2023 62nd IEEE Conference on Decision and Control (CDC)
December 13-15, 2023. Marina Bay Sands, Singapore

# On Privacy Preservation of Electric Vehicle Charging Control via State Obfuscation

Xiang Huo† and Mingxi Liu†

***Abstract*— The electric vehicle (EV) industry is rapidly evolving owing to advancements in smart grid technologies and charging control strategies. While EVs are promising in decarbonizing the transportation system and providing grid services, their widespread adoption has led to notable and erratic load injections that can disrupt the normal operation of power grid. Additionally, the unprotected collection and utilization of personal information during the EV charging process cause prevalent privacy issues. To address the scalability and data confidentiality in large-scale EV charging control, we propose a novel decentralized privacy-preserving EV charging control algorithm via state obfuscation that 1) is scalable *w.r.t.* the number of EVs and ensures optimal EV charging solutions; 2) achieves privacy preservation in the presence of honest-but-curious adversaries and eavesdroppers; and 3) is applicable to eliminate privacy concerns for general multi-agent optimization problems in large-scale cyber-physical systems. The EV charging control is structured as a constrained optimization problem with coupled objectives and constraints, then solved in a decentralized fashion. Privacy analyses and simulations demonstrate the efficiency and efficacy of the proposed approach.**

## I. Introduction

The ongoing advancements in electric vehicle (EV) technologies have accelerated the development of a sustainable power grid, owing to the EVs' green credentials and flexible charging options. Despite the multifarious benefits, the occurrence of plug-and-play EV charging events, especially those involving a significant number of EVs, can cause several negative impacts on the power grid, such as load profile fluctuations, voltage deviations, and increased power loss [1]. Therefore, advancing scalable EV charging coordination and control strategies is of paramount importance to alleviate the strain on the power grid and ultimately provide synergistic grid-edge services, such as valley-filling, peak-shaving, and frequency regulation.

In enabling such synergy between EVs and the power grid, the EV charging control problem can be framed as a constrained optimization problem. Let $\boldsymbol{x}_{\hat{\imath}} = [x_{\hat{\imath}}(1), \ldots, x_{\hat{\imath}}(T)]^{\mathsf{T}}$ denote the charging profile of EV $\hat{\imath}$ during $T$ consecutive time slots, $\mathcal{X}_{\hat{\imath}}$ denote the local feasible set that contains the charging requirements of EV $\hat{\imath}$, and function $g(\cdot)$ denote the networked constraint function. Then, the EV charging control problem can be formulated into a constrained optimization problem as

$$\begin{aligned} \min \quad & J(\{\boldsymbol{x}_{\hat{\imath}}\}_{\hat{\imath}=1}^{\hat{n}}) = F\left(\boldsymbol{p}_b, \boldsymbol{x}_1 \ldots, \boldsymbol{x}_{\hat{n}}\right) \\ \text{s.t.} \quad & \boldsymbol{x}_{\hat{\imath}} \in \mathcal{X}_{\hat{\imath}},\ \forall \hat{\imath} = 1, 2, \ldots, \hat{n} \\ & g(\boldsymbol{x}) \leq 0 \end{aligned} \tag{P1}$$

where the cost function $F(\cdot) : \mathbb{R}^T \mapsto \mathbb{R}$ is assumed convex and differentiable, $\boldsymbol{p}_b \in \mathbb{R}^T$ captures the baseline load of the network, $\boldsymbol{x} = [\boldsymbol{x}_{\hat{\imath}}^{\mathsf{T}}, \ldots, \boldsymbol{x}_{\hat{n}}^{\mathsf{T}}]^{\mathsf{T}}$, and $\hat{n}$ denotes the total number of EVs.

The use of scalable optimization methods, such as distributed and decentralized approaches, has gained popularity in solving (**P1**). In [2], a distributed multi-agent EV charging control method was developed based on the Nash certainty equivalence principle to account for network impacts. Gan *et al.* in [3] proposed a decentralized EV charging control algorithm with the objective of addressing the valley-filling problem using EVs' charging loads. To scale with the EV fleet size and the length of control periods, decentralized EV charging protocols were developed in [4] for network-constrained EV charging problems. In [5], a decentralized EV charging control scheme was developed to achieve valley filling, meanwhile accommodating individual charging needs and distribution network constraints. To further improve the scalability, a distributed optimization framework was proposed in [6] to offer two-facet scalability over both the agent population size and network dimension.

Besides scalability, the increased risk of privacy exposure is another major obstacle in deploying large-scale EV charging control strategies. To address the pressing need for privacy preservation in both EV charging control and generic multi-agent systems, one potential solution is using differential privacy (DP). Fiore and Russo in [7] designed a DP-based consensus algorithm for multi-agent systems where a subset of agents are adversaries. In [8], a distributed functional perturbation framework was developed based on DP to protect each agent's private objective function. In [9], DP-based distributed algorithms were designed to preserve privacy in finding the Nash equilibrium of stochastic aggregative games. Although DP-based methods are commonly adopted for privacy preservation, the inevitable trade-off between accuracy and privacy remains a major challenge in practical implementation.

Another frequently utilized method for preserving privacy involves cryptographic techniques, such as the Paillier cryptosystem and Shamir's secret sharing (SSS). In [10], a Paillier-based privacy-preserving algorithm was proposed for securing the average consensus of networked systems

†X. Huo and M. Liu are with the Department of Electrical and Computer Engineering at the University of Utah, 50 S Central Campus Drive, Salt Lake City, UT, 84112, USA {xiang.huo, mingxi.liu}@utah.edu.

This work is supported by NSF Award: ECCS-2145408.

