Cyber-Vulnerability Analysis for Real-Time Power Market Operation

Qiwei Zhang, *Graduate Student Member, IEEE*, and Fangxing Li, *Fellow, IEEE*

***Abstract*—With the rapid advancement and integration of communication and sensor technologies, power system operation is becoming more vulnerable to cyberattacks, particularly attacks in which malicious data could induce catastrophic consequences on market operations. Financial risks, as well as the potential physical damages, raise growing concerns about the reliable operation of the electricity market. Existing market-targeting cybersecurity research has focused on developing attack strategies or detection schemes. However, the lack of cyber-vulnerability analysis (CVA) hinders operators from systematically evaluating the real-time (RT) market-clearing model and identifying potential threats from a cybersecurity perspective. This article proposes a comprehensive CVA model for delivering a detailed analysis of four aspects of vulnerability: highly probable cyberattack targets, devastating attack targets, risky load levels, and mitigation ability under different degrees of defense. Users can simulate interactions between attackers and defending operators under different attack events, and the corresponding market settlements are also obtained. The proposed bilevel model is recast into mixed-integer linear programming through Karush–Kuhn–Tucker (KKT) conditions. A simulation study on an IEEE-30 bus system demonstrates the accuracy and effectiveness of the proposed CVA model.**

***Index Terms*—Cyber-vulnerability, cybersecurity, locational marginal prices (lmps), bilevel optimization, KKT conditions.**

NOMENCLATURE

Lower Level Variables and Parameters

Parameters

C_i	Bidding prices of i^{th} unit
d_i	Load at bus i
P_i^{max}, P_i^{min}	Up and down generation limits for unit i
GSF_{l-i}	Generation shift factor which gives the fraction of a change in the injection at bus i that appears on a branch l
L_i^{max}, L_i^{min}	Up and down transmission capacity for branch i
A_{df}	Defense degrees.

Variables

P_i	Scheduled generation for unit i
V_l^+, V_l^-	Defense decision for congestion status of l^{th} up/down line flow constraint
V_i^b, V_i^d, V_i^p V_l^{L+}, V_l^{L-}	Defense decision for bid of i^{th} unit, load at i^{th} bus, capacity of i^{th} unit, up flow limit of l^{th} branch, and down flow limit of l^{th} branch
N_i^b, N_i^d, N_i^p N_l^{L+}, N_l^L	Defense value for bid of i^{th} unit, load at i^{th} bus, capacity of i^{th} unit, up flow limit of l^{th} branch, and down flow limit of l^{th} branch.

Upper Level Variables and Parameters

Parameters

A_{ak}	Attack degrees
q_i^b, q_i^d, q_i^p q_l^{L+}, q_l^{L-}	Penetration level of data manipulation in bid of i^{th} unit, load at i^{th} bus, capacity of i^{th} unit, up flow limit of l^{th} branch, and down flow limit of l^{th} branch.

Variables

M_i^b, M_i^d, M_i^p M_l^{L+}, M_l^{L-}	Attack value for bid of i^{th} unit, load at i^{th} bus, capacity of i^{th} unit, up flow limit of l^{th} branch, and down flow limit of l^{th} branch.
δ_l^+, δ_l^-	Attack decision for congestion status of l^{th} up/down line flow constraints
B_i^b, B_i^d, B_i^p B_l^{L+}, B_l^{L-}	Attack decision for bid of i^{th} unit, load at i^{th} bus, capacity of i^{th} unit, up flow limit of l^{th} branch, and down flow limit of l^{th} branch.

Lagrange Multipliers

λ	Lagrange multiplier for power balance constraint
γ_l^+, γ_l^-	Lagrange multipliers for up and down flow limits of l^{th} branch
μ_i^+, μ_i^-	Lagrange multipliers for upper and lower generation limits of i^{th} unit
$\alpha_{l,j}^+, \alpha_{l,j}^-, \alpha_{i,j}^+,$ $\alpha_{i,j}^-$	Lagrange multipliers for the 1^{st} reformed defense mitigation limits constraints
$\kappa_{l,j}^+, \kappa_{l,j}^-, \kappa_{i,j}^+,$ $\kappa_{i,j}^-$	Lagrange multipliers for the 2^{nd} reformed defense mitigation limits constraints
β	Lagrange multipliers for defense ability constraint.

Manuscript received July 31, 2020; revised November 4, 2020 and February 3, 2021; accepted March 6, 2021. Date of publication March 17, 2021; date of current version June 21, 2021. This work was supported in part by the U.S. Department of Energy (DOE) CEDS Project "Watching Grid Infrastructure Stealthily Through Proxies (WISP)" under Award DE-OE0000899, and in part by the CURENT, which is a U.S. NSF/DOE Engineering Research Center funded through NSF Award under Grant EEC-1041877. Paper no. TSG-01169-2020. *(Corresponding author: Fangxing Li.)*

The authors are with the Min H. Kao Department of Electrical Engineering and Computer Science, The University of Tennessee, Knoxville, TN 37996 USA (e-mail: fli6@utk.edu).

Color versions of one or more figures in this article are available at https://doi.org/10.1109/TSG.2021.3066398.

Digital Object Identifier 10.1109/TSG.2021.3066398

Parameters and Variables for Reformulations

Parameters

Q_m, Q_s, Q_g	Big numbers with $Q_g >> Q_m$.

Variables

$\delta_l^+\_V_l^+$, $\delta_l^-\_V_l^-$	Binary variables represent $\delta_l^+ + V_l^+$, $\delta_l^- + V_l^-$
$\delta_l^+\_V_l^+\_P_i$, $\delta_l^-\_V_l^-\_P_i$	Continuous variables represent $(\delta_l^+ + V_l^+) \cdot P_i$, $(\delta_l^- + V_l^-) \cdot P_i$
$\delta_l^+\_V_l^+\_M_i^j$, $\delta_l^-\_V_l^-\_M_i^j$	Continuous variables represent $(\delta_l^+ + V_l^+) \cdot M_i^j$, $(\delta_l^- + V_l^-) \cdot M_i^j$, and $j \in \{p^+, p^-, d^+, d^-, b^+, b^-, L^+, L^-\}$
u_i^{p+}, u_i^{p-}	Binary variables for the reformed complementary slackness of generation capacity constraint of unit i
u_l^{L+}, u_l^{L-}	Binary variables for the reformed complementary slackness of l^{th} flow limits.

I. Introduction

ALTHOUGH the growth of the Internet has expedited smart grid development, the interconnected smart grid communication network opens the modern power system operation to unprecedented threats from cyberattacks. For example, in December 2015, the information system for three distribution centers in Ukraine was compromised, and 30 substations were switched offline [1]. In March 2019, a denial-of-service attack occurred at a western utility in the U.S. disconnecting the communication between operators and remote generation sites for a minute [2]. These real-life events demonstrate that cyber intrusions are capable of penetrating the communication systems in power grid operation.

The U.S. power market clears hundreds of GW loads every hour, where electricity is produced reliably and economically. Malicious communication breaches into market operations could induce catastrophic consequences on fair financial settlements and reliable transmission services. Followed by the initial discussion of market-targeted cyberattacks presented in [3], the literature discussing various cyberattacks on power market operations is abundant.

