Dynamic-Line-Rating-Based Robust Corrective Dispatch Against Load Redistribution Attacks With Unknown Objectives

Min Zhou, *Student Member, IEEE*, Jing Wu, *Senior Member, IEEE*, Chengnian Long, *Senior Member, IEEE*, Chensheng Liu, *Member, IEEE*, and Deepa Kundur, *Fellow, IEEE*

***Abstract*—Load redistribution (LR) attacks have proven to be hard-detectable and damaging, which require effective corrective schemes to mitigate the impact on power grid operations. Traditional game-theoretic methods and corrective dispatches employing static line rating (SLR) have been studied for attack mitigation based on specific attack objectives but have high dispatch cost and limited performance of attack mitigation. This is because the power transfer capacity of the existing transmission network is underestimated with SLR, and in practical operations, the specific objective of the adversary is not available to the defender, which would introduce uncertainties to the design of corrective schemes. As such, this article incorporates the dynamic line rating (DLR) technology, which enhances the power transfer capability of the existing network, to develop the cost-effective corrective dispatch for mitigating LR attacks with unknown objectives. Specifically, a DLR-based robust corrective (DRC) dispatch model is presented, which guarantees the system security as well as the economic performance. A methodology utilizing the robust counterpart technique and column constraint generation (CCG) algorithm is proposed to solve the dispatch model in a decomposition framework. Case studies based on the IEEE 14- and 118-bus systems verify the performance of the proposed DRC dispatch in enhancing the cyber–physical security of power grids.**

***Index Terms*—Attack mitigation, cyber–physical systems, dynamic line rating (DLR), load redistribution (LR) attacks, robustness.**

I. Introduction

POWER grids are increasingly vulnerable to cyberattacks due to the integration of Internet of Things (IoT) technologies. Vulnerabilities of the IoT devices and IoT communication protocols make it possible for adversaries to disrupt system operations through compromising sensor measurements [1]–[3]. For example, load redistribution (LR) attacks [4], which coordinately compromise load and line flow measurements, can mislead generation dispatch without being detected by system operators. Due to its low cost and great stealthiness, the LR attack is widely used in various attack cases as a crucial part and has been shown to cause severe physical and economic consequences, including power loss [4], [5], line overload [6]–[8], increased generation cost [9], [10], etc. Therefore, it is imperative to investigate effective strategies to reduce the malicious impact of the LR attack on IoT-based power grids.

In the literature, countermeasures have been widely studied to protect the IoT-based power grids from the LR attacks. Various attack prevention methods, such as protection of critical meters [11]–[13], strengthening of vulnerable transmission lines [14]–[16], reconfiguration of system parameters [17]–[19], etc., were studied to reduce the attack surfaces and increase the attack difficulty. However, due to the operational cost and resource constraints, it is unrealistic to secure all critical and vulnerable assets and to apply frequent parameter reconfigurations. Therefore, it is vital to deploy attack mitigation schemes to reduce or alleviate the potential disruptions and damages caused by the LR attacks.

To reduce the impact of attacks, some previous studies have developed attack mitigation strategies based on attack detection results. Li *et al.* [20] designed an attack mitigation scheme for load frequency control application, where the system adjustment signal that is detected abnormal is replaced with the signal generated by a GAN network to recover the system stability. In [21], a cyber-secured unit commitment model was proposed to generate the cyber-secured operating point, which is used to alleviate the attack-induced overloads if the LR attack is detected. In [22], with the combinations of observable PMUs or smart sensors, a logic judgment matrix-based algorithm was proposed to isolate the attacks through comparing the detection decision with the columns of the judgment matrix. In [23], an iterative optimization-based method was proposed to recover the preattack values by correcting the outliers detected by the attack detection algorithm in [24]. However, heavy reliance on the detection schemes

Manuscript received 26 October 2021; revised 24 February 2022; accepted 14 March 2022. Date of publication 21 March 2022; date of current version 7 September 2022. This work was supported by the National Natural Science Foundation of China under Grant 62136006, Grant 62073215, Grant 62073138, and Grant 61873166. *(Corresponding authors: Jing Wu; Chengnian Long.)*

Min Zhou, Jing Wu, and Chengnian Long are with the Department of Automation, Shanghai Jiao Tong University, Shanghai 200240, China, and also with the Key Laboratory of System Control and Information Processing, Ministry of Education, Shanghai 200240, China (e-mail: zhoumin15@sjtu.edu.cn; jingwu@sjtu.edu.cn; longcn@sjtu.edu.cn).

Chensheng Liu is with the Key Laboratory of Smart Manufacturing in Energy Chemical Processes, Ministry of Education, East China University of Science and Technology, Shanghai 200237, China (e-mail: cliu@ecust.edu.cn).

Deepa Kundur is with the Department of Electrical and Computer Engineering, University of Toronto, Toronto, ON M5S 3G4, Canada (e-mail: dkundur@ece.utoronto.ca).

Digital Object Identifier 10.1109/JIOT.2022.3160864

might induce extra computational costs and result in a delay in attack mitigation. Considering these issues, attack mitigation strategies that are independent of detection schemes have been recently studied using the game-theoretic framework. For example, a minimax-regret criterion-based model was presented in [25] to determine the optimal security resources allocation for reducing the damage after an LR attack, where the attack objective is modeled as maximizing the system operation cost. Similarly, a tri-level model considering interactions among defenders, attackers, and operators was developed in [26] to mitigate the impact of LR attacks on both load shedding and line overloads, where the attack objective is modeled as maximizing the load shedding. Moreover, taking into account the presence of insider threats in practical operations, a defender–attacker model with information leakage was proposed in [27] to mitigate the impact of LR attacks on system operation cost, where the payoffs of the defender and attacker at the Nash Equilibrium are calculated. In addition to these game-theoretic methods, various corrective generation dispatches have also been investigated for attack mitigation, such as the real-time cyber-secured generation dispatch [28] and the two-stage scheme incorporating both day-ahead and real-time generation dispatch [29], where the line overload problem caused by the LR attacks can be addressed without attack detection schemes.

Although the studies listed above have yielded fruitful results on mitigating the LR attacks, there are still challenges involved. On the one hand, the mitigation strategies developed in the game-theoretic framework are attack-specific, as they are designed based on the assumption that the attack objective is known to the defender. In reality, however, the attacks can have various objectives, and it is difficult for system defenders to realize the specific objective of the attack, which might significantly reduce the performance of the proposed methods. That is, the mitigation strategies based on a specific attack objective are infeasible to deal with diverse LR attacks in practical operations. On the other hand, even though the corrective generation dispatches in [28] and [29] make efforts to address the attack objective uncertainties, the flexibility of the dispatch is limited due to the underestimated power transfer capability of the transmission network, which results in unnecessary generation cost and limited attack-mitigation performance. Specifically, in these studies, static line rating (SLR) was utilized to represent the capacity of a line, which is conservative because the actual line capacity varies depending on real-time meteorological conditions and is greater than the SLR most of the time [30]. In practice, the technology of dynamic line rating (DLR) that calculates the real-time thermal rating has been recently investigated [31], [32], which can be used to enhance the power transfer capability of the existing transmission network.

Motivated by the above challenges, this article takes advantage of the DLR technology to design a robust corrective dispatch to ensure the cyber–physical security of power grids after diverse LR attacks without assuming specific attack objectives. The main contributions are listed as follows.

1) This article proposes a DLR-based robust corrective (DRC) dispatch strategy to mitigate diverse LR attacks with unknown objectives without relying on attack detection results. It shows that the proposed DRC dispatch is able to keep the power grids secure against all possible LR attacks while ensuring the operating economy.
2) This article reveals the tradeoff between costs and benefits of incorporating DLR into mitigation of LR attacks and formulates a weighted multiobjective robust optimization to coordinately determine the optimal line rating and the associated mitigation strategy, where the risk of violating the operation safety arising from increased line ratings can be reduced while eliminating the attack impacts.
3) A solution method based on the robust counterpart technique and the cutting-plane algorithm is designed, which can solve the formulated optimization in a decomposition framework with reasonable computational resources.
4) Numerical studies based on IEEE 14- and 118-bus test systems validate the cost effectiveness of the proposed DRC dispatch. The results help to identify the most vulnerable transmission lines under the LR attacks.

