Cyber-Resilient Multi-Energy Management for Complex Systems

Pengfei Zhao, Zhidong Cao, Daniel Dajun Zeng, *Fellow, IEEE,* Chenghong Gu, *Member, IEEE,* Zhaoyu Wang, *Senior Member, IEEE,* Yue Xiang, *Senior Member, IEEE,* Meysam Qadrdan, *Senior Member, IEEE,* Xinlei Chen, Xiaohe Yan, *Member, IEEE,* and Shuangqi Li, *Student Member, IEEE*

***Abstract*—Resilience problems from cyber-attacks on information communication technologies (ICT) exist under their wide usage. False data injection (FDI) judiciously designed by attackers may cause severe consequences such as uneconomic operation and blackouts, particularly multi-vector energy distribution systems (MEDS), which are closely linked and interdependent. This paper addresses the cyber resilient issues of an MEDS caused by FDI, considering the uncertainty from renewable resources. A novel two-stage distributionally robust optimization (DRO) is proposed to realize the day-ahead and real-time resilience improvement. The ambiguity set is based on both the Wasserstein distance and moment information. Compared to robust optimization which considers the worst case, DRO yields less-conservative solutions and thus provides more economic operation schemes. The Wasserstein metric-based ambiguity set enables to provide additional flexibility hedging against renewable uncertainty. Case studies are demonstrated on two representative MEDS networked with energy hubs, illustrating the effectiveness of the proposed cyber-secured model. The produced adaptive robust economic operation for MEDS can reduce load shedding and enhance system resilience against severe cyber-attacks.**

***Index Terms*—Cyber-attacks, energy hubs, distribution systems, load redistribution attacks, multi energy systems, real-time operation, resilience enhancement.**

NOMENCLATURE

A. Indices and sets

t, T	Index and set for time periods.
b , B	Index and set for electricity buses.
i_e, I_e	Index and set for traditional distributed generators (DG) .
i_g, I_g	Index and set for natural gas sources.
j, J	Index and set for renewable DGs.
l_e, L_e	Index and set for power lines.
l_g, L_g	Index and set for gas pipelines.
k_e, K_e	Index and set for electric loads.
k_g, K_g	Index and set for gas loads.

B. Parameters

KP	Bus-generator incidence matrix.
KD	Bus-load incidence matrix.
SF	Shift factor matrix.
β	Attack injection level.
λ_m^s, λ_m^{re}	Power price from day-ahead and real-time market.
$\lambda_{i_e}^a$, $\lambda_{i_e}^b$, $\lambda_{i_e}^c$	Cost coefficients for generation of traditional DG i_e.
λ_{i_g}	Cost coefficient for output of natural gas source i_g.
$\lambda_{i_e}^+$, $\lambda_{i_e}^-$	Cost coefficient for up and down reserve of traditional DG i_e.
$\lambda_{i_g}^+$, $\lambda_{i_g}^-$	Cost coefficient for up and down reserve of natural gas source i_g.
$\lambda_{i_e}^{re}$, λ_j^{re}	Regulation cost coefficient for traditional DG i_e and renewable DG j.
$\lambda_{k_e}^{ls}$, $\lambda_{k_g}^{ls}$	Penalty cost coefficient for power and gas load shedding.
$\omega_j^s(t)$	Forecasted output of renewable DG j at time t.
$R_{i_e}^+$, $R_{i_e}^-$	Maximum up and down reserve capacity of traditional DG i_e at time t.
$R_{i_g}^+$, $R_{i_g}^-$	Maximum up and down reserve capacity of natural gas source i_g at time t.
$P_{i_e,max}$, $P_{i_e,min}$	Maximum and minimum active power output of traditional DG i_e.
$P_{i_g,max}$, $P_{i_g,min}$	Maximum and minimum output of traditional DG i_g.
$Q_{i_e,max}$, $Q_{i_e,min}$	Maximum and minimum reactive power output of traditional DG i_e.
$V_{b,max}$,$V_{b,min}$	Maximum and minimum voltage limit.
x_{l_e}, r_{l_e}	Reactance and resistance of power line l_e.
V_0	Reference voltage magnitude.
$f_{l_e,max}$, $qf_{l_e,max}$	Maximum active and reactive power flow of line l_e.
$f_{l_g,max}$,	Maximum gas flow of line l_g.
$Pr_{l_g,max}$,	Maximum and minimum gas pressure of gas pipeline l_g.

This work was supported by the National Science Fund for Distinguished Young Scholars, No. 72025404, the National Natural Science Foundation of China (Nos. 71621002, 72074209), and Beijing Nova Program (Z201100006820085).

P. Zhao, Z. Cao (corresponding author) and D. Zeng are with the Institute of Automation, Chinese Academy of Sciences, Beijing, China, School of Artificial Intelligence, University of Chinese Academy of Sciences, Beijing, China, and Shenzhen Artificial Intelligence and Data Science Institute (Longhua), Shenzhen , China. (email: Pengfei.zhao@ia.ac.cn, Zhidong.Cao@ia.ac.cn, Dajun. Zeng@ia.ac.cn).

C.Gu and S. Li are with the Department of Electronic & Electrical Engineering, University of Bath, Bath, UK.(email: C.Gu@bath.ac.uk and S. Li@bath.ac.uk).

Z. Wang is with the Department of Electrical and Computer Engineering, Iowa State University, Ames, IA 50011 USA (wzy@iastate.edu).

Y. Xiang is with College of Electrical Engineering, Sichuan University, China. (email: xiang@scu.edu.cn)

M. Qadrdan is with the School of Engineering, Cardiff University, CF24 3AA Cardiff, U.K. (e-mail: qadrdanm@cardiff.ac.uk).

X. Chen is with the Electrical Engineering Department, Carnegie Mellon University, Pittsburgh, USA. (email: xinlei.chen@sv.cmu.edu).

X. Yan is with the Department of Electronic and Electrical Engineering, North China Electric Power University, Beijing 102206, China (e-mail: x.yan@ncepu.edu.cn)

$Pr_{l_g,min}$	
γ_{l_g}	Coefficient for Weymouth equation.
$P_{k_e,t}Q_{k_e,t}, P_{k_g,t}$	Active and reactive power load and gas load at time t.
$P^{ls}_{k_e,max}$, $P^{ls}_{k_g,max}$	Maximum power and gas load shedding at time t.
$\eta_{i_e,t}$, $\eta_{i_g,t}$	Participation factor for reserves of traditional DG and natural gas source at time t.
η_{cp^e}, η_{cp^e}	Electric and heating efficiency for combined heat and power (CHP).
$\eta_{COP,}\eta_{GF}$	Coefficient of performance of ground source heat pump (GSHP) and efficiency of gas furnace (GF).
$P^i_{cp,max}, P^i_{cp,min}$, $P^i_{HP,max}, P^i_{HP,min}$ $P^i_{GF,max}, P^i_{GF,min}$	Maximum and minimum input limits of CHP, GSHP and GF.
$P^{ch}_{BS,max}, P^{ch}_{BS,min}$ $P^{dch}_{BS,max}, P^{dch}_{BS,min}$	Maximum and minimum charging and discharging power for battery storage.
$P^{ch}_{HS,max}, P^{ch}_{BS,min}$ $P^{dch}_{HS,max}, P^{dch}_{HS,min}$	Maximum and minimum charging and discharging heat for heat storage.
$\eta^{ch}_{BS}, \eta^{dch}_{BS}, \eta^{ch}_{HS}$, η^{dch}_{HS}	Charging and discharging efficiency for battery and heat storage.
$E_{BS,max}, E_{BS,min}$ $E_{HS,max}, E_{HS,min}$	Maximum and minimum remaining energy limits of battery and heat storage.
$L_{e,t}, L_{h,t}$	Electricity and heat load of energy hub system.

C. Variables and functions

G, D, BP, PL	Generation vector of generator output, load demand, bus power injection and line flow.
ΔG,ΔD, ΔBP, ΔPL	Incremental vector of generator output, bus power injection and line flow.
$P^s_{m,t}$,$P^{re}_{m,t}$	Power purchase from day-ahead and real-time market.
$P^s_{i_e,t}$,$P^{re}_{i_e,t}$	Scheduled and regulated active power output of traditional DG i_e at time t.
$Q^s_{i_e,t}$,$Q^{re}_{i_e,t}$	Scheduled and regulated reactive power output of traditional DG i_e at time t.
$P^s_{i_g,t}$,$P^{re}_{i_g,t}$	Scheduled and regulated output of natural gas source i_g at time t.
$r^+_{i_e,t}$, $r^-_{i_e,t}$	Up and down reserve capacity of traditional DG i_e at time t.
$r^+_{i_g,t}$, $r^-_{i_g,t}$	Up and down reserve capacity of natural gas source i_g at time t.
$V^s_{b,t}, V^{re}_{b,t}$	Scheduled and regulated voltage of bus b at time t.
$f^s_{l_e,t}$, $qf^s_{l_e,t}$	Scheduled active and reactive power flow.
$f^{re}_{l_e,t}$, $qf^{re}_{l_e,t}$	Regulated active and reactive power flow.
$f^s_{l_g,t}$, $f^{re}_{l_g,t}$	Scheduled and regulated gas flow.
$f^{ini}_{l_g,t}$, $f^{ter}_{l_g,t}$	Gas flow from initial node and to terminal node of pipeline l_g at time t.
$\omega^s_{j,t}$	Scheduled renewable generation at time t.
$Pr^s_{l_g,t}$, $Pr^{re}_{l_g,t}$	Scheduled and regulated gas pressure of gas pipeline l_g at time t.
$Pr^{s,ini}_{l_g,t}$, $Pr^{s,ter}_{l_g,t}$	Scheduled gas pressure of initial and terminal nodes of pipeline l_g at time t.
$Pr^{re,ini}_{l_g,t}$, $Pr^{re,ter}_{l_g,t}$	Regulated gas pressure of initial and terminal nodes of pipeline l_g at time t.
$P^{ls}_{k_e,t}$, $Q^{ls}_{k_e,t}$	Power load shedding at time t.
$P^{ls}_{k_g,t}$	Gas load shedding at time t.
$f^{inj}_{l_e,t}$, $f^{inj}_{l_g,t}$	Power and gas flow injection to EHSs.
$P^i_{COP,t}, P^o_{COP,t}$,	Power input and heat output of GSHP.
$P^i_{GF,t}, P^o_{GF,t}$	Gas input and output of gas furnace.
$P^{s,i}_{cp,t}, P^{s,o}_{cp^e,t}, P^{s,o}_{cp^h}$	Gas input and power and heat output of CHP.
$P^{ch}_{BS,t}, P^{dch}_{BS,t}$, $P^{ch}_{HS,t}, P^{dch}_{HS,t}$	Charging and discharging power and heat of battery and heat storage.
$E_{BS,t}, E_{HS,t}$	Remaining energy of battery and heat storage.
$v_{e,t}, v_{g,t}$	Dispatch factors of power and gas.

D. Uncertainty Modelling

x, y	Vectors of first and second stage variables.
$E_{\mathbb{P}}[Q(x,\xi)]$	The expectation of the second-stage objective function result.
$\xi, \xi^{\dagger}$	Random variables in the candidate and empirical distributions
$\mathbb{P}, \widehat{\mathbb{P}}$	Set of random variables in the candidate and empirical distributions
$\mathscr{S}$	Wasserstein ambiguity set.
η	Wasserstein distance.
$\mathscr{A}$	Lifted Wasserstein ambiguity set.
φ	Auxiliary variable to limit the distribution distance.
μ	Mean value of random variable ξ.
$Q_{LDR}(x,\xi,\varphi,\tilde{s})$	Second-stage objective function with linear decision rule.
τ, ψ, λ	Dual variables.

