Distributed Differentially Private Energy Management of Virtual Power Plants

Mingyu Huang, Xueyuan Cui* and Yi Wang
Department of Electrical and Electronic Engineering, The University of Hong Kong, Hong Kong
*Corresponding author, xycui@eee.hku.hk

***Abstract*—Prosumers with flexible distributed energy resources (DERs) can be aggregated as a virtual power plant (VPP) to participate in the electricity market. However, the VPP's energy management requires the prosumers to share individual data, which poses privacy concerns. This paper proposes a distributed differentially private energy management strategy for the VPP to maximize its profit by coordinating the prosumers and at the same time mitigate the privacy risks of local prosumers. Specifically, the coordination of prosumers is first formulated as an optimization problem, which includes the operation constraints of each individual prosumer and the VPP coordination process. On this basis, this paper proposes to solve the optimization problem with a two-level privacy protection strategy. For the individual level, a distributed solution framework is proposed to keep the private information of each prosumer preserved locally. For the communication level, a differential privacy mechanism is integrated into the information exchange process thus reducing the privacy leakage risk. Both theoretical and practical results are provided to verify the performance of the proposed method in terms of optimality and privacy protection levels.**

***Index Terms*—Virtual power plant, prosumer energy management, distributed optimization, differential privacy**

I. Introduction

The increasing penetration of distributed energy resources (DERs) prompts traditional electricity consumers as prosumers, from the role of passive energy consumption to active power management. Under such a transition, prosumers could interact with the power network to provide services and thus make profits [1]. However, it is challenging for massive small-scale prosumers to directly interact with the power network due to the limitations on the control infrastructure and market access conditions [2]. A promising solution is to aggregate a number of prosumers into a virtual power plant (VPP) to provide network services as a single entity. Through the VPP aggregator, the energy scheduling of prosumers can be coordinated, which promotes the flexibility and efficiency of the overall system [3].

The energy management strategy of VPPs is generally cast as a constrained optimization problem with both economic and technical considerations. From an economic perspective, the VPP aims to maximize its profit in energy trading with the electricity market by coordinating internal prosumers using communication technologies. The interaction mechanism with prosumers needs to be carefully designed to incentivize more prosumers to participate. This can be achieved through predefined contracts or post-profit allocation. In [2], VPPs signed contracts with the prosumers to buy/sell electricity at local market prices and thus got the rights for energy scheduling. An auction-theoretic scheme was proposed in [4] to enable the VPP to make energy allocation decisions for strategic prosumers. From a technical perspective, the energy scheduling within a VPP must ensure the feasibility of disaggregation, which requires the operation constraints to be integrated. For example, in [5], the physical constraints of individual DERs and the distribution network were incorporated into the operation model of VPP.

To solve the optimal energy management problem of VPPs, the prosumers' local data need to be revealed to the VPP, which would incur privacy concerns. For example, each prosumer's load and renewable profiles have to be revealed to satisfy the prosumer's individual operation constraints. Apart from the above sensitive information at the individual level, the net power output of prosumers also needs to be exchanged and coordinated to address global constraints (e.g., the upper limit of the VPP's capacity). In this case, there is another privacy risk that a third party or an adversary could infer the prosumer's output profile through the exchanged data at the communication level. Thus, VPP's energy management strategy should be designed to preserve the prosumer's privacy at both the individual level and communication level.

As for individual-level privacy protection, distributed solution algorithms have been proposed to address this issue, including primal-dual decomposition, alternating direction method of multipliers (ADMM), and distributed accelerated gradient descent algorithms. Specifically, in [6], a distributed energy management strategy for residential distributed energy resources in a VPP was proposed, where each user's private information was protected locally by the primal-dual decomposition method. Although the information of users could be preserved locally through parallel problem solving, the convergence of the algorithm requires a strong convexity of the problem. In [7], an ADMM-based algorithm is applied to solve the energy trading problem of VPP in a distributed manner with improved convergence. Besides, an accelerated gradient descent method was proposed in [8] to promote

This work was supported in part by the National Key R&D Program of China (2022YFB2403300) and in part by the Research Grants Council of the Hong Kong SAR (HKU 27203723).

the convergence speed for the energy management of VPP, which could improve the scalability of the solution algorithm. However, these algorithms depend greatly on the information exchange at the communication level, which raises potential privacy risks.

To mitigate the privacy risk at the communication level, encryption-based techniques have been proposed for the management of energy systems. For example, in [9], the authors proposed an encryption-based communication strategy for the iterative update process of ADMM to address the inter-communication privacy issue in active distribution networks. However, the integration of encryption-based algorithms will pose high computation complexity, which is not applicable to large-scale VPP with massive prosumers. In this case, the integration of Differential Privacy (DP) mechanisms into the data exchange process emerges as a viable solution [10]. Different from encryption algorithms, DP is not limited to specific computational tasks and exhibits better scalability. Benefiting from its advantages, DP mechanisms have been applied to various scheduling problems of energy systems [11]. In [12], a differentially private distributed solution framework was proposed for constrained optimization problems and applied in the context of electrical vehicle charging. The trade-off between privacy and utility of the proposed algorithm was demonstrated through the suboptimality analysis. Similarly, a differentially private distributed model predictive control approach was proposed in [13] to optimally operate the energy storage devices of consumers with a privacy guarantee. The existing works show that the integration of DP into the distributed optimization framework is an efficient way to realize privacy-preserving throughout the optimization process.

Although the privacy-preserving schemes at the individual level and the communication level have been preliminarily investigated, there are few works focusing on the two-level privacy protection of VPP's energy management problem. It is essential for the VPP to guarantee the privacy protection level throughout the optimization process for secure energy trading. To this end, this paper proposes a distributed differentially private optimization scheme to solve the energy management of VPP, where the VPP's profit is maximized while protecting the two-level privacy of each prosumer. Compared with the existing works, this paper makes the following contributions:

1) Propose a two-level privacy-preserving energy management scheme for VPPs to guarantee the privacy of prosumers throughout the optimization process, where the distributed optimization framework is integrated with a DP mechanism to mitigate the privacy leakage risk at both the individual level and the communication level;
2) Establish a novel distributed differentially private solution algorithm that can be implemented in parallel, which improves the computation efficiency and scalability of the solution scheme;
3) Provide both theoretical and practical results to verify the performance in terms of privacy and accuracy levels.