The three main directions of market-targeted cyberattack research can be summarized as: (1) developing new attack strategies, (2) developing new detection schemes, and (3) investigating the sensitivity of cyberattacks. In the first category, state estimation (SE) is the most popular intrusion path. In [4], a robust false-data injection attack (FDIA) on SE is designed to create a financial bias on market settlements along with bogus bids. In [5], an undetectable parameter attack on the system model is designed for financial profit in market operations. In [6], a topology attack is combined with an FDIA to lead customers to pay a higher bill through undetectable price deviations. In [7], three new topology attacks on SE are developed to mislead both economic dispatch and reliable operation. Next, [8] determines that the grid topology is too extensive to be known by attackers, and a new profitable attack method without prior information on grid topology is proposed. Similarly, imperfect topology information is dealt with via robust optimization and stochastic programming in [9] and [10]. Various new attack paths and scenarios on market operation have been identified: a transmission line rating attack [11], a ramping constraints attack [12], and very short-term load forecasting [13]. For the second category of market-targeting cyberattack research, developing new detection schemes, detecting cyberattacks on market operations mainly focuses on SE level protections. In [14], a least-budget defense algorithm is proposed to secure preselected sensors, leading to the failure of bad data detection attacks. Refs. [15] and [16] have focused on enhancing the bad data detection algorithm itself by investigating the statistical difference between the random noise and the FDIA. In the last category of market-targeted cyberattack research, the sensitivity of cyberattacks, sensitivities of SE manipulation on market-clearing results have been fully investigated. In [18] and [19], the sensitivity of locational marginal prices (LMPs) to bad meter data has been formulated, and buses with higher sensitivity are found prone to being attack targets. In [20], the mathematic representation for the sensitivity of profitability to topology data is investigated. In [21], the sensitivity of renewable generation curtailments to profitability is formed. Although the curtailments in [21] are described as a strategy, the malicious attack could lead to the same results.

Various market cyberattacks and their corresponding defense strategies have been identified and demonstrated in existing research works. They generally focus on elaborating the attack paths or specific strategies, for example, the attacker's injection of false data to SE which changes the congestion pattern to modify LMPs. However, from the market operators' viewpoint, no matter where the attack path lays, whether in SE or the market gateway, the potential targets in a market operation are as follows: unit bids, demand management, generation capacities, line ratings, and congestion patterns. Therefore, it is important for the market operator to identify the vulnerability among all those attack paths. To the best of our knowledge, no previous research has developed a comprehensive analysis model regarding the vulnerability of the electricity market model involving all potential attack objectives and targets. Therefore, this article first provides an impact analysis model that emulates market-clearing under various cyberattacks, and then proposes a set of algorithms to identify the vulnerability from different aspects.

The detailed contributions of this article are as follows:

- A comprehensive cyber-vulnerability analysis (CVA) model is proposed in which market data from all sources is assumed to be susceptible to attacks, including line ratings, congestion patterns, generation capacity withholds, market-interface, etc. Namely, all parameters in the ISO's market model are assumed to be attackable. Next, various attack objectives are categorized and considered. The market operator can apply the proposed model to perform impact analysis on market cyberattacks.
- Four specific impact analysis algorithms are proposed to identify the vulnerability of power market parameters comprehensively. The four proposed algorithms target four vital aspects of the vulnerability of power

market parameters: (1) Vulnerability in terms of possibility: which attack paths are most likely to be attacked? (2) Vulnerability in terms of severity: which attack paths have the most impact on market operation? (3) Vulnerability in terms of load level: at which load level are attacks more likely to occur? (4) Vulnerability in terms of defense strategies: how defense degrees impact the effectiveness of market cyberattacks?

The rest of this paper is organized as follows. Section II first presents the formulation of the proposed CVA model. Section III describes the proposed algorithms based on the CVA model in detail. In Section IV, the reformulation and linearization steps for solving the proposed model are presented. Section V conducts a detailed simulation study on an IEEE 30-bus system to demonstrate the effectiveness of the proposed vulnerability analysis. Finally, conclusions and future studies are discussed in Section VI.

II. Proposed Analysis Model on Market FDIAs

A. Preliminary on Real-Time (RT) Market Model

Ex-ante and ex-post are two primary models for RT market-clearing [22]. In the ex-ante model, generation dispatches and LMPs are calculated based on the forecasted conditions for the next trading period. Optimal generation dispatches are determined given the expected load and physical security constraints. The ex-post model is purely a price-setting model in which generation dispatches are determined via the ex-ante model, while the LMPs are calculated by the ex-post model. The proposed analytical model can be applied to both the ex-ante and ex-post models. The ex-ante model is applied here as an illustration, shown in (1)-(5).

$$\min \sum_i C_i(p_i) \tag{1}$$

$$\sum_i P_i - \sum_i d_i = 0 \tag{2}$$

$$P_i^{\min} \le P_i \le P_i^{\max}, \quad \forall i \in NG \tag{3}$$

$$\sum_{i=1}^{N_b} GSF_{l-i}(P_i - d_i) \le L_l^{\max} \quad \forall l \in L \tag{4}$$

$$\sum_{i=1}^{N_b} GSF_{l-i}(P_i - d_i) \ge L_l^{\min} \quad \forall l \in L \tag{5}$$

The details of the RT market model can be found in [22]. The market-clearing price is composed of the Lagrange multipliers associated with (2)-(5), as shown in (6).

$$LMP = \lambda + \sum_L GSF_{l-i}\left(\gamma_l^+ - \gamma_l^-\right). \tag{6}$$

B. Proposed CVA Model

The proposed analytic model provides a flexible platform to emulate different attack strategies and defense degrees under various assumptions. The details of the vulnerability analysis algorithms are discussed in the next section. This section presents the construction of the CVA model.

The CVA model contains an attacker and a defending market operator. The attacker wants to optimize its objective (e.g., LMP manipulations), then it anticipates the optimal response from the market operator. In this setting, the attack's optimization problem contains a nested optimization task that corresponds to the market operator's optimization problem. The defending ability is modeled for the impact analysis of defense degrees, which is clarified in detail in Section III-D. Therefore, the proposed model is constructed as a bilevel optimization problem. The attacker modifies the parameters that impact the market-clearing result, and the market operator clears the market with defending variables, which in turn affects the attacker's objective. The overall structure of the proposed model for CVA is shown in Fig. 1.

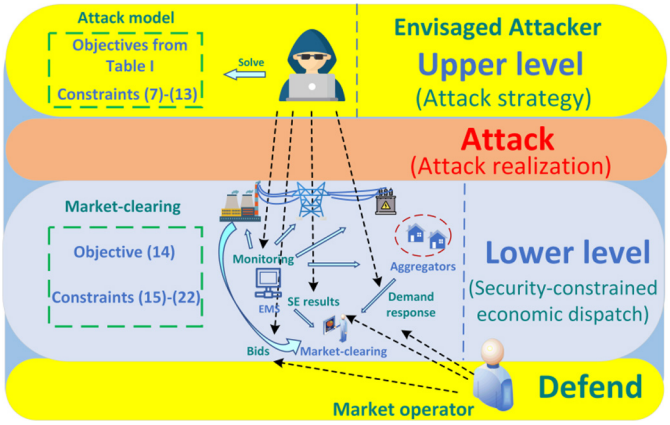


Fig. 1. Proposed CVA model structure.

TABLE I
Potential Attack Objectives

Type	*Objective*	*Model*
Financial settlements	LMP	LMP_i
	Social-welfare	$\sum C_i(P_i)$
Generation	Generation dispatch	P_i
Transmission	Congestion price	$LMP_i - LMP_j$
	Congestion pattern	L

1) Upper Level (Attacker): Although most of the existing research assumes that attacks on the market are profit-driven, the purpose of cyberattacks on market operation varies from one attacker to another. Generally, potential objectives for power market cyberattacks can be categorized into three types: (1) financial settlements, (2) generation dispatches, and (3) transmission congestions. Therefore, the proposed model considers different attack objectives from each of the above categories, as shown in Table I to provide a general attack evaluation. The objective of the upper level model can be selected from Table I based on different analysis purposes, which are discussed in Section III.