The remainder of this article is organized as follows. Section II introduces the model of the LR attacks and the DLR technology. Section III presents the proposed DRC dispatch for mitigating LR attacks with unknown objectives. The corresponding solution methodology is presented in Section IV. The numerical simulation results are provided in Section V before concluding this article in Section VI.

TABLE I
SUMMARY OF NOMENCLATURE

Notation	Definition
$\mathbf{SF}$	shift factor matrix
$\mathbf{KP}$	bus-generator incidence matrix
$\mathbf{KD}$	bus-load incidence matrix
$\boldsymbol{P}_d^t$	vector of actual load distribution
$\boldsymbol{P}_d$	vector of observed load distribution
$\Delta\boldsymbol{P}_d$	vector of injected load measurements of LR attack
$\Delta\boldsymbol{P}_f$	vector of injected line flow measurements of LR attack
$\boldsymbol{P}_g$	vector of robust generation dispatch
${P_f}_k^t$	actual power flow at line k
I_k	determined thermal rating of line k
$\underline{I}_k$, $\overline{I}_k$	SLR and DLR of line k
$\underline{P}_{g_i}$, $\overline{P}_{g_i}$	minimum, maximum power of generator i
τ	Upper bound of $\Delta P_{di}/P_{di}^{true}$ for each bus i
$\Omega(\tau)$	Uncertainty set of LR attacks within magnitude τ
$\lvert\mathcal{L}\rvert$	the cardinality of the set $\mathcal{L}$

II. PRELIMINARIES

We consider a power grid $\mathcal{G} = \{\mathcal{N}, \mathcal{L}\}$ with the set $\mathcal{N}$ of buses and the set $\mathcal{L}$ of transmission lines. The sets $\mathcal{N}_g \subseteq \mathcal{N}$ and $\mathcal{N}_d \subseteq \mathcal{N}$ denote the sets of generator buses and load buses, respectively. Some important notations in this article are summarized in Table I.

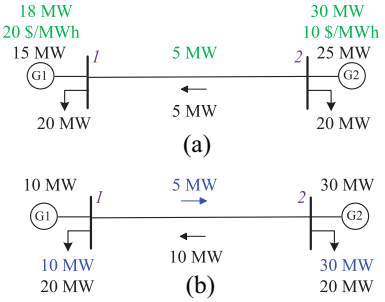

Fig. 1. Example to show the impact of LR attacks: (a) system without attack and (b) system with attack.

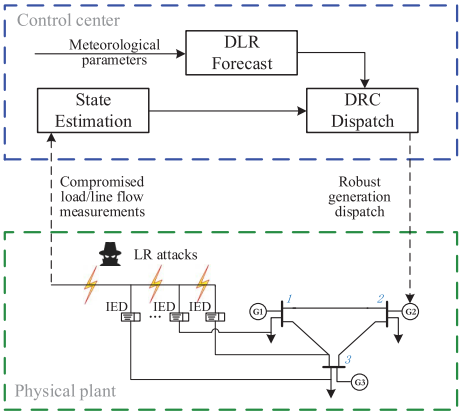

Fig. 2. System employing DRC dispatch under LR attacks.

A. LR Attack Model

The LR attack [4] is a type of data injection attack that achieves its attack objectives through masking the real load distribution. It manipulates the load measurements with the attack vector ΔP_d, such that the load distribution observed by system operators is

$$\mathbf{P}_d = \mathbf{P}_d^t + \Delta \mathbf{P}_d \tag{1}$$

where P_d^t is the actual value of the load distribution. To avoid being detected, the attack vector ΔP_d satisfies

$$\mathbf{1}^T \cdot \Delta \mathbf{P}_d = 0 \tag{2a}$$

$$-\tau \mathbf{P}_d^t \leq \Delta \mathbf{P}_d \leq \tau \mathbf{P}_d^t \tag{2b}$$

where (2a) ensures that the observed total load value remains unchanged, and (2b) represents the attack magnitude limitation, i.e., the attack on the load measurements does not exceed fraction τ (such as 50%) of its actual value. Also, the attacker cooperatively manipulates the line flow measurements to bypass the bad data detection according to

$$\Delta \mathbf{P}_f = -\mathbf{SF} \cdot \mathbf{KD} \cdot \Delta \mathbf{P}_d \tag{3}$$

where ΔP_f represents the attack on the line flow measurements, **SF** is the shift factor matrix of which the (k, i)th element denotes the change of the power flow at line k with a change in power injection of bus i, and **KD** is the bus-load incidence matrix.

The impact of the LR attacks can be seen from a simple 2-bus toy system shown in Fig. 1. The generator capacity, marginal cost, and line capacity are marked in green in Fig. 1(a). The actual load is 20 MW at both buses. For the system without attack, as shown in Fig. 1(a), the determined dispatch $P_{g_1} = 15$ MW and $P_{g_2} = 25$ MW enables the optimal economic operation without violating the safety requirements. However, in the system with an LR attack, as shown in Fig. 1(b), the generation dispatch is changed to $P_{g_1} = 10$ MW and $P_{g_2} = 30$ MW based on the observed measurements (marked in blue), making the actual line flow (10 MW) exceed the line capacity.

B. DLR Technology

DLR is developed to better exploit the power transfer capability of the power grid, by dynamically adapting the thermal rating of transmission lines based on the real-time meteorological conditions [33]. Even though the actual capacity of a transmission line for specific meteorological conditions is determined by its maximum allowable conductor temperature, which is selected to minimize the loss of conductor strength and to limit sag to maintain the allowed electrical clearance along the line, the line thermal rating is usually expressed in the form of line currents based on the current–temperature relationship of the line conductor. Specifically, according to the IEEE 738 standard [34], if the steady-state meteorological parameters and the conductor temperature are known, the real-time line conductor current can be calculated based on the steady-state heat balance

$$q_c + q_r = q_s + I^2 \cdot R(T_c) \tag{4}$$

where q_c, q_r, and q_s are the convective heat loss, radiative heat loss, and solar heating, respectively; and $R(T_c)$ represents the conductor resistance, which is a function of the conductor temperature T_c. Therefore, with a given maximum allowable conductor temperature $T_c^{\max}$, the thermal rating of the line is given by

$$I_{\max} = \sqrt{\frac{q_c + q_r - q_s}{R\left(T_c^{\max}\right)}} \tag{5}$$

where q_c, q_r, and q_s in (5) can be calculated using the formulas given in [34] with monitored or predicted meteorological parameters.

Note that finding accurate DLR is beyond the scope of this article. Refer to [32] for detailed information about calculating accurate forecast of DLR. In the remainder of this article, we assume that the forecast of DLR is available during the determination of the robust dispatch against the LR attacks.

III. DRC Dispatch Against LR Attacks With Unknown Objectives

In this article, in order to mitigate LR attacks with unknown objectives at a low dispatch cost, the robust dispatch taking advantage of the DLR technology is analyzed, and a DRC dispatch method is developed to ensure the system security. The system employing the DRC dispatch under LR attacks is shown in Fig. 2.

A. Robust Dispatch for Attack Mitigation

The objective of the robust dispatch is to mitigate uncertain LR attacks without depending on the attack detection results. From the defender's perspective, the observed load vector P_d is untrustworthy due to the potential threat of the LR attack. Suppose the defender makes a generation dispatch P_g based on the observed load data, the actual power flow of line k ($k \in \mathcal{L}$) resulting from the dispatch can be expressed as

$$P_{f_k}^t = \mathbf{SF}_{k\cdot} \cdot \left[\mathbf{KP} \cdot \mathbf{P}_g - \mathbf{KD} \cdot (\mathbf{P}_d - \Delta\mathbf{P}_d)\right]. \tag{6}$$

Note that the defender would face uncertainties about the actual power flow $P_{f_k}^t$, because it is difficult for the defender to estimate the attack value without the knowledge of the specific control objective of the attack.