I. INTRODUCTION

In recent years, the high integration of information and communication technologies (ICTs) is significant for better decision making and control of power systems, but they also increase the risks of cyber-attacks [1]. Attackers impose these low frequency and high impact cyber-attacks on the generation, transmission and demand side of the energy system, causing uneconomic operation and reliability issues, e.g., overloading and even load shedding. As a common type of cyber-attacks, false data injection (FDI) brings challenges to state estimators and mislead system operators by falsified data. The 2015 Ukraine power grid cyber-attack caused 30 substations switched off and 225,000 customers were not able to use electricity for up to 6 hours [2-4]. The grid control system in Utah, U.S. was disabled due to FDI on 5 March, 2019 [5].

The existing literature of FDI attacks focuses on i) mimicking stealthy designed FDI attacks and assessing impacts [6-8] and ii) designing strategies to defend or mitigate the impact on power grid [9, 10]. In terms of attack modelling, a bilevel optimization model is proposed to maximize the targeted and overall transmission branches [6]. Three types of cyber-topology FDI attacks, i.e., line-addition attack, line-removal attack and line-switching attack are established and solved by metaheuristic methods [7]. A relaxed incomplete information of power networks is used to attack AC state estimation [8]. As for

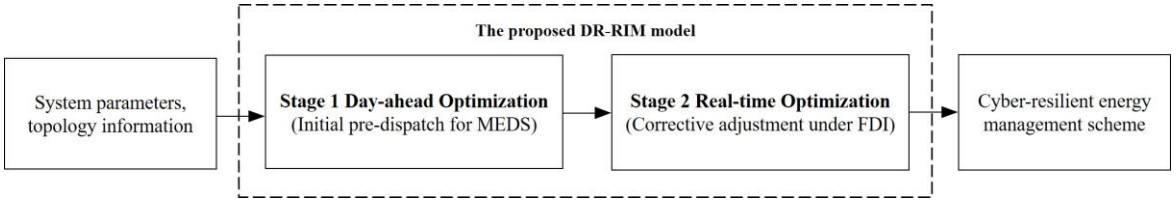


Fig. 1. The proposed two-stage optimization framework.

defencing and mitigation strategies of cyber-attacks, game theory [11-13], state estimation [14-16] and filter based FDI detection methods [17-19] have been widely used in previous literature. A game-theoretic analysis is proposed for cyber switching attacks to describe the interactions between electric power utility and attackers [13]. An interval state estimation is developed for detecting cyber-attacks and nonlinear electric load data is extracted by deep learning algorithms [15]. Kalman filter with a novel distributed dynamic state estimator is employed to improve the attack detection of the power grid [18].

State estimation plays a vital role in detecting and filtering bad measurement data. However, malicious FDI attacks are judiciously designed to pass the detection [8]. Load redistribution (LR) is a particular type of FDI, which is launched by false load data to consequently affect the operation actions, causing economic loss and physical damages to devices due to wrong operation decisions. The mask of LR attacks is the key to evade detection, i.e., the residue of bad data detection can be avoided by a well-designed LR attack, proved by [20, 21]. LR attacks could manipulate falsified measurement vector and affect operation schedule. Therefore, mitigating the uneconomic operation considering potential LR attacks is necessary.

On the other hand, due to the lower fuel cost and lower pollutant emissions of gas-fired generators, the interdependency of electricity and gas systems is significantly increasing. System operations for multi-vector energy distribution systems (MEDS) are widely investigated. An MEDS model for Great Britain is developed in [22], where deterministic method, two-stage stochastic method, multistage stochastic method and perfect foresight method are widely used and compared to handle wind uncertainty. A day-ahead scheduling model is proposed for an MEDS which incorporates combined heat and power (CHP) units, energy conversion devices and responsive loads [23]. In [24], a stochastic optimization (SO) based MEDS is designed to achieve the optimal coordination of energy converters with high energy efficiency for smart cities. Combining the advantages of robust optimization (RO) and SO, reference [25] applies distributionally robust optimization (DRO) to a security-based optimal power flow in distribution systems considering electric vehicle aggregators.

Additionally, the increasing level of renewable energy resources has brought non-optimality and infeasibility due to its perturbation. The uncertain nature of renewable generation poses severe challenges on MEDS operation. References [22], [26] and [25] have tackled the randomness of renewable generation by SO, RO and DRO respectively. SO requires the explicit uncertain data distributions with large samples and can yield accurate and economic results. However, the dataset is not always sufficiently large which will inevitably cause errors when assigning distributions. RO deals with uncertainties using the worst-case scenario by uncertainty set, which has a very low probability and thus is too conservative. DRO combines the advantages of SO and RO [27]: i) compared with SO, it does not require a large number of uncertain data samples and ii) compared with RO, it minimizes the worst-distributed scenario with less-conservative solutions.

From the attacker's point of view, the aim is to maximize the impact of LR attacks on the power grid but, from the operator's point of view, the impact should be minimized. The resilience of MEDS against the attacks is becoming vital, particularly with increasing fluctuating renewables integrated. In summary, there are four main problems in the existing literature: i) The mitigation schemes for uneconomic operation caused by cyber-attacks have been only investigated on power systems but never implemented on MEDS; ii) The presence of renewable uncertainties have never been incorporated with cyber-attacks simultaneously; iii) The mitigation scheme for uneconomic operation from RO is too conservative with massive load shedding; iv) Existing research only investigates single-stage mitigation schemes for uneconomic operation, unable to fully express the impact of cyber-attacks and renewable uncertainties in real-time scenarios.

Therefore, to address the above problems and fill the research gap, this paper mitigates the resilience impacts of MEDS caused by random, masked and hard-detectable LR attacks. A two-stage DRO model is developed to mitigate the uneconomic operation of MEDS caused by LR attacks, where renewable uncertainty is also considered. The interaction among the two-stage model enables a flexible adjustment in an iterative manner. The first stage determines an initial day-ahead operation plan before the realization of renewable generation uncertainties without considering LR attacks. The second stage minimizes real-time recourse costs based on the real renewable generation and potential LR attacks. A conditional Wasserstein metric-based ambiguity set is designed to hedge against the LR attacks and renewable uncertainty. Fig. 1 briefly presents the proposed two-stage framework. Based on the affine recourse approximation, the robust counterpart is obtained. This proposed two-stage **d**istributionally **r**obust **r**esilience **i**mprovement for **M**EDS operation under cyber-attacks is defined as **DR-RIM** for simplicity. Compared to RO which considers extreme LR attacks in a very low probability, this DR-RIM mitigates the conservatism and thus produces lower operation cost.

The LR attacks will lead to the LR deviations and further impact on the economic operation and energy imbalance. When there is a generation-load imbalance due to LR attacks, either excessive generation or load shedding will be caused. The former consequence yields uneconomic operation decisions and the latter consequence will cause load shedding. Therefore, the unpredictable LR attacks will inevitably cause economic and physical losses. The proposed cyber-resilient energy

management enables to provide a day-ahead initial operational plan and an optimal load shedding strategy as the emergency response under LR attacks. Moreover, the DR-RIM algorithm is sufficiently robust since the DRO approach considers the worst-case attack distribution.

Based on the previous works of the authors [28, 29], this paper aims at addressing a more crucial cyber-resilient problem for energy systems, i.e., distribution systems in urban areas are more vulnerable to cyber-attacks. Instead of conducting cyber-attacks on transmission systems, which has been extensively studied in academia with effective protective measures, it is also highly probable that the adversaries manipulate cyber-attacks on distribution systems. The existing research has focused on investigating the attack design and detection for energy distribution systems. Nevertheless, there is a lack of research on resilience improvement for energy system operation schemes. Furthermore, even though DRO has been broadly applied in energy system problems, the modelling of ambiguity sets directly influences the computational performance, which should be critically investigated. The proposed Wasserstein-based DRO is essentially different from the moment-based DRO. The former technique utilizes the statistical moment information whilst the latter technique defines the uncertain distributions via the nominal distribution and distribution closeness. The detailed improvement and contributions based on our previous works are given below:

1) The existing works are designed for risk mitigation of multi-energy systems in the transmission level. However, a resilience improvement scheme is particularly desired for multi-energy systems in the distribution level. Energy distribution and transmission systems are fundamentally different in terms of the functionality, structure, scale, equipment, etc. Energy distribution systems are integrated with large-scale renewable generators. The renewable fluctuation challenges the system operation considerably regarding the supply-demand balance and voltage rise/drop. In addition, distribution systems are required to maintain the dynamic balance of both active and reactive power via controlling the voltage regulating devices. Thus this paper targets at addressing the resilience impact caused by stealthy-designed FDI considering the unique characteristics of MEDS.

2) A Wasserstein metric-based ambiguity set is adopted to characterize the FDI and random renewable generation for deriving the true probability distribution. The existing papers of the authors apply moment-based ambiguity sets with identical moments [28, 29], such as mean, variance and covariance of the distributions. Furthermore, the structural properties of the distributions cannot be modelled, e.g., shape and modality of empirical distributions. Instead of utilizing traditional moment-based ambiguity sets based on statistical moment information, the metric-based ambiguity sets specify the closeness of uncertain distributions with empirical distributions based on statistical metrics, e.g., KL divergence and Wasserstein metric. The proposed Wasserstein metric-based ambiguity set is more suitable for characterizing FDI than moment-based ambiguity sets. Since there is a low frequency of FDI attacks manipulated on energy systems, which affects the historical data availability. Therefore, compared to the moment-based ambiguity sets, the proposed Wasserstein metric-based ambiguity set with less reliance on FDI historical data provides a more feasible FDI handling solution.

The main achievements of this paper are as follows:

1) Existing literature has not investigated the impact of LR attacks on MEDS, which is studied in this paper to fill the gap. The energy interdependencies among power, gas and heat are extensively modelled.
2) Both LR attacks and renewable uncertainties are modelled by DRO method. Compared to SO, DRO only requires moment information, which is easy to obtain from historical data; compared to RO, DRO considers additional statistical information to resolve the conservatism of RO. The innovative conditional Wasserstein metric-based ambiguity set enables to flexibly control the distance among the reference and candidate probability distributions.
3) Compared to bilevel and trilevel optimization models, a two-stage adaptive robust uneconomic operation mitigation scheme is proposed, which incorporates both day-ahead and real-time operation and is more practical for systems.

The rest of this paper is organized as follows. Section II models LR attacks. Section III presents the objective function and constraints of the DR-RIM. The methodology regarding DRO and reformulations are presented in section IV. Section V demonstrates case studies and the performance of the DR-RIM. Section VI concludes this paper.

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 equipment. This section firstly proposes how attack manipulators can evade the detection by state estimation and then presents the modelling of LR attacks.

This work is based on [20, 21], assuming that the system estimator utilizes DC state estimation (DSSE). Previous research has investigated designing risk mitigation strategies under the assumption that the adversary can evade DSSE. However, in real practice, as the approximation of AC state estimation (ASSE), DSSE is not accurate to monitor state variables in distribution systems due to the low *x/r* ratio [30-32]. This work aims to design a multi-energy management model under FDI attacks, concentrating on investigating the multi-energy coordination, DRO approach for modelling FDI, and two-stage mitigation framework. The extensively cited and accepted works [20, 21] provides the fundamental mitigation model for this proposed paper. Nevertheless, building the accurate risk mitigation model with ASSE background will be the future work.