The upper level of the analysis model incorporates all potential attack targets in market operations. When the market operator solves a RT economic dispatch problem, data from multiple sources are used, including: (1) short-term load forecasts and demand management from energy

management systems (EMSs); (2) bidding prices and generator capacities from market gateway; and (3) congestion patterns and line ratings from EMSs. Therefore, to conduct a comprehensive analysis, all of the above data sources are assumed to be susceptible to attacks, as shown in (7)-(11). Although some parameters may not be easily compromised unless the cyber threats are from insiders, the proposed CVA model in this article considers comprehensive scenarios to provide a general analytic framework for market operators to identify possible cyber vulnerabilities. Specific constraints and variables can be simplified or removed if decision makers consider these parameters to be perfectly secure. The maximum amount of those attacks is constrained by the penetration level value q and the targets' original value.

$$-q_i^b c_i B_i^b \le M_i^b \le q_i^b c_i B_i^b, \quad \forall i \in NG \tag{7}$$

$$-q_i^d d_i B_i^d \le M_i^d \le q_i^d d_i B_i^d, \quad \forall i \in L \tag{8}$$

$$-q_i^p P_i^{\max} B_i^p \le M_i^p \le q_i^p P_i^{\max} B_i^p, \quad \forall i \in NG \tag{9}$$

$$-q_l^{L+} L_l^{\max} B_l^{L+} \le M_l^{L+} \le q_l^{L+} L_l^{\max} B_l^{L+}, \quad \forall \mathrm{i} \in L_{\delta_l^+} \tag{10}$$

$$q_l^{L-} L_l^{\min} B_l^{L-} \le M_l^{L-} \le -q_l^{L+} L_l^{\min} B_l^{L-}, \quad \forall i \in L_{\delta_l^-} \tag{11}$$

$$\delta_l^- + \delta_l^+ \le 1, \quad \forall l \in L \tag{12}$$

$$\sum_l \delta_l^- + \delta_l^+ + B_l^{L+} + B_l^{L-} + \sum_i B_i^b + B_i^p + B_i^d \le A_{ak} \tag{13}$$

Constraint (12) means that congestion pattern attacks happen either at upper or lower limits because a line flow can either be on the upper or lower limit. The attacker degree is constrained in (13), which represents how many targets the attacker can compromise.

2) Lower Level (Market Operator): The market operator is placed at a lower level equipped with the capability to defend against attacks. The original economic dispatch model (1)-(5) becomes (14)-(18) with the considered attacks and corresponding defenses. To identify the critical attack path and defense efficiency, the defense degree is constrained in (19), which represents the number of attacks that can be defended against. Although operators want to defend against all possible attacks, there is always a recourse limit such that they have to defend against the attacks that they identify as most threatening. It worth noting that the defender knows where the attacker attacked in this bilevel formulation. However, the defender proposed analysis presented in this work is aimed at analyzing the effectiveness of the defense degree, which is explained in detail in Section III-D. Equations (20) and (21) indicate that if an attack is identified, then it is totally countered, and equation (22) shows the defense is only placed where the attack happens.

$$\min \sum_i \left(C_i + M_i^b - N_i^b\right) P_i \tag{14}$$

$$\sum_i P_i - \sum_i \left(d_i + M_i^d - N_i^d\right) = 0 \tag{15}$$

$$0 \le P_i \le P_i^{\max} + M_i^p - N_i^p, \quad \forall i \in NG \tag{16}$$

$$\left(\delta_l^+ | V_l^{\delta+}\right) \sum_{i=1}^{N_b} GSF_{l-i}\left(P_i - \left(d_i - M_i^d + N_i^d\right)\right)$$

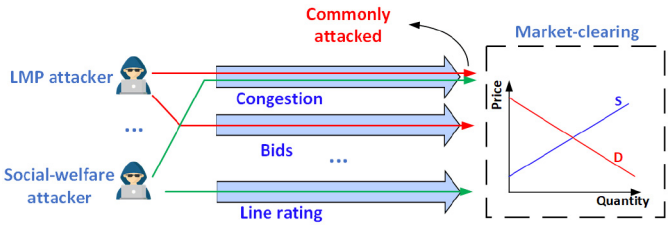


Fig. 2. Identifying highly probable attack targets.

$$\le L_l^{\max} + M_l^{L+} - \mathrm{N}_l^{L+}, \quad \forall l \in L \tag{17}$$

$$\left(\delta_l^- | V_l^{\delta-}\right) \sum_i^{N_b} GSF_{l-i}\left(P_i - \left(d_i - M_i^d + N_i^d\right)\right)$$

$$\ge L_l^{\min} + M_l^{L-} - \mathrm{N}_l^{L-}, \quad \forall l \in L \tag{18}$$

$$\sum_i \sum_j V_i^j + \sum_l \sum_j V_l^j + \sum_l V_l^{\delta^+} + \sum_l V_l^{\delta^-} - A_{df} \le 0 \tag{19}$$

$$N_i^j = V_i^j M_i^j, \quad \forall \mathrm{i} \in N^b, \ \forall \mathrm{j} \in \{d, p, b\} \tag{20}$$

$$N_l^j = V_l^j M_l^j, \quad \forall l \in L, \ \forall \mathrm{j} \in \left\{L^+, L^-\right\} \tag{21}$$

$$V_i \le B_i, \quad \forall \mathrm{i} \in \left\{d, p, b, L^+, L^-\right\} \tag{22}$$

The proposed CVA model is used to perform a vulnerability analysis from four different aspects, which will be elaborated in the next section.

III. The Capability of the Proposed Analysis Model

As discussed in the introduction, potential attack targets, risky operating conditions, and defense effectiveness are the most vital elements in developing a defense strategy. Therefore, the following four aspects are selected to construct the CVA model.

A. Identifying Highly Probable Attack Targets (Algorithm 1)

Some parameters are compromised more frequently than others. For example, congestion patterns can be a vital attack route for both LMP manipulation and diminishing social-welfare. As shown in Fig. 2, protection of the congestion pattern makes it hard for those two types of market attackers to achieve their desired goals. Therefore, in Algorithm 1, the CVA model is solved iteratively for all interested attack objectives, and the attack route for each attack objective is recorded. The frequently attacked parameters (routes) are identified as vulnerable parameters in terms of the probability of being attacked. Providing protection to the identified parameters diminishes overall attack interest in the market operation. Further, the attacker has different optimal attack routes when they have different attack degrees.

Therefore, market operators can also identify vital attack routes under different attack degrees through Algorithm 1. The detailed procedure of this identification is shown in Algorithm 1 HPA, where HPA stands for "highly probable attack" analysis.

Algorithm 1 Function HPA (Market Parameters, Attack Objectives)

Input Real-time market parameters and interested attack objectives
Output Highly probable attack targets

For each possible attack degree **do**
  For each attack objective in Table I **do**
    Solving the CVA model (7) - (22)
    Record the attack binary variable B for each target
  End for
  Sum variable B in all attack objectives for each target
End for
Identify targets that have high values of sum (B)
Return the Identified Targets

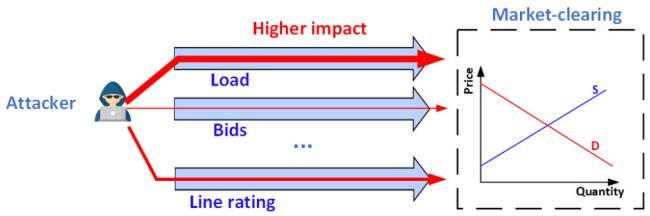


Fig. 3. Identifying devasting attack targets.

B. Identifying Devasting Attack Targets (Algorithm 2)

Different from highly probable attack targets (Algorithm 1), devasting attack targets vary from one attack objective to another. The attacks on one parameter could be more effective than the attacks on other parameters for a particular attack objective. As shown in Fig. 3, modifying load information could be more effective than modifying line rating. Thus, protection of these attack targets largely diminishes the attackers' interest in a specific attack objective. It should be noted that an attack on the congestion pattern is not applicable to this algorithm because the congestion status is a binary variable that does not have a penetration level.