In practice, even though the value of the attack vector $\Delta\mathbf{P}_d$ is not known to the defender, he knows that the attack must satisfy the certain conditions given by (1) and (2). That is, given the observed load data P_d, the defender is certain that for any attack within magnitude bound τ, the attack vector belongs to the set

$$\Omega(\tau) = \left\{\Delta\mathbf{P}_d | \mathbf{1}^T \cdot \Delta\mathbf{P}_d = 0,\ \frac{\tau\mathbf{P}_d}{\tau - 1} \le \Delta\mathbf{P}_d \le \frac{\tau\mathbf{P}_d}{\tau + 1}\right\}. \tag{7}$$

If the defender makes a dispatch such that for any attack in the set $\Omega(\tau)$ the actual power flow of the transmission network can remain within acceptable operating conditions, then it indicates that such dispatch can tolerate any attack realization bounded within τ. Motivated by this, we define the τ-robust dispatch as follows.

Definition 1 (Robust Dispatch): A dispatch P_g is called τ-robust if, with the dispatch P_g, the actual power flow satisfies[1]

$$\left|P_{f_k}^t\right| \le I_k \ \forall k \in \mathcal{L}\ \forall \Delta\mathbf{P}_d \in \Omega(\tau) \tag{8}$$

where I_k is the thermal rating of line k. In the remainder of this article, $|P_{f_k}^t| - I_k$ is used to represent the value of overload whose positive values indicate the abnormal operating conditions at line k.

Remark 1: While keeping the total load demand unchanged helps LR attacks avoid being detected, this characteristic also makes it reliable to design the robust dispatch without attack detection, because the robust dispatch determined based on the observed load data will not result in an imbalance between generation and load. This makes the robust dispatch a feasible defense method.

Remark 2: In the τ-robust dispatch, for a given value of τ, the set $\Omega(\tau)$ can be calculated with the real-time load measurements. Therefore, there is no need to make assumptions about the uncertainty set of the actual load distributions based on prior experience or data-driven approaches. Also, the τ-robust dispatch is effective in ensuring the operating safety no matter what the attack objective would be. These make the robust dispatch more practical than previous work [25] which assumes that the actual load belongs to a predefined load set and specifies the attack objective as maximizing the total system operation cost.

[1]Equation (8) represents the power flow limits at 1 p.u. voltage.

B. Benefits and Costs of Incorporating DLR

The robust dispatch described above can deal with the uncertainties about the LR attacks but is limited by the power transfer capacity of the transmission network. On the other hand, even though the existing transmission network allows the robust dispatch to have feasible solutions, the defender would implement the robust dispatch at the risk of increasing the generation cost. These drawbacks can be overcome by incorporating DLR into the design of the robust dispatch. Specifically, the extra available transmission line capacity from DLR could increase the possibility that the robustness design can have feasible solutions, and allow accommodating more low-cost generation to replace high-cost generation, which helps to keep the generation cost within the defender's budget.

However, due to the strong dependence of DLR on the meteorological conditions, meteorological uncertainties may cause forecast errors of DLR. Hence, the actual capacity cannot be perfectly estimated by the forecast of DLR, which may bring safety risk to the system operation. For example, if the actual capacity is less than the DLR due to the forecast error, then it is possible that the conductor heating makes the line sag into obstructions below such as trees or telephone lines without overload alarms. To avoid the risk of violating the operation safety arising from the forecast errors, the safety margins between the determined thermal ratings and the actual capacities of lines have to be taken into account. In this article, considering that: 1) SLR is too conservative and 2) the forecast of DLR is uncertain, we aim to find the optimal thermal rating in the range between SLR and DLR to design the generation dispatch, such that a τ-robust dispatch against LR attacks can be obtained with increased transmission capacity while ensuring reliability against forecast errors of DLR.

C. DRC Dispatch

Based on the above analysis, the DRC dispatch is proposed to determine the optimal thermal rating and the associated τ-robust dispatch, with the objectives of cooperatively minimizing the total generation cost and maximizing the safety margin of the transmission capacity. As there exists a fundamental tradeoff between these two objectives, the objective function is constructed as a weighted sum of the total generation cost and the determined thermal ratings to strike the balance. Similar to the traditional economic dispatch, the proposed DRC dispatch is a real-time application which should be performed every 15 min to maintain the system security. The mathematical formulation of the DRC dispatch is given as follows:

$$\text{(P0)}: \min_{\mathbf{P}_g, \mathbf{I}}\ \omega \cdot \sum_{i \in \mathcal{N}_g} c_i^g P_{g_i} + (1 - \omega) \cdot \sum_{k \in \mathcal{L}} I_k \tag{9a}$$

$$\text{s.t.}\ \sum_{i \in \mathcal{N}_g} P_{g_i} = \sum_{i \in \mathcal{N}_d} P_{d_i} \tag{9b}$$

$$\underline{P}_{g_i} \le P_{g_i} \le \overline{P}_{g_i},\quad i \in \mathcal{N}_g \tag{9c}$$

$$\underline{I}_k \le I_k \le \overline{I}_k,\quad k \in \mathcal{L} \tag{9d}$$

$$\left|\mathbf{SF}_{k\cdot} \cdot \left[\mathbf{KP} \cdot \mathbf{P}_g - \mathbf{KD} \cdot (\mathbf{P}_d - \Delta\mathbf{P}_d)\right]\right| \le I_k$$
$$\forall \Delta\mathbf{P}_d \in \Omega(\tau),\quad k \in \mathcal{L} \tag{9e}$$

where ω is a preset weight, and $\{P_g, I\}$ are the decision variables of the problem. The equality constraint (9b) is the power balance equation. Note that it is feasible to get the actual total load demand for the constraint (9b) from the observed load vector without detecting the LR attack, because the LR attack does not change the total value of the load distribution. The inequality (9c) represents the generation limits. The inequality (9d) represents the constraints on the determined thermal ratings, where $\underline{I}_k$ and $\overline{I}_k$ are the SLR and DLR, respectively, of line k. Here, the DLR value should be updated within 15 min, since the DLR value should be established prior to the real-time DRC dispatch [35]; this is viable because advanced tools have made it feasible to establish DLR in near real time, for example, the ensemble-learning method [32] has been used to generate the forecast value of DLR within 10 min. Inequality (9e) is the constraint ensuring the robustness of the dispatch according to (6) and Definition 1. Note that in this model, the incorporation of DLR technology can increase the possibility of finding feasible solutions for the robustness design simultaneously with the reduction of the dispatch cost incurred by the robustness design. That is, by coordinating the DLR technology with the robustness design, the system defenders are able to cost effectively address the issue that the attack objectives are unknown to them when mitigating the LR attacks.

The DRC dispatch model (P0) is a τ-robust dispatch where τ acts as a constant parameter. Given a specified value of τ, the optimal generation dispatch P_g obtained by solving the problem (P0) is able to mitigate all possible LR attacks whose attack magnitudes are less than or equal to the value of τ. Therefore, the larger the value of τ that is used to design the DRC dispatch, the better for system security under unknown LR attacks. However, the larger the value of τ used in the DRC dispatch, the more power transfer capacity will be required to ensure feasible solutions. Consequently, there are tradeoffs between the requirement of using physical system resources and security performance when selecting the value of τ in practical operations. Fortunately, since the power systems usually behave in a quasistatic manner [36], and the proposed dispatch method is a real-time application which is performed every 15 min (a very short period), it is expected that the load does not change much in normal conditions; thus, it is reasonable to assume that a rational adversary would implement LR attacks with small attack magnitude in case the attacks will be easily detected. As a result, it is unnecessary to set a large value of τ for the DRC dispatch in practical operations, for instance, the defender can set the value of τ equal to the upper bound of the historical load perturbation in a 15-min sampling time.

IV. Solution Methodology

The model (P0) formulated in Section III is a robust programming problem, where finitely many variables $\{P_g, I\}$ are subject to infinitely many inequality constraints given by (9e). As the problem (P0) is intractable in its current form, we apply the robust counterpart techniques to transform it into a bilevel optimization and solve it based on the column and constraint generation (C&CG) algorithm.

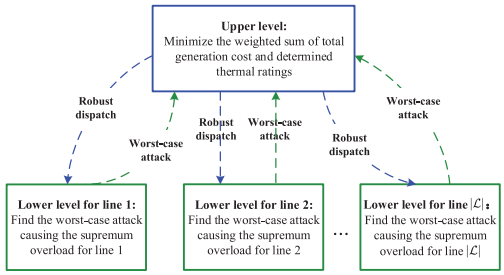

Fig. 3. Bilevel model of DLR-based robust dispatch.

