Cyber-Resilience Enhancement and Protection for Uneconomic Power Dispatch under Cyber-Attacks

Pengfei Zhao, Chenghong Gu, *Member, IEEE,* Yucheng Ding, Hong Liu, *Member, IEEE,* Yuankai Bian and Shuangqi Li, *Student Member, IEEE*

***Abstract*—False data injection (FDI), could cause severe uneconomic system operation and even large blackout, which is further compounded by the increasingly integrated fluctuating renewable generation. As a commonly conducted type of FDI, load redistribution (LR) attack is judiciously manipulated by attackers to alter the load measurement on power buses and affect the normal operation of power systems. In particular, LR attacks have been proved to easily bypass the detection of state estimation. This paper presents a novel distributionally robust optimization (DRO) for operating transmission systems against cyber-attacks while considering the uncertainty of renewable generation. The FDI imposed by an adversary aims to maximally alter system parameters and mislead system operations while the proposed optimization method is used to reduce the risks caused by FDI. Unlike the worst-case-oriented robust optimization, DRO neglects the extremely low-probability case and thus weakens the conservatism, resulting in more economical operation schemes. To obtain computational tractability, a semidefinite programming problem is reformulated and a constraint generation algorithm is utilized to efficiently solve the original problem in a hierarchical master and sub-problem framework. The proposed method can produce more secure and economic operation for the system of rich renewable under LR attacks, reducing load shedding and operation cost to benefit end customers, network operators, and renewable generation.**

***Index Terms*—Cyber-attacks, distributionally robust optimization, false data injections, load redistribution attacks, real-time economic dispatch, transmission network.**

I. INTRODUCTION

ADVANCEMENT of information and communication technology (ICT) has a significant impact on power systems by improving operation efficiency in an interactive and dynamic paradigm [1-4]. However, power systems with high integration of ICT, consisting of cyber infrastructures, are vulnerable to cyber-attacks [5]. Cyber-attacks may originate from anonymous attackers, causing low probability/high impact consequences on power systems, such as overloading, load shedding, and uneconomical operation. Attackers launch false data injections (FDI) that deceive the energy management with wrong data injection, thus causing system operators to execute wrong actions. In 2003, Davis-Besse nuclear power plant was hacked remotely in the U.S [6]. In 2015, the cyber-attack on the Ukraine power grid has caused 225,000 customers to lose power [7]. A "denial-of-service" attack disabled a grid control system in Utah, U.S. in March 2019 [8]. Existing research of FDI attacks against power systems can be generally categorized into: i) launching valid FDI attacks with impact assessment model of attacks [9-11] and ii) designing defence strategies to protect the power system [9-11[12]].

From attacker's perspective, reference [9] proposes an attack model against AC state estimation. Rather than acquiring the complete information of entire power networks, it relaxes the requirement by only requiring network information of attack regions. Paper [10] reveals the potential link between FDI and contingency, and designs a bi-level model to mitigate maximum potential attacks. Cyber-attacks targeting at system topology including removal, addition and switching of lines are proposed in [11] to mislead decision making.

On the other side, to defend and address the impact of cyber-attacks against power systems, studies have been widely conducted using state estimation [13], game-theoretical frameworks [14] and filter based FDI detection algorithms [15]. Based on dynamic state estimation, a risk mitigation strategy is proposed to guarantee the elimination of threats from cyber-attacks [13]. Reference [15] proposes an online algorithm for FDI considering adversary, which can design stealthy attacks by Kalman filter. The proposed quick and reliable detection mechanism offers effective detection with a recovery functionality to mitigate attacks. A stochastic game-theoretic method is used to generate optimal strategies for grid defender against cyber-physical attacks in [14].

State estimation is a significant approach to filter and detect FDI in case that it misleads the operation and control of power systems by inferring with metered operational parameters [16-18]. However, it is vulnerable to malicious attacks [9, 19], such as load redistribution (LR). As a type of FDI, LR is defined as the attack on load bus measurements through increasing load at some buses and decreasing load at other buses by adversary [20]. LR attacks consequently mislead system operators with wrong load data information and thus could cause wrong dispatch schemes if corrective actions are not implemented. According to [20, 21], from an adversary's perspective, the goals of LR attacks can be categorized into immediate attacks and delayed attacks. Reference [9] proves that the residue of bad data detection can be avoided by a stealthy LR design,

This work was supported by the National Science Fund for Distinguished Young Scholars, No. 72025404. This work was supported by the National Natural Science Foundation of China (Nos. 72042018, 71621002).

P. Zhao is with the Institute of Automation, Chinese Academy of Sciences, Beijing, China and School of Artificial Intelligence, University of Chinese Academy of Sciences, Beijing, China.

P. Zhao, C.Gu (corresponding author), Y. Bian and S. Li are with the Department of Electronic & Electrical Engineering, University of Bath, Bath, UK.(email: P. Zhao@bath.ac.uk; C.Gu@bath.ac.uk; Y. Bian@bath.ac.uk and S. Li@bath.ac.uk).

Y. Ding is with the China Electric Power Research Institute, Beijing, China. (email: yjs-dyc@epri.sgcc.com.cn)

H. Liu is with the School of Electrical and Information Engineering, Tianjin University, Tianjin, China. (email: liuhong@tju.edu.cn).

which can evade detection. Therefore, adversaries can manipulate these masked and hidden attacks, consequently causing a series of disruptive impacts on power systems, e.g., equipment overheating and even cascading failures.

In addition to physical disruptions, the disruptions of LR attacks on power system operation could cause huge economic loss as the system operator may deliver wrong dispatch schedules after attackers manipulate falsified measurement vectors. Under the masking and failed detection of LR, it is of high necessity to ensure the supply security and mitigate the uneconomic dispatch under potential LR attacks.

Economic dispatch (ED) is one of the most significant decision-making problems in power system operation that could be affected by LR attacks. A corrective dispatch scheme is proposed for an ED problem considering LR attacks that can evade the detection [22], which aims at mitigating overloading under the worst-case attack scenarios. Reference [23] proposes a network-constrained unit commitment model against cyber-attacks considering the worst-case LR attacks. Both papers use robust optimization (RO) based models [22, 23], which ensure the system security under the worst-case LR attacks. However, in practice, the worst-case scenario rarely happens and could lead to unnecessarily high operation cost.

Thus, it is summarised that from the attacker's perspective, LR is a malicious and stealthy designed attack to mislead system operators and cause uneconomic operation. From the system operators' perspective, LR is a random, masked, and hard-detectable attack, which requires an effective mitigation scheme. Therefore, the random LR attacks can be modelled as uncertainty in ED from the operator's perspective.

RO and stochastic optimization (SO) are the two major approaches to handle the uncertainties in ED problems [24-27]. RO includes uncertainties by predefined uncertainty sets considering the worst-case scenario. The uncertainty sets are easily constructed from empirical uncertainty regions. However, they neglect the distributional information of uncertainties, potentially leading to overly conservative results. SO hedges against uncertainties with specifically known probability distributions and thus provide relatively optimistic solutions. However, the estimation of probability distributions in SO is difficult and often requires a large number of data samples.

Inheriting the advantages of SO and RO, distributionally robust optimization (DRO) weakens the assumption of using exact probability distributions of uncertain variables compared with SO. DRO also takes advantage of distributional information to and considers the worst distribution scenario while RO ignores construct the ambiguity sets the probability characteristics. In this way, DRO can generate less conservative results compared to RO and has been widely applied to power system operations [28-31]. A security-constrained ED is proposed by using DRO considering renewable generation uncertainties [32]. In summary, DRO has been used to model random renewable generation [32, 33], resilience , and resilience problems , proved to be effective and tractable. To the best knowledge of authors, DRO has not been applied to model and resolve LR attacks.

One of the major resilience issues of the power system is the cybersecurity problem. Supervisory control and data acquisition (SCADA) is a software-enabled platform for monitoring and operating power systems. However, cyber-attacks are threats to SCADA and this would eventually operate the power system incorrectly, thus causing resilience and security issues. Cyber-attacks are one of the major threats that affect the reliable and economic operation of power systems. Thus, it is critically significant to design a resilience enhancement of the unprotected system operation against cyber-attacks. Through considering possible cyber-attacks conducted in the real-time operation, the capacity reserve of generators are scheduled in the first stage. In addition, the second-stage enables to take adaptive recourse actions by redispatch and implement load shedding to counteract the cyber-attacks. In summary, the aforementioned measures can enhance the resilience of the system under exposure to cyber-attacks. A more reliable operation scheme will be determined based on the proposed two-stage resilience enhancement.