2023 62nd IEEE Conference on Decision and Control (CDC) | 979-8-3503-0124-3/23/$31.00 ©2023 IEEE | DOI: 10.1109/CDC49753.2023.10383455

with high-order dynamics. Zhang *et al.* in [11] developed a privacy-preserving power exchange service system that uses data encryption to protect EV users' privacy. In [12], a decentralized privacy-preserving multi-agent cooperative optimization paradigm was designed based on cryptography for large-scale industrial cyber-physical systems. In [13], a novel decentralized privacy preservation approach was designed by integrating a partially homomorphic cryptosystem into the decentralized optimization architecture. Compared to encryption-based methods that rely on large integer calculations, SSS-based privacy-preserving approaches are more efficient in the computation of shares while offering information-theoretical security [14]. In [15], an SSS-based privacy-preserving algorithm was developed to solve the consensus problem while concurrently protecting each individual's private information. Rottondi *et al.* in [16] designed a privacy-preserving vehicle-to-grid architecture based on SSS to ensure the confidentiality of the private information of EV owners from aggregators. Huo and Liu in [17] proposed an SSS-based privacy-preserving EV charging control protocol, which eliminates the need for a system operator (SO) in achieving overnight valley filling. While cryptographic methods effectively achieve high levels of accuracy and privacy, the accompanying increased computation and communication complexity become the bottleneck in their practical use. Non-cryptographic approaches like state decomposition (SD) decompose the true state into two sub-states, and only one sub-state is visible to others, therefore protecting the true value of the original state. However, state-of-the-art SD-based strategies are not applicable to solve (**P1**) as they mainly focus on consensus problems [18], [19].

This paper aims to design a decentralized privacy-preserving optimization algorithm, which is scalable and low in complexity, suitable for large-scale multi-agent optimization, specifically for EV charging control. The contributions of this paper are three-fold: 1) the proposed decentralized privacy-preserving algorithm can scale with the number of EVs and provide optimal decentralized EV charging solutions; 2) privacy preservation is achieved in the presence of honest-but-curious adversaries and external eavesdroppers; and 3) the proposed approach has low computing and communication overhead, making it widely applicable for preserving privacy in coupled multi-agent optimization problems in cyber-physical systems.

## II. Problem Formulation

### A. Distribution Network Model

In a radial distribution network, the power flow can be represented by DistFlow branch equations that consist of the real power, reactive power, and voltage magnitude [20]. Consider a re-indexed radial distribution network and define $\mathbb{N} = \{i \mid i = 1, \dots, n\}$ as the set of downstream buses. Let $|V_i(t)|$ denote the voltage magnitude of bus $i$ at time $t$, $|V_0|$ denote the voltage magnitude of the slack bus, and $p_i(t)$ and $q_i(t)$ denote the active and reactive loads of bus $i$ at time $t$.

Following the linear DistFlow branch equations [20], the squared voltage magnitude at node $i$ is

$$\boldsymbol{V}_i = \boldsymbol{V}_0 - 2\sum_{j=1}^{n} \boldsymbol{R}_{ij}\boldsymbol{p}_j - 2\sum_{j=1}^{n} \boldsymbol{X}_{ij}\boldsymbol{q}_j \tag{1}$$

where $\boldsymbol{V}_i = [|V_i(1)|^2, \dots, |V_i(T)|^2]^\mathsf{T} \in \mathbb{R}^T$, $\boldsymbol{V}_0 = [|V_0|^2, \dots, |V_0|^2]^\mathsf{T} \in \mathbb{R}^T$, $\boldsymbol{p}_i = [p_i(1), \dots, p_i(T)]^\mathsf{T} \in \mathbb{R}^T$, $\boldsymbol{q}_i = [q_i(1), \dots, q_i(T)]^\mathsf{T} \in \mathbb{R}^T$, and the adjacency matrices $\boldsymbol{R}$ and $\boldsymbol{X}$ are defined as

$$\boldsymbol{R} \in \mathbb{R}^{n\times n},\ \boldsymbol{R}_{ij} = \sum_{(\hat{\imath},\hat{\jmath})\in\mathbb{E}_i\cap\mathbb{E}_j} r_{\hat{\imath}\hat{\jmath}}$$
$$\boldsymbol{X} \in \mathbb{R}^{n\times n},\ \boldsymbol{X}_{ij} = \sum_{(\hat{\imath},\hat{\jmath})\in\mathbb{E}_i\cap\mathbb{E}_j} x_{\hat{\imath}\hat{\jmath}}$$

where $r_{\hat{\imath}\hat{\jmath}}$ and $x_{\hat{\imath}\hat{\jmath}}$ denote the resistance and reactance from bus $\hat{\imath}$ to bus $\hat{\jmath}$, respectively. The sets of line segments that connect the slack bus to bus $i$ and bus $j$ are denoted by $\mathbb{E}_i$ and $\mathbb{E}_j$, respectively. In this paper, we focus on the charging control of plug-in EVs on radial distribution networks. A 13-bus distribution network with charging stations situated at different nodes is shown in Fig. 1.

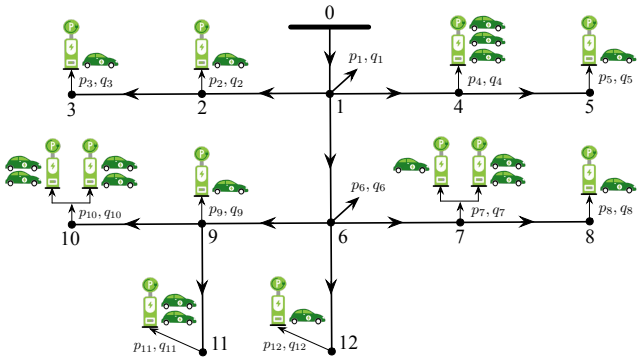


Fig. 1: A 13-bus distribution network connected with EVs.

### B. EV Charging Model

Let $\boldsymbol{r}_{\hat{\imath}} \in \mathbb{R}^T$ denote the piece-wise constant charging power of the $\hat{\imath}$th EV during $T$ time intervals, and $\boldsymbol{r}_{\hat{\imath}}$ is constrained by

$$\boldsymbol{0} \le \boldsymbol{r}_{\hat{\imath}} \le \overline{\boldsymbol{r}}_{\hat{\imath}} \tag{2}$$

where $\overline{\boldsymbol{r}}_{\hat{\imath}} = [\overline{r}_{\hat{\imath}}, \dots, \overline{r}_{\hat{\imath}}]^\mathsf{T} \in \mathbb{R}^T$ and $\overline{r}_{\hat{\imath}}$ denotes the maximum charging power.