The remainder of this paper is presented as follows. Section II formulates the VPP's energy management problem and discusses the privacy issues. Section III presents the proposed distributed differentially private optimization method in detail. Section IV provides case studies to verify the performance. Section V concludes the paper.

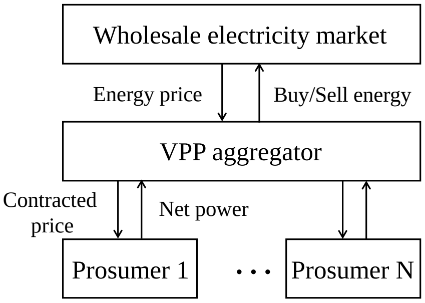

Fig. 1. A block diagram of the operation strategy of VPP.

II. Problem Formulation

In this study, the VPP aggregator acts as a coordinator to facilitate energy trading between the prosumers and the wholesale electricity market, as depicted in Fig. 1. In this framework, the VPP signs contracts with the prosumers to schedule the aggregated power output and interact with the electricity market to maximize its own profits within a given time horizon T. This section presents the detailed model of prosumers, the VPP aggregator, and the energy trading mechanism.

A. Prosumer Model

Prosumers have a set of flexible assets, including PV systems, energy storage systems (ESS), and controllable loads like Heating, Ventilation, and Air Conditioning (HVAC) systems, as illustrated in Fig. 2. The flexible assets enable the prosumers to actively manage their net output. At the individual level, prosumers cannot directly participate in the wholesale electricity market to sell their energy surplus due to the small-scale generation. In this case, individual prosumer participates in the retail market and can only shift their demand to reduce their energy costs. Through the VPP aggregator, prosumers sign energy import and export contracts with the VPP and thus conduct energy trading to make profits [14], such as time-of-use (ToU) tariff and Feed-in Tariff (FiT) schemes [15]. Generally, the local energy price defined in contracts is lower than the retail market to incentivize the prosumers to participate [2]. On this basis, the interaction of prosumers with the VPP aggregator is described as:

$$f_{i,t}\left(P_{i,t}^{\text{net}}\right)=\begin{cases} u_t^{\text{tou}}P_{i,t}^{\text{net}},\ P_{i,t}^{\text{net}}\leq 0, \\ u_t^{\text{fit}}P_{i,t}^{\text{net}},\ P_{i,t}^{\text{net}}>0, \end{cases} \tag{1}$$

where $P_{i,t}^{\text{net}}$ is the net power that prosumer i interacts with the VPP at time t. $P_{i,t}^{\text{net}}$ takes negative (positive) values when prosumer i needs to import (export) energy from (to) VPP. u_t^{tou} and u_t^{fit} are the local energy prices determined in the contract

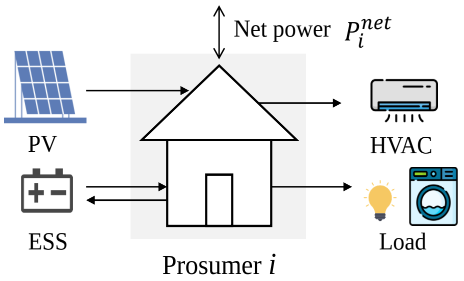

Fig. 2. Flexible assets of a prosumer.

with the VPP. $f_{i,t}\left(P_{i,t}^{\text{net}}\right)$ is the revenue of the prosumers paid by the VPP.

For each prosumer i, its net power $P_{i,t}^{\text{net}}$ is associated with its individual power balance. Specifically, at each time t, the prosumer i's power output $P_{i,t}^{\text{net}}$ is described as

$$P_{i,t}^{\text{net}} = P_{i,t}^{\text{PV}} + P_{i,t}^{\text{ESS}} - \left(P_{i,t}^{\text{HVAC}} + L_{i,t}\right), \tag{2}$$

where $P_{i,t}^{\text{PV}}$ represents the PV system's output. $P_{i,t}^{\text{ESS}}$ is the power output of ESS, which can be positive for discharging and negative for charging. $P_{i,t}^{\text{HVAC}}$ denotes HVAC's power demand. $L_{i,t}$ is the uncontrollable load.

Prosumer i's operation must satisfy its individual constraints, which are determined by the feasible region of DERs.

1) PV system: The power output of a PV system is limited by the maximum available output.

$$0 \le P_{i,t}^{\text{PV}} \le P_{i,t}^{\text{PV,av}}, \tag{3}$$

where $P_{i,t}^{\text{PV,av}}$ is the forecasted maximum PV output.

2) ESS: The operation constraints of ESS include the power capacity limits, energy capacity limits, and the energy balance equation as

$$P_i^{\text{ESS,min}} \le P_{i,t}^{\text{ESS}} \le P_i^{\text{ESS,max}}, \tag{4a}$$

$$E_i^{\text{min}} \le E_{i,t} \le E_i^{\text{max}}, \tag{4b}$$

$$E_{i,t} = \gamma_i E_{i,t-1} - P_{i,t}^{\text{ESS}}, \; E_{i,0} = E_{i,T}, \tag{4c}$$

where $P_i^{\text{ESS,min}}$ and $P_i^{\text{ESS,max}}$ are the minimum and maximum power limits of ESS's output. $E_{i,t}$ is the reserved energy of ESS. E_i^{min} and E_i^{max} are the minimum and maximum energy limits of ESS. γ_i is the self-discharging coefficient of the ESS.

3) HVAC system: HVAC system includes the heating and cooling system, which is used to regulate indoor temperature. The operation constraints of the HVAC system include power output limits, indoor temperature limits, and the discrete dynamic equation of indoor temperature.

$$P_i^{\text{HVAC, min}} \le P_{i,t}^{\text{HVAC}} \le P_i^{\text{HVAC, max}}, \tag{5a}$$

$$F_i^{\text{in,min}} \le F_{i,t}^{\text{in}} \le F_i^{\text{in,max}}, \tag{5b}$$

$$F_{i,t}^{\text{in}} = F_{i,t-1}^{\text{in}} + \alpha_i \cdot \left(F_{i,t}^{\text{out}} - F_{i,t-1}^{\text{in}}\right) + \beta_i \cdot P_{i,t}^{\text{HVAC}}, \tag{5c}$$

where (5a) restricts the power output of the HVAC system. $P_i^{\text{HVAC, min}}$ and $P_i^{\text{HVAC, max}}$ are the minimum and maximum power demand of HVAC, respectively. $F_{i,t}^{\text{in}}$ denotes the indoor temperature. (5b) limits the indoor temperature within the comfortable range, i.e. required minimum temperature $F_i^{\text{in,min}}$ and maximum temperature $F_i^{\text{in,max}}$. (5c) represents the dynamic model of the indoor temperature, where α_i and β_i are the parameters specifying the thermal characteristics of the buildings and the environment [16]. $F_{i,t}^{\text{out}}$ represents the outdoor temperature.

