$$O_{j,\min}^{\mathrm{C}} \le O_j^{\mathrm{C}} \le O_{j,\max}^{\mathrm{C}} \quad \forall j \in \mathcal{N}_{\mathrm{v}} \tag{2}$$

$$O_{j,\min}^{\mathrm{M}} \le O_j^{\mathrm{M}} \le O_{j,\max}^{\mathrm{M}} \quad \forall j \in \mathcal{N}_{\mathrm{v}} \tag{3}$$

(1) Defender model: reduction of expected capacity compensation payment deviations: As mentioned in Sect. 2, the manipulation of offer prices of vulnerable aggregators will cause expected capacity compensation payment deviations. These deviations are detrimental to participants' interests. The two-part payment mechanism offers participants a market-based capacity payment and a performance payment. In this paper, it supposes that the attacker and the defender only game over the capacity payment, and the defender wants to minimize the expected capacity payment deviations:

$$\min_{O_j^{\mathrm{C}},O_j^{\mathrm{M}},j\in\mathcal{N}_{\mathrm{d}}} \sum\nolimits_{j\in\mathcal{N}_{\mathrm{n}}} (p_{\mathrm{cl}}^{\mathrm{C}} r_j^{\mathrm{C}} - p_{\mathrm{cl},0}^{\mathrm{C}} r_{j,0}^{\mathrm{C}})^2 \tag{4}$$

where $j \in \mathcal{N}_{\mathrm{d}}$ represents the set of defensive participants, and $j \in \mathcal{N}_{\mathrm{n}}$ represents the set of units other than defensive and vulnerable units. $p_{\mathrm{cl},0}^{\mathrm{C}} r_{j,0}^{\mathrm{C}}$ represents the expected capacity compensation payment for participant j. It assumes that the FRM is less competitive and reserve requirements are inflexible. In this situation, participants tend to submit the same bid. Hence, the defender can use the clearing results from the prior interval to obtain $p_{\mathrm{cl},0}^{\mathrm{C}} r_{j,0}^{\mathrm{C}}$. The defender uses offer prices of defensive participants to rectify the expected capacity compensation payment, and these offer prices should be within certain limits, as:

$$O_{j,\min}^{\mathrm{C}} \le O_j^{\mathrm{C}} \le O_{j,\max}^{\mathrm{C}} \quad \forall j \in \mathcal{N}_{\mathrm{d}} \tag{5}$$

$$O_{j,\min}^{\mathrm{M}} \le O_j^{\mathrm{M}} \le O_{j,\max}^{\mathrm{M}} \quad \forall j \in \mathcal{N}_{\mathrm{d}} \tag{6}$$

where $O_{j,\min}^{\mathrm{C}}$ and $O_{j,\max}^{\mathrm{C}}$ represent the minimum and maximum regulation capacity offer prices, respectively. $O_{j,\min}^{\mathrm{M}}$

and $O^{\mathrm{M}}_{j,\max}$ represent the minimum and maximum regulation mileage offer prices, respectively.

(2) Operator model: performance-based frequency control ancillary service market clearing formulation: FERC Order No. 755 requires ISOs or RTOs to offer FRM participants a two-part payment including a market-based capacity payment and market-based payment for performance [15]. Correspondingly, participants submit both the regulation capacity offer price and regulation mileage offer price. The resulting regulation cost minimization-oriented clearing model is thus written by:

$$\min_{r_j^{\mathrm{C}}, r_j^{\mathrm{M}}} \sum\nolimits_{j\in\mathcal{N}_{\mathrm{p}}} (O_j^{\mathrm{C}} r_j^{\mathrm{C}} + O_j^{\mathrm{M}} r_j^{\mathrm{M}}) \tag{7}$$

where the subscript j represents the index for market participants. $\mathcal{N}_{\mathrm{p}}$ is the set of participants, while O_j^{C} and O_j^{M} represent the regulation capacity offer price and the regulation mileage offer price, respectively. r_j^{C} and r_j^{M} represent the cleared regulation capacity and regulation mileage, respectively.

The constraints of the clearing model are described in (8)–(13) below.

$$\sum\nolimits_{j\in\mathcal{N}_{\mathrm{p}}} r_j^{\mathrm{C}} = R^{\mathrm{C}} \tag{8}$$

where R^{C} represents the regulation capacity requirement.

$$\sum\nolimits_{j\in\mathcal{N}_{\mathrm{p}}} r_j^{\mathrm{C}} = \min(m_{\mathrm{s}} R^{\mathrm{C}}, R_0^{\mathrm{M}}, \sum\nolimits_{j\in\mathcal{N}_{\mathrm{p}}} m_j U_j) \tag{9}$$

where m_{s} and m_j represent the system-level and the participant-level mileage multiplier, respectively. R_0^{M} represents the regulation mileage requirement from the prior regulation interval, and U_j is the bid (maximum regulation capacity) of participant j. Equation (9) avoids mileage scarcity and situations where regulation mileage requirements may drive increased regulation capacity procurement above the regulation capacity requirement.

$$r_j^{\mathrm{C}} \geq 0 \quad \forall j \in \mathcal{N}_{\mathrm{p}} \tag{10}$$

$$r_j^{\mathrm{C}} \leq U_j \quad \forall j \in \mathcal{N}_{\mathrm{p}} \tag{11}$$

where U_j represents the bid for regulation capacity. Equations (10) and (11) present the operational limits.