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 an adversary's stealthy design [8, 31, 33, 34]. The nonlinear relationship between state variable x and measurement z is given in (1), where $h(x)$ 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 H represents the Jacobian matrix.

$$z = h(x) + e \quad (1)$$

$$z = Hx + e \quad (2)$$

After the realization of FDI, the measurement vector z becomes $z_{bad} = z + a$, and the estimated state vector can be represented as $\hat{x}_{bad} = \hat{x} + c$ where a is the attack vector and c is the resulted deviation vector of state variable after FDI attacks. Accordingly, to determine the estimated state variable, $\hat{x}_{bad}$ can be formulated as (3), where W represents the diagonal error matrix.

$$\hat{x}_{bad} = (H'WH)^{-1}H'Wz_{bad} \quad (3)$$

The largest normalized residual (LNR) can be used to detect and identify measurement errors by (4). If the residual is less than a threshold ε, then the state estimate is valid without FDI.

$$LNR = \|z - H\hat{x}\| \leq \varepsilon \quad (4)$$

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

$$LNR = \|z + a - H((H'WH)^{-1}H'Wz_{bad})\| \quad (5)$$

$$LNR = \|z - H\hat{x} + (a - Hc)\| \quad (6)$$

If a is the linear combination of H and c, i.e., $a = Hc$, then $LNR = \|z - H\hat{x}\|$ 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 Δz is the multiplication of Jacobian matrix and amount of changes Δx:

$$\Delta z = a = Hc = H\Delta x \quad (7)$$

B. LR Modelling

The original bus power injection and line flow are illustrated in (8) and (9), where KP and KD are bus-generator incidence matrix and bus-load incidence matrix respectively. SF is the shift factor matrix which approximates the change in active power flow. Due to LR attacks, (10) and (11) show the incremental matrices of BP and PL [18-21].

$$BP = KP \cdot G - KD \cdot D \quad (8)$$

$$PL = SF \cdot BP \quad (9)$$

$$\Delta BP = KP \cdot \Delta G - KD \cdot \Delta D \quad (10)$$

$$\Delta PL = SF \cdot \Delta BP \quad (11)$$

To model successful LR attacks, the following assumptions are normally considered:

1. The attack on the output measurement of generators is ignored because the attack can be detected and corrected easily. Therefore, $\Delta G = 0$.
2. Zero injection buses which have neither loads nor generators connected are not attackable.
3. Load measurements can be attacked.
4. Branch flow measurements can be changed since load measurement is attackable.

Based on above assumptions, (10) and (11) are reformulated as (12).

$$\Delta PL = -SF \cdot KD \cdot \Delta D \quad (12)$$

$$\sum \Delta D = 0 \quad (13)$$

$$-\beta D \leq \Delta D \leq \beta D \quad (14)$$

Equation (13) shows the stealthy LR designed by the adversary, which increases and decreases some loads simultaneously to maintain the total load unchanged. The LR deviation is limited in (14) with the attack injection level (AIL) β, which is used to ensure the attack magnitude for a load measurement is not beyond the limit and thus to lower the risk of being suspected. β ranges from 0% to 100%.

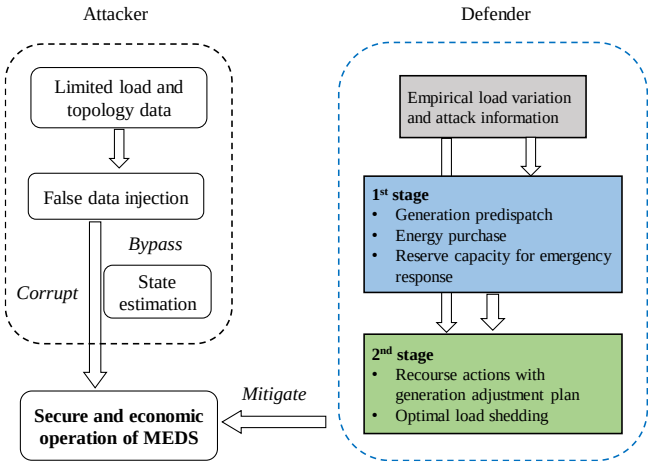


Fig. 2. The proposed two-stage cyber-resilience energy management framework.

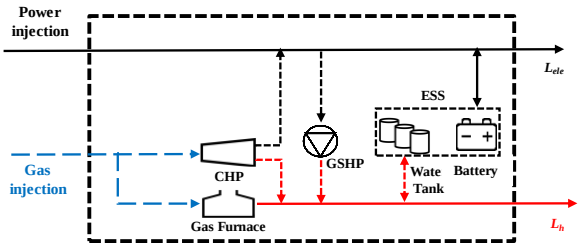


Fig. 3. The proposed energy hub model.

Constraint (15) shows that the initial power flow should be between line capacity. Due to LR attacks, the branch flow deviation ΔPL should be considered and eliminated in (16).

$$\underline{PL} \leq PL \leq \overline{PL} \quad (15)$$

$$\underline{PL} + SF \cdot KD \cdot \Delta D \leq PL \leq \overline{PL} + SF \cdot KD \cdot \Delta D \quad (16)$$

As a special case of FDI attacks, load measurement can be attacked according to [20, 21] by enforcing the sum of load attack vector to be zero in (17). Equation (18) constraints the attack deviation by AIL β.

$$\sum \Delta P_{k_e,t} = 0 \quad (17)$$

$$-\beta_{k_e} P_{k_e,t} \leq \Delta P_{k_e,t} \leq \beta_{k_e} P_{k_e,t} \quad (18)$$

III. Two-Stage Mitigation for Uneconomic Operation

The proposed MEDS contains a distribution system in multi-energy vectors connected with energy hubs. To mitigate the uneconomic operation of MEDS caused by LR attacks, a two-stage mitigation scheme is proposed. The overall illustration is shown in Fig. 2.

- The first-stage optimization is a day-ahead operation which is implemented under the normal operation without meter reading being tampered.
- The second stage takes corrective action on the adjustment of the generation of traditional DGs, natural gas sources, electricity purchase from the upper day-ahead market and implement load shedding.

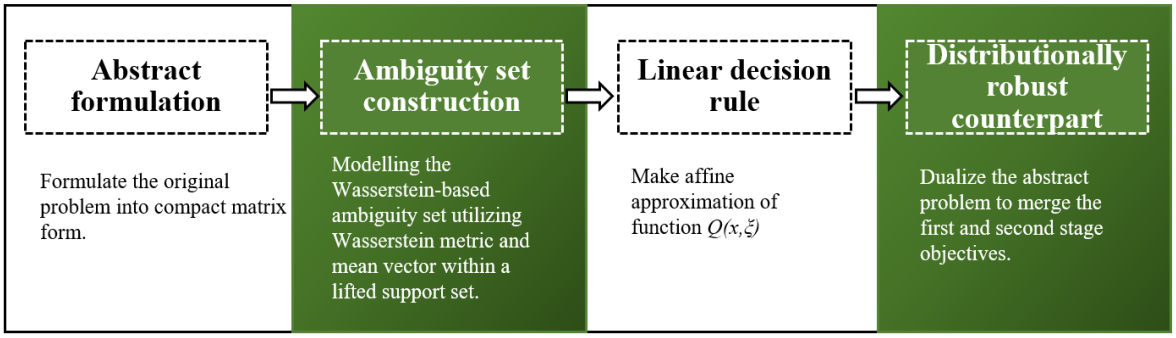


Fig. 4. Illustration of the overall methodology.

Specifically, this two-stage DR-RIM includes i) stage one: day-ahead operation that schedules traditional DGs and gas sources and ii) stage two: real-time operation that reschedules traditional DGs and gas sources as well as considering load shedding, based on random LR attacks and renewable uncertainty. 'Regulation' is used to describe regulation actions on generation outputs conducted by the system operator. The objective functions and constraints are presented and explained in section A-C.

Note that in the day-ahead operation, forecasting is done with the third-party vendors [35, 36]. Day-ahead operation conducts initial system operational planning for the following day based on the limited information of the uncertainties, e.g., uncertainties of renewable generation and load demand [37]. High-quality forecasting significantly improves the controllability of power system dispatch, supporting system operators with cost-effective operation schemes, enhanced system reliability and minimized renewable power curtailment via preparing to anticipate up- and down-reserves. However, the delivery of the forecast information can also be cyber-attacked [38]. By now, there is no existing literature focusing on modelling the cyber-attacked forecast information exchange between the forecast authorities and system operators, which is beyond the scope of this paper. This paper targets at mitigating the cyber risks caused by LR attacks. The risk mitigation model for transferring the renewable forecast information will be incorporated in future work.

To mitigate the disruption caused by FDI, the proposed DR-RIM conducts cyber-resilient measures at both the day-ahead and real-time stages. During the day-ahead stage, the reserve capacity of controllable DGs and gas sources is prepared for emergency response under potential FDI attacks, which is modelled in constraints (22)-(25). At the real-time stage, the optimal load shedding program is adopted to properly prioritize critical demand areas and implement load shedding at certain areas. The corresponding constraints are presented in (49)-(52). Meanwhile, the adjustive actions of generation and energy flow dispatch are made, which are given in constraints (46). As a consequence, the security of the overall system is maintained.

A. DR-RIM Objective Function

The first-stage objective function is shown in (19), including i) power purchase cost from the day-ahead market, ii) generation cost of traditional DGs and gas sources and iii) reserve cost of traditional DGs and gas sources. It should be noted that the proposed reserve capacity of traditional DGs and gas sources are prepared for LR attacks and renewable uncertainties.

$$\begin{aligned}\Gamma_1 = \min \sum_{i_e\in I_e, i_g\in I_g, t\in T} & \lambda_m^s P_{m,t}^s + \lambda_{i_e}^a {P_{i_e,t}^s}^2 + \lambda_{i_e}^b P_{i_e,t}^s \\ & + \lambda_{i_e}^c + \lambda_{i_g} P_{i_g,t}^s + \lambda_{i_g} P_{i_g,t}^s \\ & + \lambda_{i_e}^+ r_{i_e,t}^+ + \lambda_{i_e}^- r_{i_e,t}^- + \lambda_{i_g}^+ r_{i_g,t}^+ \\ & + \lambda_{i_g}^- r_{i_g,t}^-\end{aligned} \tag{19}$$

The second-stage objective function is shown in (20) including i) the power purchase cost from real-time market if power purchased from the day-ahead market is not sufficient or the penalty cost for excessive power purchased from the day-ahead market, ii) the penalty cost for renewable power deviation, iii) regulated generation cost of traditional DGs and gas sources and iv) load shedding cost of power and gas loads.

$$\begin{aligned}\Gamma_2 = \min \sum_{i_e\in I_e, i_g\in I_g, t\in T, k_e\in K_e, k_g\in K_g} & \lambda_m^{re} \left| P_{m,t}^{re} - P_{m,t}^s \right| \\ & + \lambda_j^{re} \left| \omega_{j,t}^s - \xi_{j,t} \right| \\ & + \lambda_{i_e}^{re} \left| P_{i_e,t}^s - P_{i_e,t}^{re} \right| + \lambda_{i_g}^{re} \left| P_{i_g,t}^s \right. \\ & \left. - P_{i_g,t}^{re} \right| + \lambda_{k_e}^{ls} P_{k_e,t}^{ls} + \lambda_{k_g}^{ls} P_{k_g,t}^{ls}\end{aligned} \tag{20}$$

B. Day-ahead Operation

The actual distribution systems are inherently unbalanced since the three-phase line configuration is asymmetric, connected with unbalanced three-phase loads. In addition, the proliferating DG connections aggravate the imbalance. Many research has considered the impacts of unbalance in the distribution system management and control [30, 39, 40]. However, this paper studies the risk mitigation scheme against cyber-attacks on a simplified distribution system. Since the main focus of this paper is to provide a cyber-resilient multi-energy management model with the two-stage corrective approach. Indeed, modelling a cyber-resilient energy management model in an unbalanced distribution system is more practical with enhanced computational accuracy, which should be considered in the future extension of this work.

In the first stage, the day-ahead operation scheme is based on the renewable output forecast and load before LR attacks. The system constraints are as follows (21)-(45). Constraint (21) limits power purchase from the day-ahead market. The reserve capacity of traditional DGs and gas turbines are shown in (22)-(23). Constraints (24)-(25) ensure that generation output is within the predefined limit considering reserve. The reactive power output is limited in (26). In distribution systems, the linearized DistFlow equation is widely used for both active and reactive power flows, which are shown in (27)-(30). Constraints (31) and (32) ensure the balancing conditions for active and reactive power at each node. Gas pressure is constrained in (33) and (34). It should be noted that in radial gas networks, the higher pressure is always on

initial nodes and the gas flow direction is from initial nodes to terminal nodes. Thus, constraint (34) is considered. Weymouth equation is shown in (35), which characterizes the relationship between gas flow and pressure. Equation (36) constrains gas flow and nodal power balance of gas networks, presented in (37).