Let $\delta_t$ denote the sampling period and $[1 : T\delta_t]$ denote the charging duration. To ensure EVs are charged to the desired energy levels by the end of the charging period, the total energy charged for the $\hat{\imath}$th EV should satisfy

$$\boldsymbol{G}\boldsymbol{r}_{\hat{\imath}} = d_{\hat{\imath}} \tag{3}$$

where $\boldsymbol{G}{=}[\delta_t\eta, \dots, \delta_t\eta]{\in}\mathbb{R}^{1\times T}$ denotes the aggregation vector, $\eta$ denotes the charging efficiency, and $d_{\hat{\imath}}$ denotes the charging demand request of the $\hat{\imath}$th EV.

### C. Valley-Filling Optimization Problem

The valley-filling problem aims at filling the aggregated load valley and smoothing the aggregated load profile of the entire distribution network. This service is typically provisioned during the late evening and early morning when significant energy use reduction occurs. In this paper, the controllable charging loads of EVs, e.g., from community overnight parking and charging lot, are scheduled and shifted to flatten the valley in the power load profile. To this end, the valley-filling problem is formulated as a constrained optimization problem at the grid scale aiming at determining the optimal charging schedules of all EVs.

Suppose in total $\hat{n}$ EVs need to be fully charged during the time period $[1 : T\delta_t]$. This paper takes the nodal voltage constraint, which manifests as the global constraint, for example, to illustrate the impacts of EV charging on the distribution network as

$$\underline{\boldsymbol{V}} \le \boldsymbol{V}_i \le \overline{\boldsymbol{V}},\ \forall i = 1, 2, \ldots, n \tag{4}$$

where $\underline{\boldsymbol{V}}=[\underline{V}, \ldots, \underline{V}]^\mathsf{T}\in\mathbb{R}^T$, $\overline{\boldsymbol{V}}=[\overline{V}, \ldots, \overline{V}]^\mathsf{T}\in\mathbb{R}^T$, $\underline{V}$ and $\overline{V}$ denote the lower and upper voltage bounds, respectively.

The optimal EV charging control problem is then formulated into a quadratic programming problem as

$$\begin{aligned} \min \quad & J(\{\boldsymbol{r}_{\hat{i}}\}_{\hat{i}=1}^{\hat{n}}) = \frac{1}{2}\left\|\boldsymbol{p}_b + \sum_{\hat{i}=1}^{\hat{n}} \boldsymbol{r}_{\hat{i}}\right\|_2^2 \\ \text{s.t.} \quad & \boldsymbol{r}_{\hat{i}} \in \mathcal{R}_{\hat{i}},\ \forall \hat{i} = 1, 2, \ldots, \hat{n} \\ & \underline{\boldsymbol{V}} \le \boldsymbol{V}_i \le \overline{\boldsymbol{V}},\ \forall i = 1, 2, \ldots, n \end{aligned} \tag{P2}$$

where $\boldsymbol{p}_b$ denotes the aggregated baseline load and $\mathcal{R}_{\hat{i}}$ denotes the local feasible set of EV $\hat{i}$ that is defined by

$$\mathcal{R}_{\hat{i}} = \{\boldsymbol{r}_{\hat{i}} |\ 0 \le \boldsymbol{r}_{\hat{i}} \le \overline{\boldsymbol{r}}_{\hat{i}}, \boldsymbol{G}\boldsymbol{r}_{\hat{i}} = d_{\hat{i}}\}. \tag{5}$$

Note that (2) and (3) are basic constraints that describe the EV charging process, additional constraints that introduce EVs' local characteristics can be included in the feasible set $\mathcal{R}_{\hat{i}}$ without affecting the algorithm design.

## III. Main Results

### A. Decentralized PGM

To solve the constrained optimization problem in (**P2**) via a decentralized manner, EVs (agents) can work cooperatively by adopting the projected gradient method (PGM) [21]. In PGM, the $\hat{i}$th EV can update its decision variable (primal variable) by

$$\boldsymbol{r}_{\hat{i}}^{(\ell+1)} = \Pi_{\mathcal{R}_{\hat{i}}}[\boldsymbol{r}_{\hat{i}}^{(\ell)} - \gamma_{\hat{i}}^{(\ell)}\Phi_{\hat{i}}^{(\ell)}(\boldsymbol{r}^{(\ell)})] \tag{6}$$

where $\ell$ denotes the iteration index, $\boldsymbol{r}^{(\ell)} = [{\boldsymbol{r}_1^{(\ell)}}^\mathsf{T}, \ldots, {\boldsymbol{r}_{\hat{n}}^{(\ell)}}^\mathsf{T}]^\mathsf{T}$, $\gamma_{\hat{i}}^{(\ell)}$ denotes the primal update step size of EV $\hat{i}$, $\Phi_{\hat{i}}^{(\ell)}(\cdot)$ denotes the first-order gradient of the Lagrangian function *w.r.t.* $\boldsymbol{r}_{\hat{i}}^{(\ell)}$, and $\Pi_{\mathcal{R}_{\hat{i}}}[\cdot]$ denotes the Euclidean projection operation onto $\mathcal{R}_{\hat{i}}$.

The relaxed Lagrangian of (**P2**) can be derived as

$$\mathcal{L}(\boldsymbol{r}, \boldsymbol{\lambda}) = \frac{1}{2}\left\|\boldsymbol{p}_b + \sum_{\hat{i}=1}^{\hat{n}} \boldsymbol{r}_{\hat{i}}\right\|_2^2 + \sum_{i=1}^{n} \boldsymbol{\lambda}_i^\mathsf{T}(\underline{\boldsymbol{V}} - \boldsymbol{V}_i) \tag{7}$$

where $\boldsymbol{\lambda} = [\boldsymbol{\lambda}_1^\mathsf{T}, \ldots, \boldsymbol{\lambda}_n^\mathsf{T}]^\mathsf{T}$ and $\boldsymbol{\lambda}_i$ denotes the dual variable associated with the $i$th inequality constraint. Note that the Lagrangian in (7) is relaxed by moving EVs' local constraints into $\mathcal{R}_{\hat{i}}$. Only the lower bound constraint on the bus voltage magnitudes is considered, as the charging loads of EVs are the only active power consumption within the distribution network.