Further, LMPs experience step changes regarding some attack routes, such as attacks in load levels, which means the LMP does not change until the modified parameter is large enough. For these attack scenarios, Algorithm 2 can identify the critical attack penetration level that leads to the step change. In Algorithm 2, the CVA model is solved iteratively with a gradual increase of the penetration level Δq under an interested attack objective. The selection of Δq is based on the market operator's need, and the smaller the Δq, the higher the level of accuracy that can be obtained. The detailed procedure of this identification is shown in Algorithm 2 DAT, where DAT stands for "devasting attack targets" analysis.

C. Formulating Risky Load Levels (Algorithm 3)

Different load levels result in different market settlements and dispatches. Therefore, the load level is a critical element of a successful cyberattack. As shown in Fig. 4, an attacker with the same ability could obtain different profits from market-clearing under different load levels. Therefore, the higher the profitability is, the riskier the load level is. In Algorithm 3, the CVA model is solved iteratively with all interested attack objectives at different load levels. The obtained attack objective values are scaled and summed for each load level. If the value is higher than a certain threshold, then the load level can be identified as risky. In this study, the same load participation factors are assumed. If the market operator interests in different load participation factors, the load level and the participation factors are both recorded when solving the CVA model, and the risky load level becomes a risky set containing a load level and load participation factors.

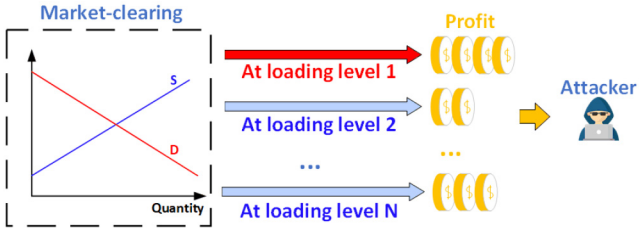


Fig. 4. Formulating risky load levels.

Algorithm 2 Function DAT (Market Parameters, Attack Objectives)

Input Real-time market parameters and interested attack objectives
Output Devasting attack targets

Select interested attack objective from Table I
For each attack target **do**
  Set attack variables B associated with other attack targets equal to 0
  While penetration level q is less than a threshold
    Solving the CVA model (7) - (22)
    $q = q + \Delta q$
    Record the value of attack objective
  End while
End for
Compare the slope of different attack targets
Identify targets that have steep slopes
Return the Identified Targets

Algorithm 3 Function RLL (Market Parameters, Attack Objectives)

Input Real-time market parameters and interested attack objectives
Output Risky load levels

For each load level **do**
  Obtain market-clearing result without attacks
  For each interested attack objective **do**
    Solving the CVA model (7) - (22)
    Record the difference between the attacked value and the normal value
  End for
  Sum attack objectives with specified weights $\sum W_i \cdot obj_i$
End for
Identify load levels that have high weighted values
Return the Identified Load Levels

D. Investigating the Mitigation Ability of Different Defense Degrees (Algorithm 4)

The goal of Algorithm 4 is to investigate the impact of defense degrees on the effectiveness of the attack. As shown in Fig. 5, if some of the most effective attack routes are

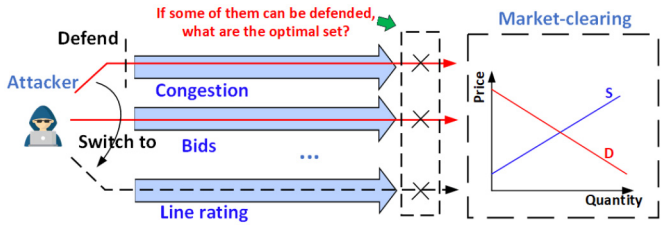


Fig. 5. Mitigation ability of different degrees.

Algorithm 4 Function DDD (Market Parameters, Attack Objectives)

Input	Real-time market parameters and interested attack objectives
Output	Defense mitigation ability plot/list
1	**For** each attack objective **do**
2	Set an interested attack degree A_{ak} and set the defense degree $A_{df} = A_{ak}$
3	**while** defense degree A_{df} is larger than 0 **do**
4	Solving the CVA model (7) - (22)
5	Record the objective value
6	$A_{df} = A_{df} - 1$
7	**End while**
8	Plot/list the objective value versus defense degree
9	**End for**
10	**Return** the plot/list

defended by the operator, the attacker might switch to other attack routes. However, those backup attack routes are not as effective. Therefore, investigation of the defense degree to which the attacker may lose the attack interests is an important aspect of the development of defense strategies. The proposed Algorithm 4 solves the CVA model iteratively with a gradual increase of defense degrees, and the corresponding value of the attack objective is recorded. When the value of the attack objective discourages the attack, the defense degree is identified as the critical defense degree.

The detailed procedure of this identification is shown in Algorithm 4 DDD, where DDD stands for "different defense degrees" analysis.

The above four proposed analysis algorithms are demonstrated with examples in Section V. Analysis in this article is performed using the attack objectives in Table I, but future users can integrate any additional attack objectives in a similar way. The proposed analysis algorithms aim to solve the CVA model iteratively, which could raise a concern about scalability. Indeed, the number of combinations of attack objectives and attack targets can be astronomical for a real system. However, the potential attack objectives and attack targets can be filtered to a much smaller portion depending on ISOs or the decision maker's preference. For example, the ISO New England system has 2771 branches, but the average active transmission constraint in January 2020, their winter peak month, is just 142 branches [25]. The attacker's ability is also limited because the attacker may not have access to all parameters. Therefore, the number of combinations can be reduced. Further, the proposed algorithms are for the purpose of analyzing vulnerability, not for protecting market operation in RT. Thus, the proposed analysis could be performed offline and in the cycle of a few weeks (or even months) depending on the market operator's preference. Therefore, the computation is a minor concern for the proposed vulnerability analysis algorithms.

IV. Reformulations of the Proposed CVA Model

Section II describes the mathematical model for CVA, and Section III discusses how to apply the CVA model to identify cyber vulnerability for an RT market model. This section presents the steps to solve the CVA model.

Normally, the lower-level problem can be converted to constraints through Karush-Kuhn-Tucker (KKT) conditions [23]. Then, the bilevel problem becomes a single-level problem [24]. However, the lower-level problem of the CVA model contains binary variables, which violate the optimality condition of the KKT conditions. Here, we apply the following reformulations to convert the lower-level problem with binary variables through KKT conditions.

Step 1) Constraints (20) and (21) Linearization: Constraints (20) and (21) contain the multiplication of binary variables and continuous variables. The detailed equations for linearizing (20) and (21) can be found in *Appendix A*.

Step 2) Lower-Level Problem Convexification: The binary variables in the lower-level problem are convexified through a penalty function before the KKT conversion. The binary defense decision variable V is reformed with continuous representation. Equation (23) redefines V as a finite continuous value with an upper limit W. Then, equation (24) restricts the feasible value for the continuous variable V to be either 1 or 0. It is worth noting that although now the binary variable V is remodeled through continuous representation, the feasibility region is still non-convex.

$$W \geq V \geq 0 \tag{23}$$

$$V(V-1) = 0 \tag{24}$$

$$\min \cos t + Q(V(V-1))^2 \tag{25}$$

Then, constraint (24) is removed by adding a penalty term in the objective function, as shown in (25). The large number Q will penalize the objective function unless V is either 1 or 0. The square of $V(V-1)$ has the same feasible region as $V(V-1)$, but the square is a convex representation. In this formulation, the lower-level problem is convexified. The selection of the large number Q is a challenge for optimization problems involving penalties because a penalty term may not be exactly zero at the obtained optimal solution. In this study, a large value is assigned to Q initially, and then it is gradually increased until an optimal solution is obtained (i.e., the solution does not change and the value of V is close to binary). When the penalized variables are close but not exactly binary (e.g., 0.99 or 0.01), they are rounded to 0 or 1.