The proposed energy hubs contain CHP, ground source heat pump (GSHP) and gas furnace. Fig. 3 presents the proposed energy hub structure. The technical constraints of energy hubs are given in (38)-(45). The energy conversion constraints are presented in (38)-(40), followed by the input limit of conversion technologies in (41). Constraints (42)-(44) regulate the charging and discharging process of ESS. Finally, the inner energy balance constraint of energy hubs is given in (45).

$$0 \le P^s_{m,t} \le P_{m,max} \tag{21}$$

$$0 \le r^+_{\{\cdot\},t} \le R^+_{\{\cdot\}}, \{\cdot\} = i_e, gt \tag{22}$$

$$0 \le r^-_{\{\cdot\},t} \le R^-_{\{\cdot\}}, \{\cdot\} = i_e, gt \tag{23}$$

$$P^s_{\{\cdot\},t} + r^+_{\{\cdot\},t} \le P_{\{\cdot\},max}, \{\cdot\} = i_e, gt \tag{24}$$

$$P_{\{\cdot\},min} \le P^s_{\{\cdot\},t} - r^-_{\{\cdot\},t}, \{\cdot\} = i_e, gt \tag{25}$$

$$Q_{i_e,min} \le Q^{re}_{i_e,t} \le Q_{i_e,max} \tag{26}$$

$$V_{b,min} \le V^s_{b,t} \le V_{b,max} \tag{27}$$

$$V^{s,ini}_b - V^{s,ter}_b = \left(f^s_{l_e,t} r_{l_e} + q f^s_{l_e,t} x_{l_e}\right)/V_0 \tag{28}$$

$$0 \le f^s_{l_e,t} \le f^s_{l_e,max} \tag{29}$$

$$0 \le q f^s_{l_e,t} \le q f^s_{l_e,max} \tag{30}$$

$$\sum_{i_e \in I_e} P^s_{i_e,t} + \sum_{j \in J} \omega^s_{j,t} + \sum_{l_e \in L_e} f^{s,ini}_{l_e,t} - \sum_{l_e \in L_e} f^{s,ter}_{l_e,t} = \sum_{k_e \in K_e} P_{k_e,t} \tag{31}$$

$$\sum_{i_e \in I_e} Q^s_{i_e,t} + \sum_{l_e \in L_e} q f^{s,ini}_{l_e,t} - \sum_{l_e \in L_e} q f^{s,ter}_{l_e,t} = \sum_{k_e \in K_e} Q_{k_e,t} \tag{32}$$

$$Pr^2_{l_g,min} \le Pr^{s^2}_{l_g,t} \le Pr^2_{l_g,max} \tag{33}$$

$$Pr^{s,ini}_{l_g,t} \ge Pr^{s,ter}_{l_g,t} \tag{34}$$

$$f^s_{l_g,t} \left|f^s_{l_g,t}\right| = \gamma_{l_g} \left(Pr^{s,ini^2}_{l_g,t} - Pr^{s,ter^2}_{l_g,t}\right) \tag{35}$$

$$0 \le f^s_{l_g,t} \le f^s_{l_g,max} \tag{36}$$

$$\sum_{i_g \in I_g} P^s_{i_g,t} + \sum_{l_g \in L_g} f^{s,ini}_{l_g,t} - \sum_{l_g \in L_g} f^{s,ter}_{l_g,t} = \sum_{k_g \in K_g} P_{k_g,t} \tag{37}$$

$$P^{s,o}_{\{\cdot\},t} = \eta_{\{\cdot\}} P^{s,i}_{\{\cdot\},t}, \{\cdot\} = COP, GF \tag{38}$$

$$P^{s,o}_{cp^e,t} = \eta_{cp^e} P^{s,i}_{cp,t} \tag{39}$$

$$P^{s,o}_{cp^h,t} = \eta_{cp^h} P^{s,i}_{cp,t} \tag{40}$$

$$P^i_{\{\cdot\},min} \le P^i_{\{\cdot\},t} \le P^i_{\{\cdot\},max}, \{\cdot\} = cp, COP, GF \tag{41}$$

$$P^{s,ch/dch}_{\{\cdot\},min} \le P^{s,ch/dch}_{\{\cdot\},t} \le P^{s,ch/dch}_{\{\cdot\},max}, \{\cdot\} = BS, HS \tag{42}$$

$$E^s_{\{\cdot\},t} = E^s_{\{\cdot\},t-1} + \sum\nolimits_1^t P^{s,ch}_{\{\cdot\},t} \eta^{ch}_{\{\cdot\}} - P^{s,dch}_{\{\cdot\},t} / \eta^{dch}_{\{\cdot\}}, \{\cdot\} = BS, HS \tag{43}$$

$$E_{\{\cdot\},min} \le E^s_{\{\cdot\},t} \le E_{\{\cdot\},max}, \{\cdot\} = BS, HS \tag{44}$$

$$\begin{bmatrix} L_{e,t} + P^s_{BS,t} \\ L_{h,t} + P^s_{HS,t} \end{bmatrix} = \begin{bmatrix} 1 - v^s_{e,t} & v^s_{g,t}\eta_{CHP^e}(1 - v^s_{e,t}) \\ v^s_{e,t}\eta_{COP} & v^s_{g,t}(\eta_{CHP^h} + \eta_{CHP^e} v^s_{e,t} \eta_{COP} + \eta_{GF} - v^s_{g,t} \end{bmatrix} \times \begin{bmatrix} f^{s,inj}_{l_e,t} \\ f^{s,inj}_{l_g,t} \end{bmatrix} \tag{45}$$

C. Real-time Operation

In the second stage, corrective operation schemes are deployed, considering LR attacks and renewable output deviations from the forecasting. The corrective actions for addressing the potential impacts from LR attacks consist of i) the power purchase adjustment in the real-time market, ii) the penalty for renewable power output deviation to reduce the renewable power shortage or curtailment, iii) generation adjustment for traditional DGs and natural gas sources due to LR attacks and the renewable fluctuation and iv) load shedding to maintain the system balance in both power and gas systems.

Equation (46) is the regulated output of generators, gas turbines. Equations (47)-(48) model the stealthy designed LR on power system. The load shedding is given in (49). The new balancing conditions of power and gas systems are presented in (50)-(52).

$$P^s_{\{\cdot\},t} - r^-_{\{\cdot\},t} \le P^{re}_{\{\cdot\},t} \le P^s_{\{\cdot\},t} + r^+_{\{\cdot\},t}, \{\cdot\} = i_e, gt \tag{46}$$

$$\sum_{k_e \in K_e} \Delta P_{k_e,t} = 0 \tag{47}$$

$$-\beta_{k_e} P_{k_e,t} \le \Delta P_{k_e,t} \le \beta_{k_e} P_{k_e,t} \tag{48}$$

$$0 \le P^{ls}_{\{\cdot\},t} \le P^{ls}_{\{\cdot\},max}, \{\cdot\} = k_e, k_g \tag{49}$$

$$\sum_{i_e \in I_e} P^{re}_{i_e,t} + \sum_{j \in J} \xi_{j,t} + \sum_{l_e \in L_e} f^{s,ini}_{l_e,t} - \sum_{l_e \in L_e} f^{s,ter}_{l_e,t} = \sum_{k_e \in K_e} P_{k_e,t} + \Delta P_{k_e,t} - P^{ls}_{k_e,t} \tag{50}$$

$$\sum_{i_e \in I_e} Q^{re}_{i_e,t} + \sum_{l_e \in L_e} q f^{re,ini}_{l_e,t} - \sum_{l_e \in L_e} q f^{re,ter}_{l_e,t} = \sum_{k_e \in K_e} Q_{k_e,t} \tag{51}$$

$$\sum_{i_g \in I_g} P^{re}_{i_g,t} + \sum_{l_g \in L_g} f^{re,ini}_{l_g,t} - \sum_{l_g \in L_g} f^{re,ter}_{l_g,t} = \sum_{k_g \in K_g} P_{k_g,t} - P^{ls}_{k_g,t} \tag{52}$$

The rest of the second-stage constraints are not listed due to space limitation. Apart from (46)-(52), the constraints of the second stage are the same as the first-stage constraints when the superscript '*s*' is replaced by '*re*', which denotes the regulated decision variables.

IV. Solution Procedures via Distributionally Robust Optimization

This section proposes the solutions procedures of the DRO-based energy management model for counteracting cyber-attacks. To begin with, a compact matrix formulation is made for describing the two-stage optimization framework. Section B proposes the DRO ambiguity set. A set of distributions containing the true distributions of FDI attacks and renewable generation are constructed. The decision is made based on the worst-case distribution, which leads to a mildly conservative energy management program. The Wasserstein metric considers

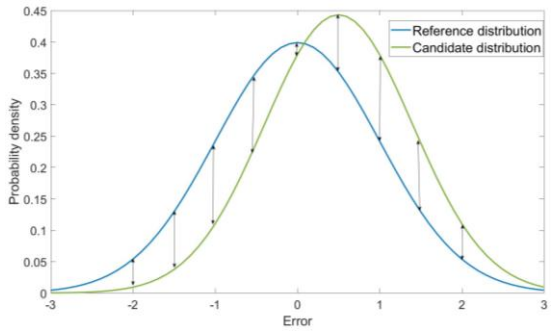


Fig. 5. Wasserstein metric for measuring two distributions.

distributions that are close to the empirical distribution. The radius η can be adjusted by the system operator to balance between the risk and computational efficiency. Finally, the distributionally robust counterpart of the reformulated problems is derived.

A. Compact Matrix Formulation

The illustration of the overall methodology is given in Fig. 4. For clear presentation and notation brevity, the original problem is given as a compact matrix formulation. The first-stage problem is given in (53) and (54), where the first-stage variables are represented by vector *x*. Objective (53) represents (19)-(20) and constraint (54) represents (21)-(45) in the first stage. The second-stage objective $Q(x,\xi)$ is the wait-and-see adaptive objective given the here-and-now decision *x*.

$$\min_{x\in X} c^T x + \sup_{\mathbb{P}\in\Omega} E_{\mathbb{P}}[Q(x,\xi)] \tag{53}$$

$$\text{s.t. } Ax \le b, x \in \mathbb{R}^{V_1}, b \in \mathbb{R}^{C_1}, A \in \mathbb{R}^{C_1\times V_1} \tag{54}$$

The second-stage problem is shown in (55) and (56) and *y* denotes the second-stage variables. Constraints (21)-(45) with superscript '*re*' and (46)-(52) are summarized as (56). Vector $h(\xi)$ is composed of the constant vector h^0 and uncertain vector h_i^{ξ}.

$$Q(x,\xi) = \min_{y} f'y, y \in \mathbb{R}^{V_2} \tag{55}$$

$$\text{s.t. } Bx + Cy \le h(\xi), y \in \mathbb{R}^{V_2}, h \in \mathbb{R}^{C_2}, B \in \mathbb{R}^{C_2\times V_1}, \quad C \in \mathbb{R}^{C_2\times V_2}, D \in \mathbb{R}^{C_2\times i} \tag{56}$$

$$h(\xi) = h^0 + h_i^{\xi}\xi_i \tag{57}$$

B. DRO Ambiguity Set

According to the data-driven setting with empirical distribution $\widehat{\mathbb{P}} = 1/S\sum_{s\in S}\delta_{\hat{\xi}}$, the Wasserstein metric between the candidate and empirical distributions is given in (58) [41]. The Wasserstein metric for measuring the similarity of two distributions is given in Fig. 5. The random variables in the candidate and empirical distributions are denoted as ξ and $\xi^{\dagger}$, respectively. The distance metric is represented by $\rho(\xi,\xi^{\dagger})$.

$$d(\mathbb{P},\widehat{\mathbb{P}}) = \inf E_{\mathbb{Q}}[\rho(\xi,\xi^{\dagger})], \xi\sim\mathbb{P}, \xi^{\dagger}\sim\widehat{\mathbb{P}} \tag{58}$$

The ambiguity set considering the Wasserstein distance is presented in (59), where η is the radius of the ball set. The set of all the possible distributions is denoted as $\boldsymbol{P}$.

