IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

IEEE ON IEEE POWER & ENERGY SOCIETY SECTION

Received October 9, 2020, accepted November 1, 2020, date of publication November 17, 2020, date of current version December 7, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.3038527

Preventive Dispatch Strategy Against FDIA Induced Overloads in Power Systems With High Wind Penetration

KEHE WU[1], JIAWEI LI[1], BO ZHANG[3], ZONGCHAO YU[2], (Graduate Student Member, IEEE), AND XUAN LIU[2], (Member, IEEE)

[1]Electrical and Information Engineering, North China Electric Power University, Beijing 102206, China
[2]Electrical and Information Engineering, Hunan University, Changsha 410082, China
[3]Global Energy Internet Research Institute, Beijing 102206, China

Corresponding author: Xuan Liu (xliu@hnu.edu.cn)

This work was supported in part by the National Natural Science Foundation of China under Grant 51777062, and in part by the Project of the Industrial Internet Innovation and Development: Smart Energy Internet Security Situational Awareness.

ABSTRACT The penetration of renewable energy generations, e.g., wind power, not only introduces the randomness and fluctuations into power system operations but also increases the possibilities of cybersecurity issues. Among them, false data injection attack (FDIA) can access and falsify the readings of smart meters, which would impede the functionalities of power systems. In this paper, we first set up an evaluation model to identify the set of high-risk lines by investigating the relationship between FDIA and wind power uncertainty. Then, for a power system with a high wind penetration, a tri-level preventive dispatch strategy is proposed to ensure the system security even under the worst-case of FDIA. It is demonstrated that the impacts of FDIA can cause more serious security issues as the wind penetration level increases. The effectiveness of the proposed tri-level preventive dispatch strategy in mitigating the FDIA caused overloading risk is validated using the IEEE 118-bus system.

INDEX TERMS FDIA, high-risk line, line overloads, preventive dispatch strategy, wind power.

I. INTRODUCTION

With the growing penetration of renewable energy resources, advanced information and control infrastructures, current power systems integrate multi-source electrical networks and multiple information networks [1]–[3]. The rapid increasing penetration of wind power helps significantly alleviate potential energy and environmental crises. The proportion of wind power output reached more than 30% of electricity demand in Iowa and South Dakota in 2016 [4]. In 2018, the total installed capacity of wind power in the world achieved approximately 591.55GW, and China accounted for more than 35% [5]. Furthermore, the Global Wind Energy Council (GWEC) expects that a quarter of the world electricity can be provided by renewable energy in 2035 [6]. Also, the advanced information and communication technologies are widely adopted for enhancing power system efficiency, which inherently induces potential cyber vulnerabilities. Here, this paper aims to address the cybersecurity issues in power systems with high wind penetration.

In recent years, cyber-attacks pose a great threat to the secure operation of power systems, and the recent cyber events proved the plausibility of the cyber-attacks against power grids in real life. In 2015, a massive power outage occurred in Ukraine's power grid caused by an automatic malware cyber-attack [7]. In July 2017, a nuclear power plant in the United States was attacked by digital attacks from cyber hackers [8]. Also, cyber-attackers invaded the Irish power grid by breaking the routers and illegally obtaining some communication information from the company in August 2017 [9].

These cyber-attack incidents and the corresponding severe impacts have raised extensive concerns about the emerging cybersecurity threats in smart grids. Great efforts have been committed to research on false data injection attacks (FDIA). The FDIA can distort the meter measurements by injecting a set of predetermined false data in a concealed fashion by bypassing the existing bad data detection (BDD) [10]. The set of contaminated measurements can mislead the decision-making of the control center, which would cause transmission line overloads [11], [12] and even cascading failures [13] in the system. In [11], an optimization model was proposed for determining the worst-case of cyber-overloading attacks. Reference [12] proposed a model to minimize the number of attacked measurements while maintaining transmission line at a high loading level. In [13],

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

a multi-stage screening model was proposed to identify the severe cascading failures. Reference [14] demonstrated that the adversaries with imperfect information can also launch effective false data injection attacks in electricity markets. Moreover, reference [15] revealed that attackers can earn profits from the electricity market by modifying the load and generation distribution. It indicates that wind power and load can be tampered to launch a combination attack, and the uncertainty of wind power would make tampered data more difficult to be detected. Some detection methods considering the spatiotemporal patterns of load and wind power have been studied in [16], [17]. However, these existing approaches only consider the variable wind power as uncertainties while ignoring the potential cyber risks. No corresponding preventive dispatch strategy has been proposed to mitigate the combined risk of FDIA against loads and forecasted wind power data.

The operator uses the forecasted loads and wind power as the input data of the security constraint economic dispatch (SCED) model to obtain the dispatch solution. Then, the accuracy of the forecasted wind power would impact the system security. If the predicted wind power outputs are maliciously modified, the improper decision-making might result in severe power system security issues. It is revealed that wind power can cause system security problems, e.g., line overloads [18], [19]. Recently, reinforcement learning is applied to improve the accuracy of FDIA detection and wind power prediction [20]–[22]. However, these methods fail to reduce the cyber security risk, in which wind power data may be tampered. The predicted wind power data is usually transmitted remotely from the wind farm to the control center in plaintext, while the defense measures during the data transmission process is insufficient. In 2017, researchers at the University of Tulsa conducted penetration tests on five wind farms, and all these wind farms failed to withstand hackers [23].

However, all the existing literature [10]–[19] ignored the factor that wind data could be tampered, and most of them studied the FDIAs and forecasted wind power separately. This is not consistent with the real situation in the power grid, because renewable energy is highly integrated into the power system. In [24], a cyber-security corrective dispatch scheme was proposed to mitigate the line overloads caused by FDIAs while the impact of wind power was not considered. Different from the existing work, this paper aims to investigate the combined risk of FDIA against loads and forecasted wind power data in the power system with high wind penetration (denoted as FDIA-DW) by answering the following questions: 1) Will the risk level of the system be significantly underestimated without considering the FDIA against forecasted wind power? And will the penetration of wind power cover the risk of FDIA? 2) How to adjust the dispatch strategy to mitigate the FDIA caused overloading risks in power systems with high wind power penetration? These questions motivate us to propose an evaluation model and develop a preventive dispatch strategy as effective countermeasures. Noting that the focus of this paper is not to study the FDIA attack and then the attack mechanism of an FDIA is the same as that in the existing literature. The main contributions of this paper are summarized as follows:

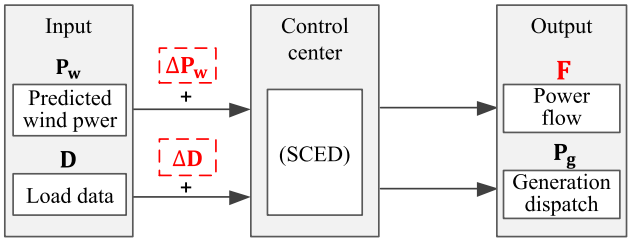

FIGURE 1. Schematic diagram of a power system dispatch strategy.

1. We take the first attempt to analyze the risk of wind power be tampered, and investigate the risk of FDIA-DW in the system with high wind penetration by formulating an evaluation model of line overloads.

2. We demonstrate that the relationship between the FDIA-DW and the penetration level of wind power is not a simple linear one, and show that the high integration of wind power could cover the risk of FDIA.

3. We propose a tri-level preventive dispatch for mitigating the FDIA-DW caused transmission line overloads with considering the worst-case. A Benders-like decomposition method is proposed to solve the tri-level model.

4. We demonstrate that the proposed preventive strategy can effectively eliminate the line overloading risk by determining a cost-efficient strategy.