This paper addresses the uneconomic dispatch issue of power systems under cyber-attacks by using a novel data-driven robust optimization, i.e. DRO approach. A two-stage **DR**O is proposed for **c**yber-resilient **ED** problems in transmission networks against potential cyber-attacks (DR-CED) considering the uncertainties from inaccurate renewable generation forecasting. The first stage minimizes the day-ahead dispatch costs based on forecasted load and renewable generation. The second-stage takes recourse actions on real-time dispatch under LR attacks and meanwhile considers renewable uncertainties, which is then dualized. The overall problem is transformed into a semi-definite programming formulation (SDP). Constraint generation algorithm (CGA) is utilized to solve the DR-CED under the two-stage framework. The case studies illustrate that the model can ensure the economical and secure performance of ED under cyber-attacks, providing transmission system operators (TSO) a powerful decision-making tool to conduct system operation.

To sum up, the main contributions are summarized as follows:

1) It develops a DRO method for protective measures of power systems under cyber-attacks, where DR-CED can address the uneconomic dispatch generated by traditional optimization approaches considering the risks of LR.
2) Compared to the existing works which only models cyber-attacks but ignore renewable uncertainties, the proposed DR-CED can effectively incorporate renewable generation into the operation and their uncertainties.
3) The proposed optimization only uses moment information of uncertainties, resolving the difficulty of collecting a large amount of data regarding the uncertain renewable generation and false data injections.
4) Compared with day-ahead corrective actions handled by bi-level or tri-level optimization models, this paper formulates a novel two-stage cyber-secured optimization scheme, considering both day-ahead and real-time ED, which is more practical in reality.

The rest of this paper is organized as follows. Section II models LR attack. Section III presents the objective function

and constraints of the proposed DR-CED. The methodology and mathematical reformulations are in section IV. Section V demonstrates case studies and the performance of the DR-CED. Conclusions are given in section VI.

II. Modelling of Load Redistribution Attacks

LR attacks are launched by false load data to affect system operation schedules. The tempered load meter reading deviates from the real reading and thus system operators make decisions based on the falsified load demand [18-21]. Consequently, this can cause economic loss and physical damages to the equipment. This section firstly proposes how attack manipulators can evade the detection by state estimation and then presents the modelling of LR attacks.

A. State estimation

State estimation is a powerful tool to detect FDI by processing raw data measurements, but a successful FDI can be undetectable by the adversary's stealthy design [9, 34-36]. The nonlinear relationship between state variable x and measurement z is given in (1), where $\mathbf{h}(\mathbf{x})$ denotes the nonlinear vector function of x and e is the error measurement. Based on DC state estimation, equation (1) can be transformed into (2), where $\mathbf{J}$ represents the Jacobian matrix.

$$\mathbf{z} = \mathbf{h}(\mathbf{x}) + \mathbf{e} \tag{1}$$

$$\mathbf{z} = \mathbf{J}\mathbf{x} + \mathbf{e} \tag{2}$$

After FDI realization, the measurement vector $\mathbf{z}$ becomes $\mathbf{z_{bad}} = \mathbf{z} + \mathbf{a}$, and the estimated state vector is represented as $\hat{\mathbf{x}}_{\mathbf{bad}} = \hat{\mathbf{x}} + \mathbf{c}$ where $\mathbf{a}$ is attack vector and $\mathbf{c}$ is the resulted deviation vector of state variable after FDI. Accordingly, to determine the estimated state variable, $\hat{\mathbf{x}}_{\mathbf{bad}}$ can be formulated as:

$$\hat{\mathbf{x}}_{\mathbf{bad}} = (\mathbf{J}'\mathbf{W}\mathbf{J})^{-1}\mathbf{J}'\mathbf{W}\mathbf{z}_{\mathbf{bad}} \tag{3}$$

Note that $\mathbf{J}'$ represents the transpose of $\mathbf{J}$. The main bad data detection utilizes a normalized residual approach, utilizing the L_2 norm $\|\mathbf{z} - \mathbf{J}\hat{\mathbf{x}}\|$ to detect the bad data [37, 38]. If the residual is less than a threshold ε, then the state estimate is valid without FDI.

L_2 norm of the measurement residual: $\|\mathbf{z} - \mathbf{J}\hat{\mathbf{x}}\| \leq \boldsymbol{\varepsilon}$ (4)

Then, equation (5) is given based on (3) and (4). Finally, equation (6) is obtained.

$$\|\mathbf{z} + \mathbf{a} - \mathbf{J}((\mathbf{J}'\mathbf{W}\mathbf{J})^{-1}\mathbf{J}'\mathbf{W}\mathbf{z}_{\mathbf{bad}})\| \tag{5}$$

$$\|\mathbf{z} - \mathbf{J}\hat{\mathbf{x}} + (\mathbf{a} - \mathbf{J}\mathbf{c})\| \tag{6}$$

If $\mathbf{a}$ is the linear combination of $\mathbf{J}$ and $\mathbf{c}$, i.e., $\mathbf{a} = \mathbf{J}\mathbf{c}$, then $\|\mathbf{z} - \mathbf{J}\hat{\mathbf{x}}\|$ has no change of residual. Therefore, a successful FDI attack is launched which can evade detection. Traditional bad data detection easily fails when the FDI vector $\mathbf{\Delta z}$ is the multiplication of Jacobian matrix $\mathbf{J}$ and amount of changes $\mathbf{\Delta x}$ [37]:

$$\mathbf{\Delta z} = \mathbf{a} = \mathbf{J}\mathbf{c} = \mathbf{J}\mathbf{\Delta x} \tag{7}$$

The bus power injection in (8) and power flow in (9) are:

$$\mathbf{BP} = \mathbf{KP} \cdot \mathbf{G} - \mathbf{KD} \cdot \mathbf{D} \tag{8}$$

$$\mathbf{PL} = \mathbf{SF} \cdot \mathbf{BP} \tag{9}$$

The incremental matrice of $\mathbf{BP}$ and $\mathbf{PL}$ are in (10) and (11) respectively.

$$\mathbf{\Delta BP} = \mathbf{KP} \cdot \mathbf{\Delta G} - \mathbf{KD} \cdot \mathbf{\Delta D} \tag{10}$$

$$\mathbf{\Delta PL} = \mathbf{SF} \cdot \mathbf{\Delta BP} \tag{11}$$

According to the assumptions of successful launch [20], LR attacks normally have the following characteristics.

1. The output measurement of generators cannot be attacked since the attacks can be detected easily. Thus, $\mathbf{\Delta G} = 0$.
2. Buses to be attacked have either load or generators, i.e., zero injection buses cannot be attacked.
3. Load measurements are attackable.
4. Branch flow measurement is attackable since it is influenced by the attacked load.

Therefore, (10) and (11) can be recast as (12) based on the above assumptions.

$$\mathbf{\Delta PL} = -\mathbf{SF} \cdot \mathbf{KD} \cdot \mathbf{\Delta D} \tag{12}$$

$$\sum \Delta D_k = 0 \tag{13}$$

$$-\gamma D_k \leq \Delta D_k \leq \gamma D_k \tag{14}$$

To evade the detection by state estimation, in attacks, some loads are manipulated to be increasing and some are decreasing, ensuring the total load to be unchanged, shown in (13). Constraint (14) ensures ΔD_k is within the upper and lower limits defined by the maximum percentage γ of attack magnitude.

The initial branch flow is constrained by (15). Since the flow is corrupted by $\mathbf{\Delta D}$ in (12), the deviation $\mathbf{\Delta PL}$ should be eliminated and the actual flow after LR attacks is constrained by (16), which could cause overloading with the addition of $|\mathbf{SF} \cdot \mathbf{KD} \cdot \mathbf{\Delta D}|$.

$$\underline{\mathbf{PL}} \leq \mathbf{PL} \leq \overline{\mathbf{PL}} \tag{15}$$

$$\underline{\mathbf{PL}} + \mathbf{SF} \cdot \mathbf{KD} \cdot \mathbf{\Delta D} \leq \mathbf{PL} \leq \overline{\mathbf{PL}} + \mathbf{SF} \cdot \mathbf{KD} \cdot \mathbf{\Delta D} \tag{16}$$

It should be noted that this paper considers affected flow and conducts load shedding when overloading occurs.

III. Two-Stage Mitigation for Uneconomic Dispatch

The proposed two-stage DR-CED consists of: i) initial day-ahead dispatch in the first stage and ii) real-time recourse dispatch after renewable uncertainty is revealed and LR attacks are launched in the second stage. The objective functions for the two stages are introduced respectively, followed by the constraints of day-ahead and real-time ED. Each equation in the mitigation scheme modelling hereafter, i.e., equations (17)-(34), represents a set of constraints. For instance, equation (19) denotes the constraints at time slot t for renewable generator w.