A. Robust Counterpart of the Problem (P0)

To obtain the computationally tractable robust counterpart of (P0), the infinitely many constraints (9e) can be equivalently reformulated as the following finite set of constraints:

$$\max_{\Delta \mathbf{P}_d \in \Omega(\tau)} \left| \mathbf{SF}_{k\cdot} \cdot \left[\mathbf{KP} \cdot \mathbf{P}_g - \mathbf{KD} \cdot (\mathbf{P}_d - \Delta \mathbf{P}_d) \right] \right| \le I_k, \ \ k \in \mathcal{L} \tag{10}$$

because the feasibility of keeping the actual power flow within the rating value for all values of $\Omega(\tau)$ is equivalent to ensuring the supremum of the actual power flow over $\Omega(\tau)$ remains within the rating value.

Based on this reformulation, the original problem (P0) can be transformed into a bilevel optimization with $|\mathcal{L}|$ inner problems shown in Fig. 3. The mathematical formulation of the bilevel model is

$$(\text{P1}): \min_{\mathbf{P}_g, \mathbf{I}} \ \ \omega \cdot \sum_{i \in \mathcal{N}_g} c_i^g P_{g_i} + (1-\omega) \cdot \sum_{k \in \mathcal{L}} I_k \tag{11a}$$

$$\text{s.t.} \ \sum_{i \in \mathcal{N}_g} P_{g_i} = \sum_{i \in \mathcal{N}_d} P_{d_i} \tag{11b}$$

$$\underline{P}_{g_i} \le P_{g_i} \le \overline{P}_{g_i}, \ \ i \in \mathcal{N}_g \tag{11c}$$

$$\underline{I}_k \le I_k \le \overline{I}_k, \ \ k \in \mathcal{L} \tag{11d}$$

$$O_k^* \le 0, \ \ k \in \mathcal{L} \tag{11e}$$

$$O_k^* = \max_{\Delta \mathbf{P}_d} \left\{ \left| \mathbf{SF}_{k\cdot} \cdot \left[\mathbf{KP} \cdot \mathbf{P}_g - \mathbf{KD} \cdot (\mathbf{P}_d - \Delta \mathbf{P}_d) \right] \right| - I_k \right. \tag{11f}$$

$$\text{s.t.} \ \ \mathbf{1}^T \cdot \Delta \mathbf{P}_d = 0 \tag{11g}$$

$$\left. \frac{\tau \mathbf{P}_d}{\tau - 1} \le \Delta \mathbf{P}_d \le \frac{\tau \mathbf{P}_d}{\tau + 1} \right\}, \ \ k \in \mathcal{L}. \tag{11h}$$

Different from the traditional bilevel optimization in which the upper level problem interacts with only one lower level problem, problem (P1) has $|\mathcal{L}|$ lower level problems interacting with the upper level. Specifically, given the value of $\{P_g, I\}$ from the upper level, each lower level problem (11f)–(11h) indexed by k identifies the supremum of overload of line k under all LR attacks. The supremum values O_k^*, $k \in \mathcal{L}$ are then transferred to the upper level to update the robust dispatch strategy and the thermal ratings.

B. C&CG Algorithm

Since the lower level problems of (P1) are nonconvex due to the absolute function in (11f) and the convexification would introduce binary variables, it is difficult to directly

apply either the Karush–Kuhn–Tucker conditions or the strong duality theorem to obtain the equivalent single-level formulation of (P1). Hence, it is better to solve problem (P1) in a master-subproblem decomposition framework with cutting-plane methods. As the binary variables for convexifying the absolute function prevent deriving dual variables to formulate dual cuts, the C&CG algorithm [37] generating primal cuts for solving the problem is used in this article.

1) Subproblem: For each transmission line k, the subproblem of (P1) calculates the corresponding worst case LR attack that causes the maximal overload for a given master problem solution $\{P_g, I\}$. To obtain the tractable subproblem, the objective function (11f) needs to be linearized. Specifically, we introduce auxiliary variables s_k, t_k and use big-M reformulations to remove the absolute functions in (11f) as follows:

$$\begin{aligned}
&\left|\mathbf{SF}_{k\cdot}\cdot\left[\mathbf{KP}\cdot\mathbf{P}_g-\mathbf{KD}\cdot(\mathbf{P}_d-\Delta\mathbf{P}_d)\right]\right|=s_k+t_k\\
&\mathbf{SF}_{k\cdot}\cdot\left[\mathbf{KP}\cdot\mathbf{P}_g-\mathbf{KD}\cdot(\mathbf{P}_d-\Delta\mathbf{P}_d)\right]=s_k-t_k\\
&0\le s_k\le M\cdot\sigma_k\\
&0\le t_k\le M\cdot(1-\sigma_k)\\
&\sigma_k\in\{0,1\}. \qquad (12)
\end{aligned}$$

By substituting (12) into (11f), we obtain the subproblem consisting of a set of mixed-integer linear problems indexed by k. The mathematical formulation is given by

$$\begin{aligned}
(\mathrm{SP}):\ &\left\{O_k^*=\max_{\Delta\mathbf{P}_d,s_k,t_k,\sigma_k} s_k+t_k-I_k \right. && (13a)\\
\text{s.t. }&\mathbf{SF}_{k\cdot}\cdot\left[\mathbf{KP}\cdot\mathbf{P}_g-\mathbf{KD}\cdot(\mathbf{P}_d-\Delta\mathbf{P}_d)\right]=s_k-t_k && (13b)\\
&0\le s_k\le M\cdot\sigma_k && (13c)\\
&0\le t_k\le M\cdot(1-\sigma_k) && (13d)\\
&\sigma_k\in\{0,1\} && (13e)\\
&\mathbf{1}^T\cdot\Delta\mathbf{P}_d=0 && (13f)\\
&\left.\frac{\tau\mathbf{P}_d}{\tau-1}\le\Delta\mathbf{P}_d\le\frac{\tau\mathbf{P}_d}{\tau+1}\right\},\quad k\in\mathcal{L} && (13g)
\end{aligned}$$

which can be solved using commercial solvers, such as "MOSEK" [38]. The optimal solution is a set of worst case attack vectors, each of which corresponds to the maximal overload for every transmission line. Let

$$\left\{\Delta\mathbf{P}_d^*(1,j),\ \Delta\mathbf{P}_d^*(2,j),\ldots,\Delta\mathbf{P}_d^*(|\mathcal{L}|,j)\right\}$$

denote the set of worst case attacks obtained at the jth interaction, then a set of cutting planes in the form of

$$\left|\mathbf{SF}_{k\cdot}\cdot\left[\mathbf{KP}\cdot\mathbf{P}_g-\mathbf{KD}\cdot\left(\mathbf{P}_d-\Delta\mathbf{P}_d^*(k,j)\right)\right]\right|\le I_k,\quad k\in\mathcal{L} \qquad (14)$$

can be generated, which are then included into the master problem.

2) Master Problem: The master problem is a valid relaxation of the original problem (P1). The initial master problem is obtained from (P1) by removing constraints (11e)–(11h). During the C&CG calculation procedure, the cutting planes generated from the subproblem are iteratively added to the master problem. Given any master problem solution, the optimal solution of the subproblem is an extreme point of its feasible region, thus the generated cutting planes are the feasibility cuts of the original problem (P1). Hence, adding the cutting planes would narrow the search space to include the feasible solutions of (P1). After j iterations, the master problem is

$$\begin{aligned}
(\mathrm{MP}):\ &\min_{\mathbf{P}_g,\mathbf{I}}\ \omega\cdot\sum_{i\in\mathcal{N}_g}c_i^gP_{g_i}+(1-\omega)\cdot\sum_{k\in\mathcal{L}}I_k && (15a)\\
\text{s.t. }&\sum_{i\in\mathcal{N}_g}P_{g_i}=\sum_{i\in\mathcal{N}_d}P_{d_i} && (15b)\\
&\underline{P}_{g_i}\le P_{g_i}\le\overline{P}_{g_i},\quad i\in\mathcal{N}_g && (15c)\\
&\underline{I}_k\le I_k\le\overline{I}_k,\quad k\in\mathcal{L} && (15d)\\
&\left|\mathbf{SF}_{k\cdot}\cdot\left[\mathbf{KP}\cdot\mathbf{P}_g-\mathbf{KD}\cdot\left(\mathbf{P}_d-\Delta\mathbf{P}_d^*(k,l)\right)\right]\right|\le I_k\\
&k\in\mathcal{L}\ \ \forall l\le j. && (15e)
\end{aligned}$$

3) Detailed Procedure of C&CG Algorithm: The detailed algorithm to solve problem (P1) is summarized as follows.