The subgradients of $\mathcal{L}(\boldsymbol{r}, \boldsymbol{\lambda})$ *w.r.t.* $\boldsymbol{r}_{\hat{i}}$ and $\boldsymbol{\lambda}_i$ are

$$\nabla_{\boldsymbol{r}_{\hat{i}}}\mathcal{L}(\boldsymbol{r}, \boldsymbol{\lambda}) = \boldsymbol{p}_b + \sum_{\hat{i}=1}^{\hat{n}} \boldsymbol{r}_{\hat{i}} - \sum_{i=1}^{n} \nabla_{\boldsymbol{r}_{\hat{i}}}(\boldsymbol{\lambda}_i^\mathsf{T}\boldsymbol{V}_i) \tag{8a}$$

$$\nabla_{\boldsymbol{\lambda}_i}\mathcal{L}(\boldsymbol{r}, \boldsymbol{\lambda}) = \underline{\boldsymbol{V}} - \boldsymbol{V}_i. \tag{8b}$$

Substitute the linear DistFlow branch equation (1) into (8), we have

$$\nabla_{\boldsymbol{r}_{\hat{i}}}\mathcal{L}(\boldsymbol{r}, \boldsymbol{\lambda}) = \boldsymbol{p}_b + \sum_{i=1}^{n} \boldsymbol{p}_i - \hat{\boldsymbol{s}}_{\hat{i}} \tag{9a}$$

$$\nabla_{\boldsymbol{\lambda}_i}\mathcal{L}(\boldsymbol{r}, \boldsymbol{\lambda}) = \tilde{\boldsymbol{V}} + 2\sum_{j=1}^{n} \boldsymbol{R}_{ij}\boldsymbol{p}_j \tag{9b}$$

where $\hat{\boldsymbol{s}}_{\hat{i}} = \sum_{i=1}^{n} \nabla_{\boldsymbol{r}_{\hat{i}}}(\boldsymbol{\lambda}_i^\mathsf{T}\boldsymbol{V}_i)$, $\tilde{\boldsymbol{V}} = \underline{\boldsymbol{V}} - \boldsymbol{V}_0$, $\boldsymbol{p}_i = \sum_{\hat{i}=1}^{\hat{n}_i} \boldsymbol{r}_{\hat{i}}$, and $\hat{n}_i$ denotes the number of EVs connected at bus $i$. Note that the exact form of $\hat{\boldsymbol{s}}_{\hat{i}}$ is decided based on the bus location of the $\hat{i}$th EV, e.g., if the $\hat{i}$th EV is connected at bus $k$, then $\hat{\boldsymbol{s}}_{\hat{i}} = 2\sum_{i=1}^{n} \boldsymbol{R}_{ik}\boldsymbol{\lambda}_i$.

Based on the subgradients in (9), the primal and dual variables can be updated through the PGM by

$$\boldsymbol{r}_{\hat{i}}^{(\ell+1)} = \Pi_{\mathcal{R}_{\hat{i}}}\left(\boldsymbol{r}_{\hat{i}}^{(\ell)} - \gamma_{\hat{i}}\nabla_{\boldsymbol{r}_{\hat{i}}}\mathcal{L}\left(\boldsymbol{r}^{(\ell)}, \boldsymbol{\lambda}^{(\ell)}\right)\right) \tag{10a}$$

$$\boldsymbol{\lambda}_i^{(\ell+1)} = \Pi_{\mathcal{D}_i}\left(\boldsymbol{\lambda}_i^{(\ell)} + \beta_i\nabla_{\boldsymbol{\lambda}_i}\mathcal{L}\left(\boldsymbol{r}^{(\ell)}, \boldsymbol{\lambda}^{(\ell)}\right)\right) \tag{10b}$$

where $\mathcal{D}_i = \{\boldsymbol{\lambda}_i \mid \boldsymbol{\lambda}_i \ge \boldsymbol{0}\}$ denotes the feasible set of $\boldsymbol{\lambda}_i$ and $\beta_i$ denotes the associated dual update step size.

The PGM update in (10) is scalable *w.r.t.* the number of EVs owing to the parallel computing structure. However, due to the couplings of decision variables in both the objective function and the global voltage constraint, the primal and dual updates require the exchange of decision variables between all EVs, e.g., calculating the subgradient in (9a) requires $\boldsymbol{r}_{\hat{i}}$'s from all EVs. Therefore, without appropriate privacy preservation measures, the inevitable and frequent information exchange can put EVs' private data at breaching risks. To address this concern, we aim to develop a privacy-preserving EV charging control framework via state obfuscation to protect EVs' true decision variables.

### B. Privacy-Preserving EV Charging Control Via State Obfuscation

The goal of privacy preservation is to ensure EV owners' private information is protected during the charging schedules. Specifically, private data of the $\hat{i}$th EV are defined to include the charging profiles $\boldsymbol{r}_{\hat{i}}^{(\ell)}$ in all iterations, charging demand $d_{\hat{i}}$, and the maximum charging power $\overline{\boldsymbol{r}}_{\hat{i}}$. The primal update in (10a) naturally inherits local privacy preservation owing to the independent projection operation $\Pi_{\mathcal{R}_{\hat{i}}}$. This is because the private data such as the charging demand $d_{\hat{i}}$ and

the maximum charging power $\overline{\boldsymbol{r}}_{\hat{\imath}}$ are exclusive to the $\hat{\imath}$th EV and only contained in the feasible set $\mathcal{R}_{\hat{\imath}}$ for implementing the primal update. Therefore, the local private information is securely retained within $\mathcal{R}_{\hat{\imath}}$ and will not be disclosed to other parties.

Despite the scalability of decentralized EV charging architectures, they require frequent exchange of EVs' charging profiles through communication channels between EVs and the SO, making the entire system prone to privacy leakages. To resolve this issue, we propose a state-obfuscation-based algorithm that can protect EVs' charging profiles during any planned charging window. The basic concept behind state obfuscation is to obfuscate EVs' true decision variables by using the values of random variables drawn from a probability distribution. Regarding a set of mutually independent random variables, e.g., drawn from a normal distribution, we have the following theorem

**Theorem 1** [22]: If $X_1, \ldots, X_z$ are mutually independent normal random variables with means $\mu_1, \ldots, \mu_z$ and variances $\sigma_1^2, \ldots, \sigma_z^2$, then the linear combination $Y = \sum_{i=1}^{z} c_i X_i$ follows the normal distribution $\mathcal{N}(\sum_{i=1}^{z} c_i \mu_i, \sum_{i=1}^{z} c_i^2 \sigma_i^2)$. ■

To integrate state obfuscation into EV charging control, we propose a novel communicating architecture, as shown in Fig. 2, for the privacy-preserving algorithm implementation. The EVs in the distribution network layer first send