B. VPP Aggregator Model

As an aggregator of the prosumers, VPP interacts with the wholesale electricity market by purchasing/selling the aggregated power. The cost/revenue of VPP in the electricity market is given by the following piecewise linear function:

$$g_t^{\text{VPP}}\left(X_t\right) = \begin{cases} c_t^{\text{buy}} X_t, & X_t \le 0, \\ c_t^{\text{sell}} X_t, & X_t > 0, \end{cases} \tag{6}$$

where X_t is the aggregated power output of the VPP at time t. c_t^{buy} and c_t^{sell} are the electricity prices of the wholesale market. $g_t^{\text{VPP}}\left(X_t\right)$ represents the cost/revenue of VPP by purchasing/selling power. Considering there are N prosumers that are managed by the VPP, the aggregated power X_t participating in the electricity market is presented by the sum of all the prosumer's net power. The aggregated power output X_t is constrained by the capacity limits of the system resources [4]. We denote the limits on X_t as minimum X_t^{min} and maximum X_t^{max}. The VPP's operation constraints are represented as

$$X_t = \sum_{i=1}^{N} P_{i,t}^{\text{net}}, \tag{7a}$$

$$X_t^{\text{min}} \le X_t \le X_t^{\text{max}}. \tag{7b}$$

From the VPP's perspective, the objective is to maximize its own profits, which include the revenue from the electricity market and the cost paid to prosumers. Meanwhile, the aggregated power capacity of VPP and each prosumer's operating constraints are integrated as global constraints and local constraints, respectively. For the given time horizon T, the optimization problem $\mathcal{O}$ is formulated in (8).

$$\mathcal{O}: \max \left[G^{\text{VPP}}\left(X\right) - \sum_{i=1}^{N} F_i\left(P_i^{\text{net}}\right)\right] \tag{8a}$$

$$s.t. \begin{cases} X = \sum\limits_{i=1}^{N} P_i^{\text{net}}, \\ X^{\text{min}} \le X \le X^{\text{max}}, \\ (2)-(5), \quad \forall i = 1, 2, \ldots, N, \end{cases} \tag{8b}$$

where the decision variables are reformulated in a compact form as $X = \left[X_1, \ldots, X_T\right]^{\text{T}}$, $P_i^{\text{net}} = \left[P_{i,1}^{\text{net}}, \ldots, P_{i,T}^{\text{net}}\right]^{\text{T}}$, and $X^{\text{min}} = \left[X_1^{\text{min}}, \ldots, X_T^{\text{min}}\right]^{\text{T}}$, $X^{\text{max}} = \left[X_1^{\text{max}}, \ldots, X_T^{\text{max}}\right]^{\text{T}}$. The objective function is reformulated as vector functions $G^{\text{VPP}}\left(X\right) = \sum\limits_{t=1}^{T} g_t^{\text{VPP}}\left(X_t\right)$ and $F_i\left(P_i^{\text{net}}\right) = \sum\limits_{t=1}^{T} f_{i,t}\left(P_{i,t}^{\text{net}}\right)$.

Remark 2.1: The cost/revenue associated with the VPP's power output is represented by the piecewise linear function as in (6). In practical scenarios, the c_t^{buy} is higher than the c_t^{sell} to avoid large reserve power transmission to the grid. In this case, the objective function (8) maintains convex, which could be solved by distributed convex optimization techniques.

C. Privacy Issues

To solve the optimization problem (8), the prosumers have to reveal all of their operation information to the VPP, which incurs great privacy concerns. The privacy concerns are divided into two levels. Specifically, at the individual level, the privacy information $\mathcal{P}_i$ of each prosumer i includes the uncontrollable load demand, available PV output, ESS capacity, HVAC demand, and comfortable indoor temperature region, which are associated with the individual operation constraints (2)-(5) as in (9a). Besides, at the communication level, the prosumers need to share their energy management decisions (9b) with the VPP for coordinated operation. Since the VPP has signed contracts with the prosumers, the VPP is considered a trustworthy entity that has the right to obtain the net power P_i^{net} of prosumers. However, there is another privacy risk that a third party or an adversary could obtain sensitive information of prosumers from the shared data.

$$\mathcal{P}_i = \left\{ \begin{array}{l} L_{i,t}, P_{i,t}^{\mathrm{PV,av}}, P_i^{\mathrm{ESS,min}}, P_i^{\mathrm{ESS,max}}, E_i^{\mathrm{min}}, E_i^{\mathrm{max}}, \\ \gamma_i, P_i^{\mathrm{HVAC,min}}, P_i^{\mathrm{HVAC,max}}, F_i^{\mathrm{in,min}}, F_i^{\mathrm{in,max}} \end{array} \right\} \tag{9a}$$

$$\mathcal{C}_i = \left\{ P_{i,t}^{\mathrm{net}} \right\}, \ \forall t = 1, 2, \ldots, T. \tag{9b}$$

This study aims to address the two-level privacy issues at the same time.

III. Methodology

A distributed differentially private energy management strategy of VPP is proposed to address the above two-level privacy issues. Specifically, a distributed optimization framework is first proposed to decompose the problem (8), which enables the problem to be solved locally and thus protects the private information of prosumers at the individual level. Meanwhile, for the communication level where each prosumer i exchanges its local energy management decision P_i^{net} with the VPP, the DP mechanism is integrated to further mitigate privacy risks from a deliberate third party.

A. Distributed Optimization Framework

The distributed optimization framework is based on the predictor-corrector proximal multiplier (PCPM) algorithm. Compared with other distributed solution algorithms, it features better convergence for problems with non-smooth objective functions [17]. Specifically, the integration of proximal terms will guarantee the strict convexity of the primal problems. Additionally, compared with ADMM which requires alternating calculation of the primal problems, the PCPM algorithm outperforms in parallel computation, which improves the computation efficiency for large-scale problems. As the VPP's profit model is a piecewise linear function, the PCPM-based algorithm is well suited for the VPP's energy management problem. The Lagrangian function L of (8) is derived as

$$L := G^{\mathrm{VPP}}(X) - \sum_{i=1}^{N} F_i \left(P_i^{\mathrm{net}} \right) + \lambda \left(X - \sum_{i=1}^{N} P_i^{\mathrm{net}} \right), \tag{10}$$

where λ is the dual variable. Problem (8) is reformulated as

$$\max_{X \in \mathcal{X}, \ P_i^{\mathrm{net}} \in \mathcal{Y}_i} \min_{\lambda} L \left(X, \ P^{\mathrm{net}}, \ \lambda \right), \tag{11}$$

where the VPP's aggregated output X and prosumer's net power P_i^{net} are constrained within their feasible regions $\mathcal{X}$: (7a)-(7b) and $\mathcal{Y}_i$: (2)-(5), respectively.