1) Initialization with the number of iteration $j=0$.
2) Solve the master problem (15) (or the initial master problem when $j=0$), determine the optimal solution $\{P_g(j), I(j)\}$.
3) Solve the subproblem (13) based on $\{\mathbf{P}_g(j), \mathbf{I}(j)\}$, determine the set of worst case attack vectors, i.e.,

$$\left\{\Delta\mathbf{P}_d^*(1,j),\ \Delta\mathbf{P}_d^*(2,j),\ldots,\Delta\mathbf{P}_d^*(|\mathcal{L}|,j)\right\}$$

and update the corresponding maximal overload $O_k^*(j)$ for each transmission line, i.e.,

$$O_k^*(j)=\left|\mathbf{SF}_{k\cdot}\cdot\left[\mathbf{KP}\cdot\mathbf{P}_g(j)-\mathbf{KD}\cdot\left(\mathbf{P}_d-\Delta\mathbf{P}_d^*(k,j)\right)\right]\right|-I_k(j).$$

4) If $O_k^*(j)\le 0$ for all $k\in\mathcal{L}$, return $\{P_g(j), I(j)\}$ and terminate. Otherwise, set $j\leftarrow j+1$, generate the new set of cuts based on (14) and go to step 2).

V. Case Studies

In this section, case studies based on the IEEE 14- and 118-bus test systems are conducted to validate the effectiveness of the DRC dispatch against uncertain LR attacks and to demonstrate the impact of incorporating DLR on the economic and secure performance of power systems. We also compare the effects of the proposed DRC dispatch and traditional corrective dispatch. The software toolbox MATPOWER [39] is used to provide initial information of the test systems. The toolbox "YALMIP" [40] together with the "MOSEK" solver [38] are used to solve the subproblem and master problem to obtain the optimal DRC dispatch.

A. Cost Effectiveness of the DRC Dispatch

To show the effectiveness of the proposed DRC dispatch in detail, we use the IEEE 14-bus system as the test system. The load data used in the tests and the generator parameters are given in Tables II and III, respectively. The value of SLR is 60 MW for all the transmission lines, and the value of DLR is set to be 1.4 times SLR. Other configuration data of the test system is obtained from the MATPOWER package [41].

For comparison, we implement the following two types of dispatches.

TABLE II
LOAD DATA (MW)

Bus	2	3	4	5	6	9	10	11	12	13	14
Case 1	26.04	113.04	57.36	9.12	13.44	35.4	10.8	4.2	7.32	16.2	17.88
Case 2	36.7	224.2	17.8	52.6	11.2	29.5	9.0	3.5	6.1	13.5	39.9

TABLE III
GENERATOR PARAMETERS

Gen. bus	1	2	3	6	8
Gen. cost ($/MWh)	20	20	40	40	40
Gen. capacity (MW)	332.4	140	100	100	100

TABLE IV
GENERATION OUTPUTS (MW) AND COST OF THE BASE-CASE DISPATCH AND THE DRC DISPATCH

Gen. bus	Base-case disp.	DRC disp.		
		$\tau = 0.1$	$\tau = 0.3$	$\tau = 0.5$
1	114.37	146.57	141.13	135.12
2	135.36	140	129.60	118
3	45.45	24.23	40.08	54.76
6	0	0	0	2.93
8	15.63	0	0	0
Total cost ($/h)	7437.5	6700.5	7017.5	7369.8

1) *Base-Case Dispatch:* economic dispatch where SLR is applied and LR attacks are not considered.
2) Proposed DRC dispatch with different values of τ. (Note that adversaries usually do not launch the LR attacks whose magnitude level is greater than 0.5 for the purpose of avoiding detection. Hence, the value of τ considered in our tests will not exceed 0.5.)

Table IV shows the generation outputs and total generation cost corresponding to the base-case dispatch and the DRC dispatches with $\tau = 0.1$, $\tau = 0.3$, and $\tau = 0.5$. The actual load is case 1. It can be seen that the total generation cost of the base-case dispatch is 7437.5 $/h. Compared to the base-case dispatch which only considers the economic performance of the system, the DRC dispatch results in lower total generation cost, even when $\tau = 0.5$. This is because in the base-case dispatch, SLR limits the output of the low-cost generator at bus 1. In contrast, in the DRC dispatch, the additional power transfer capacity allows the low-cost generator at bus 1 to generate more power, and thus, results in a cost reduction.

Table V provides the information about the optimally determined thermal ratings in the different DRC dispatches and the corresponding safety margins. $\mathcal{L}_D$ represents the index of transmission lines that have thermal ratings greater than the SLR, and the indices in the bold text refer to the lines where the optimally determined thermal rating is equal to the DLR. It shows that in the DRC dispatch with a higher level of robustness, more transmission lines benefit from the DLR technology as their capacities are better utilized. For example, in the DRC dispatch with $\tau = 0.5$, nine transmission lines, i.e., {**1**, 2, **3**, 4, 5, 7, 8, **10**, 15}, have increased thermal ratings, where the capacity of lines 1, 3, and 10 is fully utilized with the thermal rating equal to the DLR. It can be inferred that the transmission lines 1, 3, and 10 are more vulnerable to LR attacks since they would carry more power under attack. In addition, the results show that the DRC dispatch with $\tau = 0.1$, $\tau = 0.3$, and $\tau = 0.5$ are able to avoid the safety risk resulting from the forecast errors of DLR, with the safety margins being 417.32, 396.75, and 369.57 MW, respectively. These sufficient safety margins indicate that with the proposed DRC dispatch, the risk of violating the operation safety due to the increased line ratings can be avoided.

TABLE V
LINES WITH INCREASED THERMAL RATINGS AND SAFETY MARGINS IN DIFFERENT DRC DISPATCHES

	$\mathcal{L}_D$	Safety margin (MW)
$\tau = 0.1$	$\{\mathbf{1}, 2, 3, 4, 7\}$	417.32
$\tau = 0.3$	$\{\mathbf{1}, 2, \mathbf{3}, 4, 7, 10\}$	396.75
$\tau = 0.5$	$\{\mathbf{1}, 2, \mathbf{3}, 4, 5, 7, 8, \mathbf{10}, 15\}$	369.57

TABLE VI
OVERLOADS (MW) OF EACH TRANSMISSION LINE CAUSED BY THE CORRESPONDING WORST CASE LR ATTACK UNDER THE BASE-CASE DISPATCH AND DRC DISPATCH

# of	$\tau = 0.1$		$\tau = 0.3$		$\tau = 0.5$	
line	Base-case	DRC	Base-case	DRC	Base-case	DRC
1	**1.77**	0	**4.89**	0	**7.97**	0
2	-4.06	0	-1.23	0	**1.24**	0
3	**5.45**	0	**19.07**	0	**27.54**	0
4	**2.52**	0	**7.03**	0	**10.91**	0
5	-8.13	-2.88	-3.54	-0.23	**0.48**	0
6	-44.34	-36.77	-25.83	-25.39	-14.03	-19.79
7	-8.57	0	-1.00	0	**8.35**	0
8	-30.86	-21.18	-19.02	-9.19	-6.22	0
9	-39.80	-37.34	-32.89	-30.34	-25.42	-23.15
10	-7.81	-4.32	**6.73**	0	**22.92**	0
11	-52.58	-50.48	-47.9	-45.94	-40.74	-38.33
12	-50.19	-49.88	-47.24	-4695	-42.19	-41.84
13	-38.18	-37.09	-31.41	-30.40	-20.19	-18.85
14	-44.37	-60	-44.37	-60	-44.37	-60
15	-15.23	-21.18	-3.39	-9.19	**9.41**	0
16	-47.97	-50.07	-41.69	-43.65	-31.48	-33.89
17	-44.2	-45.58	-37.64	-38.93	-26.67	-28.27
18	-56.85	-54.75	-52.57	-50.62	-46.47	-44.05
19	-57.62	-57.31	-55.37	-55.08	-52.01	-51.65
20	-53.41	-52.02	-48.62	-47.32	-41.29	-39.7

Table VI illustrates the maximum attack-induced overload of each transmission line in the systems employing the base-case dispatch and the DRC dispatch. The value of overload is calculated using $|P_{f_k}^t| - I_k$ as indicated in Definition 1, which would be positive during the abnormal operating conditions. The results show that in the system employing the base-case dispatch, the numbers of transmission lines that could be in abnormal operating conditions are 3, 5, and 8 under the LR attacks of the magnitude levels 0.1, 0.3, and 0.5, respectively. However, in the system employing the DRC dispatches, all the transmission lines are operating within their capacities even under the worst case LR attacks. In summary, the results from Tables IV–VI indicate the cost effectiveness of the proposed DRC dispatch and its ability to tolerate DLR forecast errors.