Step 3) Formulating KKT Conditions: The optimality conditions of the lower-level problem in a bilevel formulation are well-established in [26] and [27]. Therefore, the complete KKT constraint set is not elaborated here.

Step 4) Linearizing Nonlinear Terms: The CVA model contains nonlinear elements that render the implementation of the optimizations. In particular, the multiplication of the status of

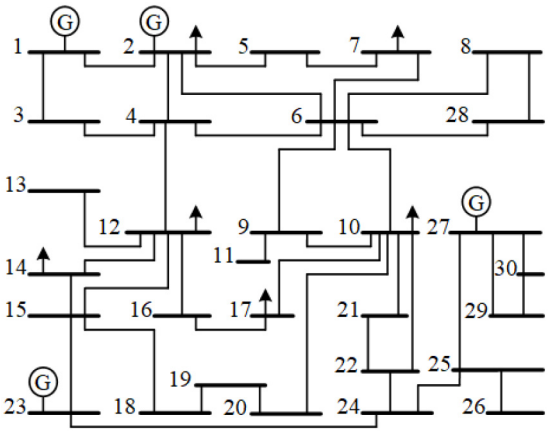


Fig. 6. One-line diagram of IEEE-30 bus system.

congestion attacks and other variables leads to various nonlinear elements. The constraints that contain nonlinear terms are listed in *Appendix B*. The detailed steps for linearizing all the nonlinear elements in those constraints are attached in *Appendix C*, *Appendix D,* and *Appendix E*.

V. Case Study

A thorough simulation study of an IEEE 30-bus system is given in this section to demonstrate the effectiveness of the proposed vulnerability analysis algorithms. The system topology is shown in Fig. 6.

The detailed system parameters can be found in [28]. The simulation studies were performed with MATLAB 2018 on a PC with Intel i7-8650U processor and 8GB RAM.

A. Identifying Highly Probable Attack Targets

This study aims to demonstrate Algorithm 1 in Section III-A. The CVA model is solved iteratively for various attack objectives from Table I. The computational time of Algorithm 1 in this study is 70.32 s.

Fig. 7 shows various attacked parameters for each attack objective. The Y-axis shows different objectives of the attacks, and the X-axis shows different attack targets in market operation. Triangles on a specific row represent optimal attack targets for a specific attack objective. For example, for the attack that is to maximize the LMP at bus 1, the optimal attack targets are the load at bus 12 and the line rating at line 15. In other words, an attack on these two parameters will more effectively alter the LMP at bus 1 than the attacks on any other different combination of two parameters.

Therefore, by enumerating the number of triangles on each column, the probability of being attacked can be estimated for each parameter from the perspective of being a highly probably attack target. In other words, the column that has the most triangles indicates the parameter that has the highest probability of being attacked. In this study, the line rating of line 15 is the most vulnerable parameter, which will be the most frequent attack target. Therefore, when this target is protected, most attacks become less effective. Although the attackers' objective is usually unknown in reality, protection

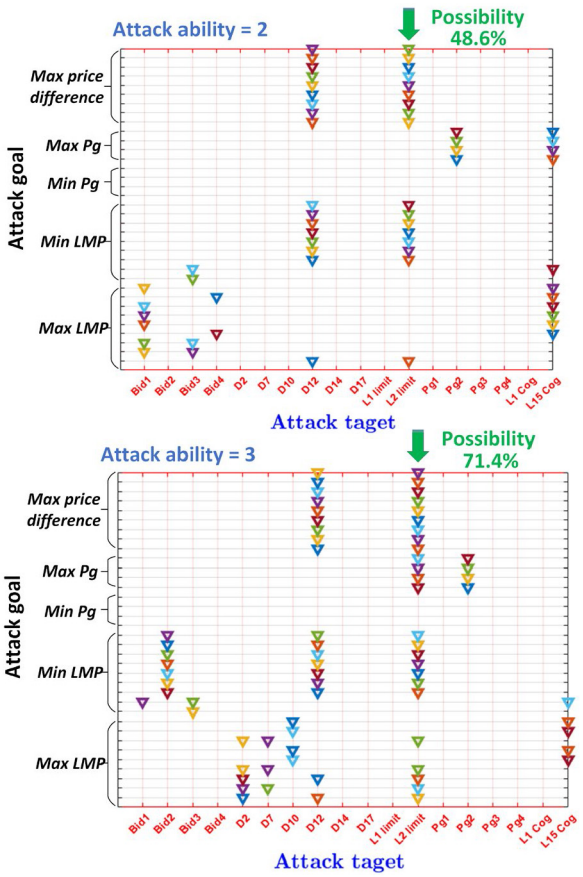


Fig. 7. Identifying the most likely attack target.

of highly probable targets reduces overall attack interest in the market operation. The upper subplot and lower subplot in Fig. 7 represent different attack degrees (2 and 3), namely, how many parameters the attacker is able to modify. When the attack degree increases from 2 to 3, the possibility of attacking the line rating of line 15 increases from 48.6% to 71.6%. Therefore, if the line rating of line 15 is immune from attacks, interests in most attacks on this market are greatly reduced.

B. Identifying Devasting Attack Targets

This study aims to demonstrate Algorithm 2 in Section III-A. The CVA model for interested attack objectives is solved iteratively for a gradual increase of the penetration levels of different attack targets. The deviations between the objective value under normal operation and under attack are recorded. The computational time of Algorithm 2 in this study is 135.25 s. We select the most popular two attack objectives in the literature as examples: (1) diminishing the social welfare and (2) manipulating LMPs (bus 10). The impact analyses of 4 different attack targets on those two objectives are shown in Table II and Table III. Simulations on other attack objectives and targets can be performed similarly.

For LMP manipulation, an attack on unit 4's bid is more effective when the penetration level is low, and an attack on unit 3's capacity becomes more effective when the penetration level is higher than 40%. For diminishing social-welfare,

TABLE II
IMPACT ANALYSIS ON LMP MANIPULATIONS

P. Levels / Deviation ($) / Targets	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
Bids of G3	0	0	3.0	5.4	7.7	10.2	12.6	14.9	17.3	19.7
Bids of G4	2.6	5.1	7.7	10.3	12.8	15.4	18.0	20.6	23.1	25.7
Capacity of G3	0	0	0	0	51.9	51.9	51.9	51.9	51.9	51.9
Load at bus 2	0	0	0	0	0	0	0	0	0	0

TABLE III
IMPACT ANALYSIS ON DIMINISHING SOCIAL-WELFARE

P. Levels / Deviation ($) / Targets	10%	20%	30%	40%	50%	60%	70%	80%	90%	100%
Bids of G3	0	0	207.1	207.1	207.1	207.1	207.1	207.1	207.1	207.1
Bids of G4	0	0	0	0	0	22.0	22.0	22.0	22.0	22.0
Capacity of G3	1.2	3.6	5.5	7.3	9.1	10.9	12.7	14.5	16.4	18.1
Load at bus 2	30.0	60.0	90.0	120.0	150.0	180.0	210.0	240.0	270.0	300.0

attacking the load at bus 2 is more effective when the penetration level is lower than 30% or higher than 90%, and attacking unit 3's bid is more effective for other penetration levels. Further, a step-change phenomenon is observed for both attack objectives. The social welfare loss exhibits a step-change pattern with the bid modification attack and continuously changes with the remaining attacks. By comparison, the LMP continuously changes with the bid modification attack and exhibits a step-change pattern with the remaining attacks. This indicates that the bid modification attack does not impact social welfare unless it changes the dispatch results since it does not change the generation cost in practice, but the bids of marginal units directly impact the LMP. If the most sensitive attack target is identified and protected, the attack interests for a specific attack are significantly reduced.