A. DR-CED Objective Function

In (17), the first-stage objective includes minimizing generation costs and spinning reserve costs. The generation cost function is quadratic with coefficients a_i, b_i and c_i . The up and down spinning reserves are separately considered with different cost coefficients λ^+ and λ^-. Quadratic generation costs in (17) can be approximated by piecewise-linear functions.

$$\Gamma_1 = \min \sum_{i \in I, t \in T} a_i P_i^s(t)^2 + b_i P_i^s(t) + c_i + \lambda^+ res_i^+(t) + \lambda^- res_i^-(t) \tag{17}$$

The second-stage optimization objective is to minimize the regulation costs from recourse actions, given in (18). The three terms from left to right represent i) regulated renewable power generation cost ii) regulated generation cost and iii) load shedding cost, respectively. It is to be noted that '$|\omega_w^s(t) - \omega_w^{re}(t)|$' and '$|P_i^s(t) - P_i^{re}(t)|$' are linearized via auxiliary

variables. For instance, '$|P_i^s(t) - P_i^{re}(t)|$' can be represented by $(P_i^s(t) - P_i^{re}(t)^-)$ and $(P_i^{re}(t)^+ - P_i^s(t))$.

$$\Gamma_2 = \min \sum_{i\in I, t\in T} \lambda_j^{re} |\omega_w^s(t) - \omega_w^{re}(t)| + \lambda_i^{re} |P_i^s(t) - P_i^{re}(t)| + \lambda_k^{ls} P_k^{ls}(t) \quad (18)$$

B. Day-ahead ED

The first-stage DR-CED conducts day-ahead operation based on forecasted renewable generation and demand. Because the day-ahead ED is the preparation prior to real-time dispatch, this plan does not consider LR risks. The renewable output is constrained within the forecastings in (19). Constraints (20) and (21) ensure that the up and down spinning reserve capacities do not exceed the predefined limits. Constraints (22) and (23) ensure generation spinning reserve is within capacity. Branch power flow is constrained in (24) and (25), between initial and terminal nodes, where DC flow is adopted. It should be noted that the range of the phase angle (θ) is between -π and π. The power balance at each node is in (26). It is to be noted that $PL_l^{s,ini}(t)$ and $PL_l^{s,ter}(t)$ represent the power flow injected and flowing out at the bus.

$$0 \le \omega_w^s(t) \le \omega_w^f(t) \quad (19)$$

$$0 \le res_i^+(t) \le Res_i^+ \quad (20)$$

$$0 \le res_i^-(t) \le Res_i^- \quad (21)$$

$$P_i^s(t) + res_i^+(t) \le P_{i,max} \quad (22)$$

$$P_{i,min} \le P_i^s(t) - res_i^-(t) \quad (23)$$

$$x_l PL_l^s(t) = \left(\theta_l^{s,ini}(t) - \theta_l^{s,ter}(t)\right) \quad (24)$$

$$-PL_{l,max} \le PL_l^s(t) \le PL_{l,max} \quad (25)$$

$$\sum_{i\in I} P_i^s(t) + \sum_{w\in W} \omega_w^s(t) + \sum_{l\in L} PL_l^{s,ini}(t) - \sum_{l\in L} PL_l^{s,ter}(t) = \sum_{k\in K} P_k(t) \quad (26)$$

C. Real-time ED

The second-stage DR-CED determines the corrective dispatch plan after LR attacks and the realization of renewable output uncertainties. In (27), the regulated renewable output is constrained within the new availability, considering the uncertainties of renewable forecasting errors. The regulated generator output is constrained with the spinning reserve in (28). Constraints (29) and (30) model the LR launched by attackers, which is the explicit expressions of (13) and (14). Load shedding is constrained in (31). Constraints (32) and (33) ensure no overloading along branches. The real-time power balance at each node is in (34).

$$0 \le \omega_w^{re}(t) \le \omega_w^f(t) + \xi_r(t) \quad (27)$$

$$P_i^s(t) - res_i^-(t) \le P_i^{re}(t) \le P_i^s(t) + res_i^+(t) \quad (28)$$

$$\sum_{k\in K} \Delta P_k(t) = 0 \quad (29)$$

$$-\gamma P_k(t) \le \Delta P_k(t) \le \gamma P_k(t) \quad (30)$$

$$0 \le P_k^{ls}(t) \le P_{k,max}^{ls}(t) \quad (31)$$

$$x_l PL_l^{re}(t) = \left(\theta_l^{re,ini}(t) - \theta_l^{re,ter}(t)\right) \quad (32)$$

$$-PL_{l,max} \le PL_l^{re}(t) \le PL_{l,max} \quad (33)$$

$$\sum_{i\in I} P_i^{re}(t) + \sum_{w\in W} \omega_w^{re}(t) + \sum_{l\in L} PL_l^{re,ini}(t) - \sum_{l\in L} PL_l^{re,ter}(t) = \sum_{k\in K} P_k(t) + \Delta P_k(t) - P_k^{ls}(t) \quad (34)$$

IV. Methodology

The methodology for solving the DR-CED is introduced in this section. Firstly, the abstract form of matrices and vectors are presented to represent the objective function and constraints. Then, ambiguity sets to accommodate random LR attacks and renewable uncertainties are proposed. Finally, the proposed DR-CED is transformed into a dual formulation and CGA is utilized to solve it.

A. Abstract Formulation

For simplicity, the compact form of the overall objective function combining (17) and (18) is as follows:

$$\min_{\mathbf{x}\in X} \mathbf{c}'\mathbf{x} + \sup_{Pr\in D} E_P[Q(\mathbf{x}, \boldsymbol{\xi})] \quad (35)$$

$$\text{s.t. } \mathbf{Ax} \le \mathbf{b}, \quad (36)$$

Where

$$Q(\mathbf{x}, \boldsymbol{\xi}) = \min_{\mathbf{y}} f'\mathbf{y} \quad (37)$$

$$\text{s.t. } \mathbf{Ex} + \mathbf{Fy} + \mathbf{G}\boldsymbol{\xi} \le \mathbf{h}, \quad (38)$$

Where, (36) and (38) represent constraints in the first and second stages, vector *f* corresponds to the coefficients of (18) and *y* represents the second-stage decision variables.

B. Ambiguity Sets of DRO

Similar to the uncertainty set for RO, the ambiguity set for DRO is to handle uncertain variables. Because LR attacks are of low probability and high impact, it is not practical to obtain sufficient information from historic data. Moment information including mean and covariance is used to construct the ambiguity set in (39). Similarly, (40) models the ambiguity set for renewable forecasting uncertainties.

$$D_k = \left\{ f(\Delta\mathbf{P_k}) \middle| \begin{array}{c} \mathrm{P}\{\Delta\mathbf{P_k}\} = 1 \\ \mathrm{E}\{\Delta\mathbf{P_k}\} = \boldsymbol{\mu_k} \\ -\gamma\mathbf{P_k} \le \Delta\mathbf{P_k} \le \gamma\mathbf{P_k} \\ \mathrm{E}\{\Delta\mathbf{P_k}(\Delta\mathbf{P_k})'\} = \boldsymbol{\Sigma_k} + \boldsymbol{\mu_k}(\boldsymbol{\mu_k})' \end{array} \right\} \quad (39)$$

$$D_r = \left\{ f(\boldsymbol{\xi_r}) \middle| \begin{array}{c} \mathrm{P}\{\boldsymbol{\xi_r}\} = 1 \\ \mathrm{E}\{\boldsymbol{\xi_r}\} = \boldsymbol{\mu_r} \\ \mathrm{E}\{\boldsymbol{\xi_r}(\boldsymbol{\xi_r})'\} = \boldsymbol{\Sigma_r} + \boldsymbol{\mu_r}(\boldsymbol{\mu_r})' \end{array} \right\} \quad (40)$$

Where, (39) and (40) illustrate the integral of probability distribution $\Delta\mathbf{P_k}$ or $\boldsymbol{\xi_r}$ is 1.

All possible distributions of $f(\Delta\mathbf{P_k})$ have the same mean vector and covariance matrix. All possible distributions of $f(\boldsymbol{\xi_r})$ have the same mean vector and covariance matrix.