$$\mathscr{S} = \left\{ \mathbb{P} \in \boldsymbol{P}(\mathbb{R}^i) \,\middle|\, \begin{matrix} \xi\sim\mathbb{P} \\ d(\mathbb{P},\widehat{\mathbb{P}}) \le \eta \end{matrix} \right\} \tag{59}$$

With the lifted representation of the Wasserstein ambiguity set, (59) can be written as (60). The ambiguity set $\mathscr{S}$ is equivalent to the marginal uncertain distribution of ξ under $\mathbb{P}$.

$$\mathscr{S} = \left\{ \mathbb{P} \in \boldsymbol{P}(\mathbb{R}^i \times \mathbb{R}^j) \,\middle|\, \begin{matrix} (\xi,\tilde{s})\sim\mathbb{P} \\ E_{\mathbb{P}}[\rho(\xi,\xi_s)|\tilde{s}\in\boldsymbol{S}] \le \eta_s \\ \mathbb{P}[(\xi\in\boldsymbol{S})|\tilde{s}=s] = 1 \\ \mathbb{P}[\tilde{s}=s] = 1/S \end{matrix} \right\} \tag{60}$$

The explicit conditional Wasserstein-based ambiguity set is given in (61), where the scenarios are distinguished by $\tilde{s}$, representing the support of ξ is different based on different scenarios. The ambiguity set in (61) ensures i) the uncertain variables ξ, φ and $\tilde{s}$ are within the distribution; ii) the expectation of uncertain variable ξ is μ_s; iii) the auxiliary variable φ is used to ensure limited the distribution distance and iv) ξ and φ are limited within the lifted support set Ξ.

$$\mathscr{S} = \left\{ \mathbb{P} \in \boldsymbol{P}(\mathbb{R}^i \times \mathbb{R}^j) \,\middle|\, \begin{matrix} ((\xi,\varphi),\tilde{s})\sim\mathbb{P} \\ E_{\mathbb{P}}[\xi|\tilde{s}\in\boldsymbol{S}] = \mu_s \\ E_{\mathbb{P}}[\varphi|\tilde{s}\in\boldsymbol{S}] \le \eta_s \\ \Xi = \{(\xi,\varphi)\in\mathbb{R}^i\times\mathbb{R}^j : Gx + Hy \le r\} \\ \mathbb{P}[(\xi,\varphi)|\tilde{s}\in\boldsymbol{S}] = 1 \\ \mathbb{P}[\tilde{s}\in\boldsymbol{S}] = 1 \end{matrix} \right\} \tag{61}$$

C. Approximation via Linear Decision Rule

Equation (62) is obtained as is equivalent to $Q(x,\xi)$, where $y(\xi)$ is the adaptive recourse function as shown in (63). Determining the worst-case expectation $Q(x,\xi) = \sup_{\mathbb{P}\in\Omega} E_{\mathbb{P}}[Q(x,\xi)]$ is generally intractable since all the possible realizations pertaining to the uncertainties are involved [42]. Employing the LDR in (64) can address the problem [43], which approximates $y(\xi)$ by linear affine functions of ξ and φ.

$$Q(x,\xi) = \sup_{\mathbb{P}\in\Omega} E_{\mathbb{P}}[Q(x,\xi)] = \sup_{\mathbb{P}\in\Omega} E_{\mathbb{P}}[f'y(\xi)] \tag{62}$$

$$y(\xi) \in \arg\min\{f'y:\ Bx + Cy \le h(\xi)\}, y \in \mathbb{R}^{V_2}, h \in \mathbb{R}^{C_2}, B \in \mathbb{R}^{C_2\times V_1}, C \in \mathbb{R}^{C_2\times V_2}, D \in \mathbb{R}^{C_2\times i} \tag{63}$$

$$y_n(\xi,\varphi) = y_n^0 + \textstyle\sum_{\xi\in\tilde{\xi}} y_n^{\xi}\xi + \sum_{\varphi\in\tilde{\varphi}} y_n^{\varphi}\varphi \tag{64}$$

The approximation of function $Q(x,\xi)$ can be obtained when the recourse decision $y(\xi)$ is replaced by the LDR expression in (65), which is denoted as $Q_{LDR}(x,\xi)$.

$$Q_{LDR}(x,\xi,\varphi,\tilde{s}) = \min \sup_{\mathbb{P}\in\Omega} E_{\mathbb{P}}[f'y(\xi,\varphi,\tilde{s})] \tag{65}$$

$$\text{s.t. } Bx + Cy(\xi,\varphi,\tilde{s}) \le h(\xi),\ \forall(\xi,\varphi)\in\Xi \tag{66}$$

D. Dual Reformulation and Distributionally Robust Counterpart

In order to convert the original 'min sup' framework of the second stage into 'min' and thus mixed with the first-stage objective, a dual reformulation for the inner maximation problem is made [44] in (67)-(70), where ψ and λ are dual variables.

$$Q_{LDR} = \min \tau + \psi\eta_s + \lambda\mu_s \tag{67}$$

$$\text{s.t.}\quad \tau + \xi'\lambda + \varphi'\psi \ge f'y(\xi,\varphi,\tilde{s}),\ \forall(\xi,\varphi)\in\Xi \tag{68}$$

$$Bx + Cy(\xi,\varphi,\tilde{s}) \le h(\xi), \forall(\xi,\varphi)\in\Xi \tag{69}$$

$$\psi \ge 0, \psi\in\mathbb{R}^j, \tau\in\mathbb{R}, \lambda\in\mathbb{R}^i \tag{70}$$

The proof of (67)-(70) is given below. Firstly, the conic representation of (67)-(70) is given:

$$Q_I^* = \min \boldsymbol{F} \tag{71}$$

$$\text{s.t.} \quad (\boldsymbol{F}, -\psi, -\lambda)'(1,\eta,\mu) \geq 0 \qquad \forall (1,\eta,\mu) \in \kappa(B) \tag{72}$$

$$(\tau - f'y(\xi,\varphi,s), \lambda, \psi)'(1,\xi,\varphi) \geq 0 \quad \forall (1,\xi,\varphi) \in \kappa(C) \tag{73}$$

$$\left(Bx - h^0, Cy^{\xi s} - h^{\xi}, Cy^{\varphi s}\right)'(1,\xi,\varphi) \geq 0 \quad \forall (1,\xi,\varphi) \in \kappa(C) \tag{74}$$

The below formulation is derived based on the dual cone, where are dual multipliers for representing the original expressions in implicit and compact forms.

$$Q^*_{II} = \min \boldsymbol{F} \tag{75}$$

$$\text{s.t.} \quad \left(\boldsymbol{F}, \underbrace{-\psi}_{\Lambda}, \underbrace{-\lambda}_{\Pi}\right) \in \kappa(B) \tag{76}$$

$$\left(\underbrace{\tau - f'y(\xi,\varphi,s)}_{\Theta}, \underbrace{\lambda}_{\Phi}, \underbrace{\psi}_{\Psi}\right) \in \kappa(C) \tag{77}$$

$$\left(Bx - h^0, \underbrace{Cy^{\xi s} - h^{\xi}}_{M}, \underbrace{Cy^{\varphi s}}_{\vartheta}\right) \in \kappa(C) \tag{78}$$

Based on the conic duality, the dual representation of (75)-(78) is:

$$Q^*_{III} = \max \left(\Theta f' y^{0s} + (\Theta f' - MC)y^{\xi s} + (\Theta f' - \vartheta C)y^{\varphi s} + h^0 - Bx - Cy^{0s} + h^{\xi} M\right) \tag{79}$$

$$\text{s.t.} \quad \Theta = -\tau, \tag{80}$$

$$\Pi - \Phi \geq 0, \tag{81}$$

$$\Lambda = \Psi \tag{82}$$

The slaters condition is satisfied based on the assumption made in *Theorem 1.4.2* of [45]: i) a strictly feasible solution can be obtained from (79)-(82) and ii) according to the duality theory, the strong duality holds and $Q^*_{III} = Q_{LDR}$ is derived. Accordingly, problems (67)-(70) are solvable. The reformulated (67)-(70) is a robust linear program, which can be written as the distributionally robust counterpart in (83)-(90).

$$Q_{LDR} = \min \tau + \psi\eta_s + \lambda\mu_s \tag{83}$$

$$\text{s.t.} \quad \tau - f' y^{0s} + \chi_0' r \geq 0 \tag{84}$$

$$\chi_{0s}' G_{si} = \sum_n q_n y_{ni}^{\xi s} - \lambda_i, \forall i \in I, \forall s \in S \tag{85}$$

$$\chi_{0s}' H_{sj} = \sum_n q_n y_{nj}^{\varphi s} - \psi_j, \forall j \in J, \forall s \in S \tag{86}$$

$$\chi_{ms}' G_{si} = \sum_n C_{mn} y_{ni}^{\xi s} - h_{mi}^{\xi}, \forall i \in I, \forall s \in S \tag{87}$$

$$\chi_{ms}' H_{sj} = \sum_n C_{mn} y_{nj}^{\varphi s}, \forall j \in J, \forall s \in S \tag{88}$$

$$B_m' x + C_m' y^{0s} - h_m^0 + r' \chi_{ms}, \forall s \in S \tag{89}$$

$$\psi \geq 0, \chi_0 \geq 0, \chi_m \geq 0, \tau \in \mathbb{R}, \lambda \in \mathbb{R}^i, \psi \in \mathbb{R}^j \tag{90}$$

The new dual variables are represented as χ_0 and χ_m, respectively. Accordingly, the tractable approximation of the original DR-RIM is derived in (83)-(90).

V. Case Studies

The extensive case studies of DR-RIM are tested in three MEDSs with different scales, i.e., a modified IEEE 33-bus distribution system, a 69-bus distribution system and a 123-bus distribution system connected with 20-node gas systems. Both the power and gas systems are in radial topology and 8 cases are studied for each system. The three case studies are implemented in MATLAB and solved by MOSEK on a PC with 16GB RAM

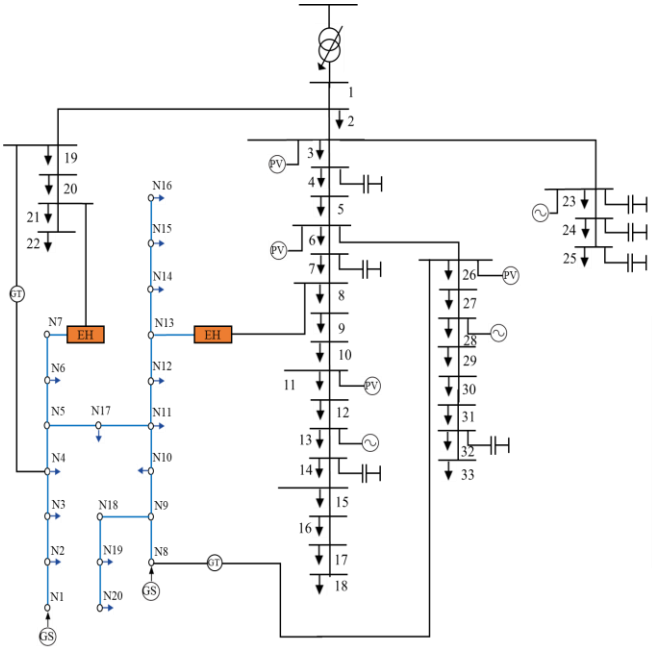


Fig. 6. Modified IEEE 33-bus system.