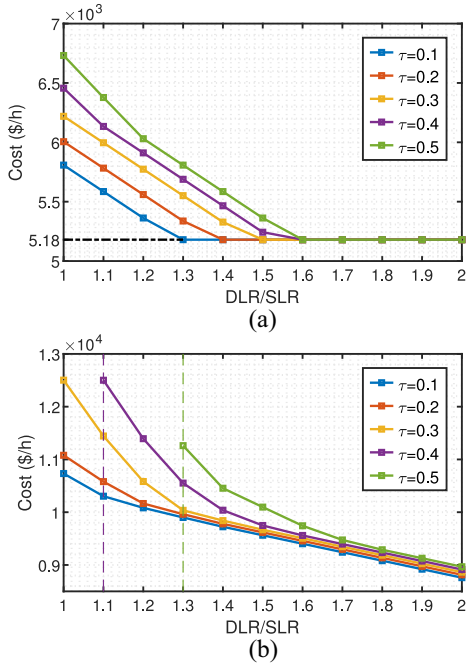

Fig. 4. Impact of DLR incorporation on power systems operating at different load levels. (a) Base-case load level. (b) High load level.

B. Impact of DLR Incorporation

To show the impact of the incorporation of DLR, we implement

1) robust corrective dispatch without incorporating DLR;
2) proposed DRC dispatch

to compare their effects in mitigating LR attacks of different magnitude levels. Here, we use the IEEE 14-bus test system as an example. In the implementation of the proposed DRC dispatch, different ratios of DLR to SLR are used to simulate different meteorological conditions, considering the possible influence of varying meteorological environment. In the robust dispatch without incorporating DLR, the value of SLR is used to establish the corresponding robustness constraint, and the objective is set to only minimize the total generation cost. Moreover, two different load scenarios are used in the tests to include the effect of load level.

Fig. 4 shows the simulation results corresponding to a base-case load level and a high load level, where the total generation costs for maintaining robustness against LR attacks of magnitude (i.e., τ) ranging from 0.1 to 0.5 are illustrated. The base-case load is obtained from the MATPOWER package [41], and the high load level is set to be 150% of the base-case load level. It should be noted that with DLR/SLR=1, the total generation cost corresponds to the robust corrective dispatch without incorporating DLR. And for the dispatches that have no feasible solution, the total generation cost is null, which will not be displayed on the graph.

As shown in Fig. 4(a), at the base-case load level, both types of the robust corrective dispatches are feasible to mitigate LR attacks even when $\tau = 0.5$. However, the robust corrective dispatch without incorporating DLR has a higher total generation cost compared to the proposed DRC dispatch. In fact, for the proposed DRC dispatch, the total generation cost decreases with the value of DLR and will reach the minimum cost, i.e., $5.18e^3$\$/h, under some good meteorological conditions. Therefore, at a low load level, incorporating DLR into the robust dispatch makes it possible to mitigate uncertain LR attacks with the minimum dispatch cost. By comparison, as shown in Fig. 4(b), when the system is operating at a high load level, the robust corrective dispatch without incorporating DLR is infeasible to mitigate the LR attacks of high magnitude levels, while the proposed DRC dispatch is feasible to mitigate the LR attacks of these magnitudes under some good meteorological conditions. For example, when the proposed DRC dispatch is applied, the LR attacks bounded within $\tau = 0.4$ and $\tau = 0.5$ can be mitigated under the meteorological conditions where DLR/SLR$\geq$1.1 and DLR/SLR$\geq$1.3, respectively. In summary, the incorporation of DLR can significantly improve both the economic and secure performance of power systems, especially when the systems are operating at a high load level.

C. Comparison of Mitigation Strategies With and Without Assuming Specific Attack Objectives

To show the advantage of not specifying attack objectives in the design of mitigation strategies, we test both the proposed DRC dispatch that does not specify attack objectives and a traditional attack-specific mitigation strategies for comparison. Similar to [25], the traditional attack-specific strategy is simulated as a game-theoretic optimization that assumes the attack objective as maximizing the system operation cost, and the DLR technology is also used in the traditional attack-specific strategy to exclude the effect of DLR incorporation on the comparison results. The actual attack is simulated as an LR attack whose objective is to maximize the post-attack overload at the transmission line 3 (the line connecting bus 2 and bus 3). The IEEE 14-bus system is used as an example, where the actual load is case 2 given in Table II.

Table VII shows the control decisions of the two mitigation strategies and the corresponding consequences for the physical system. Both of the strategies determine the optimal thermal ratings and the associated generation dispatch for attack mitigation. It can be seen that compared to the traditional strategy where only line 3 has the determined thermal rating greater than the SLR, the DRC dispatch where most of the lines have the determined thermal rating greater than the SLR makes better utilization of the power transfer capacity of the transmission network. With the determined line ratings and the generation dispatches, the actual power flows of the transmission network in the presence of attack are given in the 8th and 9th columns. It shows that under the DRC dispatch, all the power flows of the transmission network are within the line thermal ratings. However, under the traditional strategy, the power flows of lines 1, 3, and 6 are 70.2, 106.8, and -84.3 MW, respectively, which exceed the corresponding thermal ratings and would incur unnecessary relay actions. The dispatch costs of the DRC and the traditional strategy are 1.314×10^4 \$/h and 1.274×10^4 \$/h, respectively. It is reasonable that the DRC dispatch has a higher cost, because both

TABLE VII
COMPARISON RESULTS BETWEEN THE DRC AND THE TRADITIONAL MITIGATION STRATEGIES

Decision						Consequences				
Generation			Determined ratings			Power flow			Cost($\times 10^4$)	
Bus	DRC	Trad.	Line	DRC	Trad.	Line	DRC	Trad.	DRC	Trad.
1	126.5	111	1	84	60	1	80.8	**70.2**	1.314	1.274
			2	66.2	60	2	45.7	40.8		
			3	84	69.9	3	76.9	**106.8**		
2	104.5	140	4	64.9	60	4	40.5	38.2		
			5	64.4	60	5	31.2	28.4		
			6	60	60	6	-47.3	**-84.3**		
			7	60	60	7	-40.7	-42.5		
			8	68.8	60	8	8.2	-21.3		
3	100	33.0	9	60	60	9	7.9	-0.2		
			10	60	60	10	-16.4	-25.8		
			11	60	60	11	24.3	19.9		
			12	60	60	12	12.3	11.6		
6	97.8	100	13	79.8	60	13	33.6	31.4		
			14	60	60	14	-15.2	-60		
			15	84	60	15	23.4	38.7		
			16	60	60	16	-11.8	-7.5		
8	15.2	60	17	74.4	60	17	13.6	16.5		
			18	60	60	18	-20.8	-16.5		
			19	60	60	19	6.2	5.5		
			20	64.7	60	20	26.3	23.4		

TABLE VIII
RUNTIME FOR DIFFERENT DISPATCHES

	Base-case disp.	Economic disp. with DLR	DRC disp.
Time (s)	0.26	4.38	42.35

of the strategies employ the DLR technology but the DRC dispatch is robust against diverse LR attacks.

D. Scalability of Proposed DRC Dispatch

To demonstrate the scalability of the proposed method, we test the DRC dispatch on the modified IEEE 118-bus test system which has 186 transmission lines and 54 generators. The base-case dispatch and the economic dispatch with DLR applied are also conducted to provide a comparison. The DLR is assumed to be 1.4 times SLR and the value of τ is set to be 0.3 in the tests.