C. Second-stage Dual Formulation

For tractability, the 'sup min' framework of the second-stage problem needs to be reformulated into the dualized form with

only 'min'. It can be reformed explicitly as (41), where *S(x)* is the objective function of the second-stage problem, $\sup_{P\in D} E_P[Q(\mathbf{x},\boldsymbol{\xi})]$. The dual variables $\boldsymbol{\psi_0}$, $\boldsymbol{\psi_j}$ and Ψ_{jk} are associated with constraints (27) to (34). It is noted that ξ represents both $\Delta\mathbf{P_k}$ and $\boldsymbol{\xi_r}$ in this section for simplicity. $Pr(\boldsymbol{\xi})$ is the probability density function.

$$S(\mathbf{x})^{primal} = \max_{Pr(\xi)\in D} \int_{\Xi} Q(\mathbf{x},\boldsymbol{\xi})\, Pr(\boldsymbol{\xi}) d\boldsymbol{\xi} \tag{41}$$

$$\text{s.t. } Pr(\boldsymbol{\xi}) \geq 0, \forall \boldsymbol{\xi} \in \Xi \tag{42}$$

$$\int_{\Xi} Pr(\boldsymbol{\xi}) d\boldsymbol{\xi} = 1 \tag{43}$$

$$\int_{\Xi} \boldsymbol{\xi}^{\mathbf{m}} Pr(\boldsymbol{\xi}) d\boldsymbol{\xi} = \boldsymbol{\mu}_{\mathbf{m}} \quad m=1,2,\ldots,\Xi \tag{44}$$

$$\int_{\Xi} \boldsymbol{\xi}^{\mathbf{m}}\boldsymbol{\xi}^{\mathbf{n}} Pr(\boldsymbol{\xi}) d\boldsymbol{\xi} = \boldsymbol{\Sigma}_{\mathbf{mn}} + \boldsymbol{\mu}_{\mathbf{m}}\boldsymbol{\mu}_{\mathbf{n}} \quad m, n=1,2,\ldots,\Xi \tag{45}$$

In (41), the probability densities are decision variables to be optimized. The number of constraints is finite but the number of variables is infinite. The dual formulation is used to ensure tractability, which transforms the infinite-dimensional linear primal form (41)-(45) to the dual form (46) and (47) based on dual theory [39]. When the covariance matrix is strictly positive [40], strong duality holds and the results of (46) are equal to those of (41). Thus, the primal problem with an infinite number of variables and a finite number of constraints is transformed into the dual form, i.e., a semi-infinite program with a finite number of variables and an infinite number of constraints. Therefore, the problem (46) is easier to solve. With associated dual variables, i.e., $\boldsymbol{\psi_0}$, $\boldsymbol{\psi_j}$ and Ψ_{jk}, equation (41) in the 'max' problem can be dualized to 'min' problem and thus can be integrated with the first-stage objective.

Preposition: Equation (46) is the dual form of the primal form in (41) based on the dual theory [39], which proves that with strong duality, the results of (46) are equal to those of (41) when the covariance matrix is strictly positive, i.e., $S(\mathbf{x})^{dual} = S(\mathbf{x})^{primal}$.

$$S(\mathbf{x})^{dual} = \min_{\Psi,\psi,\psi_0} \langle \boldsymbol{\Psi}'\boldsymbol{\Theta}\rangle + \boldsymbol{\psi}'\boldsymbol{\mu} + \boldsymbol{\psi_0} \tag{46}$$

$$\text{s.t. } (\boldsymbol{\xi})'\boldsymbol{\Psi}\boldsymbol{\xi} + \boldsymbol{\psi}'\boldsymbol{\xi} + \boldsymbol{\psi_0} \geq Q(\mathbf{x},\boldsymbol{\xi}) \quad \forall \boldsymbol{\xi} \in \Xi \tag{47}$$

Where $\langle\mathbf{A}\rangle$ is the trace of matrix $\mathbf{A}$, and $\boldsymbol{\Theta}$ represents $\boldsymbol{\Sigma} + \boldsymbol{\mu}(\boldsymbol{\mu})'$.

The new compact form of the DR-CED is

$$\min_{x\in X} \mathbf{c}'\mathbf{x} + S(\mathbf{x})^{dual} \tag{48}$$

D. SDP Reformulation

The two challenges that prevent the DR-CED from being solved directly are:

i) problem (46) is not in a closed-form;

ii) the dual form (46) contains an infinite number of constraints [41], which is a semi-infinite problem.

A new dual reformulation is made and given in (49) and (50) with the new dual variable τ. And the positive quadratic function is obtained as the new representation of (37), where VS is the polyhedral set of extreme points [41].

$$\max_{u\in VS} \boldsymbol{\tau}'(\mathbf{b} - \mathbf{E}\mathbf{x} - \mathbf{G}\boldsymbol{\xi}) \tag{49}$$

$$VS = \{\boldsymbol{\tau} | \mathbf{F}'\boldsymbol{\tau} = \mathbf{f}, \boldsymbol{\tau} \leq 0\} \tag{50}$$

Equation (47) can be expressed as (51) based on the new dual variable τ, which is a positive quadratic function of ξ. N_v is the vertices set of feasible region in VS.

$$(\boldsymbol{\xi})'\boldsymbol{\Psi}\boldsymbol{\xi} + (\boldsymbol{\psi} + \mathbf{G}'\boldsymbol{\tau}^{\mathbf{i}})'\boldsymbol{\xi} + \boldsymbol{\psi_0} - (\mathbf{h} - \mathbf{E}\mathbf{x})\boldsymbol{\tau}^{\mathbf{i}} \geq 0 \quad \forall \boldsymbol{\xi} \in \Xi,\ i=1,2,\ldots,N_v \tag{51}$$

which can be rewritten in the following compact matrix form:

$$\begin{bmatrix}\boldsymbol{\xi}\\ 1\end{bmatrix}' \begin{bmatrix} \boldsymbol{\Psi} & \frac{1}{2}(\boldsymbol{\psi} + \mathbf{G}'\boldsymbol{\tau}^{\mathbf{i}}) \\ \frac{1}{2}(\boldsymbol{\psi} + \mathbf{G}'\boldsymbol{\tau}^{\mathbf{i}})' & \boldsymbol{\psi_0} - (\mathbf{h} - \mathbf{E}\mathbf{x})'\boldsymbol{\tau}^{\mathbf{i}} \end{bmatrix} \begin{bmatrix}\boldsymbol{\xi}\\ 1\end{bmatrix} \geq 0 \quad \forall \boldsymbol{\xi} \in \Xi,\ i=1,2,\ldots,N_v \tag{52}$$

The final SDP formulation of DR-CED is built as follows:

$$\min_{x,\Psi,\psi,\psi_0} \mathbf{c}'\mathbf{x} + \langle \boldsymbol{\Psi}'\boldsymbol{\Theta}\rangle + \boldsymbol{\psi}'\boldsymbol{\mu} + \boldsymbol{\psi_0} \tag{53}$$

$$\text{s.t. } \begin{bmatrix} \boldsymbol{\Psi} & \frac{1}{2}(\boldsymbol{\psi} + \mathbf{G}'\boldsymbol{\tau}^{\mathbf{i}}) \\ \frac{1}{2}(\boldsymbol{\psi} + \mathbf{G}'\boldsymbol{\tau}^{\mathbf{i}})' & \boldsymbol{\psi_0} - (\mathbf{h} - \mathbf{E}\mathbf{x})'\boldsymbol{\tau}^{\mathbf{i}} \end{bmatrix} \geq 0 \quad i=1,2,\ldots,N_v,\ x\in X \tag{54}$$

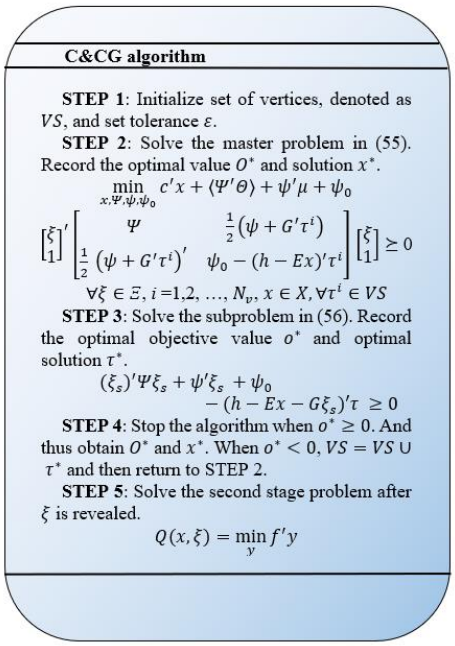


Fig. 1. Flowchart of the constrained generation algorithm

E. Constraint Generation Algorithm

It is not practical to directly solve the SDP problem (53) because there are a large number of constraints in (54) with an extremely large cardinality of VS. The most practical approach is to firstly enumerate a subset of vertices under the relaxation of SDP problem and then incorporate more vertices iteratively until the optimal solution is obtained. CGA separates the original problem into master and sub problems and solves them iteratively.