According to FERC Order No. 755, cleared regulation mileage r_j^{M} of participant j should be no less than cleared regulation capacity r_j^{C}, but no more than the product of its mileage multiplier m_j and the cleared regulation capacity. It follows that:

$$r_j^{\mathrm{M}} \geq r_j^{\mathrm{C}} \quad \forall j \in \mathcal{N}_{\mathrm{p}} \tag{12}$$

$$r_j^{\mathrm{M}} \leq m_j r_j^{\mathrm{C}} \quad \forall j \in \mathcal{N}_{\mathrm{p}} \tag{13}$$

Based on (7)–(13), the tri-level ADO interdiction model can be rewritten as:

$$\begin{aligned} &attacker \begin{cases} obj.(1) \\ s.t.(2)-(3) \end{cases} \\ &defender \begin{cases} obj.(4) \\ s.t.(5)-(6) \end{cases} \\ &operator \begin{cases} obj.(7) \\ s.t.(8)-(13) \end{cases} \end{aligned} \tag{14}$$

4 Market equilibrium in a non-cooperative game between the defender and the attacker

The proposed tri-level ADO model is used to assess the market equilibrium where both the defender and the attacker achieve the optimal condition upon the strategy of their opponent. The study of market equilibrium under cyber attacks is essential for analyzing how the attacker and the defender may affect the market. This helps system operators make informed decisions about market intervention, trading correction, and even termination. Market equilibrium under an attack-and-defense game can give system operators insights into how advanced attacker and defender interplay affects the market operation, thus guiding the post-game decision-making.

In this paper, Bender's primal decomposition framework is adopted to analyze the tri-level ADO model. The first step is to merge the middle-level and lower-level problems into a single-level problem using either the strong duality theorem [25–27] or KKT optimality conditions [28]. Previous research mainly assumes that the defender takes proactive measures. In this case, the middle-level and lower-level problems constitute a max–min bilevel sub-problem. Instead, it assumes that the attacker moves before the defender in the Stackelberg game. This is because in many real-world situations, the attacker has the advantage of surprise and can launch an attack before the defender has a chance to react. From the third party's perspective, we can reformulate the tri-level model as a two-stage optimization problem:

$$\max_{\boldsymbol{y}\in\boldsymbol{S}_y} \sum\nolimits_{j\in\mathcal{N}_{\mathrm{a}}} p_{\mathrm{cl}}^{\mathrm{C}} r_j^{\mathrm{C}} + \min_{\boldsymbol{x}\in\boldsymbol{S}_x} \sum\nolimits_{j\in\mathcal{N}_{\mathrm{n}}} (p_{\mathrm{cl}}^{\mathrm{C}} r_j^{\mathrm{C}} - p_{\mathrm{cl},0}^{\mathrm{C}} r_{j,0}^{\mathrm{C}})^2 \tag{15}$$

where $\boldsymbol{y} \in \boldsymbol{S}_y$ represents the feasible domain of the upper-level variables, i.e., $O_j^{\mathrm{C}}, O_j^{\mathrm{M}}, \forall j \in \mathcal{N}_{\mathrm{v}}$. $\boldsymbol{x} \in \boldsymbol{S}_x$ represents the feasible domain of the middle-level and lower-level variables, i.e., (5)–(6), and (7)–(13). The first-stage problem corresponds to the upper-level attacker problem, while the second-stage problem is to model the

decision-making of the FRM operator after the attack and defense strategies are revealed.

It is noted that the second-stage problem is a bilevel problem. Hence single-level reduction is performed using the Karush–Kuhn–Tucker (KKT) conditions. The Lagrangian function of the lower-level optimization model is given as:

$$\begin{aligned} L(\boldsymbol{r}, p_{\mathrm{cl}}^{\mathrm{M}}, p_{\mathrm{cl}}^{\mathrm{C}}, \boldsymbol{\lambda}) = & \sum_j (O_j^{\mathrm{C}} r_j^{\mathrm{C}} + O_j^{\mathrm{M}} r_j^{\mathrm{M}}) \\ & + p_{\mathrm{cl}}^{\mathrm{M}} (R^{\mathrm{M}} - \sum_j r_j^{\mathrm{M}}) + p_{\mathrm{cl}}^{\mathrm{C}} (R^{\mathrm{C}} - \sum_j r_j^{\mathrm{C}}) \\ & + \sum_j \lambda_j^{\mathrm{C\,min}} (-r_j^{\mathrm{C}}) + \sum_j \lambda_j^{\mathrm{C\,max}} (r_j^{\mathrm{C}} - U_j) \\ & + \sum_j \lambda_j^{\mathrm{M\,min}} (r_j^{\mathrm{C}} - r_j^{\mathrm{M}}) + \sum_j \lambda_j^{\mathrm{M\,max}} (r_j^{\mathrm{M}} - m_j r_j^{\mathrm{C}}) \end{aligned} \tag{16}$$

where $\boldsymbol{r}$ is the set of cleared capacity and mileage, and $\boldsymbol{\lambda}$ is the set of dual variables. $\lambda_j^{\mathrm{C\,min}}$ and $\lambda_j^{\mathrm{C\,max}}$ are the dual variables corresponding to (10) and (11), respectively, while $\lambda_j^{\mathrm{M\,min}}$ and $\lambda_j^{\mathrm{M\,max}}$ are the dual variables corresponding to (12) and (13), respectively. Then, KKT optimality conditions are (8), (9) and:

$$\frac{\partial L}{\partial r_j^{\mathrm{C}}} = O_j^{\mathrm{C}} - p_{\mathrm{cl}}^{\mathrm{C}} - \lambda_j^{\mathrm{C\,min}} + \lambda_j^{\mathrm{C\,max}} + \lambda_j^{\mathrm{M\,min}} - m_j \lambda_j^{\mathrm{M\,max}} = 0 \tag{17}$$

$$\frac{\partial L}{\partial r_j^{\mathrm{M}}} = O_j^{\mathrm{M}} - p_{\mathrm{cl}}^{\mathrm{M}} - \lambda_j^{\mathrm{M\,min}} + \lambda_j^{\mathrm{M\,max}} = 0 \tag{18}$$

$$0 \le r_j^{\mathrm{C}} \perp \lambda_j^{\mathrm{C\,min}} \ge 0 \tag{19}$$

$$0 \le (U_j - r_j^{\mathrm{C}}) \perp \lambda_j^{\mathrm{C\,max}} \ge 0 \tag{20}$$

$$0 \le (r_j^{\mathrm{M}} - r_j^{\mathrm{C}}) \perp \lambda_j^{\mathrm{M\,min}} \ge 0 \tag{21}$$

$$0 \le (m_j r_j^{\mathrm{C}} - r_j^{\mathrm{M}}) \perp \lambda_j^{\mathrm{M\,max}} \ge 0 \tag{22}$$

The sub-problem model is expressed as:

$$\min_{O_j^{\mathrm{C}}, O_j^{\mathrm{M}}, j \in \mathcal{N}_{\mathrm{d}}, \Xi} \sum_{j \in \mathcal{N}_{\mathrm{n}}} (p_{\mathrm{cl}}^{\mathrm{C}} r_j^{\mathrm{C}} - p_{\mathrm{cl},0}^{\mathrm{C}} r_{j,0}^{\mathrm{C}})^2 \tag{23}$$

where $\Xi = \{\boldsymbol{r}, p_{\mathrm{cl}}^{\mathrm{C}}, p_{\mathrm{cl}}^{\mathrm{M}}, \boldsymbol{\lambda}\}$. The constraints are (5), (6), and (17)–(20). It is noted that both the objective function and (19)–(22) have nonlinearity. As for $p_{cl}^{\mathrm{C}} r_j^{\mathrm{C}}$ in the objective function, the McCormick Envelope relaxation is used to transform it into a linear term, making the new objective a quadratic one. The complementary slackness in (17)–(32) is linearized using big M methods. Finally, the sub-problem is transformed into a mixed integer quadratic programming problem, as:

$$\begin{aligned} & \min \ \boldsymbol{x}^T \boldsymbol{Q} \boldsymbol{x} \\ & s.t. \quad \boldsymbol{x} \in \boldsymbol{F} \\ & x_i \in \{0, 1\}, \quad \forall i \in \mathcal{N}_{\mathrm{b}} \end{aligned} \tag{24}$$

Appendix gives the details of (24). The master problem is formulated as a mixed integer quadratically constrained programming problem, as:

$$\begin{aligned} & \min \ c^T y + \eta \\ & \quad s.t. \quad \eta \le \boldsymbol{x}^T \boldsymbol{Q} \boldsymbol{x} \\ & \quad \boldsymbol{y} \in \boldsymbol{S}_y, \quad \boldsymbol{x} \in \boldsymbol{F} \end{aligned} \tag{25}$$

Appendix also gives the details of (25). Considering the integer variables in the sub-problem, Bender's dual-cutting plane algorithm cannot be used to gradually construct the value function of the master problem using dual solutions of the sub-problem. Therefore, the column-and-constraint generation (C&CG) method is used to obtain the market equilibrium based on (24) and (25). This dynamically generates constraints with sub-problem decision variables in the primal space [29]. The complete C&CG-based market equilibrium computational procedure is as follows:

Step 1: Set the lower bound $LB = -\infty$ and upper bound $UB = -\infty$. Set the initial attack strategies $O_j^{\mathrm{C}} = O_{j,0}^{\mathrm{C}}, O_j^{\mathrm{M}} = O_{j,0}^{\mathrm{M}}$, and $\forall j \in \mathcal{N}_{\mathrm{v}}$, and then send them to the sub-problem.

Step 2: Solve the sub-problem and obtain the value of the objective function. Update the upper bound as $UB = \min(UB, \sum_{j \in N_{\mathrm{n}}} (\omega_j^{\mathrm{C}} - p_{\mathrm{cl},0}^{\mathrm{C}} r_{j,0}^{\mathrm{C}})^2)$. Obtain the defensive strategies $O_j^{\mathrm{C}}, O_j^{\mathrm{M}}$, and $\forall j \in \mathcal{N}_{\mathrm{d}}$, and send them to the master problem.

Step 3: Solve the master problem and obtain the value of the objective function. Update the lower bound as $LB = \max(LB, \sum_{j \in N_{\mathrm{a}}} \omega_j^{\mathrm{C}} + \eta)$. If $(UB - LB)/LB \le CT$, stop; otherwise, obtain the attack strategies $O_j^{\mathrm{C}}, O_j^{\mathrm{M}}$, and $\forall j \in \mathcal{N}_{\mathrm{v}}$, send them to the sub-problem, and then go to Step 2.