By utilizing the PCPM algorithm, (10) can be solved iteratively at each iteration step k as follows.

Predictor Step: For the given dual variable λ^k, a predictor variable μ^{k+1} is introduced as

$$\mu_{k+1} = \lambda_k + \rho \left[X_k - \sum_{i=1}^{N} \left(P_i^{\mathrm{net}} \right)_k \right], \tag{12}$$

where ρ is the pre-defined step size. The predictor variable μ^{k+1} is then broadcast to all the prosumers.

Primal solution update step: The VPP acts as an agent and solves its own primal problem along with all the prosumers.

For the VPP, update the aggregated output as

$$X_{k+1} = \arg\max_{X \in \mathcal{X}} G^{\mathrm{VPP}}(X) + \mu_{k+1} X - \frac{1}{2\rho} \left\| X - X_k \right\|_2^2, \tag{13}$$

where the added proximal term $\frac{1}{2\rho} \left\| X - X_k \right\|_2^2$ is used to promote the convergence of the algorithm.

For each prosumer i, update the net power as

$$\left(P_i^{\mathrm{net}} \right)_{k+1} = \arg\max_{P_i^{\mathrm{net}} \in \mathcal{Y}_i} \left[\begin{array}{c} -F_i \left(P_i^{\mathrm{net}} \right) - \mu_{k+1} P_i^{\mathrm{net}} \\ -\frac{1}{2\rho} \left\| P_i^{\mathrm{net}} - \left(P_i^{\mathrm{net}} \right)_k \right\|_2^2 \end{array} \right]. \tag{14}$$

Corrector Step: After the primal update, the PCPM corrects the dual variable as

$$\lambda_{k+1} = \lambda_k + \rho \left[X_{k+1} - \sum_{i=1}^{N} \left(P_i^{\mathrm{net}} \right)_{k+1} \right]. \tag{15}$$

The termination condition for PCPM algorithm is $\left\| \mu^{k+1} - \mu^k \right\| \leq \eta$, where η is a given tolerace parameter. The convergence of the PCPM algorithm to solve linearly constrained convex optimization problems has been widely studied [18]. Referred to [18], the global convergence of the PCPM algorithm can be achieved by choosing a step size ρ that satisfies $0 < \rho \leq \frac{1-\xi}{N}$, where $0 < \xi < 1$ is a given scalar. The convergence condition is applicable to the energy management problem (8). Through the distributed optimization framework, the prosumers only need to share their net power P_i^{net} with the VPP for decision-making. In this case, the private information $\mathcal{P}_i$ associated with the prosumer's individual constraints, including the load demand, renewable generation, and BESS operations could be preserved.

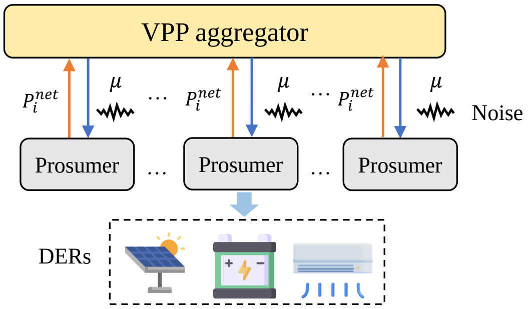

Fig. 3. Schematic of the distributed differentially private optimization method.

B. Distributed Differentially Private Solution Algorithm

The distributed optimization framework provides privacy protection at the individual level. For the communication level of the PCPM algorithm, P_i^{net} of each prosumer i is sent to the VPP, which can also reveal the sensitive information of the prosumer. In this study, we consider the case that the VPP can be trusted since the prosumers have signed contracts with the VPP and transferred the energy management rights to the VPP. The privacy leakage issue is that other prosumers (or an external adversary) may be able to infer the prosumer i's profile through the predictor variable μ broadcast by the VPP. To guarantee the global variable is insensitive to any prosumer's net power, a DP mechanism is integrated into the information exchange process to protect the private information $\mathcal{C}_i$. As illustrated in Fig. 4, noise is added to the predictor variable μ.

In the following, we focus on the differential privacy analysis of the proposed method. Firstly, we present several standard definitions of differential privacy tailored to our problem.

Denote the Database D as the net power of all prosumers, i.e. $D = \{P_i^{\text{net}}\}_{i=1}^{N}$.

Definition 3.1: (Adjacency): Two databases D and $D^{'}$ are adjacent, if and only if there exists an i such that $P_i^{\text{net}} \neq (P_i^{\text{net}})^{'}$ and $P_i^{\text{net}} = \left(P_j^{\text{net}}\right)^{'}$ for all $i \neq j$.

Definition 3.2: (Differential Privacy): Given $\varepsilon,\ \delta > 0$, a mechanism $\mathcal{M}$ is $(\varepsilon,\ \delta)$-differentially private if for every pair of neighboring databases $D,\ D^{'}$, and for every subset of output $\mathcal{S}$, it holds that

$$\Pr\left[\mathcal{M}\left(D\right) \in \mathcal{S}\right] \leq e^{\varepsilon} \Pr\left[\mathcal{M}\left(D^{'}\right) \in \mathcal{S}\right] + \delta, \tag{16}$$

where $\Pr\left[\cdot\right]$ represents the probability.

The objective of differential privacy is to make adjacent databases almost indistinguishable based on the output information. In this study, the mechanism $\mathcal{M}$ is the derivation of the predictor variable $\mu\left(D\right)$ in (12). The difference in the databases (l_2 sensitivity considered in this study) that need to be protected determines the privacy granularity.