II. EVALUATION MODEL OF THE RISK OF FDIA

In this section, we first study the mechanism of FDIA-DW induced overloads. Then, we formulate a linear programming model to evaluate the risk of line overloads.

A. PRINCIPLE OF FDIA-DW INDUCED OVERLOADS

The dispatch strategy (such as thermal power output $\mathbf{P_g}$ and wind power $\mathbf{P_w}$) is usually determined by the SCED model. In Fig.1, in the absence of cyber-attacks, the power flow $\mathbf{F}$ is calculated based on the predicted wind power $\mathbf{P_w}$ and load data $\mathbf{D}$, and the power flow $\mathbf{F}$ also satisfies the system security constraints. However, the predicted data of wind power outputs and loads may be tampered by attackers. In such circumstances, the power flow $\mathbf{F}$ will be modified and the security constraints might be violated. In Fig.1, the power flow $\mathbf{F}$ (red font) represents the false power flow due to the false data injections of $\Delta\mathbf{P_w}$ and $\Delta\mathbf{D}$.

On one hand, the load data $\mathbf{D}$ can be maliciously modified. Liu *et al.* [11] first studied the principle of FDIA and revealed that an attacker can construct an attacking vector that can avoid being detected by the state estimator. The false data induces the control center to make the incorrect dispatch strategy that causes severe line overloads. To bypass the BDD, the attacking vector is usually limited to a certain range and designed as a vector with a sum of zero [24], stated as:

$$\mathbf{1^T} \cdot \Delta\mathbf{D} = 0 \tag{1.1}$$

$$-\varepsilon \cdot \mathbf{D} \leq \Delta\mathbf{D} \leq \varepsilon \cdot \mathbf{D} \tag{1.2}$$

Constraint (1.1) ensures the power balance in the system, and constraint (1.2) limits the attacked level for each measurement. A larger value of ε represents a more serious attack.

In the presence of attacking vector $\Delta\mathbf{D}$, the original power flow will be modified and rewritten as:

$$\mathbf{F} = \mathbf{SF} \cdot \left(\mathbf{KP} \cdot (\mathbf{P_g} + \mathbf{P_w}) - \mathbf{KD} \cdot (\mathbf{D} + \Delta\mathbf{D})\right) \quad (1.3)$$

$$-\mathbf{F^r} \leq \mathbf{F} \leq \mathbf{F^r} \quad (1.4)$$

where $\mathbf{F^r}$ represents the line flow limit vector. Because line flows in (1.3) are calculated based on the corrupted load vector $\mathbf{D}+\Delta\mathbf{D}$, constraint (1.4) only enforces the false power flow vector $\mathbf{F}$. In other words, the security of the actual line flows cannot be ensured.

Since the true load vector is $\mathbf{D}$, and the true line flow $\mathbf{F^0}$ is:

$$\mathbf{F^0} = \mathbf{SF} \cdot \left(\mathbf{KP} \cdot (\mathbf{P_g} + \mathbf{P_w}) - \mathbf{KD} \cdot \mathbf{D}\right) \quad (1.5)$$

Introducing (1.5) to (1.3), there is:

$$\mathbf{F} = \mathbf{F^0} - \mathbf{SF} \cdot \mathbf{KD} \cdot \Delta\mathbf{D} \quad (1.6)$$

By introducing (1.6) to (1.4), we have:

$$-\mathbf{F^r} + \mathbf{SF} \cdot \mathbf{KD} \cdot \Delta\mathbf{D} \leq \mathbf{F^0} \leq \mathbf{F^r} + \mathbf{SF} \cdot \mathbf{KD} \cdot \Delta\mathbf{D} \quad (1.7)$$

In (1.7), the upper and lower bounds of the true power flows can exceed the line flow limit vector $\mathbf{F^r}$ due to the false data $\mathbf{SF} \cdot \mathbf{KD} \cdot \Delta\mathbf{D}$. This implies that the attacker can construct the attacking vector $\Delta\mathbf{D}$ to cause the target lines to be physical overloads.

On the other hand, due to the proliferation of wind power in power systems, the prediction errors may also cause some line overloads [18], [19]. Moreover, the predicted wind power data might be tampered due to the insufficient cybersecurity defense resources in current wind farms. Besides, the tampered wind data are difficult to be detected because of the strong stochastic and variable nature of wind power. The variation of wind power in 10 minutes can reach 20% in 2009, which provides natural coverage to the injected false data of the predicted wind power [25], [26].

However, the existing FDIA studies failed to consider the data attacks targeting the forecasted wind power $\mathbf{P_w}$, and the cyber risk might be underestimated. Here, we will investigate the cyber risk of a power system with high wind penetration by considering the FDIA targeting loads and predicted wind power data. Fig.2 illustrates the principle of the FDIA-DW induced line overloads.

Based on (1.3), assuming that there is another attacking vector $\Delta\mathbf{P_w}$ injected into the predicted wind power, the true line flow $\mathbf{F^0}$ is stated as:

$$\mathbf{F^0} = \mathbf{SF} \cdot \left(\mathbf{KP} \cdot (\mathbf{P_g} + \mathbf{P_w} + \Delta\mathbf{P_w}) - \mathbf{KD} \cdot (\mathbf{D} + \Delta\mathbf{D})\right) \quad (2.1)$$

Accordingly, constraint (1.7) is rewritten as:

$$\begin{cases} \mathbf{F^0} \leq \mathbf{F^r} + \mathbf{SF} \cdot (\mathbf{KP} \cdot \Delta\mathbf{P_w} + \mathbf{KD} \cdot \Delta\mathbf{D}) \\ \mathbf{F^0} \geq -\mathbf{F^r} + \mathbf{SF} \cdot (\mathbf{KP} \cdot \Delta\mathbf{P_w} + \mathbf{KD} \cdot \Delta\mathbf{D}) \end{cases} \quad (2.2)$$

Constraint (2.2) indicates that the true power flow vector $\mathbf{F^0}$ could exceed the line flow limit vector $\mathbf{F^r}$ due to the false data $\mathbf{SF} \cdot \mathbf{KD} \cdot \Delta\mathbf{D}$ and $\mathbf{SF} \cdot \mathbf{KP} \cdot \Delta\mathbf{P_w}$. The FDIA will cause more serious line overloads in the power grid when the attacks against wind power data are considered. The FDIA-DW caused overloading level will be analyzed by construing the corresponding evaluation model in the next subsection.

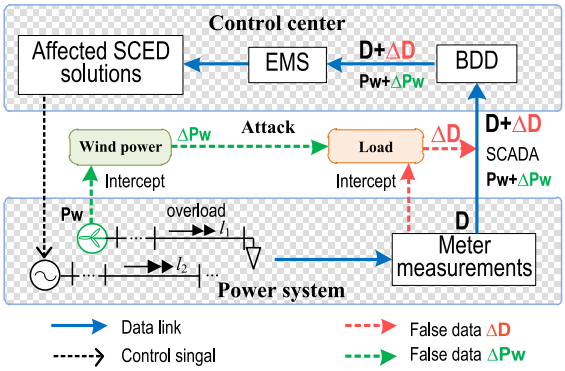

FIGURE 2. Illustration of the line overloads induced by the FDIA-DW.

B. EVALUATION MODEL OF LINE OVERLOADS

Normally, in an FDIA, the meter reading of a thermal generator cannot be easily falsified due to the strong communication between the control center and power plants. But the predicted wind power value can be injected by false data $\Delta\mathbf{P_w}$. Specifically, stealthy adversaries can elaborately construct the false data combining $\Delta\mathbf{P_w}$ with $\Delta\mathbf{D}$ for deteriorating power system security.