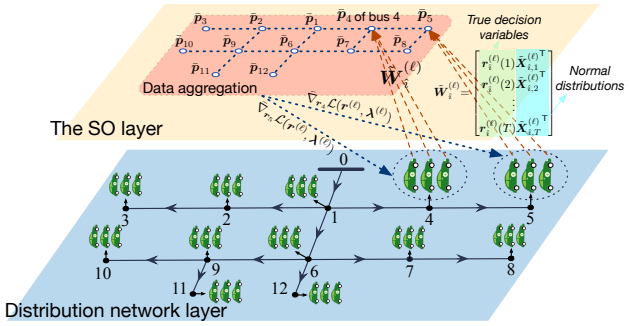


Fig. 2: Communicating structure of the proposed privacy-preserving algorithm (the communications of the EVs connected at buses 4 and 5 are given).

the obfuscated charging profiles to the SO, the SO then aggregates the obfuscated data bus by bus according to EVs' bus locations. Specifically, suppose the $\hat{\imath}$th EV is connected at bus $i$. At the $\ell$th iteration, the $\hat{\imath}$th EV uses a random normal variable $X_{\hat{\imath}} \sim \mathcal{N}(\mu_i, \sigma_i^2)$ to generate $T$ random sets $\tilde{X}_{\hat{\imath},t}^{(\ell)} = \{e_{\hat{\imath},t,1}^{(\ell)}, \ldots, e_{\hat{\imath},t,m}^{(\ell)}\}$, $\forall t = 1, \ldots, T$ where each set contains $m$ random elements. For clarity, we represent $\tilde{X}_{\hat{\imath},t}^{(\ell)}$ by a vector as $\tilde{\boldsymbol{X}}_{\hat{\imath},t}^{(\ell)} = [e_{\hat{\imath},t,1}^{(\ell)}, \ldots, e_{\hat{\imath},t,m}^{(\ell)}]^{\mathsf{T}}$.

The $\hat{\imath}$th EV then extracts each element from its decision variable $\boldsymbol{r}_{\hat{\imath}}^{(\ell)}$ to calculate $\boldsymbol{r}_{\hat{\imath}}^{(\ell)}(t)\tilde{\boldsymbol{X}}_{\hat{\imath},t}^{(\ell)}$, $\forall t = 1, \ldots, T$. Consequently, the $\hat{\imath}$th EV can obtain a total of $T$ new vectors and reformulate them into $\tilde{\boldsymbol{W}}_{\hat{\imath}}^{(\ell)}$, defined by

$$\tilde{\boldsymbol{W}}_{\hat{\imath}}^{(\ell)} = [\boldsymbol{r}_{\hat{\imath}}^{(\ell)}(1)\tilde{\boldsymbol{X}}_{\hat{\imath},1}^{(\ell)\mathsf{T}}, \ldots, \boldsymbol{r}_{\hat{\imath}}^{(\ell)}(T)\tilde{\boldsymbol{X}}_{\hat{\imath},T}^{(\ell)\mathsf{T}}]^{\mathsf{T}}. \tag{11}$$

Subsequently, instead of sending the true decision variables directly, all EVs send their $\tilde{\boldsymbol{W}}_{\hat{\imath}}^{(\ell)}$'s, i.e., the obfuscated states, to the SO. Then the SO computes the sum of the received obfuscated states using

$$\boldsymbol{Y}_i^{(\ell)} = \sum_{\hat{\imath}=1}^{\hat{n}_i} \tilde{\boldsymbol{W}}_{\hat{\imath}}^{(\ell)} \tag{12}$$

for the EVs connected at the $i$th bus.

As shown in (11), every element in $\boldsymbol{r}_{\hat{\imath}}^{(\ell)}$ is obfuscated and expanded by $m$ random values. To retrieve the summed charging profiles for all EVs connected at bus $i$, the SO needs to calculate the mean of every $m$ elements in $\boldsymbol{Y}_i^{(\ell)}$. For example, for the first $m$ elements, the SO calculates $(\sum_{\kappa=1}^{m} \boldsymbol{Y}_i^{(\ell)}(\kappa))/m$ that is equal to $\sum_{\hat{\imath}=1}^{\hat{n}_i} \boldsymbol{r}_{\hat{\imath}}^{(\ell)}(1)\bar{\mu}_i$ where $\bar{\mu}_i$ is an approximation of $\mu_i$. Suppose the SO knows the true mean $\mu_i$, the SO can acquire $\sum_{\hat{\imath}=1}^{\hat{n}_i} \boldsymbol{r}_{\hat{\imath}}^{(\ell)}\bar{\mu}_i$, and further obtain $\tau \sum_{\hat{\imath}=1}^{\hat{n}_i} \boldsymbol{r}_{\hat{\imath}}^{(\ell)}$ where $\tau = \bar{\mu}_i/\mu_i$ denotes the approximation error. Therefore, the SO now has the approximated active power consumption $\bar{\boldsymbol{p}}_i^{(\ell)} = \tau \sum_{\hat{\imath}=1}^{\hat{n}_i} \boldsymbol{r}_{\hat{\imath}}^{(\ell)}$ of bus $i$, and it repeats the procedure to obtain $\bar{\boldsymbol{p}}_i^{(\ell)}$, $\forall i = 1, \ldots, n$.

Finally, the SO estimates the subgradients in (9) using the approximated active power consumption, then broadcasts (9a) to the $i$th EV while utilizing (9b) to conduct dual updates. Thereafter, EV $i$ can update its decision variable $\boldsymbol{r}_{\hat{\imath}}^{(\ell)}$ in parallel using (10a).

The step-by-step process of the proposed approach is outlined in **Algorithm 1**.