5 Simulations and numerical analyses

In this section, the market equilibrium of an FRM guided by CAISO rules is evaluated. The FRM contains 15 participants with No. 12 the defensive participant and No. 13–15 the vulnerable participants. Table 1 gives the corresponding FRM information. The system-level mileage multiplier is 3.26, and the regulation capacity requirement R_{C} is 1000 MW.

Figure 5 shows the intact FRM clearing results without considering the defender–attacker interaction. As can be seen, participants No. 6, 10, and 12 have empty bars,

Table 1 Basic information of an FRM containing 15 participants

No	**1**	**2**	**3**	**4**
Regulation capacity offer price O_j^C($/MW)	29	20.6	25.8	15.7
Regulation capacity offer price O_j^M($/MW)	31.3	30.0	21.0	42.1
Regulation capacity U_j (MW)	125	140	97	105
Maximal mileage U_j^r (MW)	353.8	414.4	360.8	314
No	**5**	**6**	**7**	**8**
Regulation capacity offer price O_j^C($/MW)	34	16	37.5	39.8
Regulation capacity offer price O_j^M($/MW)	27.9	44.4	29.3	26.8
Regulation capacity U_j (MW)	100	128	80	78
Maximal mileage U_j^r (MW)	354	458.2	350	259
No	**9**	**10**	**11**	**12**
Regulation capacity offer price O_j^C($/MW)	16	34	33.3	28.3
Regulation capacity offer price O_j^M($/MW)	26.5	41	29	43.3
Regulation capacity U_j (MW)	100	138	30	60
Maximal mileage U_j^r (MW)	277	320.2	76.2	262.8
No	**13**	**14**	**15**	
Regulation capacity offer price O_j^C($/MW)	32.9	25.1	39.8	
Regulation capacity offer price O_j^M($/MW)	35.5	45	35.5	
Regulation capacity U_j (MW)	160	150	50	
Maximal mileage U_j^r (MW)	476.8	492	199.5	

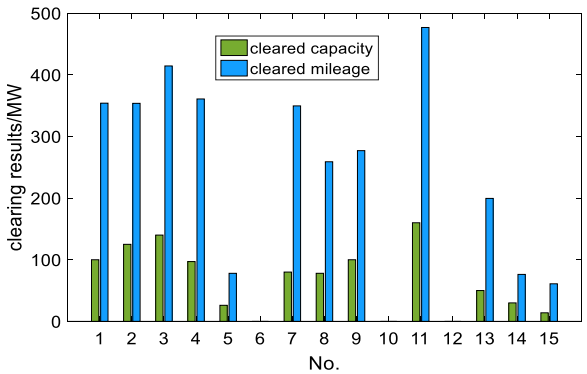

Fig. 5 FRM clearing results without attack and defense

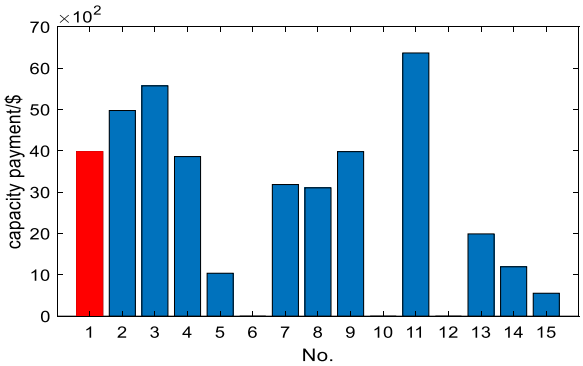

Fig. 6 Capacity payments without attack and defense

meaning that they fail to secure the bid. This is because they submit either high regulation capacity offer prices or regulation mileage offer prices, so none of them secures the bid after the FRM is cleared. Figure 6 gives the results of capacity payments for all cleared participants. The stakeholder on behalf of the attacker can get $3980. When only the presence of the attacker is considered, the attacker and the FRM form a bilevel game, and the clearing results are shown in Fig. 7. As can be seen, in order to increase the capacity payment for the stakeholder by increasing the cleared price, the attacker manipulates the offer price of vulnerable units (No. 13, 14, and 15) to high values. Hence, vulnerable participants No. 13 and 14 fail to secure the bids after attack. In this situation, the marginal units No. 5 and 15 compensate for the imbalance of capacity and mileage because of the phase-out of No. 13 and 14, while the cleared capacity and mileage of the remaining units remain the same.

Figure 8 gives the results of capacity payments for all cleared participants. As can be seen, with the presence of the attacker and the defender, the stakeholder on behalf of the attack can get $10,932, which is far larger than the