TABLE I
PARAMETERS OF NATURAL RESOURCES

Node No.	$P_{i_g,min}$ (kcf/h)	$P_{i_g,max}$ (kcf/h)	λ_{i_g}
1	0	35.31	2.2
8	0	70.63	2

TABLE II
GENERATOR PARAMETERS

Bus No.	$P_{i_e,max}$ (MW)	$P_{i_e,min}$ (MW)	R_i^+, R_i^- (MW)	a_i	b_i	c_i
13	1.2	0.3	0.2	0.1	50	62
23	1.2	0.3	0.2	0.1	50	62
28	1.0	0.1	0.2	0.15	65	86

TABLE III
ECONOMIC PERFORMANCE

Economic result	Case 1	Case 2	Case 3	Case 4
First-stage cost ($)	191760	202590	209565	189390
Expected Second-stage cost ($)	0	0	0	7730
Total cost ($)	191760	202590	209565	197120
Economic result	Case 5	Case 6	Case 7	Case 8
First-stage cost ($)	191302	203331	215339	232939
Expected Second-stage cost ($)	9645	9688	9753	13818
Total cost ($)	200947	213019	225092	246757

TABLE IV
FCR FOR CASE 3-8

FCR	Line 1-2	Line 6-7	Line 28-29
Case 3	65%	42%	37%
Case 4	63%	31%	34%
Case 5	63%	31%	34%
Case 6	63%	33%	35%
Case 7	64%	36%	37%
Case 8	65%	37%	38%

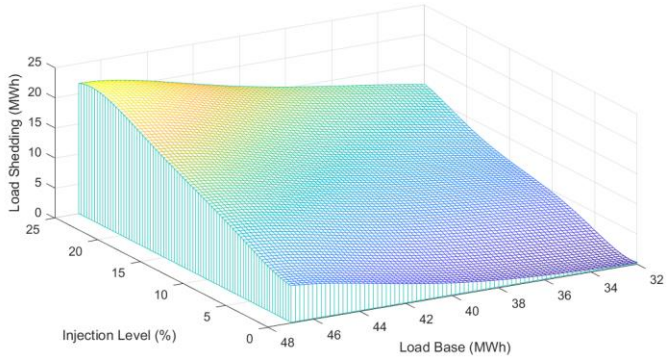


Fig. 7. Active power load shedding for modified IEEE 33-bus system.

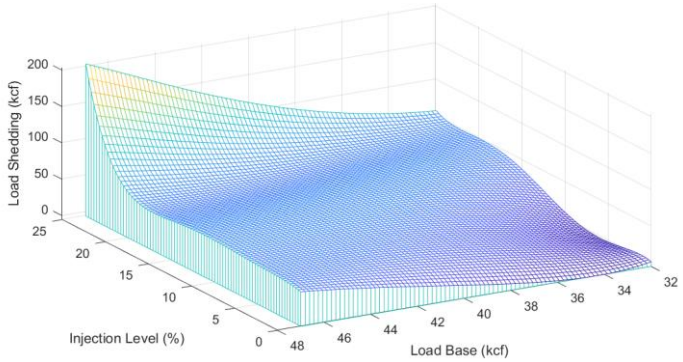


Fig. 8. Gas load shedding for modified IEEE 33-bus system.

and an Intel Core i7 CPU with 1.5GHz. The proposed model is verified using the following 8 cases:

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

Case 2: Case 1 considering LR attacks (β=5%) by using RO.

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

Case 4: Two-stage DR-RIM considering LR attacks (β=5%).

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

Case 6: Case 5 with β=10%.

Case 7: Case 5 with β=15%.

Case 8: Case 5 with β=20%.

A. Studies on Modified IEEE 33-Bus Distribution System

The MEDS is first conducted in a modified IEEE 33-bus system with the connection of a 20-node gas system, which is shown in Fig. 6. The power system has 3 traditional DGs connected to buses 13, 23 and 28. The 20-node gas network contains 2 gas resources. Two energy hubs are interconnected between power and gas systems. Tables I and II present the parameters for gas sources and traditional DGs respectively.

Each load is equipped with a meter and thus the applied MEDS is equipped with 45 load meters. The attacker enables to evade detection and launch stealthy designed LR attacks. This paper assumes that the attacker has the full knowledge of the network topology and technical parameters [20, 21], which means all the buses are exposed to LR attacks.

1) Studies on Economic Performance

The economic performance of all cases presented in Table III is analysed first. Case 1 yields the lowest total cost among all 8 cases, i.e., 191760$. However, by using DRO under the two-stage scheme, cases 4 and 5 have lower first-stage cost than case 1, i.e. 189390$ and 191302$. The reason is that under LR attacks and renewable uncertainty, dispatching sufficient generation in the

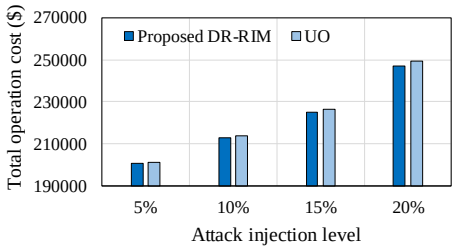


Fig. 9. Total operation cost comparison with UO.

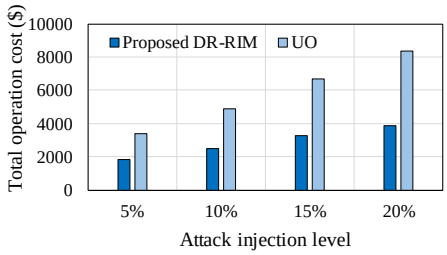


Fig. 10. Load shedding cost comparison with UO.

TABLE V
ECONOMIC PERFORMANCE OF MEDS-69

Economic result	Case 1	Case 2	Case 3	Case 4
First-stage cost ($)	594470	607542	612958	592018
Expected Second-stage cost ($)	0	0	0	12022
Total cost ($)	594470	607542	612958	604040
Economic result	**Case 5**	**Case 6**	**Case 7**	**Case 8**
First-stage cost ($)	595850	604306	613015	622850
Expected Second-stage cost ($)	13580	14634	15795	16820
Total cost ($)	609430	618940	628810	639670

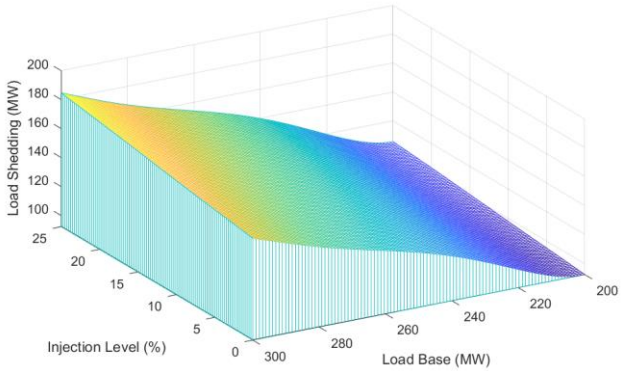


Fig. 11. Active power load shedding for modified IEEE 69-bus system.

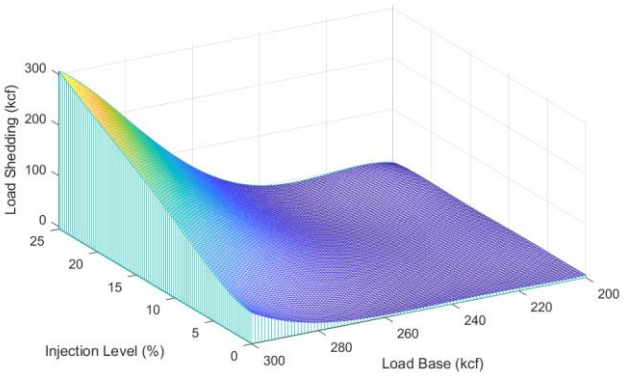


Fig. 12. Gas load shedding for modified IEEE 69-bus system.

TABLE VI
ECONOMIC PERFORMANCE OF MEDS-123

Economic result	Case 1	Case 2	Case 3	Case 4	Case 5
First-stage cost ($)	1083956	1226523	1163208	1156059	1245230
Expected Second-stage cost ($)	27784	0	30174	29830	37045
Total cost ($)	1111740	1226523	1193382	1185889	1282275

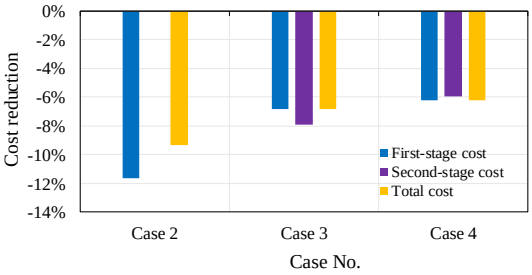


Fig. 13. Cost increase compared with Case 1.

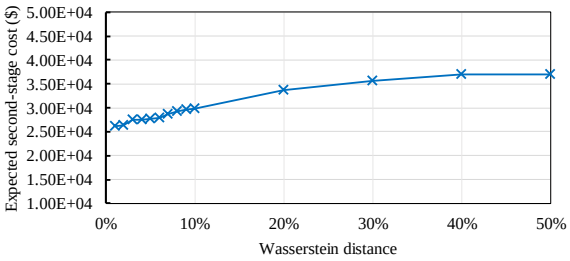


Fig. 14. The impact of Wasserstein distance on the expected result.

TABLE VII
COMPUTATIONAL EFFICIENCY IN SECONDS

Sample size	50	100	200	300	500	1000
W-DRO	25	65	221	731	1928	5402
M-DRO	55	103	317	902	2418	11025

first stage will lead to significant load shedding cost in the second stage. Thus, DR-RIM prefers to dispatch less generation in the first stage and the unmet demand will be satisfied through the redispatch in the second stage, to avoid high load shedding costs. The total cost of case 2 is higher than that of case 1 since LR attacks are modelled. When considering both LR attacks and renewable uncertainties, the cost of case 3 is 3.4% higher than that of case 2. Compared with cases 2 and 3, there are cost reduction of 5470$ and 8618$ respectively for cases 4 and 5, implying the less conservatism of DRO. From cases 5 to 8, with increasing AIL from 5% to 20%, there are 6%, 12% and 22% of the cost increase. It should be noted that the second-stage cost grows smoothly from cases 5 to 8, which indicates that under the AIL of 15%, the LR attacks have less impact on load shedding than high AIL, i.e. 20%.

2) Studies on Load Shedding

Shedding on active power load shedding (APLS) and gas load shedding (GLS) are analyzed under different AILs and load bases. The total power load (32MWh) at the first time period is set as 1 p.u. and defined as load base. Apart from considering AIL, the impact of load base on load shedding is also investigated in the case of uncertain load variations during high consumption periods or special events. s. 6-7 show the general increasing trend of load shedding with the increase of either AIL or load base. As shown in Fig. 7, the APLS is only up to 5MWh at the maximum load base when no LR attacks are imposed. However, under 25% of AIL, the APLS ranges from 12MWh to 22MWh, which reaches up to 42% of the total load. GLS in Fig. 8 shows the different changing speed with respect to different AILs and load bases. When the load base is low, i.e., under 40 MWh, GLS increases slowly. When the load base is high, GLS increases smoothly until when AIL is above 20% and increases significantly. In addition, GLS is not sensitive when AIL is between 10% and 20%.

3) FDI Impact on Flow Variation

In cases 3-8, the impact of LR attacks and renewable uncertainties on active power flow is given in TABLE IV. Lines 1-2, 6-7 and 29-29 are chosen for analysis as they are main branches. A flow capacity ratio (FCR) is defined as the percentage of flow over its capacity. In general, from cases 3-8, with increasing AIL, FCR changes smoothly. The reason is that although LR attacks cause the changes of load measurement, LR attacks cause some load to increase but some load to decrease. The overall load increment is zero, which can deceive operators and thus the influence on flow is low.

Line 1-2 is the most important branch in the system which transmits a large amount of power from the upper-level network, whose FCR is also the highest. There is a small FCR increase when AIL increases from cases 5-8, i.e., from 63% to 65%. Case 3 solved by RO has similar FCR with case 5 solved by DRO for line 1-2. For line 6-7, compared with case 5, RO in case 3 yields 12% more FCR due to the strong robustness. In addition, compared with line 1-2 and line 28-29, increasing AIL in cases 5-8 causes more sensitive FCR increase.