**Algorithm 1** Decentralized privacy-preserving EV charging control via state obfuscation

1: EVs initialize decision variables, tolerance $\epsilon_0$, iteration counter $\ell = 0$, and maximum iteration $\ell_{max}$.
2: **while** $\epsilon_{\hat{\imath}}^{(\ell)} > \epsilon_0$ and $\ell < \ell_{max}$ **do**
3: The $\hat{\imath}$th EV connected at bus $i$ generates a normal random variable $X_{\hat{\imath}} \sim \mathcal{N}(\mu_i, \sigma_i^2)$ and draws random elements from $X_{\hat{\imath}}$ to obtain $\tilde{\boldsymbol{X}}_{\hat{\imath},t}^{(\ell)} = [e_{\hat{\imath},t,1}^{(\ell)}, \ldots, e_{\hat{\imath},t,m}^{(\ell)}]^{\mathsf{T}}$, $\forall t = 1, \ldots, T$.
4: The $\hat{\imath}$th EV uses the elements of $\boldsymbol{r}_{\hat{\imath}}^{(\ell)}$ to calculate $\boldsymbol{r}_{\hat{\imath}}^{(\ell)}(t)\tilde{\boldsymbol{X}}_{\hat{\imath},t}^{(\ell)}$, $\forall t = 1, \ldots, T$ elementwisely. Then each EV formulates $\tilde{\boldsymbol{W}}_{\hat{\imath}}^{(\ell)}$ and sends it to the SO.
5: The SO calculates the summation $\boldsymbol{Y}_i^{(\ell)}$ using (12) for each bus, then calculates the mean of every $m$ elements in $\boldsymbol{Y}_i^{(\ell)}$, to obtain the approximated $\bar{\boldsymbol{p}}_i^{(\ell)}$, $\forall i = 1, \ldots, n$.
6: The SO estimates the subgradient in (9a) and broadcasts it to the $\hat{\imath}$th EV.
7: The $\hat{\imath}$th EV updates $\boldsymbol{r}_{\hat{\imath}}^{(\ell)} \to \boldsymbol{r}_{\hat{\imath}}^{(\ell+1)}$ by PGM using (10a), then calculates the error $\epsilon_{\hat{\imath}}^{(\ell)}$.
8: The SO updates the dual variables $\boldsymbol{\lambda}_i^{(\ell)} \to \boldsymbol{\lambda}_i^{(\ell+1)}$, $\forall i = 1, \ldots, n$ using (10b).
9: $\ell = \ell + 1$.
10: **end while**

**Theorem 2**: **Algorithm 1** has an accuracy level of $\tau$. With appropriate choices of $\sigma$ and $m$, the convergence of primal and dual variables is guaranteed. ■

**Theorem 2** states the correctness and convergence of the proposed algorithm. By carrying out **Algorithm 1**, the subgradients in (9) can be efficiently approximated and calculated since the mean of $\boldsymbol{Y}_i^{(\ell)}$ can be used to retrieve $\bar{\boldsymbol{p}}_i^{(\ell)}$ that is an estimation of $\boldsymbol{p}_i^{(\ell)}$. When determining the accuracy level, the standard error of the mean (SEM), defined by $SEM_m = \sigma/\sqrt{m}$, can quantify how a larger sample size produces more precise estimates of the means.

**Remark 1 :** Without the loss of generality, $\mu_i$ was set uniformly across all EVs connected at the same bus to avoid over-complicated algorithm implementation. In a broader scenario, the mean values of different EVs can be chosen independently. In other words, the mean value $\mu_{\hat{\imath}}$ serves as a unique key between the $\hat{\imath}$th EV and the SO. □

## IV. Privacy Analysis

### A. Privacy and Attack Models

To preserve EV owner's privacy, two types of adversaries are considered: 1) An *honest-but-curious adversary* is an agent who adheres to the algorithm but intends to utilize the accessible data to infer private information of other participants, and 2) an *external eavesdropper* is an external attacker who wiretaps communication links to obtain the private information of the participants.

### B. Privacy Analysis

**Algorithm 1** allows EVs to use the values of random variables drawn from a normal distribution to protect the true decision variables $\boldsymbol{r}_{\hat{\imath}}^{(\ell)}$'s. The privacy preservation properties of **Algorithm 1** are given by the following theorem

**Theorem 3**: **Algorithm 1** preserves the private data of EV owners against both honest-but-curious adversaries and external eavesdroppers. ■

*Proof*: Proof of **Theorem 3** is approached from the adversaries' perspective based on the data they can access. From the view of an honest-but-curious adversary, suppose both EV $\hat{\imath}_1$ and EV $\hat{\imath}_2$ are connected at the same bus, and EV $\hat{\imath}_1$ is curious in inferring the charging profiles of EV $\hat{\imath}_2$. At the $\ell$th iteration, EV $\hat{\imath}_1$ can have access to the data set $\mathcal{A}_{\hat{\imath}_1}^{(\ell)} = \{\boldsymbol{r}_{\hat{\imath}_1}^{(\ell)}, \overline{\boldsymbol{r}}_{\hat{\imath}_1}, d_{\hat{\imath}_1}, \mathcal{R}_{\hat{\imath}_1}, \gamma_{\hat{\imath}}, \bar{\nabla}_{\boldsymbol{r}_{\hat{\imath}_1}} \mathcal{L}(\boldsymbol{r}^{(\ell)}, \boldsymbol{\lambda}^{(\ell)})\}$ where $\overline{\boldsymbol{r}}_{\hat{\imath}_1}$, $d_{\hat{\imath}_1}$, $\mathcal{R}_{\hat{\imath}_1}$, and $\gamma_{\hat{\imath}}$ are private information of EV $\hat{\imath}_{i_1}$ and kept to EV $\hat{\imath}_1$ locally. The local information, therefore, cannot provide any useful information in inferring $\boldsymbol{r}_{\hat{\imath}_2}^{(\ell)}$. Besides, EV $\hat{\imath}_1$ also has access to the approximated subgradient $\bar{\nabla}_{\boldsymbol{r}_{\hat{\imath}_1}} \mathcal{L}(\boldsymbol{r}^{(\ell)}, \boldsymbol{\lambda}^{(\ell)})$ that is calculated by the SO. However, the baseline load $\boldsymbol{p}_b$ and the adjacency matrix $\boldsymbol{R}$ are held by the SO, and therefore remain invisible to any EVs. Therefore, EV $\hat{\imath}_1$ cannot infer the charging profiles $\boldsymbol{r}_{\hat{\imath}_2}$ of EV $\hat{\imath}_2$ based on its accessible information contained in $\mathcal{A}_{\hat{\imath}_1}^{(\ell)}$.