C. Evaluating Risk Load Levels

This study aims to demonstrate Algorithm 3 in Section III-C. The CVA model for all attack objectives is solved iteratively under different load levels. The deviations between the objective value under normal operation and under attack are recorded. The computational time of Algorithm 3 in this study is 965.36 s. Fig. 8 shows the risk evaluation of different load levels by a heat map. Different attack objectives have their own heat map (i.e., risk zone).

Here, all risk zones are summed and scaled to be between 0 and 1, where 0 means not risky, and 1 means the riskiest. Thus, the greater the overlap of the risk zones, the brighter the square is. That is, a brighter area means more impact on the market operation.

As shown in Fig. 8, at first, the heavier the load is, the more an attacker can do. However, when the load becomes higher, the impact decreases because the margin for manipulation by the attacker is decreased. In other words, when more generations are at maximum, there is less room for an attacker to manipulate the parameters without being detected.

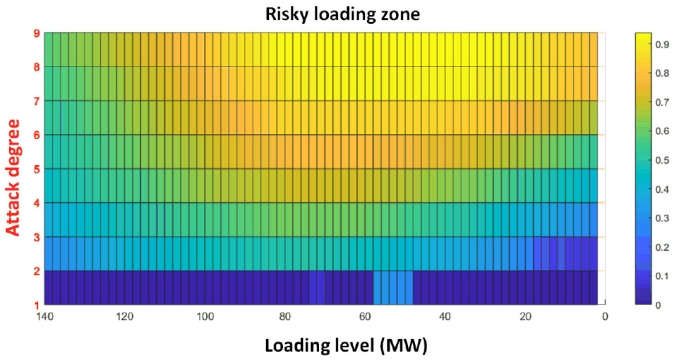


Fig. 8. Vulnerable market operating zone.

TABLE IV
IMPACT ANALYSIS ON DEFENSE DEGREE

Degree / Deviation (%) / Objective	0	1	2	3	4	5	6	7	8
Social-welfare loss	109.2	105.1	101.0	86.2	72.1	55.3	35.7	24.6	0
LMP (bus 10)	215.9	215.9	215.9	215.9	215.9	215.9	132.0	30.3	0

D. Investigating the Mitigation Ability of Different Degrees of Defense

This study aims to demonstrate Algorithm 4 in Section III-D. The understanding of how defenses improve the deviation from the optimal dispatch provides a guideline for a market operator to develop defense strategies. The CVA model is solved iteratively with a gradual increase of the defense degree. The computation time of Algorithm 4 in this study is 65.39 s. As shown in Table IV, the value of deviation from a normal value gradually decreases to zero with the increasing defense degree.

When more highly effective attack routes are blocked (i.e., at higher defense degrees), the attacker has to switch to less effective attack routes, and thus, the impact of cyberattacks is alleviated. Although the attack still impacts market operations unless all of the compromised parameters are corrected, the attacker could lose interest when the degree of defense is higher than a certain threshold such that the attacker's gain from a cyberattack is very low. The proposed analysis provides the market operator with information on critical defense degrees. As shown in the first row of Table IV, when 3 of the most effective attack routes can be protected, the maximum social welfare deviation dropped from 109.2% to 86.2%, which may discourage the attacks. Further, the social welfare loss due to cyberattacks decreases almost linearly with the increasing defense level. For an LMP manipulation attack, as in the second row of Table IV, the defense is not effective (i.e., the deviation created by the attack is 215.9%) until 5 parameters can be defended, which means the attackers can still achieve the desired outcome via the undefended measures. When the defense degree is larger than 5, the optimal value of the attack objective starts to decrease. It should be pointed out that the proposed algorithm provides useful information for a decision maker while the actual threshold to determine the number of defense degrees is a choice of the decision maker.

VI. Conclusion

In this article, the missing components in the current research on power market cybersecurity are discussed. Next, a CVA model is proposed for market operators to perform impact analysis on market cyberattacks. Then, four vital components related to cyber vulnerability in the system are discussed, and four vulnerability analysis algorithms are proposed. The proposed algorithms can help the market operator identify highly probable attack targets, devastating attack targets, risky load levels, and the mitigation ability of different defense degrees. In summary, the proposed CVA model provides a new method to identify various aspects that are vulnerable to cyberattacks in market operation, which provides valuable references for further development of cyber defense strategy.

Our future studies will focus on applying artificial intelligence algorithms to identify specific interaction patterns between attackers and defenders based on the proposed CVA model.

Appendix

The reformulations and linearization of the CVA model are included in this *Appendix*.

A. Constraint (20) and (21) Linearization

The first constraint (20) is linearized and replaced by (A1) and (A2). Similarly, (21) is replaced by (A3) and (A4).

$$-V_i^j M_{i,j}^{\min} \le N_i^j \le V_i^j M_{i,j}^{\max}, \quad \forall \mathrm{i} \in NG,\ \forall \mathrm{j} \in \{d,p,b\} \tag{A1}$$

$$M_i^j - \left(1-V_i^j\right)Q_s \le N_i^j \le M_i^j + \left(1-V_i^j\right)Q_s \quad \forall \mathrm{i} \in NG,\ \forall \mathrm{j} \in \{d,p,b\} \tag{A2}$$

$$-V_l^j M_{l,j}^{\min} \le N_l^j \le V_l^j M_{l,j}^{\max}, \quad \forall l \in L,\ \forall \mathrm{j} \in \left\{L^+, L^-\right\} \tag{A3}$$

$$M_i^j - \left(1-V_l^j\right)Q_s \le N_l^j \le M_i^j + \left(1-V_l^j\right)Q_s \quad \forall l \in L, \quad \forall \mathrm{j} \in \left\{L^+, L^-\right\}. \tag{A4}$$

B. Constraints That Contain Nonlinear Elements

Equations (17) and (18)

$$\gamma_l^+\left(\delta_l^+|V_l^{\delta+}\right)\left(\sum_i GSF_{l-i}\left(P_i - \left(d_i - M_i^d + N_i^d\right)\right) - L_l^{\max} - M_l^{L+} + N_l^{L+}\right) = 0, \quad \forall l \in L \tag{B1}$$

$$\gamma_l^-\left(\delta_l^-|V_l^{\delta-}\right)\left(\sum_i L_l^{\min} + M_l^{L-} - N_l^{L+} - GSF_{l-i}\left(P_i - \left(d_i - M_i^d + N_i^d\right)\right)\right) = 0, \quad \forall l \in L \tag{B2}$$

$$\left(C_i + M_i^b - N_i^b\right) + \lambda + \mu_i^+ - \mu_i^- + \sum_L GSF_{l-i}\left(\left(\delta_l^+ + V_l^{\delta+}\right)\gamma_l^+ - \left(\delta_l^- + V_l^{\delta-}\right)\gamma_l^-\right) = 0, \quad \forall \mathrm{i} \in \mathrm{NG} \tag{B3}$$

$$-\lambda + \sum_l GSF_{l-i}\left(\gamma_l^-\left(\delta_l^-|V_l^{\delta-}\right) - \gamma_l^+\left(\delta_l^+|V_l^{\delta+}\right)\right) + \alpha_{i,j}^+ - \alpha_{i,j}^- + \kappa_{i,j}^+ - \kappa_{i,j}^- = 0, \quad \forall \mathrm{i} \in \mathrm{NG} \tag{B4}$$

$$\gamma_l^+\left(\delta_l^+|V_l^{\delta+}\right) + \alpha_{i,j}^+ - \alpha_{i,j}^- + \kappa_{i,j}^+ - \kappa_{i,j}^- = 0, \forall \mathrm{i} \in \mathrm{NG} \tag{B5}$$

$$-\gamma_l^-\left(\delta_l^-|V_l^{\delta-}\right) + \alpha_{i,j}^+ - \alpha_{i,j}^- + \kappa_{i,j}^+ - \kappa_{i,j}^- = 0, \quad \forall \mathrm{i} \in \mathrm{NG}. \tag{B6}$$