The master and sub problems are illustrated in (55) and (56):

$$\min_{x,\Psi,\psi,\psi_0} \mathbf{c}'\mathbf{x} + \langle \boldsymbol{\Psi}'\boldsymbol{\Theta}\rangle + \boldsymbol{\psi}'\boldsymbol{\mu} + \boldsymbol{\psi_0} \tag{55}$$

$$\text{s.t.} \begin{bmatrix} \boldsymbol{\Psi} & \frac{1}{2}(\boldsymbol{\psi} + \mathbf{G}'\boldsymbol{\tau}^{\mathbf{i}}) \\ \frac{1}{2}(\boldsymbol{\psi} + \mathbf{G}'\boldsymbol{\tau}^{\mathbf{i}})' & \boldsymbol{\psi}_{\mathbf{0}} - (\mathbf{h} - \mathbf{E}\mathbf{x})'\boldsymbol{\tau}^{\mathbf{i}} \end{bmatrix} \succeq 0$$

$$\forall \tau^i \in VS, \mathbf{x} \in X$$

$$\min_{x,\Psi,\psi,\psi_0} (\boldsymbol{\xi})'\boldsymbol{\Psi}\boldsymbol{\xi} + \boldsymbol{\psi}'\boldsymbol{\xi} + \boldsymbol{\psi}_{\mathbf{0}} - (\mathbf{h} - \mathbf{E}\mathbf{x} - \mathbf{G}\boldsymbol{\xi})'\boldsymbol{\tau} \quad (56)$$

$$\text{s.t. } \forall \boldsymbol{\xi} \in \Xi, \tau \in VS$$

It should be noted that subproblem (56) is a biconvex program, which can be solved by an alternative direction oracle via separately solving linear programming and convex quadratic programming with τ and ξ fixed in each iteration.

The initial set for all the vertices is set in the first step. Then the master and sub problems are solved in turn. At each iteration, the optimal objective value is checked if it is above 0. If it is not, the set of vertices is updated to incorporate more vertices. When the terminal condition is satisfied, record the optimal value and optimal solution. Then the second-stage problem can be solved based on an expected manner. The detailed steps of the proposed CGA are given in Fig. 1.

V. Case Studies

This section presents the extensive case studies of the proposed DR-CED on a modified IEEE 30-bus system. All numerical simulations are obtained by MOSEK version 9.0 with Intel Core i7-7700 CPU and 16GB RAM. To investigate the impact of LR attacks and renewable uncertainties on the ED problem, 8 cases are studied:

Case 1: Single-stage ED without considering LR attacks or renewable uncertainty.

Case 2: Single-stage robust ED considering LR attacks (γ=5%).

Case 3: Case 2 considering renewable uncertainty (γ=5%).

Case 4: Two-stage DR-CED considering only LR attacks (γ=5%).

Case 5: Case 4 considering renewable uncertainty (γ=5%).

Case 6-8: Case 5 with γ=10%, 15% and 20%.

The test system is assumed to be fully measured, which means 21 load meters are required for the modified IEEE-30 bus system. The γ for each bus is limited at ±25% of the actual load. The attacker aims to launch LR attacks without being detected by system estimators as discussed aforementioned. The attacker is assumed to have full knowledge about system topology and parameters, and the attacker has the ability to conduct LR attack on any buses.

The modified IEEE 30-bus system is given in Fig. 2, which has 6 generators connected to buses 1, 2, 5, 8, 11 and 13. Two renewable generators are connected to buses 22 and 25. The renewable generation forecast is assumed to be 50 MW for bus 22 and 60 MW for bus 25. TABLE I shows the parameters of the penalty cost coefficients and renewable forecast. TABLE II presents the parameters and constraints of generators.

In (39) and (40), the ambiguity sets for uncertain LR attacks and renewable generation error are presented. The mean vector of ΔP_k and ξ_r are represented by μ_k and μ_r, which are zero vectors in 24 dimensions, representing the LR attack and renewable generation error have both positive and negative values. The covariance matrices of ΔP_k and ξ_r are denoted by Σ_k and Σ_r, which are 24x24 matrice. The covariance matrix of LR attack from the 20th to 22nd hours are shown in (57). And the covariance matrix of renewable generation error from the 20th to 22nd hours are shown in (58).

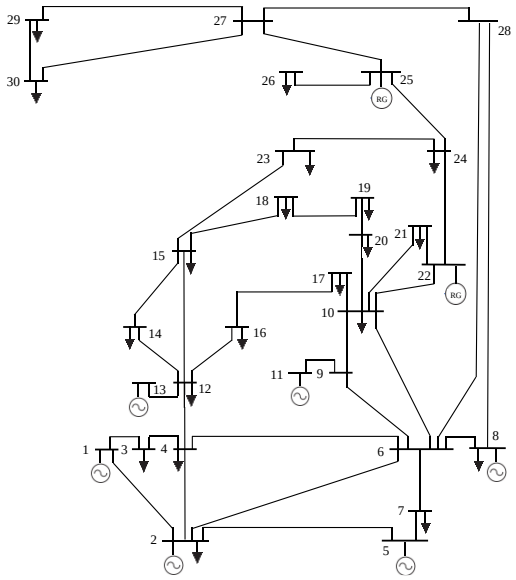


Fig. 2. Modified IEEE 30 bus system.

TABLE I
Technical Parameters

λ_j^{re}	λ_i^{re}	λ_k^{ls}	$\omega_{22}^f(t)$	$\omega_{25}^f(t)$
$100	$150	$600	50MW	60MW

. TABLE II
Generator Parameters

Bus No.	$P_{i,min}$ (MW)	$P_{i,max}$ (MW)	R_i^+, R_i^- (MW)	a_i	b_i	c_i
1	50	200	20	0.004	2	6
2	20	80	16	0.002	2	6
5	15	50	10	0.006	1	8
8	10	35	7	0.008	3	10
11	10	30	10	0.025	3	18
13	12	40	16	0.025	3	18

$$\Sigma_{k,20-23} = \begin{bmatrix} 0.125 & 0.75 & -1 \\ 0.75 & 4.5 & -6 \\ -1 & -6 & 8 \end{bmatrix} \quad (57)$$

$$\Sigma_{r,20-23} = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0.125 & 0.95 \\ 0 & 0.95 & 7.22 \end{bmatrix} \quad (58)$$

A. Computational Performance

The combined convex quadratic programming and linear programming oracle discussed in section IV are difficult to solve, which is chosen to test the computational performance for case 4-6 and shown in Fig. 3. In general, case 4 has better computational performance, whose optimality gap to 1E+02 at the 5th iteration while those for cases 5 and 6 are at the 6th and 7th. Case 4 has the quickest convergence speed, which converges at the13th iteration while cases 5 and 6 converge at the 15th iteration. The reason is that case 4 only considers LR attacks while cases 5 and 6 consider both LR attacks and renewable uncertainties, which cause more vertices and cuts generated in CGA.

The second-stage expected performance is conducted based on 1000 simulated uncertainty realizations which share the same mean and covariance information. The sample size is

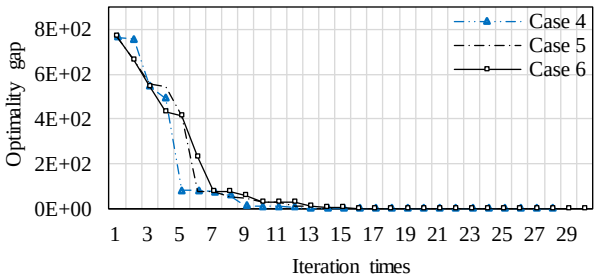


Fig. 3. Computation performance for cases 4-6 in CGA.

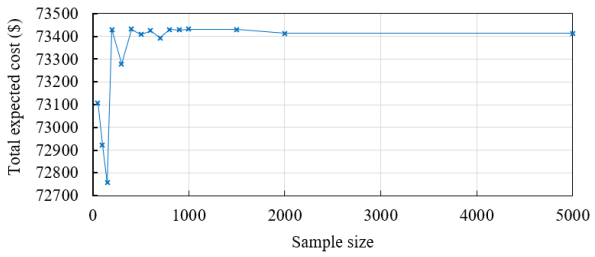


Fig. 4. Total expected cost of case 4 based on different sample sizes.

changed to investigate its impact on second-stage operation cost. In Fig. 4, the result of case 4 fluctuates when the sample is fewer than 1000 and converges toward $73400 afterward.

B. Economic Performance

The first case investigates the impact of LR attacks and renewable uncertainties on the economic performance of the system operation. TABLE III presents the economic performance under cases 1-5. Case 1 has the lowest total cost, i.e., $20087, without considering LR attacks and renewable uncertainties. When the γ is 5%, the highest total cost ($99699) is in case 3 among cases 2-5 since RO is applied and consider the worst-case for both LR attacks and renewable uncertainties. Case 2 yields a lower cost than case 3 but a higher cost than case 1. The reason is that case 2 considers LR attacks compared with case 1 and assumes deterministic renewable generation without fluctuation compared with case 3. The same scenario is investigated in case 4 with DRO, where the two-stage scheme mitigates the adverse impact of LR attacks and reduces 2.4% cost compared to case 2. Similarly, case 5 yields $3981 reduction compared to case 3 with less conservative DRO approach.

With the increase of γ, the operation cost increases. Due to the characteristics of LR, although the overall load deviation is 0, the total cost still increases with simply increasing the γ. The reason is that considering the potential LR attacks, DR-CED tends to satisfy all the loads and meanwhile prepare sufficient reserve for second-stage re-dispatch. Compared with case 5 with 5% γ, with the increase of γ, cases 6-8 has 37%, 47% and 56% higher cost.