For any external eavesdropper, by wiretapping the communication channels at the $\ell$th iteration, it can obtain the information set $\mathcal{E} = \{\tilde{\boldsymbol{W}}_{\hat{\imath}}^{(\ell)}, \bar{\nabla}_{\boldsymbol{r}_{\hat{\imath}}} \mathcal{L}(\boldsymbol{r}^{(\ell)}, \boldsymbol{\lambda}^{(\ell)}), \forall \hat{\imath} = 1, \ldots, \hat{n}\}$. Suppose an external eavesdropper knows the protocols of **Algorithm 1**. To infer $\boldsymbol{r}_{\hat{\imath}}^{(\ell)}$ by using $\mathcal{E}$, it still needs to know the cardinality $m$ and the mean value $\mu_i$ that is associated with the random variable $X_{\hat{\imath}}$. Though the approximated subgradient $\bar{\nabla}_{\boldsymbol{r}_{\hat{\imath}}} \mathcal{L}(\boldsymbol{r}^{(\ell)}, \boldsymbol{\lambda}^{(\ell)})$ could potentially reveal the converging direction of the decision variable, the eavesdropper is still blind from $\gamma_{\hat{\imath}}$ and $\mathcal{R}_{\hat{\imath}}$, therefore unable to imitate the primal update in (10a). □

**Remark 2:** A trade-off between the level of security and computing cost exists in **Algorithm 1**. When a specific accuracy requirement is decided by $\tau$ under a fixed sample size $m$, a smaller variance $\sigma_i^2$ will result in a smaller SEM and therefore require fewer data points to achieve the accuracy standard. The proposed state obfuscation refines $k$-anonymity [23] by introducing randomization of $m$ anonymous random variables for each true value. Though a smaller variance would result in less computation and communication cost, it can also lead to a higher degree of similarity in $\tilde{\boldsymbol{X}}_{\hat{\imath},t}^{(\ell)}$, thus compromising the level of randomization and privacy. □

## V. Simulation Results

The effectiveness of the proposed obfuscation-based privacy-preserving EV control strategy is verified through the simplified single-phase IEEE 13-bus test feeder as shown in Fig. 1. The baseline load profile was taken and scaled from California Independent System Operator on 09/16/2021 and 09/17/2021 [24]. We consider the penetration level of 7 EVs per bus, and in total 84 EVs are connected to the distribution network. The charging demands of all EVs randomly distribute in $[10, 40]$ kWh. The maximum charging power $\bar{r}_{\hat{\imath}}$'s are uniformly set to be 6.6 kW based on the level-2 EV charging standards and the charging efficiency is set to be $\eta = 0.85$. The valley-filling horizon is set to begin at 19:00 and lasts until 7:00 the next morning. The entire control horizon is divided into $T = 48$ time slots with 15-minute resolution. It is required that, by the end of the valley-filling period, all EVs need to be charged to the desired energy levels. The primal update step sizes are chosen based on experience as $\gamma_{\hat{\imath}} = 4 \times 10^{-4}$, $\forall \hat{\imath} = 1, \ldots, \hat{n}$, and the dual update step sizes are $\beta_i = 2 \times 10^{-3}$, $\forall i = 1, \ldots, n$. Initial values of $\boldsymbol{r}_{\hat{\imath}}^{(0)}$'s and $\boldsymbol{\lambda}_i^{(0)}$'s are all set to be zeros. The normal random variables $\tilde{X}_{\hat{\imath}}$'s generated by EVs connected at bus $i$ follow the nomral distribution $\tilde{X}_{\hat{\imath}} \sim \mathcal{N}(\mu_i = 1, \sigma_i^2 = 0.2)$. The cardinality of $\tilde{\boldsymbol{X}}_{\hat{\imath}}$'s is set uniformly to be $m = 40$.

By applying **Algorithm 1**, Fig. 3 shows that the baseline load was flattened by using EVs' charging load. The optimal charging profiles of all EVs are shown in Fig. 4. At around 1:00 a.m., when the baseline load reaches its minimum, all EVs charge at their highest power.

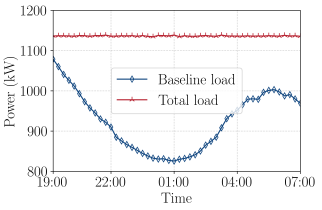


Fig. 3: The overnight valley filling.

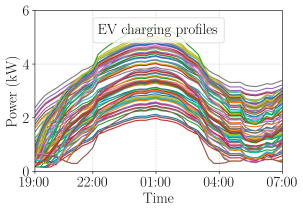


Fig. 4: Optimal charging profiles of all EVs.

To observe the privacy features, Fig. 5 presents the random values $\boldsymbol{r}_8^{(12)}(t)\tilde{\boldsymbol{X}}_{8,t}^{(12)}$, $\forall t = 1, \ldots, T$ that were generated by EV 8 at the 12th iteration. The true charging profile $\boldsymbol{r}_8^{(12)}$

was obfuscated into $\boldsymbol{r}_8^{(12)}(t)\tilde{\boldsymbol{X}}_{8,t}^{(12)}(\tilde{m})$, $\forall t = 1, \ldots, T, \tilde{m} = 1, \ldots, m$. The range of the obfuscated data is shown by the shaded area, where the obfuscation achieves nearly 50% randomization of the original data. Fig. 6 shows the nodal

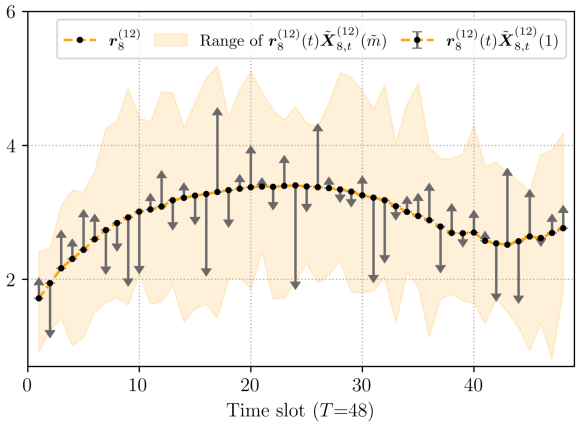


Fig. 5: The true and obfuscated data generated by EV 8 at the 12th iteration.