Definition 3.3: (l_2-sensitivity) For the function $\mu\left(D\right)$, its l_2-sensitivity under the adjacency databases is defined as

$$\Delta_2\left(\mu\right) = \max_{D,\ D'} \left\|\mu\left(D\right) - \mu\left(D^{'}\right)\right\|_2 = \rho \max_{i \neq j} \left\|P_i^{\text{net}} - P_j^{\text{net}}\right\|_2. \tag{17}$$

Algorithm 1 Distributed Differentially Private Solution Algorithm

```
Initialization: Iteration step $k \leftarrow 0$. Each prosumer $i$ sets its initial power output $(P_i^{\text{net}})_k$. The VPP aggregator sets its initial aggregated output $X_k$, dual variable $\lambda_k$, step size $\rho$, tolerance $\eta$, maximum iteration number $K$.
repeat
    Update the predictor variable : The VPP aggregator updates the predictor variable $\tilde{\mu}_{k+1}$ by
        $\tilde{\mu}_{k+1} = \lambda_k + \rho \left[X_k - \sum_{i=1}^{N} \left(P_i^{\text{net}}\right)_k\right] + \mathcal{N}\left(0,\ \sigma^2\right) \quad (19)$
    The VPP aggregator broadcasts the noised predictor variable $\tilde{\mu}_{k+1}$ to the prosumers.
    Parallel Optimization:
    For the VPP aggregator, update the aggregated output:
        $X_{k+1} = \arg\max_{X \in \mathcal{X}} G^{\text{VPP}}\left(X\right) + \tilde{\mu}_{k+1} X - \frac{1}{2\rho}\left\|X - X_k\right\|_2^2 \quad (20)$
    For each prosumer $i$, update the net power:
        $\left(P_i^{\text{net}}\right)_{k+1} = \arg\max_{P_i^{\text{net}} \in \mathcal{Y}_i} \begin{bmatrix} -F_i\left(P_i^{\text{net}}\right) - \tilde{\mu}_{k+1} P_i^{\text{net}} \\ -\frac{1}{2\rho}\left\|P_i^{\text{net}} - \left(P_i^{\text{net}}\right)_k\right\|_2^2 \end{bmatrix} \quad (21)$
    Update the dual variable: The VPP updates the dual variable through (15).
until $\left\|\mu^{k+1} - \mu^{k}\right\| \leq \eta$ or $k \geq K$ .
Output: VPP's output $X$ and prosumers' net power $P_i^{\text{net}}$
```

A basic tool to realize differential privacy is the Gaussian Mechanism, which adds Gaussian noise to the original mechanism with a scale proportional to the l_2 sensitivity.

Theorem 3.1: Given $\epsilon \geq 0,\ 0 < \delta < \frac{1}{2}$, the Gaussian Mechanism $\mu\left(D\right) + \mathcal{N}\left(0, \sigma^2\right)$ is (ε, δ)-differentially private if

$$\sigma \geq \frac{\Delta_2\left(\mu\right)}{2\varepsilon}\left(M + \sqrt{M^2 + 2\varepsilon}\right), \tag{18}$$

where the random variable $\mathcal{N}\left(0,\ \sigma^2\right)$ represents the added noise. σ is the standard deviation of the random variable. $M = Q^{-1}\left(\delta\right)$ with $Q\left(x\right) = \left(1/\sqrt{2\pi}\right)\int_x^{\infty} e^{\frac{-u^2}{2}} du$ [11].

Theorem 3.1 provides the theoretical guarantee of the privacy level, where the lower bound on the standard deviation of the added noises is derived to guarantee the (ε, δ)-privacy of the broadcast predictor variable. Based on the above principles, the detailed distributed differentially private solution algorithm is presented in Algorithm 1.

Through Theorem 3.1, the noise strength in Algorithm 1 can be designed to guarantee the specified (ε, δ)-privacy of the predictor variable μ at each iteration step k. However, Algorithm 1 requires information exchange in multiple iterations, essentially degrading the privacy-preserving performance. We cite the following result to see how the multiple iterations will affect the privacy guarantee.

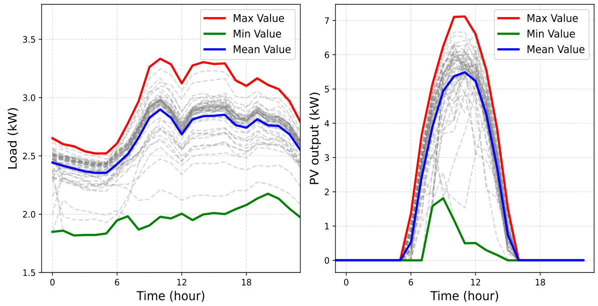

Fig. 4. Prosumers' PV and load profiles.

TABLE I
PARAMETERS FOR ALGORITHM 1

N	λ_0	μ_0	δ	ρ	K	η
50	**0**	**0**	0.05	0.016	100	0.2

Lemma 3.1: (K-fold adaptive composition [10]) A K-fold adaptive composition of (ε, δ) differentially private mechanisms satisfies the $(K\epsilon, K\delta)$-differential privacy.

Using Lamma 3.1, the differential privacy level of the proposed method after K iterations can be derived.

IV. Case Studies

Case studies are conducted in this section to evaluate the performance of the proposed method in terms of privacy and accuracy. We consider a low-voltage distribution scenario where a VPP aggregator manages 50 prosumers. Each prosumer includes a PV system, a thermostatically controlled load (HVAC system, e.g. air-conditioner), and a battery (ESS). The load information of these prosumers is sourced from a low-voltage distribution network of Jiangsu Electrical Power Grid in China. The PV generation profiles are from the NREL Baseline Measurement System [19]. The prosumers' load and PV profiles are shown in Fig. 4. The energy prices of the wholesale electricity market are from the Australian NEM. The local contracted prices are from the Australian retailer. The parameters used for the implementation of Algorithm 1 are shown in Table I, which are determined by the convergence condition of the PCPM algorithm and Theorem 3.1 to guarantee the privacy level.

A. Energy Management Results

The energy management results of problem (8) with the proposed distributed solution algorithm in Section III A are presented in this part. The iteration process of VPP's profit is presented in Fig. 5, where the optimal value obtained by the centralized solution algorithm is provided as the benchmark. It can be seen that through about 60 iterations, the solution converges to the optimal value with an error margin of 2.1%. Through the interaction with prosumers and the electricity market, the VPP finally made a profit of 58.16$.