4) Cyber-Resilience Enhancement Compared with Uneconomic Operation

To verify the effectiveness of the proposed strategy for uneconomic operation (UO), a new comparison between the DR-RIM and normal UO is investigated and results are in Figs. 9 and 10. UO is defined as system operation conducted by system operator without effective countermeasures under LR attacks, i.e. load measurement on each bus has been falsified and the operation scheme is not adjusted when false data injections are launched successfully, wrong decisions would be made. This could cause extra cost compared to the normal case with correct load measurement, where the operational decisions are made to securely operate the system while minimizing operation cost. To model UO, 1000 load variation samples are generated via Gaussian distribution with $\mu=0$ and $\sigma=0.02$. For example, at 8:00, the attacked load measurements show 80% of the predicted day-ahead load demand. Generation and energy flow schemes are determined based on this and yield smaller generation output. Nevertheless, in the real world, the total load level is 100% of the predicted day-ahead load demand, which results in a large amount of load shedding, causing economic loss. By contrast, DR-RIM considers the worst distribution of potential LR attacks and mitigates the risk. Intuitively, the second-stage inner min-max framework of DR-RIM considers LR attacks rather than trust the attacked load measurements.

Fig. 9 presents the total operation cost from DR-RIM and UO models. The costs of UO scheme under all the AIL are always higher than that of DR-RIM. When AIL is 5%, the cost from DR-RIM is $200947 while the cost from UO is $203470. Under the highest considered AIL, the cost difference between the two is $4327. In Fig. 10, UO yields higher load shedding cost compared

TABLE VIII
PERFORMANCE COMPARISON UNDER THREE TEST SYSTEMS

Economic result	33-C5	33-C8	69-C5	69-C8	123-C1	123-C2	123-C3
First-stage cost ($)	191302	232939	595850	622850	1083956	1226523	1163208
Expected Second-stage cost ($)	9645	13818	13580	16820	27784	0	30174
Total cost ($)	200947	246757	609430	639670	1111740	1226523	1193382

with DR-RIM under all considered AIL. Similarly, the cost difference increases with growing AIL. The load shedding cost from UO is 1.85 times of that from DR-RIM when AIL is 5% while the ratio increases to 2.15 times when AIL is 20%.

B. Studies on a Modified IEEE 69-Bus Distribution System

In addition, the proposed DR-RIM is tested in a modified IEEE 69-bus system connected with a 20-node gas system, namely the MEDS-69 system. Four traditional DGs are connected to bus 6, 30, 47 and 60. Two renewable DGs are connected to buses 16 and 36.

1) Studies on Economic Performance

The economic performance of the modified IEEE 69-bus system is presented in TABLE V. In case 1, deterministic optimization yields the lowest total cost (594470$). RO is applied for case 2 and 3, whose economic results are more conservative compared with case 4 and 5 applied by DRO. When renewable power uncertainty is additionally considered, there is 5416$ additional cost of case 3 compared with case 2. For case 4 and 5 whose LR attacks and renewable uncertainty are captured by DRO, case 5 yields 5390$ more total cost than case 4. When the AIL increases from 5% to 20%, both the day-ahead and real-time corrective cost increase. The total cost of case 8 is 30240$ higher than that of case 5.

2) Studies on Load Shedding

APLS and GLS are studied when AIL varies from 0% to 25% and load base varies from 200MWh to 300MWh. Same as Fig. 11 and 7 tested by the modified IEEE 33-bus system, with the increase of AIL or load base, the power and gas load shedding both increase. In Fig. 12, The APLS ranges from 91MWh to 105MWh when load base is 200MWh and the level of the range increases dramatically when load base is 300MWh, which ranges from 162MWh to 184MWh. The maximum APLS reaches at 184MWh under LR attack with 25% of AIL and 300MWh of load base. In Fig. 12, GLS shows uneven growth under different load bases, i.e., it increases slowly when load base is under 270 MWh while shows a rapid growth above 270MWh. When both the AIL and load base are at the highest level, GLS reaches 309kcf.

C. Studies on a Modified IEEE 123-Bus Distribution System

To analyse the scalability of the DR-RIM, a case study is conducted in a larger system, namely the MEDS-123 system. The MEDS-123 test system consists of 9 traditional DGs and 5 renewable DGs [46, 47]. To compare with the state-of-the-art optimization approach mitigating FDI, the proposed model is verified using the following cases:

Case 1: The proposed DR-RIM with β=5% and η=5% .
Case 2: Case 1 solved by RO.
Case 3: Case 1 solved by M-DRO.
Case 4: Case 1 with η=10%.
Case 5: Case 1 with η=50% .

TABLE VI shows the economic performance of the 5 cases. The cost reduction of Case 1 compared with Cases 2-4 is given in Fig. 13. Note that the proposed Wasserstein metric-based DRO is denoted as W-DRO and the moment-based DRO is denoted as M-DRO [28]. All the cases are conducted when β=5%. Cases 2 and 3 are designed for testing the FDI mitigation model via different optimization methods. To test the effect of the Wasserstein radius on the algorithm performance, Cases 4 and 5 are employed. Compared with Case 2 and 3, Case 1 shows 9% and 7% less total operation cost. The increase of the radius scales up the ambiguity set, which directly leads to the larger FDI variation with higher operation costs. Compared with Case 1, Cases 4 and 5 result in $74149 and $170535. In Fig. 14, the influence of the Wasserstein distance on the second-stage expected cost is quantified. When η reaches 40%, the operation cost is almost fixed at $37000. The computational time of W-DRO and M-DRO is shown in TABLE VII. The computational efficiency is decreasing with the growth of the sample size. It should be noted that the M-DRO utilizes the constraint generation algorithm in an iterative manner, which determines the end of the algorithm by an optimality gap. M-DRO shows higher computational time compared with W-DRO. When the sample size is 1000, M-DRO yields 204% of the computational time compared with the proposed W-DRO.

D. Result Discussion

In the case studies, the proposed DR-RIM is tested on three system topologies, namely, IEEE 33-bus MEDS, IEEE 69-bus MEDS, and IEEE 123-bus MEDS. Through the extensive simulation tests on economic performance, FCR, load shedding, and the computational time, the proposed DR-RIM with Wasserstein metric-based ambiguity set is proved with more computationally efficient and more resilient against cyber-attacks. For notation brevity, R-RIM and M-RIM are used for describing the **r**obust/**m**oment-based **r**esilience **i**mprovement for **M**EDS operation under cyber-attacks [9, 10, 28].

In section A-1, cases 2 and 3 employ RO to mimic the worst-case FDI attack as the traditional methods [9, 10]. Cases 4 and 5 are set particularly for comparing the reduced operation cost with cases 2 and 3 modelled by R-RIM. As discussed in section A-1, R-RIM shows 2.8% and 4.3% higher total operation cost than DR-RIM. In Figs. 9 and 10 of section A-4, DR-RIM is compared with UO (operation conducted by system operator without effective countermeasures under LR attacks). The results of Figs. 9 and 10 show that DR-RIM yields less operation cost than UO. In particular, when AIL is 20%, the load shedding cost of UO is 115% higher than that of DR-RIM. In TABLE V of section B-1, the less conservatism of DR-RIM is again proved over R-RIM. In section C, case 1 is the benchmark case modelled by DR-RIM. Cases 2 and 3 apply RO and M-DRO, respectively. In TABLE VI, it shows that case 1 results in 9% and 7% less operation cost compared with cases 2 and 3. In Fig. 13, the bar chart demonstrates again the advantage on the economic performance of DR-RIM over R-RIM and M-RIM. In addition to the reduced objective results, the proposed DR-RIM shows the reduced computational time over M-RIM. When the sample size is 1000, the DR-RIM and M-RIM require 5402 and 11025 seconds for

computation, respectively. Since R-RIM relies on the iterative decomposition method, namely constraint generation algorithm. Overall, section V is mainly used to demonstrate the proposed DR-RIM performs better than R-RIM and M-RIM in terms of optimized objective results and computational time.

In TABLE VIII, the economic performance comparison of DR-RIM tested in three test systems is given. Note that 33-C5 represents case 5 of test in the 33-bus MEDS. And the rest of the headers follows the same notation rule. 33-C5, 69-C5, and 123-C1 are used to compare the performance with β=5%. 33-C8 and 69-C8 are presented to demonstrate the performance with β=20%. When β=5%, DR-RIM yields averagely 13.9% lower result than that of β=20%. It can also be observed that with the increase of the system scale, the operation cost increases, e.g., the total operation cost of 33-C8, 69-C8, and 123-C1 are \$246757, \$639670, and \$1111740, respectively. 123-C1, 123-C2, and 123-C3 are used to investigate the less robustness of W-DRO, i.e., 123-C1 yields 9.4% and 6.8% lower results than those of 123-C2 and 123-C3.

VI. Conclusion

This paper proposes a novel DR-RIM approach for a hierarchical day-ahead and real-time operation and emergency response framework for MEDS under potential LR attacks. The proposed method can effectively mitigate uneconomic operation for MEDS under LR attacks and renewable uncertainties in both day-ahead and real-time schemes. The MEDS system resilience is ensured and operation cost is reduced, facilitating the resilience and affordability of the energy trilemma.

Through extensive simulations, the key findings are as follows:

- DRO outperforms RO by providing less-conservative results, working as a more economical method to deal with LR attacks and renewable uncertainties.
- The second-stage reschedule provides a corrective scheme to minimize operation costs and meanwhile ensures the system resilience through APLS and GLS.
- APLS is more sensitive than GLS with the increasing AIL because power load is much higher than gas load.
- Renewable generation uncertainty is essential to be considered with LR attacks simultaneously since it fluctuates and can averagely cause 3% more total cost.
- The operation cost is sensitive to the increase of AIL. e.g., from case 5 to case 8, a 15% increase of AIL causes 22% additional operation cost.

There are several limitations which require further research. Most prominently, in addition to the load meter readings, the other meter readings in MEDS are also exposed to cyber-attacks, e.g., gas pressure, voltage magnitude, etc. Therefore, we aim to apply a more complete and specified cyber-resilience operation model to counteract more complex cyber-attacks. Furthermore, the impact of cyber-attacks on voltage and power quality should be investigated for ensuring the system stability and security. Load shedding is considered as an effective measure to secure the entire system while sacrificing the non-critical load connections. Demand-side management will be incorporated into the cyber-resilience scheme to investigate its functionality to mitigate the impact of cyber-attacks.

References

[1] 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.

[2] 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.

[3] J. E. Sullivan and D. Kamensky, "How cyber-attacks in Ukraine show the vulnerability of the US power grid," *The Electricity Journal*, vol. 30, no. 3, pp. 30-35, 2017.

[4] D. U. Case, "Analysis of the cyber attack on the Ukrainian power grid," *Electricity Information Sharing and Analysis Center (E-ISAC)*, vol. 388, 2016.

[5] 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).

[6] Y. Tan, Y. Li, Y. Cao, M. Shahidehpour, and Y. Cai, "Severe Cyber Attack for Maximizing the Total Loadings of Large-Scale Attacked Branches," *IEEE Transactions on Smart Grid*, vol. 9, no. 6, pp. 6998-7000, 2018, doi: 10.1109/TSG.2018.2865136.

[7] G. Liang, S. R. Weller, J. Zhao, F. Luo, and Z. Y. Dong, "A Framework for Cyber-Topology Attacks: Line-Switching and New Attack Scenarios," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 1704-1712, 2019, doi: 10.1109/TSG.2017.2776325.

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] A. Abusorrah, A. Alabdulwahab, Z. Li, and M. Shahidehpour, "Minimax-Regret Robust Defensive Strategy Against False Data Injection Attacks," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2068-2079, 2019, doi: 10.1109/TSG.2017.2788040.

[13] A. Farraj, E. Hammad, A. A. Daoud, and D. Kundur, "A Game-Theoretic Analysis of Cyber Switching Attacks and Mitigation in Smart Grid Systems," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 1846-1855, 2016, doi: 10.1109/TSG.2015.2440095.

[14] 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.

[15] H. Wang *et al.*, "Deep Learning-Based Interval State Estimation of AC Smart Grids Against Sparse Cyber Attacks," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 11, pp. 4766-4778, 2018, doi: 10.1109/TII.2018.2804669.

[16] M. Jin, J. Lavaei, and K. H. Johansson, "Power Grid AC-Based State Estimation: Vulnerability Analysis Against Cyber Attacks," *IEEE Transactions on Automatic Control*, vol. 64, no. 5, pp. 1784-1799, 2019, doi: 10.1109/TAC.2018.2852774.