C. Linearizing $\delta\_V \cdot M$ and $\delta\_V \cdot N$

The variable δ_V represents the OR gate operation of the variable δ and V. Therefore, the relationship between δ_V, δ, and V is shown in (C1)-(C3).

$$\delta_{l\_}^j V_l^{\delta j} \ge V_l^{\delta j}, \quad \forall l \in L\ \forall j \in \{+,-\} \tag{C1}$$

$$\delta_{l\_}^j V_l^{\delta j} \ge \delta_l^j, \quad \forall l \in L\ \forall j \in \{+,-\} \tag{C2}$$

$$\delta_{l\_}^j V_l^{\delta j} \le V_l^{\delta j} + \delta_l^j, \quad \forall l \in L\ \forall j \in \{+,-\} \tag{C3}$$

Similar to (A1)-(A4), $\delta\_V \cdot M$ is replaced by a new continuous variable δ_V_M, with constraints (C4) and (C5).

$$-q_i^d \cdot d_i \cdot \left(\delta_{l\_}^j V_l^{\delta j}\right) \le \delta_{l\_}^j V_l^{\delta j}\_M_i^d \le q_i^d \cdot d_i \cdot \left(\delta_{l\_}^j V_l^{\delta j}\right) \quad \forall j \in \{+,-\} \tag{C4}$$

$$M_i^d - \left(1-\delta_{l\_}^j V_l^{\delta j}\right)Q_s \le \delta_{l\_}^j V_l^{\delta j}\_M_i^d \le M_i^d + \left(1-\delta_{l\_}^j V_l^{\delta j}\right)Q_s \quad \forall j \in \{+,-\} \tag{C5}$$

In element $\delta\_V \cdot N$, variable N is constrained by (A1)-(A4). A new continuous variable δ_V_N is introduced to replace $\delta\_V \cdot N$ with (C6)-(C10).

$$\delta_{l\_}^j V_l^{\delta j}\_V_i^d \le V_i^d, \quad \forall l \in L\ \forall j \in \{+,-\} \forall d \in D \tag{C6}$$

$$\delta_{l\_}^j V_l^{\delta j}\_V_i^d \le \delta_{l\_}^j V_l^{\delta j}, \quad \forall l \in L\ \forall j \in \{+,-\} \forall d \in D \tag{C7}$$

$$\delta_{l\_}^j V_l^{\delta j}\_V_i^d \ge \delta_{l\_}^j V_l^{\delta j} + V_i^d - 1 \quad \forall l \in L\ \forall j \in \{+,-\}\ \forall d \in D \tag{C8}$$

$$-q_i^d \cdot d_i \cdot \delta_{l\_}^j V_l^{\delta j}\_V_i^d \le \delta_{l\_}^j V_l^{\delta j}\_N_i^d \le q_i^d \cdot d_i \cdot \delta_{l\_}^j V_l^{\delta j}\_V_i^d \quad \forall l \in L\ \forall j \in \{+,-\}\ \forall d \in D \tag{C9}$$

$$M_i^d - \left(1-\delta_{l\_}^j V_l^{\delta j}\_V_i^d\right)Q_s \le \delta_{l\_}^j V_l^{\delta j}\_N_i^d \le M_i^d + \left(1-\delta_{l\_}^j V_l^{\delta j}\_V_i^d\right)Q_s \quad \forall l \in L \forall j \in \{+,-\} \forall d \in D. \tag{C10}$$

D. Linearizing $\delta\_V \cdot P$

The upper limits of P contain variables and parameters. Thus, the reformulation is applied recursively. Then, the $\delta\_V \cdot P$

is represented by a new continuous variable δ_V_P with constraints (D1) - (D10).

$$\delta_{l\_}^{j} V_{l}^{\delta j} \_P_i \le P_i^{\max} \delta_{l\_}^{j} V_{l}^{\delta j} + \delta_{l\_}^{j} V_{l}^{\delta j} \_M_i^P - \delta_{l\_}^{j} V_{l}^{\delta j} \_N_i^P \quad \forall j \in \{+,-\} \forall i \in NG \tag{D1}$$

$$P_i - \left(1 - \delta_{l\_}^{j} V_{l}^{\delta j}\right) Q_s \le \delta_{l\_}^{j} V_{l}^{\delta j} \_P_i \le P_i + \left(1 - \delta_{l\_}^{j} V_{l}^{\delta j}\right) Q_s \quad \forall j \in \{+,-\} \forall i \in NG \tag{D2}$$

$$-q_i^P P_i^{\max} \delta_{l\_}^{j} V_{l}^{\delta j} \le \delta_{l\_}^{j} V_{l}^{\delta j} \_M_i^P \le q_i^P P_i^{\max} \delta_{l\_}^{j} V_{l}^{\delta j} \quad \forall j \in \{+,-\} \forall i \in NG \tag{D3}$$

$$M_i^P - \left(1 - \delta_{l\_}^{j} V_{l}^{\delta j}\right) Q_s \le \delta_{l\_}^{j} V_{l}^{\delta j} \_M_i^P \le M_i^P + \left(1 - \delta_{l\_}^{j} V_{l}^{\delta j}\right) Q_s \quad \forall j \in \{+,-\} \forall i \in NG \tag{D4}$$

$$\delta_{l\_}^{j} V_{l}^{\delta j} \_V_i^p \le V_i^p, \quad \forall j \in \{+,-\} \forall i \in NG \tag{D5}$$

$$\delta_{l\_}^{j} V_{l}^{\delta j} \_V_i^P \le \delta_{l\_}^{j} V_{l}^{\delta j}, \quad \forall j \in \{+,-\} \forall i \in NG \tag{D6}$$

$$\delta_{l\_}^{j} V_{l}^{\delta j} \_V_i^P \ge \delta_{l\_}^{j} V_{l}^{\delta j} + V_i^P - 1, \quad \forall j \in \{+,-\} \forall i \in NG \tag{D7}$$

$$-q_i^P P_i^{\max} \delta_{l\_}^{j} V_{l}^{\delta j} \_V_i^P \le \delta_{l\_}^{j} V_{l}^{\delta j} \_N_i^P \le q_i^P P_i^{\max} \delta_{l\_}^{j} V_{l}^{\delta j} \_V_i^P \quad \forall j \in \{+,-\} \forall i \in NG \tag{D8}$$

$$M_i^d - \left(1 - \delta_{l\_}^{j} V_{l}^{\delta j} \_V_i^d\right) Q_s \le \delta_{l\_}^{j} V_{l}^{\delta j} \_N_i^d \le M_i^d + \left(1 - \delta_{l\_}^{j} V_{l}^{\delta j} \_V_i^d\right) Q_s \quad \forall j \in \{+,-\} \forall i \in NG \tag{D9}$$

$$\sum_{i=1}^{N_b} GSF_{l-i} \Big(\delta_l^{+} \_V_l^{\delta +} \_P_i - \delta_l^{+} \_V_l^{\delta +} d_i + \delta_l^{+} \_V_l^{\delta +} \_M_i^d - \delta_l^{+} \_V_l^{\delta +} \_N_i^d \Big) \le L_l^{\max} + M_l^{L+} - \mathrm{N}_l^{L+} \quad \forall j \in \{+,-\} \quad \forall i \in NG. \tag{D10, D11}$$