The results of the maximum attack-induced overload of each transmission line obtained from different dispatches are shown in Fig. 5. It can be seen that the worst case overload of all transmission lines are nonpositive only when the DRC dispatch is employed. This reveals the importance of the coordination between the robustness design and the DLR incorporation.

Moreover, we measure the runtime for the different dispatches. We average the runtime over 100 runs. The results are shown in Table VIII. It can be observed that even though it requires more time to solve the DRC dispatch, our method can still satisfy the real-time requirement.

We also illustrate the tradeoff between the costs and benefits of incorporating the DLR technology based on the IEEE 118-bus test system. First, we calculate the total operation cost and the safety margin of the optimal DRC dispatch for different values of the weight ω. The results are shown in Fig. 6 (top figure). In Fig. 6 (bottom figure), we plot the tradeoff between the safety margin and the total generation cost of the DRC

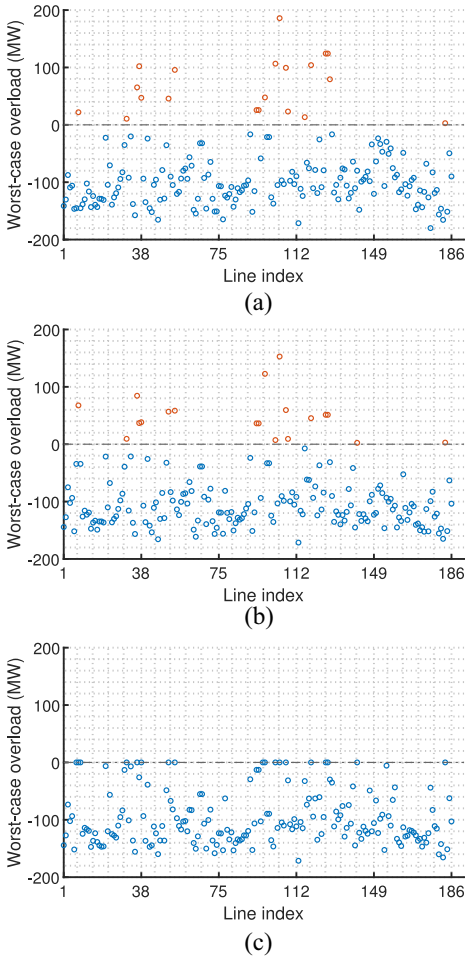

Fig. 5. Overloads (MW) of each transmission line caused by the corresponding worst case LR attack under different dispatches. (a) Base-case dispatch. (b) Economic dispatch with DLR applied. (c) Proposed DRC dispatch.

dispatch. It can be seen that the total operation cost increase with the safety margin, which confirms the intuition that the economical benefits of the DRC dispatch will decrease when the safety margin increases.

VI. CONCLUSION

This article analyzed the cost-effective mitigation strategies against uncertain LR attacks in power grids, taking advantage of the benefits of DLR technology in utilizing transmission line capacity. A DRC dispatch model considering the cost–benefit tradeoff of DLR incorporation was presented, which provides the desired level of system robustness against LR attacks without introducing excessive dispatch cost from the robust design. A methodology based on the robust counterpart techniques and C&CG algorithm was proposed to solve the DRC dispatch model. Case studies demonstrate that with the incorporation of DLR, the proposed DRC dispatch can economically mitigate all possible LR attacks within a certain magnitude level without the knowledge of the control objective of the attacks, while at the same time maintaining a sufficient safety margin to avoid the safety risk from the uncertainties of DLR forecast. The proposed model provides an insight into the application of DLR technology to enhance

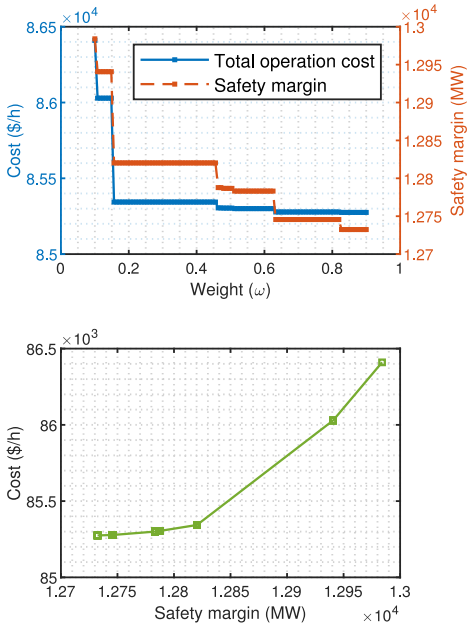

Fig. 6. Tradeoff between the costs and benefits of incorporating the DLR technology.

the cyber–physical security of power grids and helps motivate further research in learning how DLR can be optimally integrated into protective measures in power grids. Future work will address additional problems, e.g., mitigation methods for more general cyberattacks.

REFERENCES

[1] C. Liu, J. Wu, C. Long, and Y. Wang, "Dynamic state recovery for cyber-physical systems under switching location attacks," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 14–22, Mar. 2017.

[2] Z. Zhang, R. Deng, D. K. Y. Yau, and P. Chen, "Zero-parameter-information data integrity attacks and countermeasures in IoT-based smart grid," *IEEE Internet Things J.*, vol. 8, no. 8, pp. 6608–6623, Apr. 2021.

[3] Z. Zhang, R. Deng, P. Cheng, and Q. Wei, "On feasibility of coordinated time-delay and false data injection attacks on cyber-physical systems," *IEEE Internet Things J.*, early access, Oct. 6, 2021, doi: 10.1109/JIOT.2021.3118065.

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

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

[6] 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.

[7] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Bilevel model for analyzing coordinated cyber-physical attacks on power systems," *IEEE Trans. Smart Grid*, vol. 7, no. 5, pp. 2260–2272, Sep. 2016.

[8] Z. Li, M. Shahidehpour, A. Alabdulwahab, and A. Abusorrah, "Analyzing locally coordinated cyber-physical attacks for undetectable line outages," *IEEE Trans. Smart Grid*, vol. 9, no. 1, pp. 35–47, Jan. 2018.

[9] L. Jia, J. Kim, R. J. Thomas, and L. Tong, "Impact of data quality on real-time locational marginal price," *IEEE Trans. Power Syst.*, vol. 29, no. 2, pp. 627–636, Mar. 2014.

[10] 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.

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

[12] X. Liu, Z. Li, and Z. Li, "Optimal protection strategy against false data injection attacks in power systems," *IEEE Trans. Smart Grid*, vol. 8, no. 4, pp. 1802–1810, Jul. 2017.

[13] J. Tian, B. Wang, T. Li, F. Shang, K. Cao, and R. Guo, "Total: Optimal protection strategy against perfect and imperfect false data injection attacks on power grid cyber–physical systems," *IEEE Internet Things J.*, vol. 8, no. 2, pp. 1001–1015, Jan. 2021.

[14] Q. Gao, Y. Wang, X. Cheng, J. Yu, X. Chen, and T. Jing, "Identification of vulnerable lines in smart grid systems based on affinity propagation clustering," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 5163–5171, Jun. 2019.

[15] Y. Liu, S. Gao, J. Shi, X. Wei, Z. Han, and T. Huang, "Pre-overload-graph-based vulnerable correlation identification under load redistribution attacks," *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5216–5226, Nov. 2020.

[16] Y. Liu, S. Gao, J. Shi, X. Wei, and Z. Han, "Sequential-mining-based vulnerable branches identification for the transmission network under continuous load redistribution attacks," *IEEE Trans. Smart Grid*, vol. 11, no. 6, pp. 5151–5160, Nov. 2020.

[17] C. Liu, H. Liang, T. Chen, J. Wu, and C. Long, "Joint admittance perturbation and meter protection for mitigating stealthy FDI attacks against power system state estimation," *IEEE Trans. Power Syst.*, vol. 35, no. 2, pp. 1468–1478, Mar. 2020.

[18] M. Liu, C. Zhao, Z. Zhang, R. Deng, P. Cheng, and J. Chen, "Converter-based moving target defense against deception attacks in DC microgrids," *IEEE Trans. Smart Grid*, early access, Nov. 19, 2021, doi: 10.1109/TSG.2021.3129195.