[17] 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.

[18] M. N. Kurt, Y. Yılmaz, and X. Wang, "Distributed Quickest Detection of Cyber-Attacks in Smart Grid," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 8, pp. 2015-2030, 2018, doi: 10.1109/TIFS.2018.2800908.

[19] H. M. Khalid and J. C. Peng, "A Bayesian Algorithm to Enhance the Resilience of WAMS Applications Against Cyber Attacks," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 2026-2037, 2016, doi: 10.1109/TSG.2016.2544854.

[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.

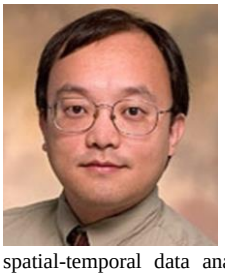
[21] Y. Yuan, Z. Li, and K. Ren, "Quantitative Analysis of Load Redistribution Attacks in Power Systems," *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 9, pp. 1731-1738, 2012, doi: 10.1109/TPDS.2012.58.

[22] M. Qadrdan, J. Wu, N. Jenkins, and J. Ekanayake, "Operating Strategies for a GB Integrated Gas and Electricity Network Considering the Uncertainty in Wind Power Forecasts," *IEEE Transactions on Sustainable Energy*, vol. 5, no. 1, pp. 128-138, 2014, doi: 10.1109/TSTE.2013.2274818.

[23] D. Huo, S. Le Blond, C. Gu, W. Wei, and D. Yu, "Optimal operation of interconnected energy hubs by using decomposed hybrid particle swarm and interior-point approach," *International Journal of Electrical Power & Energy Systems*, vol. 95, pp. 36-46, 2018/02/01/ 2018, doi: https://doi.org/10.1016/j.ijepes.2017.08.004.
[24] D. Huo, C. Gu, K. Ma, W. Wei, Y. Xiang, and S. L. Blond, "Chance-Constrained Optimization for Multienergy Hub Systems in a Smart City," *IEEE Transactions on Industrial Electronics*, vol. 66, no. 2, pp. 1402-1412, 2019, doi: 10.1109/TIE.2018.2863197.
[25] X. Lu, K. W. Chan, S. Xia, X. Zhang, G. Wang, and F. Li, "A Model to Mitigate Forecast Uncertainties in Distribution Systems Using the Temporal Flexibility of EVAs," *IEEE Transactions on Power Systems*, vol. 35, no. 3, pp. 2212-2221, 2020, doi: 10.1109/TPWRS.2019.2951108.
[26] C. He, L. Wu, T. Liu, and M. Shahidehpour, "Robust Co-Optimization Scheduling of Electricity and Natural Gas Systems via ADMM," *IEEE Transactions on Sustainable Energy*, vol. 8, no. 2, pp. 658-670, 2017, doi: 10.1109/TSTE.2016.2615104.
[27] W. Wei, F. Liu, and S. Mei, "Distributionally Robust Co-Optimization of Energy and Reserve Dispatch," *IEEE Transactions on Sustainable Energy*, vol. 7, no. 1, pp. 289-300, 2016, doi: 10.1109/TSTE.2015.2494010.
[28] P. Zhao, C. Gu, and D. Huo, "Coordinated Risk Mitigation Strategy For Integrated Energy Systems Under Cyber-Attacks," *IEEE Transactions on Power Systems*, vol. 35, no. 5, pp. 4014-4025, 2020, doi: 10.1109/TPWRS.2020.2986455.
[29] P. Zhao *et al.*, "A Cyber-Secured Operation for Water-Energy Nexus," *IEEE Transactions on Power Systems*, pp. 1-1, 2020, doi: 10.1109/TPWRS.2020.3043757.
[30] P. Zhuang, R. Deng, and H. Liang, "False Data Injection Attacks Against State Estimation in Multiphase and Unbalanced Smart Distribution Systems," *IEEE Transactions on Smart Grid*, vol. 10, no. 6, pp. 6000-6013, 2019, doi: 10.1109/TSG.2019.2895306.
[31] 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.
[32] K. Dehghanpour, Z. Wang, J. Wang, Y. Yuan, and F. Bu, "A Survey on State Estimation Techniques and Challenges in Smart Distribution Systems," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2312-2322, 2019, doi: 10.1109/TSG.2018.2870600.
[33] 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.
[34] 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.
[35] J. Á. González Ordiano, S. Waczowicz, V. Hagenmeyer, and R. Mikut, "Energy forecasting tools and services," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 8, no. 2, p. e1235, 2018.
[36] G. Sauba *et al.*, "Novel Energy Modelling and Forecasting Tools for Smart Energy Networks," in *2015 International Conference on Renewable Energy Research and Applications (ICRERA)*, 2015: IEEE, pp. 1669-1673.
[37] 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.
[38] E. W. Burger, M. D. Goodman, P. Kampanakis, and K. A. Zhu, "Taxonomy model for cyber threat intelligence information exchange technologies," in *Proceedings of the 2014 ACM Workshop on Information Sharing & Collaborative Security*, 2014, pp. 51-60.
[39] Y. Liu, J. Li, and L. Wu, "Coordinated Optimal Network Reconfiguration and Voltage Regulator/DER Control for Unbalanced Distribution Systems," *IEEE Transactions on Smart Grid*, vol. 10, no. 3, pp. 2912-2922, 2019, doi: 10.1109/TSG.2018.2815010.
[40] K. Ma, R. Li, and F. Li, "Utility-Scale Estimation of Additional Reinforcement Cost From Three-Phase Imbalance Considering Thermal Constraints," *IEEE Transactions on Power Systems*, vol. 32, no. 5, pp. 3912-3923, 2017, doi: 10.1109/TPWRS.2016.2639101.
[41] P. M. Esfahani and D. Kuhn, "Data-driven distributionally robust optimization using the Wasserstein metric: Performance guarantees and tractable reformulations," *Mathematical Programming*, vol. 171, no. 1-2, pp. 115-166, 2018.
[42] 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.
[43] A. Ben-Tal, A. Goryashko, E. Guslitzer, and A. Nemirovski, "Adjustable robust solutions of uncertain linear programs," *Mathematical programming*, vol. 99, no. 2, pp. 351-376, 2004.
[44] A. Shapiro, "On duality theory of conic linear problems," in *Semi-infinite programming*: Springer, 2001, pp. 135-165.
[45] A. Ben-Tal and A. Nemirovski, *Lectures on modern convex optimization: analysis, algorithms, and engineering applications*. SIAM, 2001.
[46] H. Xu, A. D. Domínguez-García, and P. W. Sauer, "Data-Driven Coordination of Distributed Energy Resources for Active Power Provision," *IEEE Transactions on Power Systems*, vol. 34, no. 4, pp. 3047-3058, 2019, doi: 10.1109/TPWRS.2019.2899451.
[47] I. I. o. T. Electrical and Computer Engineering Department. "Index of /data." motor.ece.iit.edu/data/ (accessed.

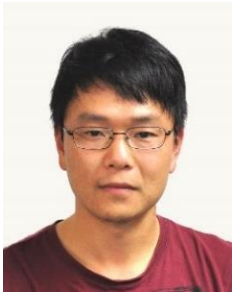
Pengfei Zhao was born in Beijing, China. He received the double B.Eng. degree from the University of Bath, U.K., and North China Electric Power University, Baoding, China, in 2017. He received the Ph.D degree from the University of Bath, U.K. He was a visiting Ph.D. student at Smart Grid Operations and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

Zhidong Cao is a Professor at the State Key Laboratory of Management and Control for Complex Systems, Institute of Automation, Chinese Academy of Sciences, Beijing, China, and the School of Computer and Control Engineering, University of Chinese Academy of Sciences, Beijing, China. His research interests include public health big data and infectious disease informatics.



Daniel Dajun Zeng (F'15) received the Ph.D. degree in industrial administration from Carnegie Mellon University, Pittsburgh, PA, USA, in 1998. He is a Professor with the Institute of Automation, Chinese Academy of Sciences, Beijing, China, and the School of Computer and Control Engineering, University of Chinese Academy of Sciences, Beijing, China. His research interests include intelligence and security informatics, infectious disease informatics, social computing, recommender systems, software agents, spatial-temporal data analysis, and business analytics. He has authored or coauthored one monograph and more than 330 peer-reviewed articles.

He served as the Editor-in-Chief of IEEE INTELLIGENT SYSTEMS from 2013–2016. He currently serves as the Editor in Chief of ACM TRANSACTIONS ON MIS and as the President of the IEEE INTELLIGENT TRANSPORTATION SYSTEMS SOCIETY. He is a Fellow of IEEE.



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.

Zhaoyu Wang (Senior Member, IEEE) received the B.S. and M.S. degrees in electrical engineering from Shanghai Jiaotong University, and the M.S. and Ph.D. degrees in electrical and computer engineering from Georgia Institute of Technology. He is the Harpole-Pentair Assistant Professor with Iowa State University. His research interests include optimization and data analytics in power distribution systems and microgrids. He was the recipient of the National Science Foundation CAREER Award, the IEEE Power and Energy Society (PES) Outstanding Young Engineer Award, College of Engineering's Early Achievement in Research Award, and the Harpole-Pentair Young Faculty Award Endowment. He is the Principal Investigator for a multitude of projects focused on these topics and funded by the National Science Foundation, the Department of Energy, National Laboratories, PSERC, and Iowa Economic Development Authority. He is the Chair of IEEE PES PSOPE Award Subcommittee, the Co-Vice Chair of PES Distribution System Operation and Planning Subcommittee, and the Vice Chair of PES Task Force on Advances in Natural Disaster Mitigation Methods. He is an Associate Editor of IEEE TRANSACTIONS ON POWER SYSTEMS, IEEE TRANSACTIONS ON SMART GRID, IEEE OPEN ACCESS JOURNAL OF POWER AND ENERGY, IEEE POWER ENGINEERING LETTERS, and IET Smart Grid.

Yue Xiang (S'12-M'16) received the B.S. and Ph.D. degrees from Sichuan University, China, in 2010 and 2016, respectively. From 2013 to 2014, he was a joint Ph.D. student at the Department of Electrical Engineering and Computer Science, University of Tennessee, Knoxville, US, a visiting scholar at the Department of Electronic and Electrical Engineering, University of Bath, UK in 2015, and also a visiting researcher at Department of Electrical and Electronic Engineering, Imperial College London, UK in 2019-2020. Now he is an associate professor in the College of Electrical Engineering, Sichuan University, China. His main research interests are distribution network planning and optimal operation, power economics, electric vehicle integration and smart grids.

Meysam Qadrdan is an EPSRC-UKRI Innovation Fellow and a Reader in Energy Networks and Systems at Cardiff University. Before joining Cardiff as a Lecturer in January 2015, he spent one year at Imperial College and two years at Cardiff University as Research Associate. Meysam Qadrdan obtained his PhD from Cardiff University, UK (2012), MSc in Energy Systems Engineering from Sharif University of Technology, Iran (2008) and BSc in Physics from Ferdowsi University, Iran (2005).

Xinlei Chen is currently a postdoctoral research associate in Electrical Engineering Department at Carnegie Mellon University. He received the B.E. and M.S. degrees in Electronic Engineering from Tsinghua University, China, in 2009 and 2012, respectively, and Ph.D degrees in Electrical Engineering from Carnegie Mellon University, Pittsburgh, PA, USA. His research interests lie in mobile computing, crowd intelligence, cyber physical system, mobile embedded system etc.

Xiaohe Yan (Member, IEEE) was born in Shaanxi, China. He received the bachelor's degree in electrical engineering from the Xi'an University of Technology, Shaanxi, China, in 2013, and the master's and Ph.D. degrees from the University of Bath, Bath, U.K., in 2015 and 2019, respectively. He was a Research Associate with Macau University, Macau, China, from 2019 to 2020. He is currently a Lecturer with the Department of Electronic and Electrical Engineering, North China Electric Power University, Beijing, China. His major research interests include energy storage, power system planning, analysis, and power system economics.

Shuangqi Li was born in Beijing, 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.