This motivates us to think about the following questions: 1) Can the FDIA-DW cause more serious security problems, and if so, how to evaluate the corresponding impacts? 2) What is the deep relationship between an FDIA and wind power uncertainty? 3) Will does a higher wind power integration aggravate the FDIA impacts on system security? To answer these questions comprehensively, we formulate a linear programming model to assess the risk of line overloads caused by the FDIA-DW, which are stated as follows:

$$\max: |F_l| / F_l^r \quad (3.1)$$

$$\text{s.t. } \mathbf{1^T} \cdot \Delta\mathbf{D} = \mathbf{1^T} \cdot \mathbf{\Delta P_w} \quad (3.2)$$

$$-\varepsilon \cdot \hat{\mathbf{D}} \leq \Delta\mathbf{D} \leq \varepsilon \cdot \hat{\mathbf{D}} \quad (3.3)$$

$$-\delta \cdot \hat{\mathbf{P}}_\mathbf{w} \leq \mathbf{\Delta}\ \mathbf{P_w} \leq \delta \cdot \hat{\mathbf{P}}_\mathbf{w} \quad (3.4)$$

$$\mathbf{F} = \mathbf{SF} \cdot \left(\mathbf{KP} \cdot (\hat{\mathbf{P}}_\mathbf{g} + \hat{\mathbf{P}}_\mathbf{w} + \Delta\mathbf{P_w}) - \mathbf{KD} \cdot (\hat{\mathbf{D}} + \Delta\mathbf{D})\right) \quad (3.5)$$

where the values of $\hat{\mathbf{P}}_\mathbf{g}$, $\hat{\mathbf{P}}_\mathbf{w}$ and $\hat{\mathbf{D}}$ are calculated using the traditional SCED model. The objective (3.1) represents the maximum overloading level for each line in the system caused by the FDIA-DW. Constraint (3.2) ensures the system power balance under FDIAs, and constraints (3.3) and (3.4) limit the attacked range of loads and wind power. Equation (3.5) represents the true power flow on each line. Here, the parameters ε and δ represent the attacking magnitude for loads and predicted wind power, which will be discussed in Section V. Normally, a high accuracy wind power forecasting

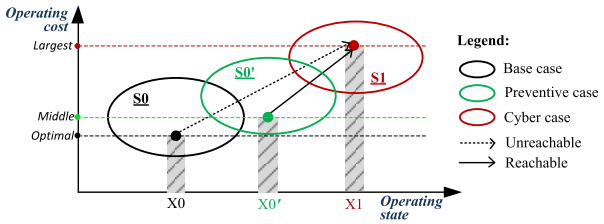

FIGURE 3. Illustration of the proposed preventive dispatch strategy.

corresponds to a small value of δ, and a low accuracy wind power forecasting corresponds to a larger value of δ. This is because if the prediction accuracy of wind power is low, $\Delta\mathbf{P_w}$ is more likely to be mistaken as caused by the prediction error of wind power, rather than malicious tampering by the attacker. On the other hand, if the value of δ is equal to 0, the constraints (3.2), (3.3) and (3.4) will become the traditional FDIA constraints (3.2) and (3.3). In this situation, this evaluation model can calculate the maximum overloading level for each line caused by the traditional FDIA, which will be used as a benchmark to compare the risks caused by FDIA-DW in Section V.

Based on the evaluation model, we can determine the maximum overloading level in the worst-case of FDIA-DW. Also, we can analyze the deep relationship between the cyber risk and wind power penetration level, as presented in Section V. In the next section, we will discuss how to adjust the dispatch strategy for mitigating the security problems.

III. MATHEMATICAL FORMULATION OF THE PREVENTIVE DISPATCH MODEL

In this section, we will first study the principle of the preventive dispatch strategy. Then, a tri-level optimization model is formulated in subsection B for effectively mitigating the FDIA-DW caused line overloads.

A. THE PRINCIPLE OF THE PREVENTIVE DISPATCH STRATEGY

To address line overloads caused by the FDIA, a preventive dispatch strategy is proposed in this paper, whose principle is discussed below.

The proposed preventive dispatch strategy employs the corrective action, which offers a cost-efficient strategy for mitigating the risk of potential FDIA-DW. In Fig.3, S0, S0', and S1 represent the base case, preventive case, and cyber case, respectively, where the operating states X0, X0′, and X1 represent the corresponding optimal operation status of each case. The arrows describe the corrective action, which represent post-contingency control adjustments for eliminating controllable contingencies. The principle of the proposed preventive dispatch strategy is illustrated in Fig.3. In normal conditions, the power system operates on the optimal state X0 determined by the SCED model. If the power system is attacked by an FDIA-DW, the system fails to shift from states X0 to X1 because some security constraints would be violated. Therefore, the proposed preventive dispatch strategy is applied to find a sub-optimal state X0′, which can ensure that the system can be successfully transferred to state X1 while

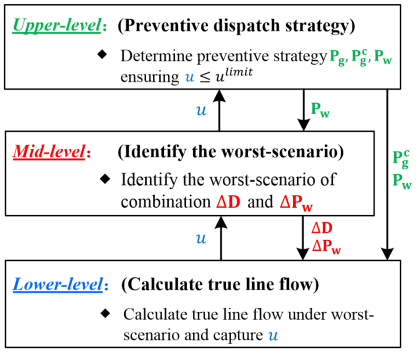

FIGURE 4. The tri-level model of the preventive dispatch strategy.

satisfying the security constraints even when the worst-case attack scenario occurs. Then, the risk of line overloads caused by the FDIA-DW is mitigated effectively. Here, the generator ramping constraint should be satisfied from state X0′ to state X1, which is stated as:

$$\left|\mathbf{P_g^{X0'}} - \mathbf{P_g^{X1}}\right| \le \mathbf{R_g} \tag{4}$$

where $\mathbf{P_g^{X0'}}$ and $\mathbf{P_g^{X1}}$ represent the generations under states X0′ and X1, respectively, and $\mathbf{R_g}$ represents the ramping limit vector of generators.

According to the mechanism of the preventive dispatch strategy, we can formulate a tri-level optimization model to mitigate line overloads caused by the FDIA-DW. Fig.4 shows the relationships between each level.

Upper: The upper level determines the proposed preventive dispatch strategy ($\mathbf{P_g}$, $\mathbf{P_g^c}$, and $\mathbf{P_w}$) for the system with high wind penetration. Then, the values of $\mathbf{P_g^c}$ and $\mathbf{P_w}$ are transferred to the middle and lower levels.

Mid: In the middle level, the worst-case scenario of the FDIA is identified to maximize the overloading level. The values of $\Delta\mathbf{D}$, $\Delta\mathbf{P_w}$ in the worst-scenario will be delivered to the lower level.

Lower: The lower level calculates the true line power flow based on $\mathbf{P_g^c}$ and $\Delta\mathbf{D}$, $\Delta\mathbf{P_w}$ determined by the upper and middle levels. The obtained maximum overloading level u will be sent to the upper level for updating the preventive dispatch strategy.