To investigate the impact of LR attacks and renewable uncertainties on scheduled generation, renewable generation and spinning reserve capacity, cases 1-5 are analysed in TABLE IV. Case 3 has the highest generation output, i.e., 1760MWh, with the least scheduled renewable generation because both LR attacks and renewable uncertainties are considered in the worst case. With the consideration of LR

TABLE III
ECONOMIC PERFORMANCE FOR CASE 1-8

Economic result ($)	Case 1	Case 2	Case 3	Case 4
First-stage cost	20087	95603	99699	19974
Expected Second-stage cost	0	0	0	73400
Total cost	20087	95603	99699	93374
Economic result ($)	**Case 5**	**Case 6**	**Case 7**	**Case 8**
First-stage cost	20718	21335	22596	24559
Expected Second-stage cost	75000	110400	118600	125000
Total cost	95718	131735	141196	149559

TABLE IV
DISPATCH PLAN FOR CASE 1-5

Scheduled model (MWh)	Case 1	Case 2	Case 3	Case 4	Case 5
Generator output	1498	1583	1760	1300	1653
Renewable generation	179	179	36	180	180
Reserve capacity	0	0	0	154	206

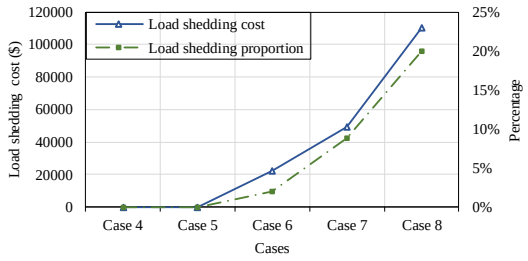


Fig. 5. Load shedding cost and proportion for cases 4-8.

attacks, case 2 yields 85MWh more generation. However, when using DRO, the generator output of case 4 is lower than case 1. The reason is that the two-stage scheme additionally considers reserve capacity in the first stage and adjusts generation scheme in the second stage, which reduces day-ahead scheduled generation, making up for the demand shortage in the real-time re-dispatch.

When renewable uncertainty is additionally considered, case 5 shows approximately similar results with case 4, i.e., both are 180 MWh, while cases 3 produces much smaller renewable generation output than case 2. The reason is that both cases 2 and 3 are the single-stage model and RO implements the worst-case by simply reducing renewable generation. However, two-stage DRO in case 5 considers the worst-distribution, which is less conservative and thus yields more renewable generation.

In cases 4-8, the γ is increasing from 5% to 20%, which means the attacker could increase the load up to 120% of the original volume. In the case of overloading of branches, load shedding is required, which is shown in Fig. 5. When the γ is 5%, no load shedding is required in cases 4 and 5, since line capacity is able to defend LR attacks. When the γ increases to 10%, $22000 load shedding cost is conducted. When the γ is up to 20%, it causes $110400 of load shedding.

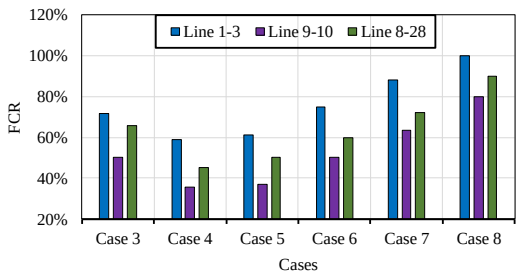


Fig. 6. FCR for time period 18 in cases 3-8.

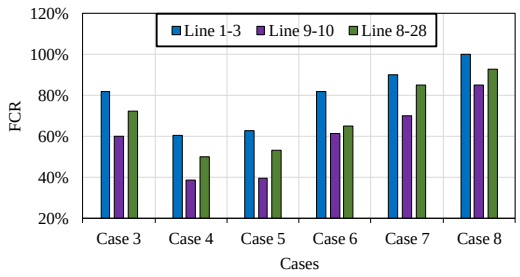


Fig. 7. FCR for time period 19 in cases 3-8.

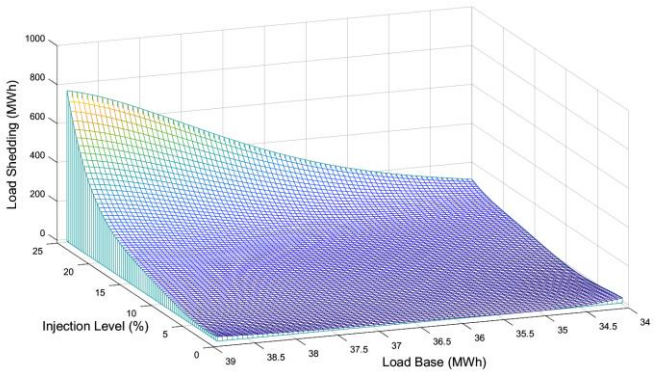


Fig. 8. Load shedding regarding different γ and load base.

C. *Analysis of Flow and Load Shedding*

LR attacks have a significant impact on transmission lines, which is investigated as the flow-capacity ratio (FCR), representing the ratio of a branch flow over line capacity. Figs. 6 and 7 present the FCR of lines 1-3, 9-10 and 8-28 for cases 3-8. It is more likely that judicious attackers target at high-loading time periods and impose severe impacts. Thus, time periods 18 and 19 are selected, which have the two highest load demand. Overall, line 1-3 has higher FCR than line 9-10 and 8-28 in all cases. In Fig. 7, it can be seen that case 4 has the lowest FCR since two-stage DRO is applied without considering renewable generation uncertainties. The FCR of case 3 is approximately 20% higher than that in case 4, which indicates that RO is more prone to causing high FCR. The FCRs of cases 4 and 5 are almost the same, which indicates that renewable uncertainty does not cause a significant rise of FCR. When the γ increases from 5% to 20%, the FCRs of cases 5-8 increase. Case 8 has the highest FCR for among three discussed lines, 100%, 80% and 90% respectively. Generally, FCR in Fig. 7 is higher than that in Fig. 6 since the load is higher.

The system total load (34MWh) in the first time period is set as 1 p.u., defined as load base. The increase of the overall load will cause more load shedding over time. To investigate the impact of both γ and load base, Fig. 8 is presented. The key findings are: i) When the load base or γ increases, the load shedding increases. ii) The load shedding is nearly zero for all load buses when γ is lower, i.e., under 5%. iii) When the load base is fixed and only γ increases, for a low-level load base, e.g., 34MWh, the load shedding increases slowly and only reaches 107MWh; for a high-level load base, e.g., 39MWh, the load shedding increases fast. iv) When the γ is fixed and only the load base increases, the load shedding increases smoothly for γ under 20% but it increases fast or γ above 20%.

VI. CONCLUSION

A two-stage DRO approach is proposed in this paper to simultaneously mitigate uneconomic dispatch under potential LR attacks and renewable forecast uncertainties. The original optimization problem is reformulated into SDP form and solved by CGA. Through extensive case study demonstrations, the following key findings are as follows:

- The real-time corrective dispatch in the second stage is useful for minimizing the dispatch costs and ensuring system security by load shedding.
- Considering renewable forecast uncertainties leads to more conservative economic results, which is thus necessary and practical to consider in the modelling.
- Both generation output and economic results are sensitive to the increase of γ. From case 5 to case 8, 15% increase of γ causes 19% additional dispatch cost.
- DRO provides less-conservative results than RO, which provides system operators a more realistic and economical tool to conduct system operation.

The proposed model can mitigate the uneconomic dispatch of power systems under LR attacks and renewable uncertainties, thus ensuring system supply security and maintaining the energy costs at the lowest level. Thus, the major beneficiaries are renewable generation, system operators and end customers. Notwithstanding the two-stage DRO framework provides an effective resilience enhancement and mitigation scheme for power system operation against cyber-attacks, the DRO technique can be further developed by constructing the recent distance-based ambiguity set. The more advanced DRO approach enables to maximally reduce the conservatism of uncertainty modelling while considering more distributional information. This paper adopts moment-base ambiguity set to handle the uncertain distribution, which may leads to strikingly different distributions and violates the real distributions. Distribution-based ambiguity sets are not constrained by parameter estimations, which incoporates all the possible distributions. This treatment yields a more reliable set and a more economic resilience enhancement strategy will be obtained. Accordingly, future research effort will be made on modelling and comparing different ambiguity sets for obtaining a more reliable optimization model.

REFERENCES

[1] A. Mahmood, N. Javaid, and S. Razzaq, "A review of wireless communications for smart grid," *Renewable and sustainable energy reviews*, vol. 41, pp. 248-260, 2015.

[2] S. Li, H. He, C. Su, and P. Zhao, "Data driven battery modeling and management method with aging phenomenon considered," *Applied Energy*, vol. 275, p. 115340, 2020/10/01/ 2020, doi: https://doi.org/10.1016/j.apenergy.2020.115340.