The energy scheduling results of the individual prosumer are shown in Fig. 6. The prosumer uses the PV, ESS, and HVAC to flexibly manage its net output. Since VPP's energy management is profit-incentive, the ESS's charging and discharging profile is associated with the price of the electricity. For example, from 1:00 a.m. to 4:00 a.m. when the electricity price in the wholesale market is lower than the contracted ToU tariff, the ESS is scheduled to charge power. On the contrary, the ESS is scheduled to discharge and help balance the demand when the price in the wholesale market is higher (from 5:00 a.m. to 6:00 a.m.). At mid-day when the PV generation is sufficient, the prosumer is scheduled to sell the power surplus to the market.

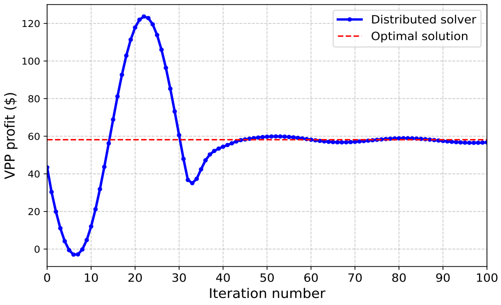

Fig. 5. Convergence of the distributed solver.

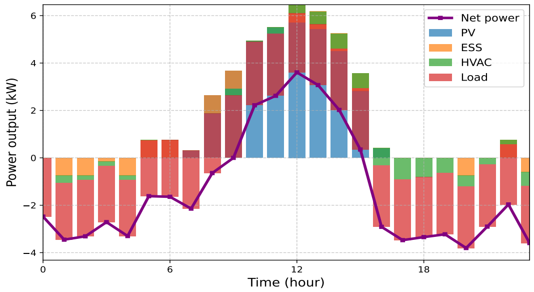

Fig. 6. Prosumer's individual energy scheduling.

For day-ahead scheduling, the maximum available PV output is obtained through day-ahead forecasting. The uncertainty of PV output may cause a real-time imbalance between the prosumer's power output with the scheduled net power. At the individual level, the PV output is considered private information. In this case, the prosumer can reserve some power output from BESS and HVAC for real-time supply-demand balance.

$$P_i^{\text{ESS,min}} + R_{i,t}^{\text{ESS}} \leq P_{i,t}^{\text{ESS}} \leq P_i^{\text{ESS,max}} - R_{i,t}^{\text{ESS}}, \tag{22a}$$

$$P_i^{\text{HVAC,min}} + R_{i,t}^{\text{HVAC}} \leq P_{i,t}^{\text{HVAC}} \leq P_i^{\text{HVAC,max}} - R_{i,t}^{\text{HVAC}}, \tag{22b}$$

$$R_{i,t}^{\text{net}} = R_{i,t}^{\text{ESS}} + R_{i,t}^{\text{HVAC}}, \tag{22c}$$

$$R_{i,t}^{\text{net}} \geq e^{\text{PV}} \cdot P_{i,t}^{\text{PV}}, \tag{22d}$$

where $R_{i,t}^{\text{ESS}}$ and $R_{i,t}^{\text{HVAC}}$ represent the power reserve of BESS and HVAC, respectively. $R_{i,t}^{\text{net}}$ is the power reserve of the prosumer i. e^{PV} is the uncertainty level of PV output.

Take 10% uncertainty of PV's power output as an example, the result of prosumer's scheduling is shown in Fig. 7. In this case, The power reserve $R_{i,t}^{\text{net}}$ will be used to balance the

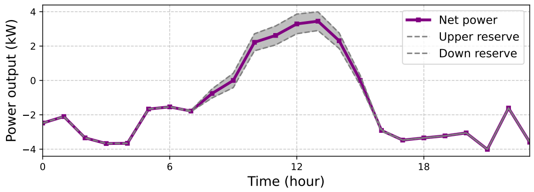

Fig. 7. Prosumer's individual energy scheduling under 10% PV uncertainty.

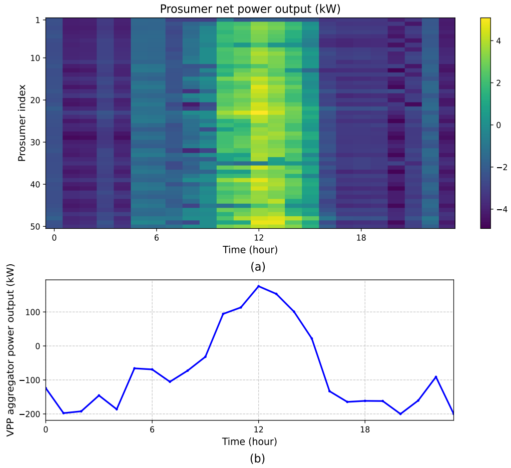

Fig. 8. (a) Prosumers' net power. (b) VPP aggregator's profile.

real-time net power $P_{i,t}^{\text{net}}$ and thus satisfy the scheduled energy trading with the VPP.

All prosumers' net power and the aggregated output of VPP are presented in Fig. 8. It can be seen that the prosumers' net power shows similar profiles. Although the individual load and flexible assets are heterogeneous, the tendency to purchase/sell energy is consistent, which is determined by the VPP.

B. Performance of the Distributed DP Algorithm

The performance of the proposed distributed differentially private algorithm is shown in this part. By adding noise to the predictor variable, the differential privacy of the prosumers can be guaranteed. Given the privacy budget ϵ as $\ln(10)$ with $\delta = 0.05$, the Gaussian noise with standard deviation $\sigma = 0.95\Delta_2(\mu)$ is integrated into the algorithm. Intuitively, the added noise will guarantee the net power of the prosumers indistinguishable as the noise scale is comparable to the worst scenario $\Delta_2(\mu)$. We set the maximum iteration step as 100 and the iteration process is presented in Fig. 9 (a). It can be seen that the noised predictor variable will degrade the convergence and optimality of the solution. The whole iteration process will fluctuate and there will be a gap between the iteration results and the optimal value. At the final iterations, the error with the optimal value will fluctuate with a maximum value of 20$. The VPP's profit in the iteration process is higher than the optimal value because the added noise will enlarge the feasible region of the original problem. Additionally, the global constraints (7a) are violated due to the added noise. From Fig. 9 (b), it can also be seen that at each time interval, there will also be a small-scale gap between the sum of the prosumers' net power and the VPP's aggregated output.