B. FORMULATION OF TRI-LEVEL MODEL

The mathematical formulation of the proposed preventive dispatch strategy is formed as follows:

$$\min : \mathbf{C_g^T} \cdot \mathbf{P_g} \tag{5.1}$$

$$\text{s.t. } \mathbf{1^T}(\mathbf{P_g} + \mathbf{P_w}) = \mathbf{1^T D} \tag{5.2}$$

$$\mathbf{1^T}(\mathbf{P_g^c} + \mathbf{P_w}) = \mathbf{1^T D} \tag{5.3}$$

$$\mathbf{F} = \mathbf{SF} \cdot (\mathbf{KP} \cdot (\mathbf{P_g} + \mathbf{P_w}) - \mathbf{KD} \cdot \mathbf{D}) \tag{5.4}$$

$$\left|\mathbf{P_g} - \mathbf{P_g^c}\right| \le \mathbf{R_g} \tag{5.5}$$

$$\mathbf{0} \le \mathbf{P_w} \le \mathbf{P_w^r} \tag{5.6}$$

$$\mathbf{0} \le \mathbf{P_g} \le \mathbf{P_g^{max}} \tag{5.7}$$
$$\mathbf{0} \le \mathbf{P_g^c} \le \mathbf{P_g^{max}} \tag{5.8}$$
$$|\mathbf{F}| \le \mathbf{F^r} \tag{5.9}$$
$$u \le u^{limit} \tag{5.10}$$
$$\max : u \tag{5.11}$$
$$\text{s.t. } -\varepsilon \cdot \mathbf{D} \le \Delta\mathbf{D} \le \varepsilon \cdot \mathbf{D} \tag{5.12}$$
$$-\delta \cdot \mathbf{P_w} \le \Delta\mathbf{P_w} \le \delta \cdot \mathbf{P_w} \tag{5.13}$$
$$\mathbf{1^T} \cdot \boldsymbol{\Delta D} = \mathbf{1^T} \cdot \boldsymbol{\Delta P_w} \tag{5.14}$$
$$\min : u \tag{5.15}$$
$$\text{s.t. } \mathbf{F^c} = \mathbf{SF} \cdot \left(\mathbf{KP} \cdot (\mathbf{P_g^c} + \mathbf{P_w} + \Delta\mathbf{P_w}) - \mathbf{KD} \cdot (\mathbf{D} + \Delta\mathbf{D})\right) \tag{5.16}$$
$$\left|\mathbf{F^c}\right| \le u \cdot \mathbf{F^r} \tag{5.17}$$

1) UPPER-LEVEL

The generation cost function (5.1) is minimized in the upper level by determining the optimal dispatch strategy under the preventive case. Constraints (5.2) and (5.3) are the power balance equations for two different operating states X0′ and X1, as shown in Fig.3. The power flow on each line is determined by (5.4) under the preventive case. Constraint (5.5) represents the generator ramping limit from states X0′ to X1. Constraint (5.6) limits the lower and upper bounds of wind power integrated into the power system. Constraints (5.7) and (5.8) limit the bounds of the generation vectors for two different operating states. Constraint (5.9) gives the limitation of the line flow vector under the preventive case. Constraint (5.10) ensures the maximum overloading level u in the system would not beyond the threshold u^{limit} even under the worst-case. Since the purpose of this model is to eliminate high-risk overloading lines in the system, the threshold u^{limit} is set as 1.4 in this paper [27].

2) MID-LEVEL

The objective (5.11) is to maximize the overloading level u by identifying the worst-case scenario of the FDIA-DW. Constraints (5.12) and (5.14) limit the ranges of the attacking vector $\Delta\mathbf{D}$ and $\Delta\mathbf{P_w}$, and constraint (5.14) limits the power balance even under the cyber-attack. The values of $\Delta\mathbf{D}$ and $\Delta\mathbf{P_w}$ are sent to the lower level.

3) LOWER-LEVEL

Based on the values of $\mathbf{P_g^c}$, $\mathbf{P_w}$ and $\Delta\mathbf{D}$, $\Delta\mathbf{P_w}$ obtained from the upper and middle levels, the true line flow is calculated using (5.16) and (5.17), and the maximum overloading level u is captured in the lower level. Using the proposed tri-level model, we can find an optimal preventive dispatch strategy, which avoids overloading lines even under the worst-case of the FDIA-DW.

IV. SOLUTION METHOD FOR THE TRI-LEVEL MODEL

Here, a Benders-like decomposition method is utilized to solve the proposed tri-level preventive model in subsection A, and the detailed algorithm for solving the optimization problem is presented in subsection B.

A. DECOMPOSITION FORMULATION FOR THE PROPOSED MODEL

For the sake of brevity, the proposed preventive dispatch strategy model can be written as the following compact form:

$$\min : \mathbf{c^T x} \tag{6.1}$$
$$\text{s.t. } \mathbf{Ax} \le \mathbf{b} \tag{6.2}$$
$$u \le u^{limit} \tag{6.3}$$
$$\max : u \tag{6.4}$$
$$\text{s.t. } \mathbf{Ey} \le \mathbf{m} \tag{6.5}$$
$$\min : u \tag{6.6}$$
$$\text{s.t. } u \ge \mathbf{Gx} + \mathbf{Hy} + \mathbf{z} \quad \boldsymbol{\lambda} \tag{6.7}$$

where $\mathbf{x}$ and $\mathbf{y}$ represent all the variables in the upper and middle levels, respectively. And $\boldsymbol{\lambda}$ represents the vector of Lagrange multipliers of constraint (6.7). $\mathbf{A}$ and $\mathbf{G}$ represent the coefficient matrix of variable $\mathbf{x}$ in upper and lower levels. $\mathbf{E}$ and $\mathbf{H}$ represent the coefficient matrix of variable $\mathbf{y}$ in middle and lower levels, $\mathbf{z}$ represents the variables in the lower level.

Based on the duality theory method [24], the middle and lower levels for a given $\hat{\mathbf{x}}$ can be rewritten as:

$$\max : (\mathbf{G\hat{x}} + \mathbf{Hy} + \mathbf{z})^{\mathbf{T}}\boldsymbol{\lambda} \tag{7.1}$$
$$\text{s.t. } \mathbf{Ey} \le \mathbf{m} \tag{7.2}$$
$$\mathbf{1}^T\boldsymbol{\lambda} = 1 \tag{7.3}$$

Then, the primal problem (6) can be relaxed as:

$$\min : \mathbf{c^T x} \tag{8.1}$$
$$\text{s.t. } \mathbf{Ax} \le \mathbf{b} \tag{8.2}$$
$$(\mathbf{G\hat{x}} + \mathbf{Hy_1} + \mathbf{z})^{\mathbf{T}}\boldsymbol{\lambda_1} \le u^{limit} \tag{8.3}$$
$$(\mathbf{G\hat{x}} + \mathbf{Hy_2} + \mathbf{z})^{\mathbf{T}}\boldsymbol{\lambda_2} \le u^{limit} \tag{8.4}$$
$$\vdots$$
$$(\mathbf{G\hat{x}} + \mathbf{Hy_i} + \mathbf{z})^{\mathbf{T}}\boldsymbol{\lambda_i} \le u^{limit} \tag{8.5}$$

where i is the number of Benders-like cuts and $0 \le i < K$.

Next, we study the method for generating the Benders-like cut. Without loss of generality, we can write the general form of the Benders-like cut as:

$$\boldsymbol{\lambda}^T(\mathbf{Gx} + \mathbf{H\hat{y}} + \mathbf{z}) \le u^{limit} \tag{8.6}$$

The lower level in the proposed tri-level model is stated as:

$$\min : u \tag{10.1}$$
$$\text{s.t. } \mathbf{1}u \ge \left[\mathbf{SF} \cdot \begin{pmatrix} \mathbf{KP} \cdot \left(\mathbf{P_g^c} + \mathbf{P_w} + \Delta\mathbf{P_w}\right) \\ -\mathbf{KD} \cdot (\mathbf{D} + \Delta\mathbf{D}) \end{pmatrix}\right] ./\mathbf{F^r} \quad \overline{\boldsymbol{\gamma}} \tag{10.2}$$
$$-\mathbf{1}u \ge \left[\mathbf{SF} \cdot \begin{pmatrix} \mathbf{KP} \cdot \left(\mathbf{P_g^c} + \mathbf{P_w} + \Delta\mathbf{P_w}\right) \\ -\mathbf{KD} \cdot (\mathbf{D} + \Delta\mathbf{D}) \end{pmatrix}\right] ./\mathbf{F^r} \quad \underline{\boldsymbol{\gamma}} \tag{10.3}$$