[3] S. Li, H. He, and J. Li, "Big data driven lithium-ion battery modeling method based on SDAE-ELM algorithm and data pre-processing technology," *Applied Energy*, vol. 242, pp. 1259-1273, 2019/05/15/ 2019, doi: https://doi.org/10.1016/j.apenergy.2019.03.154.

[4] X. Chen *et al.*, "H-DrunkWalk: Collaborative and Adaptive Navigation for Heterogeneous MAV Swarm," *ACM Trans. Sen. Netw.*, vol. 16, no. 2, p. Article 20, 2020, doi: 10.1145/3382094.

[5] G. Liang, J. Zhao, F. Luo, S. R. Weller, and Z. Y. Dong, "A Review of False Data Injection Attacks Against Modern Power Systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1630-1638, 2017, doi: 10.1109/TSG.2015.2495133.

[6] B. Kesler, "The vulnerability of nuclear facilities to cyber attack; strategic insights: Spring 2010," *Strategic Insights, Spring 2011*, 2011.

[7] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "The 2015 ukraine blackout: Implications for false data injection attacks," *IEEE Transactions on Power Systems*, vol. 32, no. 4, pp. 3317-3318, 2016.

[8] B. Sobczak. "Experts assess damage after first cyberattack on U.S. grid." E&E News. https://www.eenews.net/stories/1060281821 (accessed May. 6, 2019).

[9] X. Liu and Z. Li, "False Data Attacks Against AC State Estimation With Incomplete Network Information," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2239-2248, 2017, doi: 10.1109/TSG.2016.2521178.

[10] L. Che, X. Liu, Z. Li, and Y. Wen, "False Data Injection Attacks Induced Sequential Outages in Power Systems," *IEEE Transactions on Power Systems*, vol. 34, no. 2, pp. 1513-1523, 2019, doi: 10.1109/TPWRS.2018.2871345.

[11] 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 Transactions on Smart Grid*, vol. 10, no. 2, pp. 1704-1712, 2019, doi: 10.1109/TSG.2017.2776325.

[12] P. Zhao, C. Gu, and D. Huo, "Two-Stage Coordinated Risk Mitigation Strategy for Integrated Electricity and Gas Systems under Malicious False Data Injections," *IEEE Transactions on Power Systems*, pp. 1-1, 2020, doi: 10.1109/TPWRS.2020.2986455.

[13] A. F. Taha, J. Qi, J. Wang, and J. H. Panchal, "Risk Mitigation for Dynamic State Estimation Against Cyber Attacks and Unknown Inputs," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 886-899, 2018, doi: 10.1109/TSG.2016.2570546.

[14] L. Wei, A. I. Sarwat, W. Saad, and S. Biswas, "Stochastic Games for Power Grid Protection Against Coordinated Cyber-Physical Attacks," *IEEE Transactions on Smart Grid*, vol. 9, no. 2, pp. 684-694, 2018, doi: 10.1109/TSG.2016.2561266.

[15] M. N. Kurt, Y. Yılmaz, and X. Wang, "Real-Time Detection of Hybrid and Stealthy Cyber-Attacks in Smart Grid," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 2, pp. 498-513, 2019, doi: 10.1109/TIFS.2018.2854745.

[16] Q. Hu, D. Fooladivanda, Y. H. Chang, and C. J. Tomlin, "Secure State Estimation and Control for Cyber Security of the Nonlinear Power Systems," *IEEE Transactions on Control of Network Systems*, vol. 5, no. 3, pp. 1310-1321, 2018, doi: 10.1109/TCNS.2017.2704434.

[17] S. Soltan, M. Yannakakis, and G. Zussman, "Power Grid State Estimation Following a Joint Cyber and Physical Attack," *IEEE Transactions on Control of Network Systems*, vol. 5, no. 1, pp. 499-512, 2018, doi: 10.1109/TCNS.2016.2620807.

[18] S. Soltan and G. Zussman, "EXPOSE the Line Failures Following a Cyber-Physical Attack on the Power Grid," *IEEE Transactions on Control of Network Systems*, vol. 6, no. 1, pp. 451-461, 2019, doi: 10.1109/TCNS.2018.2844244.

[19] X. Liu, Z. Li, Z. Shuai, and Y. Wen, "Cyber Attacks Against the Economic Operation of Power Systems: A Fast Solution," *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 1023-1025, 2017, doi: 10.1109/TSG.2016.2623983.

[20] Y. Yuan, Z. Li, and K. Ren, "Modeling Load Redistribution Attacks in Power Systems," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 382-390, 2011, doi: 10.1109/TSG.2011.2123925.

[21] Y. Yuan, Z. Li, and K. Ren, "Quantitative Analysis of Load Redistribution Attacks in Power Systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1731-1738, 2012, doi: 10.1109/TPDS.2012.58.

[22] L. Che, X. Liu, and Z. Li, "Mitigating False Data Attacks Induced Overloads Using a Corrective Dispatch Scheme," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 3081-3091, 2019, doi: 10.1109/TSG.2018.2817515.

[23] H. Shayan and T. Amraee, "Network Constrained Unit Commitment Under Cyber Attacks Driven Overloads," *IEEE Transactions on Smart Grid*, pp. 1-1, 2019, doi: 10.1109/TSG.2019.2904873.

[24] P. Li, Y. Liu, H. Xin, and X. Jiang, "A Robust Distributed Economic Dispatch Strategy of Virtual Power Plant Under Cyber-Attacks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 10, pp. 4343-4352, 2018, doi: 10.1109/TII.2017.2788868.

[25] H. Zhang, D. Yue, and X. Xie, "Robust Optimization for Dynamic Economic Dispatch Under Wind Power Uncertainty With Different Levels of Uncertainty Budget," *IEEE Access*, vol. 4, pp. 7633-7644, 2016, doi: 10.1109/ACCESS.2016.2621338.

[26] Y. Liu and N. C. Nair, "A Two-Stage Stochastic Dynamic Economic Dispatch Model Considering Wind Uncertainty," *IEEE Transactions on Sustainable Energy*, vol. 7, no. 2, pp. 819-829, 2016, doi: 10.1109/TSTE.2015.2498614.

[27] Y. Gu and L. Xie, "Stochastic Look-Ahead Economic Dispatch With Variable Generation Resources," *IEEE Transactions on Power Systems*, vol. 32, no. 1, pp. 17-29, 2017, doi: 10.1109/TPWRS.2016.2520498.

[28] P. Zhao, C. Gu, D. Huo, Y. Shen, and I. Hernando-Gil, "Two-Stage Distributionally Robust Optimization for Energy Hub Systems," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 5, pp. 3460-3469, 2020, doi: 10.1109/TII.2019.2938444.

[29] P. Zhao, C. Gu, Z. Hu, X. I. E. D, I. Hernando-Gil, and Y. Shen, "Distributionally Robust Hydrogen Optimization with Ensured Security and Multi-Energy Couplings," *IEEE Transactions on Power Systems*, pp. 1-1, 2020, doi: 10.1109/TPWRS.2020.3005991.

[30] P. Zhao *et al.*, "Volt-VAR-Pressure Optimization of Integrated Energy Systems with Hydrogen Injection," *IEEE Transactions on Power Systems*, pp. 1-1, 2020, doi: 10.1109/TPWRS.2020.3028530.

[31] P. Zhao *et al.*, "Economic-Effective Multi-Energy Management with Voltage Regulation Networked with Energy Hubs," *IEEE Transactions on Power Systems*, pp. 1-1, 2020, doi: 10.1109/TPWRS.2020.3025861.

[32] X. Lu, K. W. Chan, S. Xia, B. Zhou, and X. Luo, "Security-Constrained Multiperiod Economic Dispatch With Renewable Energy Utilizing Distributionally Robust Optimization," *IEEE Transactions on Sustainable Energy*, vol. 10, no. 2, pp. 768-779, 2019, doi: 10.1109/TSTE.2018.2847419.

[33] P. Zhao, H. Wu, C. Gu, and I. H. Gil, "Optimal Home Energy Management under Hybrid PV-Storage Uncertainty: A Distributionally Robust Chance-Constrained Approach," *IET Renewable Power Generation*, p. 9, 2019.

[34] J. Zhao *et al.*, "Power System Dynamic State Estimation: Motivations, Definitions, Methodologies, and Future Work," *IEEE Transactions on Power Systems*, vol. 34, no. 4, pp. 3188-3198, 2019, doi: 10.1109/TPWRS.2019.2894769.

[35] A. Ashok, M. Govindarasu, and V. Ajjarapu, "Online Detection of Stealthy False Data Injection Attacks in Power System State Estimation," *IEEE Transactions on Smart Grid*, vol. 9, no. 3, pp. 1636-1646, 2018, doi: 10.1109/TSG.2016.2596298.