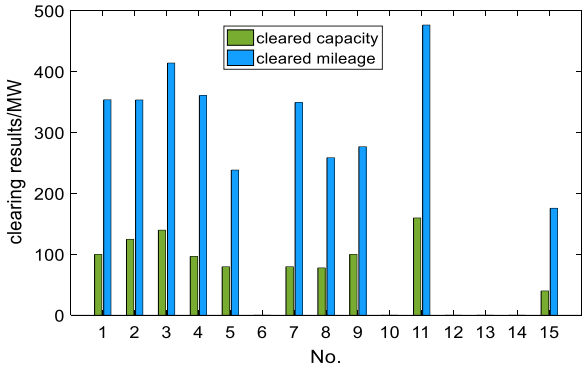

Fig. 7 FRM clearing results under attack

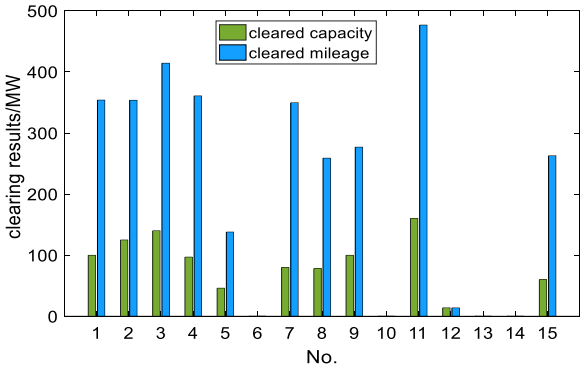

Fig. 10 FRM clearing results under the attack-and-defense situation

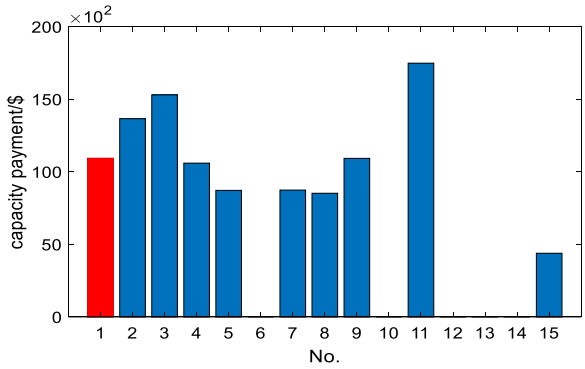

Fig. 8 Capacity payments under attack

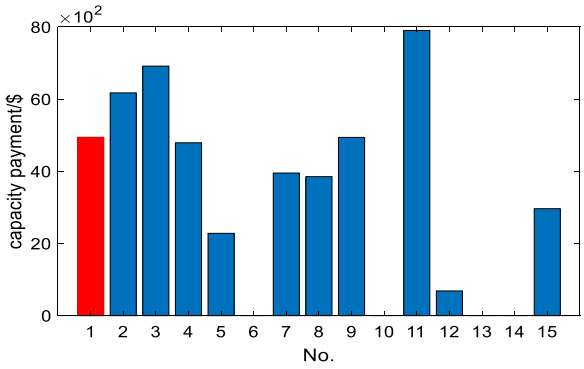

Fig. 11 Capacity payments under the attack-and-defense situation

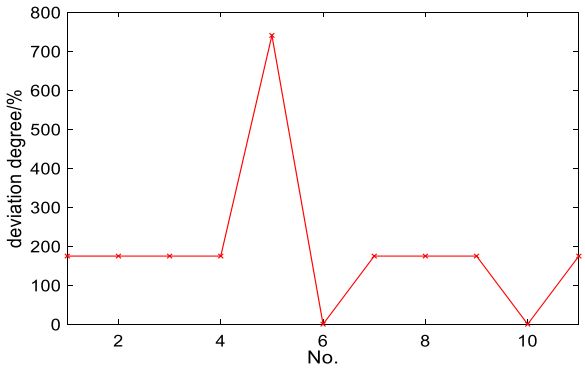

Fig. 9 Capacity payment deviations under attack

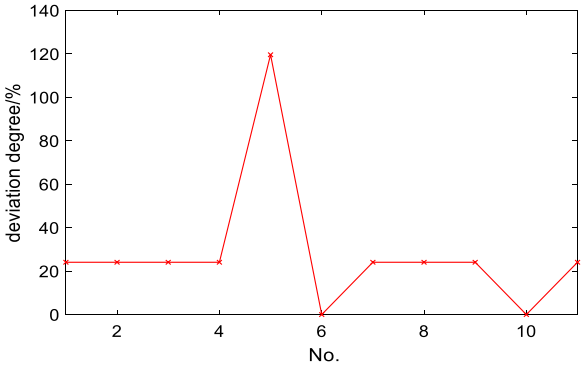

Fig. 12 Capacity payment deviations under the attack-and-defense situation

previous \$3980, meaning that the attacker can greatly increase its compensation in the bi-level game. Figure 9 shows that the attacker would disrupt the market equilibrium. Participants No. 1–4, 7–8, and 11 experience 174.7% of payment increase, and participant No. 5 experiences 740.7% of increase. The elevation of offer prices of the vulnerable No. 13–15 not only increase the compensation for the stakeholder but also other units, causing financial losses to the operator. Since participants 6 and 10 do not win any bids either in the non-attack or the attack situations, there is no compensation for them. Hence, participants 6 and 10 have no payment in both situations.

To restore market equilibrium, the defender uses defensive unit No. 12 to change its offer price and correct the market clearing process. As can be seen, the clearing results for the participants that are neither vulnerable

aggregators nor defensive units in Fig. 10 are approximately the same as those in the intact FRM shown in Fig. 5. Figure 11 shows that the capacity payment for the stakeholder decreases from the original $10,932 to $4938, which means the defense can negatively affect the gain the stakeholder makes on behalf of the attacker. Figure 12 shows the capacity payment deviations for the participants. As can be seen, participants No. 1–4, 7–8, and 11 experience 24.1% of deviation, which is far smaller than the 174.7% in Fig. 9. Participant No. 5 experiences 119.6% of deviation, which again is far smaller than the 740.7% in Fig. 9. It means that the defender can rebalance the FRM equilibrium in the attack-and-defense game.