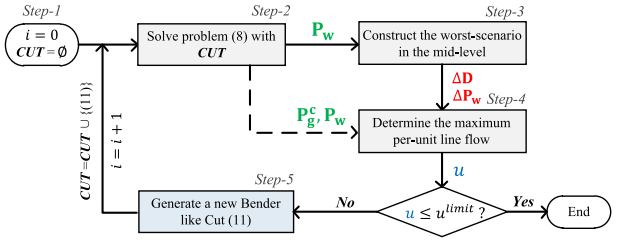

FIGURE 5. Flowchart of the solution algorithm for the proposed tri-level model.

where "./" represents an element-wise division operator, $\overline{\boldsymbol{\gamma}}$ and $\underline{\boldsymbol{\gamma}}$ are the Lagrange multipliers.

$$(\hat{\overline{\boldsymbol{\gamma}}}^{\mathrm{T}} - \hat{\underline{\boldsymbol{\gamma}}}^{\mathrm{T}}) \left[\mathbf{SF} \cdot \begin{pmatrix} \mathbf{KP} \cdot \left(\mathbf{P}_{\mathbf{g}}^{\mathbf{c}} + (\mathbf{1} + \hat{\boldsymbol{\varphi}}) .* \mathbf{P}_{\mathbf{w}} \right) \\ -\mathbf{KD} \cdot \left(\mathbf{D} + \Delta\hat{\mathbf{D}} \right) \end{pmatrix} \right] ./ \mathbf{F}^{\mathbf{r}} \leq u^{limit} \tag{11}$$

where ".*" represents an element-wise product operator, and $\hat{\boldsymbol{\varphi}} = \Delta\hat{\mathbf{P}}_{\mathbf{w}} ./ \mathbf{P}_{\mathbf{w}}$ represents the ratio of $\Delta\hat{\mathbf{P}}_{\mathbf{w}}$ to the wind power vector $\mathbf{P}_{\mathbf{w}}$. And $\mathbf{P}_{\mathbf{w}}$ is delivered from the upper-level at the same iteration. $\Delta\hat{\mathbf{D}}$ represents the attacking load vector. Constraint (11) represents the generated Benders-like cut in the proposed preventive model. According to Theorem 2 in [24], we can set $\overline{\boldsymbol{\gamma}}$ and $\underline{\boldsymbol{\gamma}}$ as binary variables without changing the solution of the tri-level model.

The primal tri-level problem (6) can be solved by iteratively solving the master problem (8) with the Benders-like cuts. First, problem (8) without any cuts is solved, and then problem (7) is solved based on the result $\hat{\mathbf{x}}$ from problem (8). If the objective value of problem (7) does not satisfy constraint (6.3), a new Benders-like cut will be generated and added into problem (8). The iteration process continues until the objective value of problem (7) is less than the threshold u^{limit}. Note that problems (8) and (7) are linear programming and mixed integer linear programming, which can be directly solved by the CPLEX solver.

B. THE SOLUTION ALGORITHM OF THE TRI-LEVEL MODEL

In Fig.5, the solution algorithm for the proposed tri-level preventive model can be summarized as below:

Algorithm of the Tri-Level Model

Step 1: Data initialization. Set the number of iteration $i = 0$. Initialize the set of Benders-like Cuts as an empty set, $\boldsymbol{CUT} = \emptyset$.

Step 2: Solve the problem (8) with set $\boldsymbol{CUT}$, determine a preventive dispatch strategy, which includes the generation under the preventive-case ($\mathbf{P_g}$), cyber-case ($\mathbf{P_g^c}$) and wind power outputs ($\mathbf{P_w}$).

Step 3: Based on the obtained $\mathbf{P_w}$ in Step 2, construct the worst-scenario of the FDIA ($\Delta\mathbf{D}$ and $\Delta\mathbf{P_w}$) according to constraints (5.12)-(5.14).

Step 4: Calculate the true line flow under the worst-scenario determined in Step 3 for capturing the maximum per-unit line flow u based on the results of $\mathbf{P_g^c}$ and $\mathbf{P_w}$.

Step 5: Check if $u \leq u^{limit}$. If not, generate a new Benders-like cut based on constraint (11), and add the new Bender-like cut into set $\boldsymbol{CUT}$ and go to Step 2. If satisfied, the iteration process stops.

V. CASE STUDY

In this section, we test the proposed evaluation model and preventive strategy on several IEEE testing systems. All the initial data come from MATPOWER 6.0 [28]. Simulations are carried out on a 3.9GHz personal computer with 8GB of RAM. The algorithm is solved by CPLEX.

A. SIMULATION SETTINGS

In this paper, 20 wind farms are added into the IEEE 118-bus system as listed in Table 1. Similar to [29], we add a wind generator every 7 buses for the first 15 wind generators, and add a wind generator every 5 buses for the other 5 wind generators. Based on the widely used piecewise-linear wind-turbine-power curve [30], the actual wind power outputs of these 20 wind farms are calculated according to 20 different historical wind speed datasets, which are obtained from

TABLE 1. The data of wind farms installation and outputs.

w	1	2	3	4	5	6	7	8	9	10
Bus	1	8	15	22	29	36	41	48	55	62
$P_{W(\mathrm{MW})}^{r}$	106	138	114	111	111	111	92	130	191	110
w	11	12	13	14	15	16	17	18	19	20
Bus	69	76	81	88	95	100	105	110	114	118
$P_{W(\mathrm{MW})}^{r}$	140	132	75	176	78	100	120	86	109	101

20 different stations in the China Meteorological Information Center [31]. The parameters of 'cut-in', 'cut-out', and 'maximum output' of method [30] are set as 1.0m/s, 14m/s, and 2.0MW for each wind turbine in this paper. It is assumed that each wind farm has 100 wind turbines and its maximum wind power output is 200MW. In Table 1, the buses of the installed wind farms and the total predicted wind power $\mathbf{P_w^r}$ are given. The total number of loads is set to 5000MW in this paper, which is allocated to each load bus.

As mentioned in Section II.B, based on the ERCOT data [26], the variation of wind speed in 10-min can reach 20% in 2009. Then, the value of δ is set as 25% and the parameter of ε is set as 25% in this paper.

B. SIMULATION RESULTS

1) CASE 1. OVERLOADING ASSESSMENT

In this case, the evaluation model is used to calculate the maximum line overloading level in the worst-case of FDIA-DW. The simulation results are shown in Table 2 and Fig.6. Column 'R_w' represents the different penetration levels of wind power in the system. And when R_w equals 1.0, the wind power is the data listed in Table 1. Columns '*FDIA-D*' and '*FDIA-DW*' represent the results of the FDIA against only load data (FDIA-D) and the FDIA against loads and wind power (FDIA-DW), respectively. Fig.6 gives the number of overload lines (bars in Fig.6 using the right Y-axis) and the maximum overloading level in the system (fold lines using

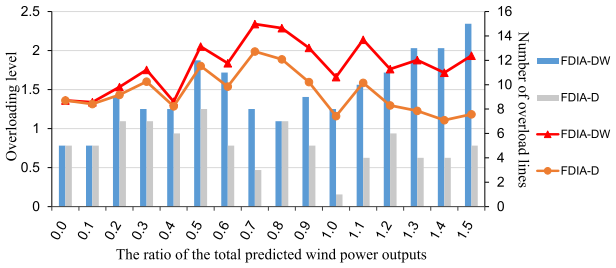

FIGURE 6. The results of the overload lines and maximum overloading level.

the left Y-axis) in different cases, and the detailed results are given in Table 2.