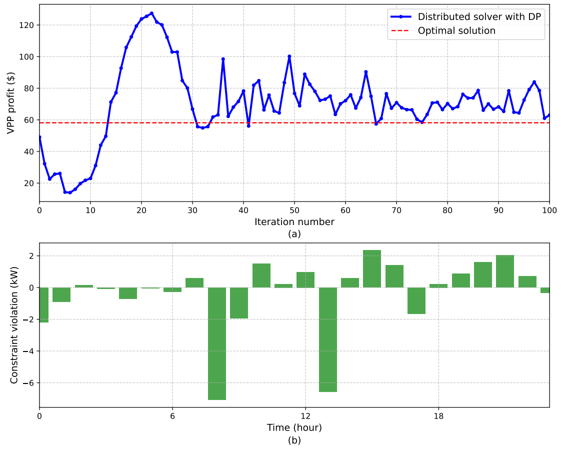

Fig. 9. (a) Iteration process with DP. (b) Global constraint violations at the final iteration step.

To analyze DP's impact on optimality, we use the concept of the optimality gap. Denote the optimal solution of problem $\mathcal{O}$ (the profit of VPP) as $\mathcal{O}(X^*)$. The optimality gap κ represents the difference between the result obtained through the proposed method $\mathcal{O}(X_K)$ and the optimal value as

$$\kappa = \left\| \mathcal{O}(X_K) - \mathcal{O}(X^*) \right\|. \tag{23}$$

The global constraints (7a) are used to guarantee that the purchasing electricity with the electricity market is equal to the aggregated output of the prosumers. Otherwise, there will be penalty costs for the VPP. For the constraint violations caused by DP integration, we introduce the sum of constraint violations χ as

$$\chi = \left\| \sum_{i=1}^{N} \left(P_i^{net} \right)_K - X_K \right\|_2. \tag{24}$$

Based on the definition of optimality gap κ and constraint violation χ, the performance of the proposed method under different privacy levels is evaluated. Several different privacy budgets ϵ ranging from low privacy $\ln 10^4$ ($\sigma = 0.34\Delta_2(\mu)$) to high privacy $\ln 2$ ($\sigma = 2.65\Delta_2(\mu)$) are considered. As the Gaussian noise is a random variable, we conducted 10 case studies under different privacy levels. The results are illustrated in Fig. 10, which presents the mean and standard deviation of the two criteria: 1) the optimality gap and 2) the global constraint violations under different privacy levels. Specifically, the blue bar represents the value of the optimality gap κ (\$), and the green bar represents the global constraint violations χ (kW). We can see that there is a trade-off between privacy and accuracy. With a higher privacy level, the convergence of the proposed method will be even worse. The penalty cost caused by constraint violations also increases with the privacy level. The relative error of the final results under different privacy levels is also shown in Fig. 10. It can be seen that a balance of privacy and accuracy is needed for

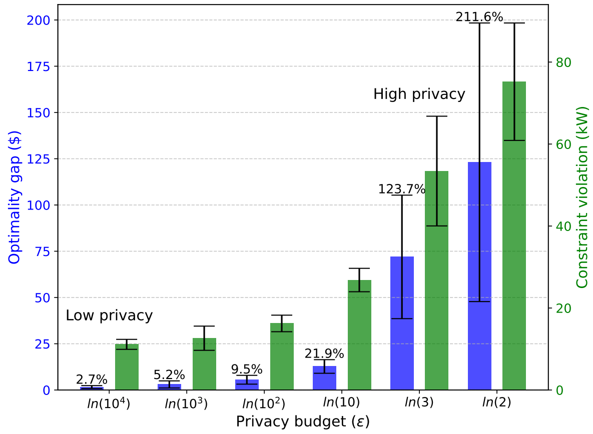

Fig. 10. Optimality gap and constraint violation under different privacy levels.

TABLE II
ECONOMIC LOSS UNDER DIFFERENT PRIVACY LEVELS

ϵ	$\ln 10^4$	$\ln 10^3$	$\ln 10^2$	$\ln 10$	$\ln 3$	$\ln 2$
χ (kW)	11.33	12.27	14.62	28.75	54.82	74.60
C ($)	1.70	1.86	2.26	4.32	8.18	11.07
$C/_{\mathcal{O}(X^*)}$	2.91%	3.21%	3.88%	7.43%	14.06%	19.03%

TABLE III
PERFORMANCE OF THE PROPOSED METHOD WITH DIFFERENT SCALE OF VPP

Number of prosumers	50	200	800
VPP profit ($)	58.16	285.88	1193.70
Terminal iteration	60	360	750
Convergence error of PCPM	1.30%	1.35%	2.78%
Computation time (s)	108.09	1036.14	20185.70
Convergence error with DP	21.9%	8.11%	3.30%
χ with DP (kW)	28.75	34.96	38.20
C with DP ($)	4.32	5.55	6.29
$C/_{\mathcal{O}(X^*)}$ with DP	7.43%	1.94%	0.52%

satisfactory performance of the energy management scheme in the given scenario.

The constraint violation χ represents the deviation between the VPP's power output X and the sum of the prosumer's net power P_i^{net}. There will be a penalty cost from the electricity market for such deviation. To quantitatively evaluate the economic losses caused by the DP, the penalty cost is calculated as follows.

$$C = \sum_{t=1}^{T} \left[r \cdot c_t \cdot \left\| \sum_{i=1}^{N} P_{i,t}^{\text{net}} - X_t \right\| \right]$$
$$s.t.\ c_t = \begin{cases} c_t^{\text{buy}}, & X_t \leq 0, \\ c_t^{\text{sell}}, & X_t > 0, \end{cases} \tag{25}$$

where r is the penalty rate determined by the electricity market. Given the penalty rate $r = 1$, the economic loss under different privacy levels is shown in Table II. From the results, the additional economic loss caused by the integration of DP is evaluated, which helps to determine the acceptable level of differential privacy.

C. Scalability Analysis

The scalability of the proposed method is analyzed in this part for larger-scale VPP with massive prosumers. The results are shown in Table III. With larger numbers of prosumers, more iteration steps are needed for convergence. For the PCPM algorithm, the convergence error with the different number of prosumers is below 3%. Regarding the computation time, the proposed solution algorithm is carried out on Intel (R) Xeon (R) W-3335 CPU @ 3.40GHz and NVIDIA GeForce RTX3080Ti with 188 GB installed RAM. From the results, the day-ahead scheduling of VPP with 800 prosumers will converge within 6 hours. The computation time is impacted by the number of prosumers and iteration steps. It's worth mentioning that in our case, the large-scale primal problems are solved in one CPU, which will limit the computation efficiency. In practical scenarios, the primal problem of each prosumer is carried out in parallel by utilizing the computation resources of the prosumers at the individual level. The primal problem in one iteration step will be completed within 0.26s, indicating highly improved computation efficiency.