6 Conclusions

In this paper, a novel profit-oriented cyber attack in the FRM is studied and the non-cooperative game relationship between the attacker and the defender is analyzed. By formulating a tri-level game considering the respective goals of the attacker and the defender, the FRM equilibrium in the attack-and-defense game situation is assessed. The case studies show that the participation of the defender can significantly rebalance the FRM equilibrium.

Appendix

Mixed integer quadratic programming model-based sub-problem

The objective function is rewritten as:

$$\min_{O_j^{\mathrm{C}},O_j^{\mathrm{M}},j\in\mathcal{N}_{\mathrm{d}},\Phi} \sum\nolimits_{j\in\mathcal{N}_{\mathrm{n}}} (\omega_j^{\mathrm{C}} - p_{\mathrm{cl},0}^{\mathrm{C}} r_{j,0}^{\mathrm{C}})^2 \tag{26}$$

$$\omega_j^{\mathrm{C}} \geq p_{\mathrm{cl,min}}^{\mathrm{C}} r_j^{\mathrm{C}} + p_{\mathrm{cl}}^{\mathrm{C}} r_{j,\mathrm{min}}^{\mathrm{C}} - p_{\mathrm{cl,min}}^{\mathrm{C}} r_{j,\mathrm{min}}^{\mathrm{C}} \quad \forall j \in \mathcal{N}_{\mathrm{d}} \tag{27}$$

$$\omega_j^{\mathrm{C}} \geq p_{\mathrm{cl,max}}^{\mathrm{C}} r_j^{\mathrm{C}} + p_{\mathrm{cl}}^{\mathrm{C}} r_{j,\mathrm{max}}^{\mathrm{C}} - p_{\mathrm{cl,max}}^{\mathrm{C}} r_{j,\mathrm{max}}^{\mathrm{C}} \quad \forall j \in \mathcal{N}_{\mathrm{d}} \tag{28}$$

$$\omega_j^{\mathrm{C}} \leq p_{\mathrm{cl,max}}^{\mathrm{C}} r_j^{\mathrm{C}} + p_{\mathrm{cl}}^{\mathrm{C}} r_{j,\mathrm{min}}^{\mathrm{C}} - p_{\mathrm{cl,max}}^{\mathrm{C}} r_{j,\mathrm{min}}^{\mathrm{C}} \quad \forall j \in \mathcal{N}_{\mathrm{d}} \tag{29}$$

$$\omega_j^{\mathrm{C}} \leq p_{\mathrm{cl}}^{\mathrm{C}} r_{j,\mathrm{max}}^{\mathrm{C}} + p_{\mathrm{cl,min}}^{\mathrm{C}} r_j^{\mathrm{C}} - p_{\mathrm{cl,min}}^{\mathrm{C}} r_{j,\mathrm{max}}^{\mathrm{C}} \quad \forall j \in \mathcal{N}_{\mathrm{d}} \tag{30}$$

where $p_{\mathrm{cl,min}}^{\mathrm{C}}$ and $p_{\mathrm{cl,max}}^{\mathrm{C}}$ represent the lower and upper limits of $p_{\mathrm{cl}}^{\mathrm{C}}$, while $r_{j,\mathrm{min}}^{\mathrm{C}}$ and $r_{j,\mathrm{max}}^{\mathrm{C}}$ represent the lower and upper limits of r_j^{C}.

The complementarity conditions in (19) to (22) can be rewritten as:

$$\lambda_j^{\mathrm{C\,min}} \geq 0, \lambda_j^{\mathrm{C\,max}} \geq 0 \quad \forall j \in \mathcal{N}_{\mathrm{p}} \tag{31}$$

$$\lambda_j^{\mathrm{M\,min}} \geq 0, \lambda_j^{\mathrm{M\,max}} \geq 0 \quad \forall j \in \mathcal{N}_p \tag{32}$$

$$r_j^{\mathrm{C}} \geq 0, U_j - r_j^{\mathrm{C}} \geq 0 \quad \forall j \in \mathcal{N}_{\mathrm{p}} \tag{33}$$

$$r_j^{\mathrm{M}} - r_j^{\mathrm{C}} \geq 0, m_j r_j^{\mathrm{C}} - r_j^{\mathrm{M}} \geq 0 \quad \forall j \in \mathcal{N}_{\mathrm{p}} \tag{34}$$

$$\lambda_j^{\mathrm{C\,min}} \leq M^{\mu P} \cdot \xi_j^{\mathrm{C\,min}} \quad \forall j \in \mathcal{N}_{\mathrm{p}} \tag{35}$$

$$r_j^{\mathrm{C}} \leq M^{\mathrm{P}}(1 - \xi_j^{\mathrm{C\,min}}) \quad \forall j \in \mathcal{N}_{\mathrm{p}} \tag{36}$$

$$\lambda_j^{\mathrm{C\,max}} \leq M^{\mu P} \cdot \xi_j^{\mathrm{C\,max}} \quad \forall j \in \mathcal{N}_{\mathrm{p}} \tag{37}$$

$$U_j - r_j^{\mathrm{C}} \leq M^{\mathrm{P}}(1 - \xi_j^{\mathrm{C\,max}}) \quad \forall j \in \mathcal{N}_{\mathrm{p}} \tag{38}$$