In Table 2 and Fig.6, the maximum overloading level '$|F_l|/F_l^r$' of the '*FDIA-DW*' case is always higher than that of the '*FDIA-D*' case, and the total number of overload lines of the '*FDIA-DW*' case is also no less than that of the '*FDIA-D*' case. When R_w is 1.0, there is only line 54 overloaded in the case '*FDIA-D*', and the maximum overloading level in case '*FDIA-D*' is 1.16. Comparatively, the total overload lines in case '*FDIA-DW*' is 8 and the maximum overloading level is 1.66, which are much larger than those in case '*FDIA-D*'. Under such a situation, if the operator fails to take into account the combined effects of the FDIA-DW, the overloading risk will be significantly underestimated.

According to [27], when the overloading level of a line is greater than 1.4, this line is likely to be tripped. In Table 2, these lines (whose maximum overloading levels are greater than 1.4) are denoted as high-risk lines that are highlighted in red. In Table 2, the number of high-risk lines of case '*FDIA-DW*' is usually larger than that of case '*FDIA-D*', especially when R_w ranges from 1.0 to 1.5.

The attacker can launch serious FDIAs to increase the risk of cascading failures by overloading some high-risk lines in the system. If we neglect the risk that wind power data might be tampered, the risk of FDIA will be underestimated and some high-risk lines will not be identified, which would make the power system vulnerable to potential FDIAs.

With the increasing wind power penetration level (R_w ranges from 1.0 to 1.5), the total number of the overloaded lines and maximum overloading level of case '*FDIA-D*' are small. More importantly, the risk of line overloads in case *FDIA-D* will become less when the high penetration level of wind power increases. This phenomenon implies that the high integration of wind power will cover the risk of FDIA. In other words, the cyber risk of a high-wind-penetrated power system might be small if we only consider the FDIA against load data (i.e., FDIA-D), but the true risk in case FDIA-DW might be very large. In this situation, the cyber risk will be significantly underestimated, which necessitates the consideration of the FDIA against both load and wind power data, i.e., FDIA-DW.

In Table 2 and Fig.6, it is observed that 1) The maximum overloading level does not necessarily increase with the increase of wind power, which implies that the relationship between the FDIA-DW and the penetration level of wind power is not a simple linear one. And the maximum overloading level of all cases always appears when the value of R_w is 0.7, which implies that a small FDIA-DW could cause a serious security problem even when wind power penetration is not high. 2) The maximum overloading level usually occurs on line 54, and such phenomenon motivates us to pay attention to a few high-risk lines, which will be discussed in the next case.

TABLE 2. The results of the overloading level in different cases.

R_w	*FDIA-D*		*FDIA-DW*	
	Line	$\|F_l\|/F_l^r$	Line	$\|F_l\|/F_l^r$
0.0	41,129,159 128,54	1.36,1.17,1.16 1.08,1.00	41,129,159 128,54	1.36,1.17,1.16 1.08,1.00
0.1	41,129,54 128,159	1.31,1.23,1.22 1.16,1.10	41,54,129 128,159	1.34,1.27,1.24 1.18,1.11
0.2	**54**,41,129 128,97,159 104	**1.43**,1.26,1.20 1.14,1.14,1.09 1.04	**54**,41,129 128,97,159 104,153,78	**1.53**,1.31,1.23 1.19,1.16,1.12 1.10,1.02,1.01
0.3	54,128,129 41,97,153 159	1.60,1.29,1.27 1.18,1.11,1.06 1.01	**54**,128,129 41,97,153 159,119	**1.75**,1.34,1.33 1.25,1.14,1.10 1.05,1.02
0.4	129,128,41 97,54,104	1.29,1.16,1.10 1.07,1.02,1.00	129,1.28,54 41,104,97 37,30	1.35,1.26,1.22 1.19,1.14,1.11 1.06,1.04
0.5	**54**,129,128 153,37,41 97,30	**1.80**,1.29,1.26 1.13,1.05,1.03 1.02,1.01	**54**,128,129 153,30,37 41,155,97 150,159,158	**2.05**,1.38,1.36 1.20,1.19,1.19 1.15,1.09,1.07 1.01,1.00,1.00
0.6	**54**,37,159 129,155	**1.54**,1.16,1.16 1.02,1.02	**54**,37,159 119,155,129 41,97,30 153,128	**1.84**,1.32,1.25 1.15,1.15,1.11 1.09,1.04,1.03 1.02,1.00
0.7	**54**,37,30	**1.99**,1.27,1.18	**54,37,30** 104,119,129 41,97	**2.34,1.46,1.42** 1.21,1.14,1.05 1.04,1.01
0.8	**54**,37,159 30,129,104 119	**1.89**,1.38,1.25 1.11,1.06,1.04 1.00	**54,37,30** 159,104,119 129	**2.29,1.59,1.40** 1.38,1.31,1.23 1.18
0.9	**119,54**,37 127,104	**1.60,1.58**,1.11 1.10,1.06	**54,119**,104 37,127,30 126,121,41	**2.03,1.85**,1.36 1.35,1.30,1.28 1.18,1.04,1.00
1.0	54	1.16	**54**,119,104 30,41,185 8,37	**1.66**,1.27,1.26 1.18,1.09,1.07 1.04,1.01
1.1	**54,37**,129 128	**1.59,1.43**,1.22 1.03	**54,37,129** 128,185,41 30,96,104 119	**2.14,1.72,1.40** 1.29,1.26,1.23 1.17,1.14,1.10 1.07
1.2	119,54,104 37,30,127	1.30,1.16,1.15 1.11,1.06,1.05	**54,119,104** **30,37**,127 185,126,41 121,129	**1.76,1.64,1.56** **1.48,1.43**,1.31 1.18,1.15,1.13 1.03,1.02
1.3	54,37,119 104	1.23,1.21,1.21 1.05	**54,119,37** **104**,185,30 127,41,126 129,79,121 96	**1.88,1.57,1.56** **1.49**,1.33,1.28 1.26,1.13,1.09 1.09,1.06,1.03 1.00
1.4	37,119,185 54	1.11,1.09,1.05 1.01	**54,119,37** **185,104**,30 127,79,129 41,121,118 126	**1.72,1.49,1.48** **1.45,1.40**,1.38 1.20,1.19,1.17 1.11,1.04,1.02 1.00
1.5	54,185,79 129,37	1.18,1.14,1.04 1.01,1.00	**54,185,30** **119,37**,79 104,129,127 97,41,118 128,121,69	**1.93,1.57,1.48** **1.41,1.40**,1.34 1.27,1.24,1.13 1.10,1.09,1.08 1.06,1.06,1.05

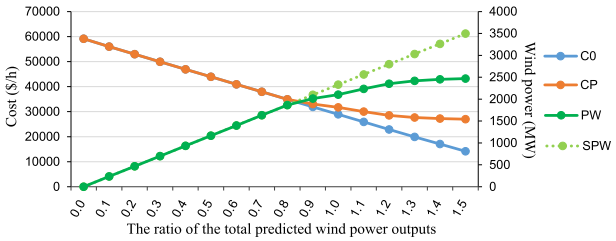

FIGURE 7. The results of the generation costs and wind power outputs in case B1.

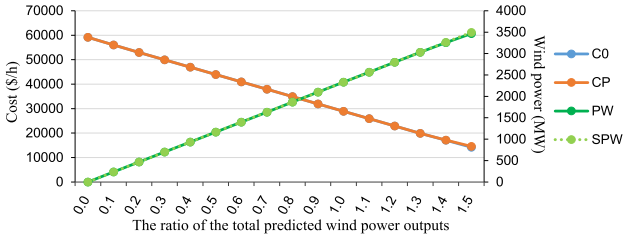

FIGURE 8. The results of the generation costs and wind power outputs in case B2.

TABLE 3. The results of generation costs and wind power outputs in case B2.