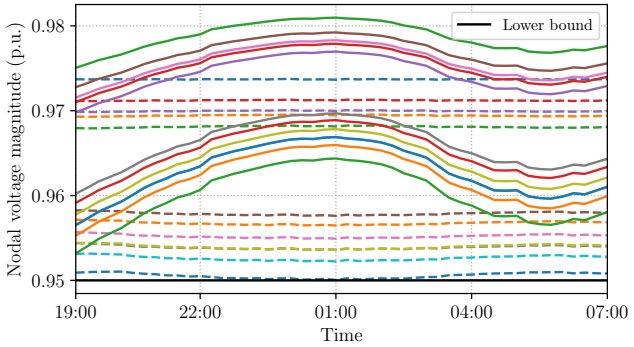


Fig. 6: Nodal voltage magnitudes of 12 buses under baseline load (solid lines) and total load (dashed lines).

voltage magnitudes of 12 buses in the distribution network, where all voltage magnitudes are above the lower voltage limit (0.95 p.u., the black line).

## VI. Conclusion

In this paper, we proposed a novel privacy-preserving decentralized algorithm to achieve privacy preservation and scalability in large-scale multi-agent cooperative optimization, particularly in the context of cooperative EV charging control. The proposed algorithm enables EVs to protect their decision variables via state obfuscation while facilitating the cooperation between EVs and the SO to achieve overnight valley filling. The privacy guarantees were theoretically analyzed and evaluated against honest-but-curious adversaries and external eavesdroppers. Simulations on an EV charging control problem validated the accuracy, efficiency, and privacy preservation properties of the proposed approach.

## References


[1] M. Yilmaz and P. T. Krein, "Review of the impact of vehicle-to-grid technologies on distribution systems and utility interfaces," *IEEE Transactions on Power Electronics*, vol. 28, no. 12, pp. 5673–5689, 2012.

[2] E. L. Karfopoulos and N. D. Hatziargyriou, "A multi-agent system for controlled charging of a large population of electric vehicles," *IEEE Transactions on Power Systems*, vol. 28, no. 2, pp. 1196–1204, 2012.

[3] L. Gan, U. Topcu, and S. H. Low, "Optimal decentralized protocol for electric vehicle charging," *IEEE Transactions on Power Systems*, vol. 28, no. 2, pp. 940–951, 2012.

[4] L. Zhang, V. Kekatos, and G. B. Giannakis, "Scalable electric vehicle charging protocols," *IEEE Transactions on Power Systems*, vol. 32, no. 2, pp. 1451–1462, 2016.

[5] M. Liu, P. K. Phanivong, Y. Shi, and D. S. Callaway, "Decentralized charging control of electric vehicles in residential distribution networks," *IEEE Transactions on Control Systems Technology*, vol. 27, no. 1, pp. 266–281, 2019.

[6] X. Huo and M. Liu, "Two-facet scalable cooperative optimization of multi-agent systems in the networked environment," *IEEE Transactions on Control Systems Technology*, vol. 30, no. 6, pp. 2317–2332, 2022.

[7] D. Fiore and G. Russo, "Resilient consensus for multi-agent systems subject to differential privacy requirements," *Automatica*, vol. 106, pp. 18–26, 2019.

[8] E. Nozari, P. Tallapragada, and J. Cortés, "Differentially private distributed convex optimization via functional perturbation," *IEEE Transactions on Control of Network Systems*, vol. 5, no. 1, pp. 395–408, 2016.

[9] J. Wang, J.-F. Zhang, and X. He, "Differentially private distributed algorithms for stochastic aggregative games," *Automatica*, vol. 142, p. 110440, 2022.

[10] W. Fang, M. Zamani, and Z. Chen, "Secure and privacy preserving consensus for second-order systems based on Paillier encryption," *Systems & Control Letters*, vol. 148, p. 104869, 2021.

[11] X. Zhang, C. Liu, K. K. Chai, and S. Poslad, "A privacy-preserving consensus mechanism for an electric vehicle charging scheme," *Journal of Network and Computer Applications*, vol. 174, p. 102908, 2021.

[12] X. Huo and M. Liu, "Encrypted decentralized multi-agent optimization for privacy preservation in cyber-physical systems," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 750–761, 2023.

[13] C. Zhang and Y. Wang, "Enabling privacy-preservation in decentralized optimization," *IEEE Transactions on Control of Network Systems*, vol. 6, no. 2, pp. 679–689, 2018.

[14] X. Huo and M. Liu, "A secret-sharing based privacy-preserving distributed energy resource control framework," in *Proceedings of the 31st International Symposium on Industrial Electronics*, Anchorage, AK, USA, Jun, 01-03 2022, pp. 963–966.

[15] Q. Li and M. G. Christensen, "A privacy-preserving asynchronous averaging algorithm based on Shamir's secret sharing," in *Proceedings of the European Signal Processing Conference*, A Coruña, Spain, Sep. 2-6 2019, pp. 1–5.

[16] C. Rottondi, S. Fontana, and G. Verticale, "Enabling privacy in vehicle-to-grid interactions for battery recharging," *Energies*, vol. 7, no. 5, pp. 2780–2798, 2014.

[17] X. Huo and M. Liu, "Distributed privacy-preserving electric vehicle charging control based on secret sharing," *Electric Power Systems Research*, vol. 211, p. 108357, 2022.

[18] Y. Wang, "Privacy-preserving average consensus via state decomposition," *IEEE Transactions on Automatic Control*, vol. 64, no. 11, pp. 4711–4716, 2019.

[19] Y. Zhang, Z. Peng, G. Wen, J. Wang, and T. Huang, "Privacy preserving-based resilient consensus for multi-agent systems via state decomposition," *IEEE Transactions on Control of Network Systems*, 2022.

[20] M. E. Baran and F. F. Wu, "Network reconfiguration in distribution systems for loss reduction and load balancing," *IEEE Power Engineering Review*, vol. 9, no. 4, pp. 101–102, 1989.

[21] D. Bertsekas and J. Tsitsiklis, *Parallel and distributed computation: Numerical methods*. Athena Scientific, 2015.

[22] S. M. Ross, *Stochastic processes*. John Wiley & Sons, 1995.

[23] P. Samarati and L. Sweeney, "Protecting privacy when disclosing information: k-anonymity and its enforcement through generalization and suppression," 1998.

[24] U.S. Energy Information Administration, "Electric power annual." [Online]. Available: https://www.eia.gov/todayinenergy/detail.php?id=49276