$$\lambda_j^{\mathrm{M\,min}} \leq M^{\mu P} \cdot \xi_j^{M\,\mathrm{min}} \quad \forall j \in \mathcal{N}_{\mathrm{p}} \tag{39}$$

$$r_j^{\mathrm{M}} - r_j^{\mathrm{C}} \leq M^{\mathrm{P}}(1 - \xi_j^{\mathrm{M\,min}}) \quad \forall j \in \mathcal{N}_{\mathrm{p}} \tag{40}$$

$$\lambda_j^{\mathrm{M\,max}} \leq M^{\mu P} \cdot \xi_j^{\mathrm{M\,max}} \quad \forall j \in \mathcal{N}_{\mathrm{p}} \tag{41}$$

$$m_j r_j^{\mathrm{C}} - r_j^{\mathrm{M}} \leq M^{\mathrm{P}}(1 - \xi_j^{M\,\mathrm{max}}) \quad \forall j \in \mathcal{N}_{\mathrm{p}} \tag{42}$$

where M^{P} and $M^{\mu P}$ are large enough constants, while $\lambda_j^{\mathrm{C\,min}}$, $\lambda_j^{\mathrm{C\,max}}$, $\lambda_j^{\mathrm{M\,min}}$, and $\lambda_j^{\mathrm{M\,max}}$ are binary variables.

The final sub-problem model includes the objective (26), and constraints (8)–(9), (5)–(6), (17)–(18), and (27)–(42).

Mixed integer quadratically constrained programming model-based master problem

As with the sub-problem, the objective of the master problem is:

$$\min_{O_j^{\mathrm{C}},O_j^{\mathrm{M}},j\in\mathcal{N}_{\mathrm{d}},\Phi} \sum\nolimits_{j\in\mathcal{N}_{\mathrm{a}}} \omega_j^{\mathrm{C}} + \eta \tag{43}$$

The constraints are (8)–(9), (2)–(3), (17)–(18), (31)–(42), and

$$\eta \leq \boldsymbol{x}^T \boldsymbol{Q} \boldsymbol{x} \tag{44}$$

$$\omega_j^{\mathrm{C}} \geq p_{\mathrm{cl,min}}^{\mathrm{C}} r_j^{\mathrm{C}} + p_{\mathrm{cl}}^{\mathrm{C}} r_{j,\mathrm{min}}^{\mathrm{C}} - p_{\mathrm{cl,min}}^{\mathrm{C}} r_{j,\mathrm{min}}^{\mathrm{C}} \quad \forall j \in \mathcal{N}_{\mathrm{v}} \tag{45}$$

$$\omega_j^{\mathrm{C}} \geq p_{\mathrm{cl,max}}^{\mathrm{C}} r_j^{\mathrm{C}} + p_{\mathrm{cl}}^{\mathrm{C}} r_{j,\mathrm{max}}^{\mathrm{C}} - p_{\mathrm{cl,max}}^{\mathrm{C}} r_{j,\mathrm{max}}^{\mathrm{C}} \quad \forall j \in \mathcal{N}_{\mathrm{v}} \tag{46}$$

$$\omega_j^{\mathrm{C}} \le p_{\mathrm{cl,max}}^{\mathrm{C}} r_j^{\mathrm{C}} + p_{\mathrm{cl}}^{\mathrm{C}} r_{j,\mathrm{min}}^{\mathrm{C}} - p_{\mathrm{cl,max}}^{\mathrm{C}} r_{j,\mathrm{min}}^{\mathrm{C}} \quad \forall j \in \mathcal{N}_{\mathrm{v}} \tag{47}$$

$$\omega_j^{C} \le p_{cl}^{C} r_{j,\mathrm{max}}^{C} + p_{cl,\mathrm{min}}^{C} r_j^{C} - p_{cl,\mathrm{min}}^{C} r_{j,\mathrm{max}}^{C} \quad \forall j \in \mathcal{N}_{v} \tag{48}$$

Acknowledgements
Not applicable.

Author contributions
YW and CC contributed to methodology formulation, analysis, article drafting and writing; SZ contributed to the supervision; YL contributed to software; CH contributed to the visualization; YD contributed to the validation. All authors read and approved the final manuscript.

Funding
This work was supported by the National Natural Science Foundation of China (Grant No. 52207142) and Natural Science Foundation of Jiangsu Province (BK20210512) and Natural Science Foundation of the Higher Education Institutions of Jiangsu Province (20KJB510050).

Availability of data and materials
The datasets used and/or analyzed during the current study are available in Sect. 5 Simulations and Numerical Analyses.

Declarations

Competing interests
The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this article.

Received: 6 March 2023 Accepted: 23 October 2023
Published online: 07 November 2023