R_W	C0($/h)	CP($/h)	PW(MW)	SPW(MW)	CUT
0.0	59142	59142	0.0	0.0	0
0.1	56022	56022	233.1	233.1	0
0.2	52947	52947	466.2	466.2	0
0.3	49943	49943	699.3	699.3	0
0.4	46939	46939	932.4	932.4	0
0.5	43935	43935	1165.5	1165.5	0
0.6	40931	40931	1398.6	1398.6	0
0.7	37927	37927	1631.7	1631.7	1
0.8	34923	34923	1864.8	1864.8	1
0.9	31918	31918	2097.9	2097.9	1
1.0	28914	28914	2331.0	2331.0	2
1.1	25910	25910	2564.1	2564.1	1
1.2	22906	22906	2797.2	2797.2	1
1.3	19913	19913	3030.3	3030.3	3
1.4	17039	17138	3255.4	3263.4	5
1.5	14165	14555	3464.9	3496.5	5

2) CASE 2. PREVENTIVE DISPATCH STRATEGY

This case aims to validate the effectiveness of the proposed preventive dispatch strategy in mitigating FDIA caused overloading risks. Here, the values of δ and ε are both set as 25%, and the value of u^{limit} is set as 1.4. Without loss of generality, the power flow limit of line 2 is changed to 500MW.

First, we use the IEEE 118-bus system to test the proposed tri-level preventive model under different R_w on this case (case B1). The results of case B1 are shown in Fig.7, and the left Y-axis and right Y-axis represent the total generation costs ($/h) and the total wind power (MW), respectively. The curves of 'C0' and 'CP' in Fig.7 represent the generation costs under the based-case (the upper-level model without constraint (5.10)) and preventive-case (the whole tri-level model). And curves of 'PW' and 'SPW' represent the total wind power $\mathbf{P_w}$ and the total predicted wind power $\mathbf{P_w^r}$, and these two lines use the right Y-axis.

In Fig.7, when R_w ranges from 0.0 to 0.8, the generation cost (CP) of the preventive-case is nearly the same as the cost (C0) of the based-case. The cost (CP) is much larger than the cost (C0) when R_w ranges from 0.9 to 1.5, while the total wind power output PW grows slowly. This implies that the system needs curtail some wind power for ensuring the system security when wind penetration is relatively high. However, this is not the fact what the operator expects, because even though the combined risk of FDIA-DW is eliminated by this preventive dispatch, the cost (CP) of the preventive dispatch is much higher than the cost (C0) of the base-case.

By revisiting the analyses in case A, the maximum overloading level usually occurs on line 54. Does this high-risk line, which is easily overloaded by the FDIA-DW, affect the integration of wind power? This motivates us to establish case B2, in which case the power flow limit of line 54 is increased to 500MW. The results of this case are shown in Fig.8, and the detailed results are given in Table 3.

In Figs.7 and 8, the generation cost (CP) in case B2 is always no larger than that in cases B1. The generation cost (CP) of the preventive-case is nearly the same as the cost (C0) of the based-case for each R_w. The total wind power (PW) of the preventive-case is almost equal to the total predicted wind power outputs (SPW), which indicates that the system can guarantee the security of the system under the FDIA-DW while without curtailing too much wind power. Then, we can conclude that line 54 is a key line of the IEEE 118-bus system, which should be strengthened in advance to ensure a more secure and economical operation of the power system.

In addition, in Table 3, the cost of CP is the same as that of C0 when R_w ranges from 0.0 to 1.3. And the cost of CP is slightly higher than the cost of C0 for other values of R_w, the largest difference is 390 ($/h) when R_w is 1.5. The maximum abandoned wind power is 31.6MW when R_w is 1.5, which implies that the system can accommodate wind power effectively. Column 'CUT' denotes the number of the Bender-like cuts (number of iterations) added into the master problem (8), and the largest value of CUT is 5, which means that the proposed decomposition method is capable of obtaining the optimal solution to the tri-level preventive model after a few iterations. It is demonstrated that the proposed tri-level preventive dispatch strategy can ensure the power system security in a cost-efficient fashion.

3) CASE 3. SOLVING TIME

In this section, we further verify the computational efficiency of the proposed preventive dispatch model using an IEEE 300-bus system and an IEEE 2383-bus system. Similar to [29], we add a wind generator every several buses in each system. The results are presented in Table 4, where '*NL*' represents the total number of transmission lines of each power system, and 'CUT' and 'TIME' represent the number of the Bender-like cuts (number of iterations) added into the master problem (8) and the total solving time, respectively.

TABLE 4. The results of solving time for different systems.

IEEE Systems	118-bus	300-bus	2383-bus
NL	186	411	2896
CUT	2	4	1
TIME(sec)	0.78	3.54	136.72

For the IEEE 118-bus system, the solving time is only 0.78 seconds, and the CUT is 2. For the IEEE 300-bus system, the solving time is only 3.54 seconds, and the CUT is 4. For the IEEE 2383-bus system, the number of iterations is 1, and the solving time is 136.72 seconds, much less than 15 minutes (i.e., the time scale of SCED). These results demonstrate that the proposed solving method can find the optimal solution by adding a few number of CUTs and feature a high scalability for handling large-scale power systems.

VI. CONCLUSION AND FUTURE WORK

In this paper, we reveal that the FDIA can cause much more serious security problems in the presence of high wind penetration, where the variable wind power would make FDIA more difficult to be detected. Hence, we propose a tri-level preventive dispatch strategy for ensuring the power system security cost-effectively even under the worst-case of the FDIA-DW.

Extensive case studies are presented to validate the effective of the proposed tri-level preventive model in mitigating the FDIA caused line overloading risks. In our future work, a fast screening method will be developed to identify the set of key lines that are strongly related to the overloading risk under the FDIA against both loads and wind power.

NOMENCLATURE

INDICES

l	subscript: index of lines
g, w	subscript: index of generators and wind turbines

PARAMETERS

u^{limit}	a per-determined flow threshold for line overloads
ε	attacking magnitude for load (p.u.)
δ	attacking magnitude for predicted wind power (p.u.)
F_l^r	upper bound of power flow on line l
$\mathbf{C_g}$	generation cost vector ($/h)
$\mathbf{D}$	load vector
$\mathbf{P_g^{max}}$	upper bound of generator output vector (MW)
$\mathbf{P_w^r}$	predicted wind power output vector (MW)
$\mathbf{F^r}$	line flow limit vector (MW)
$\mathbf{F^0}$	true line flow vector (MW)
$\mathbf{R_g}$	ramping limit vector of generators
$\mathbf{KP}$	bus-generator incidence matrix
$\mathbf{KD}$	bus-load incidence matrix
$\mathbf{SF}$	shift factor matrix
$\mathbf{P_g^{X0'}}$, $\mathbf{P_g^{X1}}$	generations under states X0′ and X1

VARIABLES

F_l	power flow on line l
u	maximum overloading level of line flows (p.u.)
$\mathbf{P_w}$	wind power output in the preventive case (MW)
$\Delta\mathbf{D}$	attacking vector (MW)
$\Delta\mathbf{P_w}$	attacking vector of forecasted wind power (MW)
$\mathbf{P_g}$, $\mathbf{P_g^c}$	generator output vector in the preventive case / cyber case in the proposed model (MW)
$\mathbf{F}$, $\mathbf{F^c}$	line flow vector in the preventive / cyber case in the proposed model (MW)
$\bar{\boldsymbol{\gamma}}$, $\underline{\boldsymbol{\gamma}}$	Lagrange multipliers (binary variables)

REFERENCES

[1] T. Ding, C. Li, C. Yan, F. Li, and Z. Bie, "A bilevel optimization model for risk assessment and contingency ranking in transmission system reliability evaluation," *IEEE Trans. Power Syst.*, vol. 32, no. 5, pp. 3803–3813, Sep. 2017.