For the performance of differential privacy, the privacy budget is chosen as $\varepsilon = \ln 10$ and $\delta = 0.05$. That is, for each iteration, the Gaussian noise with standard deviation $\sigma = 0.95\Delta_2(\mu)$ is added to the update of the predictor variable. From the results, with the increase in the number of prosumers, the convergence error decreases. The reason behind this is that Eq. (17) determines the L_2 sensitivity of μ. $\Delta_2(\mu)$ will decrease since the parameter ρ will decrease to guarantee the convergence of PCPM algorithm, which further degrades the noise level added to the predictor variable μ. However, according to Lemma 3.1, the differential privacy level will be degraded due to the increased iteration number. Besides, the constraint violation χ and penalty cost C are also shown in Table III. Although the constraint violation χ increases with the number of prosumers, the penalty cost will become insignificant compared to the profit of VPP.

V. CONCLUSIONS

This work investigates the optimal energy management strategy for the VPP to achieve its optimal profit while maintaining the privacy of prosumers, where two-level privacy protection of the prosumers is considered. A distributed solution framework with a DP mechanism integrated is proposed to mitigate the privacy leakage risks throughout the solution process. The effectiveness of the proposed method is demonstrated through case studies. The trade-off between privacy and accuracy is presented through optimality and constraint violation analysis. Results show that the proposed method can be applied to the energy management problem of VPP with a balance between privacy and utility.

References

[1] S. Riaz, H. Marzooghi, G. Verbič, A. C. Chapman, and D. J. Hill, “Generic demand model considering the impact of prosumers for future grid scenario analysis,” *IEEE Transactions on Smart Grid*, vol. 10, no. 1, pp. 819–829, 2019.

[2] R. Lyu, S. Ma, J. Yang, H. Wang, S. Ren, J. Ding, and C. Gao, “Construction method of virtual power plant based on optimized aggregation of prosumer resources,” in *2020 4th International Conference on HVDC (HVDC)*, 2020, pp. 388–393.

[3] Z. Yi, Y. Xu, W. Gu, L. Yang, and H. Sun, “Aggregate operation model for numerous small-capacity distributed energy resources considering uncertainty,” *IEEE Transactions on Smart Grid*, vol. 12, no. 5, pp. 4208–4224, 2021.

[4] G. Tsaousoglou, P. Pinson, and N. G. Paterakis, “Transactive energy for flexible prosumers using algorithmic game theory,” *IEEE Transactions on Sustainable Energy*, vol. 12, no. 3, pp. 1571–1581, 2021.

[5] X. Chen, E. Dall’Anese, C. Zhao, and N. Li, “Aggregate power flexibility in unbalanced distribution systems,” *IEEE Transactions on Smart Grid*, vol. 11, no. 1, pp. 258–269, 2020.

[6] Q. Yang, H. Wang, T. Wang, S. Zhang, X. Wu, and H. Wang, “Blockchain-based decentralized energy management platform for residential distributed energy resources in a virtual power plant,” *Applied Energy*, vol. 294, p. 117026, 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S030626192100489X

[7] H. Huang, Z. Li, L. M. I. Sampath, J. Yang, H. D. Nguyen, H. B. Gooi, R. Liang, and D. Gong, “Blockchain-enabled carbon and energy trading for network-constrained coal mines with uncertainties,” *IEEE Transactions on Sustainable Energy*, 2023.

[8] X. Chang, Y. Xu, W. Gu, H. Sun, M.-Y. Chow, and Z. Yi, “Accelerated distributed hybrid stochastic/robust energy management of smart grids,” *IEEE Transactions on Industrial Informatics*, vol. 17, no. 8, pp. 5335–5347, 2021.

[9] X. Cui, Z. Liang, Y. Chai, W. Chen, R. Yu, and G. Ruan, “Privacy-preserving operation of interconnected distribution networks with soft open points,” in *2023 IEEE Power & Energy Society General Meeting (PESGM)*. IEEE, 2023, pp. 1–5.

[10] J. Hsu, Z. Huang, A. Roth, and Z. S. Wu, “Jointly private convex programming,” in *ACM-SIAM Symposium on Discrete Algorithms*, 2014. [Online]. Available: https://api.semanticscholar.org/CorpusID:3905181

[11] Y. Xiao, X. Hou, J. Cai, and J. Hu, “A differentially private distributed solution approach to the model predictive control of building clusters,” in *2018 IEEE Conference on Decision and Control (CDC)*, 2018, pp. 7289–7295.

[12] S. Han, U. Topcu, and G. J. Pappas, “Differentially private distributed constrained optimization,” *IEEE Transactions on Automatic Control*, vol. 62, no. 1, pp. 50–64, 2017.

[13] M. Zellner, T. T. De Rubira, G. Hug, and M. Zeilinger, “Distributed differentially private model predictive control for energy storage,” *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 12 464–12 470, 2017, 20th IFAC World Congress. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2405896317325508

[14] T. Morstyn, N. Farrell, S. J. Darby, and M. D. McCulloch, “Using peer-to-peer energy-trading platforms to incentivize prosumers to form federated power plants,” *Nature energy*, vol. 3, no. 2, pp. 94–101, 2018.

[15] Z. Ren, G. Verbič, and J. Guerrero, “Reward structures for prosumers participating in virtual power plants,” in *2021 IEEE PES Innovative Smart Grid Technologies - Asia (ISGT Asia)*, 2021, pp. 1–5.

[16] N. Li, L. Chen, and S. H. Low, “Optimal demand response based on utility maximization in power networks,” in *2011 IEEE power and energy society general meeting*. IEEE, 2011, pp. 1–8.

[17] X. Chen, E. Dall’Anese, C. Zhao, and N. Li, “Aggregate power flexibility in unbalanced distribution systems,” *IEEE Transactions on Smart Grid*, vol. 11, no. 1, pp. 258–269, 2019.

[18] R. Chen, “On the extensions of the predictor-corrector proximal multiplier (pcpm) algorithm and their applications,” Ph.D. dissertation, Purdue University Graduate School, 2020.

[19] T. Stoffel and A. Andreas, “NREL Solar Radiation Research Laboratory (SRRL): Baseline Measurement System (BMS); Golden, Colorado (Data),” NREL Data Catalog, National Renewable Energy Laboratory, Golden, CO, 2015, Last updated: September 16, 2022.