[19] C. Liu, R. Deng, W. He, H. Liang, and W. Du, "Optimal coding schemes for detecting false data injection attacks in power system state estimation," *IEEE Trans. Smart Grid*, vol. 13, no. 1, pp. 738–749, Jan. 2022.

[20] Y. Li, R. Huang, and L. Ma, "False data injection attack and defense method on load frequency control," *IEEE Internet Things J.*, vol. 8, no. 4, pp. 2910–2919, Feb. 2021.

[21] H. Shayan and T. Amraee, "Network constrained unit commitment under cyber attacks driven overloads," *IEEE Trans. Smart Grid*, vol. 10, no. 6, pp. 6449–6460, Nov. 2019.

[22] X. Wang, X. Luo, M. Zhang, Z. Jiang, and X. Guan, "Detection and isolation of false data injection attacks in smart grid via unknown input interval observer," *IEEE Internet Things J.*, vol. 7, no. 4, pp. 3214–3229, Apr. 2020.

[23] M. Jorjani, H. Seifi, A. Y. Varjani, and H. Delkhosh, "An optimization-based approach to recover the detected attacked grid variables after false data injection attack," *IEEE Trans. Smart Grid*, vol. 12, no. 6, pp. 5322–5334, Nov. 2021.

[24] M. Jorjani, H. Seifi, and A. Y. Varjani, "A graph theory-based approach to detect false data injection attacks in power system AC state estimation," *IEEE Trans. Ind. Informat.*, vol. 17, no. 4, pp. 2465–2475, Apr. 2021.

[25] A. Abusorrah, A. Alabdulwahab, Z. Li, and M. Shahidehpour, "Minimax-regret robust defensive strategy against false data injection attacks," *IEEE Trans. Smart Grid*, vol. 10, no. 2, pp. 2068–2079, Mar. 2019.

[26] J. Fu *et al.*, "A tri-level defense model against load redistribution attacks," in *Proc. IEEE Sustain. Power Energy Conf. (iSPEC)*, 2019, pp. 1606–1611.

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

[28] 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.

[29] P. Zhao, C. Gu, Y. Ding, H. Liu, Y. Bian, and S. Li, "Cyber-resilience enhancement and protection for uneconomic power dispatch under cyber-attacks," *IEEE Trans. Power Del.*, vol. 36, no. 4, pp. 2253–2263, Aug. 2021.

[30] "Guidelines for increased utilization of overhead transmission lines," CIGRE, Paris, France, document WG B2.13, 2008.

[31] B. P. Bhattarai *et al.*, "Improvement of transmission line ampacity utilization by weather-based dynamic line rating," *IEEE Trans. Power Del.*, vol. 33, no. 4, pp. 1853–1863, Aug. 2018.

[32] A. Ahmadi, M. Nabipour, B. Mohammadi-Ivatloo, and V. Vahidinasab, "Ensemble learning-based dynamic line rating forecasting under cyberattacks," *IEEE Trans. Power Del.*, vol. 37, no. 1, pp. 230–238, Feb. 2022.

[33] M. W. Davis, "A new thermal rating approach: The real time thermal rating system for strategic overhead conductor transmission lines—Part I: General description and justification of the real time thermal rating system," *IEEE Trans. Power App. Syst.*, vol. TPAS-96, no. 3, pp. 803–809, May 1977.
[34] *IEEE Standard for Calculating the Current–Temperature Relationship of Bare Overhead Conductors*, IEEE Standard 738-2012, 2013, pp. 1–72.
[35] "NERC Reliability Guideline: Methods for Establishing IROLS." 2018. [Online]. Available: https://www.nerc.com/comm/RSTC_Reliability_Guidelines/Reliability_Guideline_Methods_for_Establishing_IROLs.pdf
[36] P. Kundur *et al.*, "Definition and classification of power system stability IEEE/CIGRE joint task force on stability terms and definitions," *IEEE Trans. Power Syst.*, vol. 19, no. 3, pp. 1387–1401, Aug. 2004.
[37] B. Zeng and L. Zhao, "Solving two-stage robust optimization problems using a column-and-constraint generation method," *Oper. Res. Lett.*, vol. 41, no. 5, pp. 457–461, 2013. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0167637713000618
[38] (MOSEK ApS, Copenhagen, Denmark). *The MOSEK Optimization Toolbox for MATLAB Manual. Version 9.0*, (2019). [Online]. Available: http://docs.mosek.com/9.0/toolbox/index.html
[39] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "MATPOWER: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Trans. Power Syst.*, vol. 26, no. 1, pp. 12–19, Feb. 2011.
[40] J. Löfberg, "YALMIP: A toolbox for modeling and optimization in MATLAB," in *Proc. CACSD Conf.*, Taipei, Taiwan, 2004, pp. 284–289.
[41] R. D. Zimmerman and C. E. Murillo-Sánchez. *Matpower (Version 7.1) [Software]*. 2020. [Online]. Available: https://matpower.org

Min Zhou (Student Member, IEEE) received the B.Eng. degree in information science and engineering from the East China University of Science and Technology, Shanghai, China, in 2015. She is currently pursuing the Ph.D. degree with the School of Electronic Information and Electrical Engineering, Shanghai Jiao Tong University, Shanghai.

Her current research interests include cyber–physical security analysis, robust defense, and dispatch optimization for smart grid.

Jing Wu (Senior Member, IEEE) received the B.S. degree in electrical engineering from Nanchang University, Nanchang, China, in 2000, the M.S. degree in electrical engineering from Yanshan University, Qinhuangdao, Hebei, China, in 2002, and the Ph.D. degree in electrical engineering from the University of Alberta, Edmonton, AB, Canada, in 2008.

Since 2011, she has been with Shanghai Jiao Tong University, Shanghai, China, where she is currently a Professor. Her current research interests include robust model predictive control, security control, and stability analysis and estimations for cyber–physical systems.

Prof. Wu is a registered Professional Engineer in Alberta, Canada.

Chengnian Long (Senior Member, IEEE) received the B.S., M.S., and Ph.D. degrees in control theory and engineering from Yanshan University, Qinhuangdao, Hebei, China, in 1999, 2001, and 2004, respectively.

He was a Research Associate with the Department of Computer Science and Engineering, Hong Kong University of Science and Technology, Hong Kong, and a Killam Postdoctoral Fellow with the University of Alberta, Edmonton, AB, Canada. Since 2009, he has been with Shanghai Jiao Tong University, Shanghai, China, where he has been a Full Professor since 2011. His current research interests include artificial intelligence of things, blockchain technology, deep learning, and cyber–physical system security.

Chensheng Liu (Member, IEEE) received the Ph.D. degree in control science and engineering from Shanghai Jiao Tong University, Shanghai, China, in 2018.

He was a Postdoctoral Research Fellow with the University of Alberta, Edmonton, AB, Canada, from 2018 to 2019. From 2019 to 2021, he was a Postdoctoral Research Fellow (supported by the Initiative Postdocs Supporting Program) with the East China University of Science and Technology, Shanghai, where he is currently a Distinguished Research Fellow with the School of Information Science and Engineering. His research interests include machine learning in smart grid, security of cyber–physical systems, and control and optimization of smart grid.

Deepa Kundur (Fellow, IEEE) received the B.A.Sc., M.A.Sc., and Ph.D. degrees in electrical and computer engineering from the University of Toronto, Toronto, ON, Canada, in 1993, 1995, and 1999, respectively.

She is a Professor and the Chair of The Edward S. Rogers Sr. Department of Electrical and Computer Engineering, University of Toronto. She is an author of over 200 journal and conference papers and is a recognized authority on cybersecurity issues. Her research interests lie at the interface of cybersecurity, signal processing, and complex dynamical networks.

Prof. Kundur received best paper recognitions at numerous venues, including the 2015 IEEE Smart Grid Communications Conference, the 2015 IEEE Electrical Power and Energy Conference, the 2012 IEEE Canadian Conference on Electrical and Computer Engineering, the 2011 Cyber Security and Information Intelligence Research Workshop, and the 2008 IEEE INFOCOM Workshop on Mission Critical Networks. She has also been the recipient of teaching awards at both the University of Toronto and Texas A&M University. She has served in executive roles at numerous international conferences and has participated on several editorial boards and funding panels. She is a Fellow of the Canadian Academy of Engineering and a Senior Fellow of Massey College.