E. Linearizing Complementary Slackness Constraints

The technique (Fortuny-Amat reformulation) of linearizing complementary slackness has been well established in [26] and [27]. All complementary slackness constraints in this article are dealt with via this technique. For example, (B5) is equivalent to (E1)-(E2). Similarly, other complementary slackness constraints can be reformed. However, after this reformulation, they are still not linear due to variable δ_V.

$$\delta_l^{+} \_V_l^{\delta +} \cdot \gamma_l^{+} \le u_l^{L+} \cdot Q_g, \quad \forall l \in L \tag{E1}$$

$$\delta_l^{+} \_V_l^{\delta +} \cdot \left(\mathrm{L}_l^{\max} + \mathrm{M}_l^{L+} - \sum_i GSF_{l-i} \left(P_i - \left(d_i - M_i^d \right) \right) \right) \le \left(1 - u_i^{L+}\right) \cdot Q_g, \quad \forall l \in L \tag{E2}$$

Therefore, we add a new constraint (E3) to remove δ_V from (E1) and (E2). Similarly, δ_V in other constraints can be removed.

$$\delta_l^{+} \_V_l^{\delta +} \ge u_l^{L+}, \quad \forall \mathrm{l} \in \mathrm{L}. \tag{E3}$$

DISCLAIMER

REFERENCES

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

[2] (Sep. 2019). *NERC Lesson Learned: Risks Posted by Firewall Firmware Vulnerability*. [Online]. Available: https://www.nerc.com/pa/rrm/ea/Lessons%20Learned%20Document%20Library/20190901_Risks_Posed_by_Firewall_Firmware_Vulnerabilities.pdf.

[3] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 659–666, Dec. 2011.

[4] R. Moslemi, A. Mesbahi, and J. M. Velni, "Design of robust profitable false data injection attacks in multi-settlement electricity markets," *IET Gener. Transm. Distrib.*, vol. 12, no. 6, pp. 1263–1270, Mar. 2018.

[5] H. Xu, Y. Lin, X. Zhang, and F. Wang, "Power system parameter attack for financial profits in electricity markets," *IEEE Trans. Smart Grid*, vol. 11, no. 4, pp. 3438–3446, Jul. 2020.

[6] G. Liang, S. R. Weller, F. Luo, J. Zhao, and Z. Y. Dong, "Generalized FDIA-based cyber topology attack with application to the Australian electricity market trading mechanism," *IEEE Trans. Smart Grid*, vol. 9, no. 4, pp. 3820–3829, Jul. 2018.

[7] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "A framework for cyber-topology attacks: Line-switching and new attack scenarios," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 1704–1712, Mar. 2019.

[8] M. Esmalifalak, H. Nguyen, R. Zheng, L. Xie, L. Song, and Z. Han, "A stealthy attack against electricity market using independent component analysis," *IEEE Syst. J.*, vol. 12, no. 1, pp. 297–307, Mar. 2018.

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

[10] A. Tajer, "False data injection attacks in electricity markets by limited adversaries: Stochastic robustness," *IEEE Trans. Smart Grid*, vol. 10, no. 1, pp. 128–138, Jan. 2019.

[11] H. Ye, Y. Ge, X. Liu, and Z. Li, "Transmission line rating attack in two-settlement electricity markets," *IEEE Trans. Smart Grid*, vol. 7, no. 3, pp. 1346–1355, May 2016.

[12] D.-H. Choi and L. Xie, "Ramp-induced data attacks on look-ahead dispatch in real-time power markets," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1235–1243, Sep. 2013.

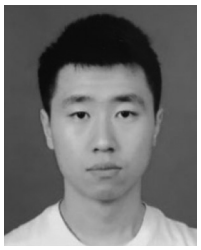
[13] C. Liu, M. Zhou, J. Wu, C. Long, and D. Kundur, "Financially motivated FDI on SCED in real-time electricity markets: Attacks and mitigation," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 1949–1959, Mar. 2019.

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

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

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

[17] S. Tan, W.-Z. Song, M. Stewart, J. Yang, and L. Tong, "Online data integrity attacks against real-time electrical market in smart grid," *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 313–322, Jan. 2018.
[18] L. Jia, J. Kim, R. J. Thomas, and L. Tong, "Impact of data quality on real-time locational marginal price," *IEEE Trans. Power Syst.*, vol. 29, no. 2, pp. 627–636, Mar. 2014.
[19] D.-H. Choi and L. Xie, "Sensitivity analysis of real-time locational marginal price to SCADA sensor data corruption," *IEEE Trans. Power Syst.*, vol. 29, no. 3, pp. 1110–1120, May 2014.
[20] D.-H. Choi and L. Xie, "Economic impact assessment of topology data attacks with virtual bids," *IEEE Trans. Smart Grid*, vol. 9, no. 2, pp. 512–520, Mar. 2018.
[21] N. A. Ruhi, K. Dvijotham, N. Chen, and A. Wierman, "Opportunities for price manipulation by aggregators in electricity markets," *IEEE Trans. Smart Grid*, vol. 9, no. 6, pp. 5687–5698, Nov. 2018.
[22] F. Li, Y. Wei, and S. Adhikari, "Improving an unjustified common practice in ex post LMP calculation," *IEEE Trans. Power Syst.*, vol. 25, no. 2, pp. 1195–1197, May 2010.
[23] J. Fortuny-Amat and B. McCarl, "A representation and economic interpretation of a two-level programming problem," *J. Oper. Res. Soc.*, vol. 32, no. 9, pp. 783–792, 1981.
[24] F. Ding, Y. Zhang, J. Simpson, A. Bernstein, and S. Vadari, "Optimal energy dispatch of distributed PVs for the next generation of distribution management systems," *IEEE Open Access J. Power Energy*, vol. 7, pp. 287–295, 2020.
[25] Q. Zhang, F. Li, H. Cui, R. Bo, and L. Ren, "Market-level defense against FDIA and a new LMP-disguising attack strategy in real-time market operations," *IEEE Trans. Power Syst.*, vol. 36, no. 2, pp. 1419–1431, Mar. 2021.
[26] S. Pineda and J. M. Morales, "Solving linear bilevel problems using big-Ms: Not all that glitters is gold," *IEEE Trans. Power Syst.*, vol. 34, no. 3, pp. 2469–2471, May 2019.
[27] A. J. Conejo and C. Ruiz, "Complementarity, not optimization, is the language of markets," *IEEE Open Access J. Power Energy*, vol. 7, pp. 344–353, 2020.
[28] F. Li and R. Bo, "Small test systems for power system economic studies," in *Proc. IEEE PES Gen. Meeting*, Minneapolis, MN, USA, Jul. 2010, pp. 1–4.



Qiwei Zhang (Graduate Student Member, IEEE) received the B.S.E.E. degree from North China Electrical Power University in 2016, and the M.S.E.E degree from The University of Tennessee in 2018, where he is currently pursuing the Ph.D. degree with the Department of Electrical Engineering and Computer Science. His research interests include cybersecurity in power systems, power system optimization, and market operation.

Fangxing Li (Fellow, IEEE) is also known as Fran Li. He received the B.S.E.E. and M.S.E.E. degrees from Southeast University, Nanjing, China, in 1994 and 1997, respectively, and the Ph.D. degree from Virginia Tech, Blacksburg, VA, USA, in 2001. He is currently the James W. McConnell Professor of Electrical Engineering and the Campus Director of the CURENT, University of Tennessee, Knoxville, TN, USA. His current research interests include renewable energy integration, demand response, distributed generation and microgrid, energy markets, and power system computing. He is currently serving as the Editor-in-Chief for IEEE OPEN ACCESS JOURNAL OF POWER AND ENERGY and the Chair of IEEE/PES Power System Operation, Planning and Economics Committee.