[36] R. Deng, P. Zhuang, and H. Liang, "False Data Injection Attacks Against State Estimation in Power Distribution Systems," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2871-2881, 2019, doi: 10.1109/TSG.2018.2813280.

[37] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, p. 13, 2011.

[38] T. T. Kim and H. V. Poor, "Strategic Protection Against Data Injection Attacks on Power Grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 326-333, 2011, doi: 10.1109/TSG.2011.2119336.

[39] E. Delage and Y. Ye, "Distributionally robust optimization under moment uncertainty with application to data-driven problems," *Operations research*, vol. 58, no. 3, pp. 595-612, 2010.

[40] D. Bertsimas, X. V. Doan, K. Natarajan, and C.-P. Teo, "Models for minimax stochastic linear optimization problems with risk aversion," *Mathematics of Operations Research*, vol. 35, no. 3, pp. 580-602, 2010.

[41] Y. Chen, W. Wei, F. Liu, and S. Mei, "Distributionally robust hydro-thermal-wind economic dispatch," *Applied Energy*, vol. 173, pp. 511-519, 2016/07/01/ 2016, doi: https://doi.org/10.1016/j.apenergy.2016.04.060.

NOMENCLATURE

A. Cyber-Attack Modelling

z, x	Measurement and state variable.
$\mathbf{h(x)}$	Nonlinear vector function of state variable.
$\mathbf{e}$	Error measurement.
$\mathbf{z_{bad}}, \hat{\mathbf{x}}_{\mathbf{bad}}$	Measurement and sate variable after the realization of false data injection (FDI).
$\mathbf{c}$	Resulted deviation vector of state variable after FDI
$\mathbf{W}$	Diagonal matrix of errors.
$\mathbf{KP}$	Bus-generator incidence matrix.
$\mathbf{KD}$	Bus-load incidence matrix.
$\mathbf{SF}$	Shift factor matrix.
γ	Attack injection level.
$\mathbf{\Delta G, \Delta D, \Delta BP, \Delta PL}$	Incremental vector of generator output, bus power injection and line flow.
$\mathbf{G}, \mathbf{D}, \mathbf{BP}, \mathbf{PL}$	Vector of generator output, load demand, bus power injection and line flow.
$\overline{\mathbf{PL}}, \underline{\mathbf{PL}}$	Upper and lower limit of intial branch flow.

B. Indices

t, T	Index and set for time periods.
i, I	Index and set for fuel generators.
w, W	Index and set for renewable generators.
l, L	Index and set for transmission lines.
k, K	Index and set for loads.

C. Parameters

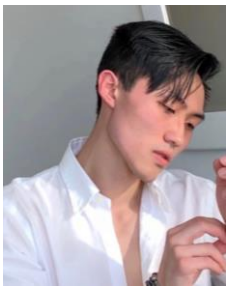
a_i, b_i, c_i	Cost coefficients for fuel generators.
λ^+, λ^-	Cost coefficient for up and down spinning reserve.
$\lambda_i^{re}, \lambda_w^{re}$	Regulation cost coefficient for fuel generator i and renewable generator w.
λ_k^{ls}	Penalty cost coefficient for load shedding on demand k.
$\omega_w^f(t)$	Forecasted output of renewable generator j at time t.
Res_i^+, Res_i^-	Maximum up and down spinning reserve capacity of fuel generator i at time t.
$P_{i,max}, P_{i,min}$	Maximum and minimum output of fuel generator i.
x_l	Reactance of line l.
$PL_{l,max}$	Maximum line flow of line l.
$P_k(t)$	Load k at time t.
$P_{k,max}^{ls}(t)$	Maximum load shedding of load d at time t.

D. Variables and functions

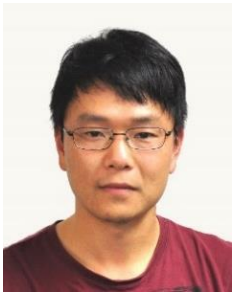
$P_i^s(t), P_i^{re}(t)$	Scheduled and regulated output of fuel generator i at time t.
$res_i^+(t), res_i^-(t)$	Up and down spinning reserve of fuel generator i at time t.
$PL_l^s(t), PL_l^{re}(t)$	Scheduled and regulated power flow at time t.
$PL_l^{s,ini}(t), PL_l^{re,ini}(t)$	Scheduled and regulated power flow injection at time t.
$PL_l^{s,ter}(t), PL_l^{re,ter}(t)$	Scheduled and regulated power flow at time t.
$\theta_l^s(t), \theta_l^{re}(t)$	Phase angle of line l in the first and second stage.
$\omega_w^s(t), \omega_w^{re}(t)$	Scheduled and regulated renewable generation at time t.
$P_k^{ls}(t)$	Load shedding of load d at time t.
x, y	Vectors of first and second stage variables.
$Pr(\ )$	Probability function.
$E_P[\ ]$	Expectation over distribution.
$\langle\ \rangle$	Trace of matrix.
$\mathbf{\psi_0}, \mathbf{\psi_j}, \Psi_{jk}, \tau$	Dual variables.

E. Uncertainty

$\mathbf{\xi_r(t)}$	Uncertainty of renewable power forecast at time t.
$\mathbf{\Delta P_k(t)}$	Load redistribution attack vector.
D_k, D_r	Ambiguity set for load redistribution attacks and renewable forecast uncertainty.
$\mathbf{\mu_k}, \mathbf{\mu_r}$	Mean vector for load redistribution attacks and renewable forecast uncertainty.
$\mathbf{\Sigma_k}, \mathbf{\Sigma_r}$	Covariance for load redistribution attacks and renewable forecast uncertainty.
$\mathbf{\Theta}$	Second moment matrix.
VS	Polyhedral set of extreme points.



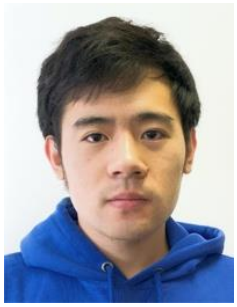
Pengfei Zhao (S'18) was born in Beijing, China. He received the double B.Eng. degree from the University of Bath, U.K., and North China Electric Power University, Baoding, China, in 2017. He received the Ph.D degree from the University of Bath, U.K. He was a visiting Ph.D. student at Smart Grid Operations and Optimization Laboratory (SGOOL), Tsinghua University, Beijing, China in 2019. He is currently an Assistant Professor at the State Key Laboratory of Management and Control for Complex Systems, Institute of Automation, Chinese Academy of Sciences. His major research interests include the intelligent decision-making of complex energy systems and public health big data.



Chenghong Gu (M'14) was born in Anhui province, China. He received the Master's degree from the Shanghai Jiao Tong University, Shanghai, China, in 2007 in electrical engineering. He received the Ph.D. degree from the University of Bath, U.K. He is currently a Lecturer and EPSRC Fellow with the Department of Electronic and Electrical Engineering, University of Bath. His major research interest is in multi-vector energy system, smart grid, and power economics.

Yucheng Ding was born in China in 1990. He received the B.S. degree in electronic and information engineering and the M.S. degree in control theory and control engineering both from Liaoning Technical University, Liaoning, China, in 2013 and 2016, respectively. He is currently pursuing Ph.D. degree at China Electric Power Research Institute. His research interests include power system security and stability, AI applications in power systems.

HONG LIU received the B.S., M.S. and Ph.D. degree in electrical engineering from Tianjin University in 2002, 2005 and 2009, respectively. He is currently a Professor with the School of Electrical and Information Engineering, Tianjin University. His research interests include planning, operation simulation and analysis in smart distribution system and integrated energy system. He has contributed to a number of research projects granted from National Natural Science Foundation of China and industry corporations as principal investigator. He has published more than 40 peer-reviewed academic papers and holds more than 10 invention patents of China. Prof. Liu has been a reviewer of IEEE Transactions on Power System, IEEE Transactions on energy conversion and Applied Energy.



Yuankai Bian received the B.Eng. degree in electrical and electronic engineering from Huazhong University of Science and Technology, Wuhan, China, and the University of Birmingham, U.K., in 2013; and the MSc and PhD degrees in Electrical Engineering from the University of Bath, U.K., in 2014 and 2019. He is currently a postdoc research associate with the University of Bath. His research interests include the optimisation of power system operation and planning, and power system economics.

Shuangqi Li was born in Beijing province, China. He received the B.Eng. degree in vehicle engineering from Beijing Institute of Technology, Beijing, China, in 2018. He worked as a research assistant at the National Engineering Laboratory for Electric Vehicles, Beijing Institute of Technology from 2018 to 2019. Currently, he is pursuing the Ph.D. degree at the Department of Electronic and Electrical Engineering, University of Bath. His major research interest is the big data analysis, deep-learning algorithm, operation and planning of smart grid system and V2G service.