[2] S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber–physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.

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

[4] Department of Energy. (Aug. 2017). *Energy Department Reports*. [Online]. Available: http://www.energy.gov/articles/energy-department-reportswind-energy-continues-rapid-growth-2016

[5] (Jul. 2019). *Data on Global Onshore and Offshore Wind Power in 2018*. [Online]. Available: http://news.bjx.com.cn/html/20190516/980725.shtml

[6] (2013). *Global Wind Report*. [Online]. Available: http://www.gwec.net/

[7] A. Greenberg. (Oct. 2017). *How Power Grid Hacks Work, and When You Should Panic Wired-Security*. [Online]. Available: www.wired.com/story/hacking-a-power-grid-in-three-not-so-easysteps/?mbid=social_twitter_onsiteshare

[8] B. News. (Jul. 2017). *Hackers Breached a US Nuclear Power Plant's Network*. [Online]. Available: www.bbc.com/news/world-us-canada-40538061

[9] I. I. Newspaper. (Aug. 2017). *EirGrid Targeted by 'State Sponsored' Hackers Leaving Networks Exposed to 'Devious Attack*. [Online]. Available: www.independent.ie/irish-news/news/exclusive-eirgrid-targeted-by-state-sponsored-hackers-leaving-networks-exposed-to-devious-attack-36003502.html

[10] Y. Liu, M. K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. Comput. Commun. Secur.*, Chicago, IL, USA, 2009, pp. 21–32.

[11] J. Liang, L. Sankar, and O. Kosut, "Vulnerability analysis and consequences of false data injection attack on power system state estimation," *IEEE Trans. Power Syst.*, vol. 31, no. 5, pp. 3864–3872, Sep. 2016.

[12] X. Liu and Z. Li, "Trilevel modeling of cyber attacks on transmission lines," *IEEE Trans. Smart Grid*, vol. 8, no. 2, pp. 720–729, Mar. 2017.

[13] L. Che, X. Liu, Z. Shuai, Z. Li, and Y. Wen, "Cyber cascades screening considering the impacts of false data injection attacks," *IEEE Trans. Power Syst.*, vol. 33, no. 6, pp. 6545–6556, Nov. 2018.

[14] 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.

[15] 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.

[16] M. Cui, J. Wang, and B. Chen, "Flexible machine learning-based cyber-attack detection using spatiotemporal patterns for distribution systems," *IEEE Trans. Smart Grid*, vol. 11, no. 2, pp. 1805–1808, Mar. 2020.

[17] R. Dubey, S. R. Samantaray, and B. K. Panigrahi, "An spatiotemporal information system based wide-area protection fault identification scheme," *Int. J. Electr. Power Energy Syst.*, vol. 89, pp. 136–145, Jul. 2017.

[18] M. Negnevitsky, D. H. Nguyen, and M. Piekutowski, "Risk assessment for power system operation planning with high wind power penetration," *IEEE Trans. Power Syst.*, vol. 30, no. 3, pp. 1359–1368, May 2015.

[19] M. H. Athari and Z. Wang, "Impacts of wind power uncertainty on grid vulnerability to cascading overload failures," *IEEE Trans. Sustain. Energy*, vol. 9, no. 1, pp. 128–137, Jan. 2018.
[20] E. Oh and H. Wang, "Reinforcement-Learning-Based energy storage system operation strategies to manage wind power forecast uncertainty," *IEEE Access*, vol. 8, pp. 20965–20976, 2020.
[21] C. Chen, M. Cui, F. F. Li, S. Yin, and X. Wang, "Model-free emergency frequency control based on reinforcement learning," *IEEE Trans. Ind. Informat.*, early access, Jun. 9, 2020, doi: 10.1109/TII.2020.3001095.
[22] M. Cui, J. Wang, A. R. Florita, and Y. Zhang, "Generalized graph Laplacian based anomaly detection for spatiotemporal MicroPMU data," *IEEE Trans. Power Syst.*, vol. 34, no. 5, pp. 3960–3963, Sep. 2019.
[23] (Jul. 2017). *Hackers Break Into Wind Farms*. [Online]. Available: www.aqniu.com/hack-geek/26368.html
[24] L. Che, X. Liu, and Z. Li, "Mitigating false data attacks induced overloads using a corrective dispatch scheme," *IEEE Trans. Smart Grid*, vol. 10, no. 3, pp. 3081–3091, May 2019.
[25] Y. Wan. (Mar. 2011). *Analysis of Wind Power Ramping Behavior in ERCOT*. [Online]. Available: www.nrel.gov/docs/fy11osti/ 49218.pdf
[26] G. Energy. (Mar. 2018). *Analysis of Wind Generation Impact on ERCOT Ancillary Services Requirements*. [Online]. Available: www.nrc.gov/docs/ML0914/ML091420464.pdf
[27] Y. Tian, L. Xiaoming, W. Qi, and L. Longnv, "Research on the influences of location selection and permeability of wind power generation on cascading failure," *J. Eng.*, vol. 2019, no. 16, pp. 1981–1985, Mar. 2019.
[28] R. D. Zimmerman, C. E. Murillo-Sanchez, and R. J. Thomas, "MATPOWER: steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, Feb. 2011.
[29] L. Che, X. Liu, X. Zhu, Y. Wen, and Z. Li, "Intra-interval security based dispatch for power systems with high wind penetration," *IEEE Trans. Power Syst.*, vol. 34, no. 2, pp. 1243–1255, Mar. 2019.
[30] L. Xu, X. Ruan, C. Mao, B. Zhang, and Y. Luo, "An improved optimal sizing method for Wind-Solar-Battery hybrid power system," *IEEE Trans. Sustain. Energy*, vol. 4, no. 3, pp. 774–785, Jul. 2013.
[31] *China Meteorological Information Center (CMDC) Database*. Accessed: Jan. 2019. [Online]. Available: http://data.cma.cn/dataService/cdcindex/datacode/A.0012.0001/show_value/normal.html

KEHE WU received the Ph.D. degree from the University of North China Electric Power University, Beijing, in 2009. He is currently a Professor with North China Electric Power University, the Director of the Chinese Association for Artificial Intelligence and Beijing Engineering Research Center of Electric Information Technology, and a committee member of the China Electric Power Information Standardization Committee and Professional Electric Power Information Committee of the Chinese Society for Electrical Engineering. His research interests include smart grid software technology, power information security, and deep learning.

JIAWEI LI received the B.S. degree from Beihang University, in 2016. He is currently pursuing the Ph.D. degree with the School of Computer Science and Engineering, North China Electric Power University, China. His research interests include cyber security in smart grid and network security situation awareness.

BO ZHANG received the B.S. degree from Hohai University, in 2007, and the M.Sc. degree from Southeast University, China, in 2012. He is currently an Engineer with the Global Energy Internet Research Institute, China. His research interests include cyber security in smart grid and network intrusion detection.

ZONGCHAO YU (Graduate Student Member, IEEE) received the B.S. degree in electrical engineering from the University of South China, Hengyang, China, in 2017. He is currently pursuing the Ph.D. degree with the College of Electrical and Information Engineering, Hunan University, Changsha, China. His research interests include renewable energy integration, operation, and economics of power systems.

XUAN LIU (Member, IEEE) received the B.S. and M.S. degrees from Sichuan University, China, in 2008 and 2011, respectively, and the Ph.D. degree from the Illinois Institute of Technology (IIT), Chicago, in 2015, all in electrical engineering. He is currently a Professor with the Electrical and Information Engineering Department, Hunan University, China. His research interests include smart grid security, operation, and economics of power systems.