References

1. Helman. U. (2021). Demand response in the us wholesale markets: Recent trends, new models, and forecasts. In *Variable generation, flexible demand* (2nd ed, ch 10, pp. 211–257). Academic Press.
2. Chen, W., Qiu, J., Zhao, J., et al. (2021). Bargaining game-based profit allocation of virtual power plant in frequency regulation market considering battery cycle life. *IEEE Transactions on Smart Grid, 12*(4), 2913–2928.
3. Srivastava, P., Chang, C. Y., & Cortés, J. (2022). Enabling der participation in frequency regulation markets. *IEEE Transactions on Control Systems Technology, 30*(6), 2391–2405.
4. Arteaga, J., & Zareipour, H. (2019). A price-maker/price-taker model for the operation of battery storage systems in electricity markets. *IEEE Transactions on Smart Grid, 10*(6), 6912–6920.
5. Dong, Y., Dong, Z., Zhao, T., et al. (2021). A strategic day-ahead bidding strategy and operation for battery energy storage system by reinforcement learning. *Electric Power Systems Research, 196*, 66.
6. Wang, Y., Zhou, Z., Botterud, A., et al. (2016). Stochastic coordinated operation of wind and battery energy storage system considering battery degradation. *Journal of Modern Power Systems and Clean Energy, 4*(4), 581–592.
7. Xu, B., Shi, Y., Kirschen, D. S., et al. (2018). Optimal battery participation in frequency regulation markets. *IEEE Transactions on Power Systems, 33*(6), 6715–6725.
8. Wu, X., Zhao, J., & Conejo, A. J. (2022). Optimal battery sizing for frequency regulation and energy arbitrage. *IEEE Transactions on Power Delivery, 37*(3), 2016–2023.
9. He, G., Chen, Q., Kang, C., et al. (2017). Cooperation of wind power and battery storage to provide frequency regulation in power markets. *IEEE Transactions on Power Systems, 32*(5), 3559–3568.
10. González-Garrido, A., Saez-de-Ibarra, A., Gaztanaga, H., et al. (2019). Annual optimized bidding and operation strategy in energy and secondary reserve markets for solar plants with storage systems. *IEEE Transactions on Power Systems, 34*(6), 5115–5124.
11. Fang, Y., & Zhao, S. (2020). Look-ahead bidding strategy for concentrating solar power plants with wind farms. *Energy, 203*, 66.
12. Xie, Y., Guo, W., Wu, Q., et al. (2021). Robust mpc-based bidding strategy for wind storage systems in real-time energy and regulation markets. *International Journal of Electrical Power & Energy Systems, 124*, 66.
13. Yang, X., Fan, L., Li, X., et al. (2023). Day-ahead and real-time market bidding and scheduling strategy for wind power participation based on shared energy storage. *Electric Power Systems Research, 214*, 66.
14. Vatandoust, B., Ahmadian, A., Golkar, M. A., et al. (2019). Risk-averse optimal bidding of electric vehicles and energy storage aggregator in day-ahead frequency regulation market. *IEEE Transactions on Power systems, 34*(3), 2036–2047.
15. Chen, Y., Leonard, R., Keyser, M., et al. (2015). Development of performance-based two-part regulating reserve compensation on miso energy and ancillary service market. *IEEE Transactions on Power Systems, 30*(1), 142–155.
16. Yang, Y., Peng, J.C.-H., & Ye, Z.-S. (2021). A market clearing mechanism considering primary frequency response rate. *IEEE Transactions on Power Systems, 36*(6), 5952–5955.
17. Shiltz, D. J., Cvetković, M., & Annaswamy, A. M. (2016). An integrated dynamic market mechanism for real-time markets and frequency regulation. *IEEE Transactions on Sustainable Energy, 7*(2), 875–885.
18. Qi, J., Hahn, A., Lu, X., et al. (2016). Cybersecurity for distributed energy resources and smart inverters. *IET Cyber-Physical Systems: Theory Applications, 1*(1), 28–39.
19. Xu, H., Lin, Y., Zhang, X., et al. (2020). Power system parameter attack for financial profits in electricity markets. *IEEE Transactions on Smart Grid, 11*(4), 3438–3446.
20. Zhang, Q., Li, F., Cui, H., et al. (2021). Market-level defense against FDIA and a new LMP-disguising attack strategy in real-time market operations. *IEEE Transactions on Power Systems, 36*(2), 1419–1431.
21. Khazaei, J. (2021). Cyberattacks with limited network information leading to transmission line overflow in cyber–physical power systems. *Sustainable Energy, Grids and Networks, 27*, 66.
22. Lu, K.-D., & Wu, Z.-G. (2022). Multi-objective false data injection attacks of cyber–physical power systems. *IEEE Transactions on Circuits and Systems II: Express Briefs, 69*(9), 3924–3928.
23. Chen, C., Wang, Y., Cui, M., et al. (2022). Data-driven detection of stealthy false data injection attack against power system state estimation. *IEEE Transactions on Industrial Informatics, 18*(12), 8467–8476.
24. Jorjani, M., Seifi, H., & Varjani, A. Y. (2021). A graph theory-based approach to detect false data injection attacks in power system ac state estimation. *IEEE Transactions on Industrial Informatics, 17*(4), 2465–2475.
25. Lai, K., Illindala, M., & Subramaniam, K. (2019). A tri-level optimization model to mitigate coordinated attacks on electric power systems in a cyber-physical environment. *Applied Energy, 235*, 204–218.
26. Wu, X., & Conejo, A. J. (2017). An efficient tri-level optimization model for electric grid defense planning. *IEEE Transactions on Power Systems, 32*(4), 2984–2994.
27. Davarikia, H., & Barati, M. (2018). A tri-level programming model for attack-resilient control of power grids. *Journal of Modern Power Systems and Clean Energy, 6*(5), 918–929.
28. Ruiz, C., & Conejo, A. J. (2015). Robust transmission expansion planning. *European Journal of Operational Research, 242*(2), 390–401.
29. Zeng, B., & Zhao, L. (2013). Solving two-stage robust optimization problems using a column-and-constraint generation method. *Operations Research Letters, 41*(5), 457–461.