Electric Power Systems Research 211 (2022) 108357

Contents lists available at ScienceDirect

Electric Power Systems Research

journal homepage: www.elsevier.com/locate/epsr

Distributed privacy-preserving electric vehicle charging control based on secret sharing☆

Xiang Huo, Mingxi Liu *

Department of Electrical and Computer Engineering, University of Utah, Salt Lake City, UT, USA

ARTICLE INFO

Keywords:
Distributed optimization
Electric vehicle
Privacy preservation
Secret sharing
Valley filling

ABSTRACT

Cooperative electric vehicle (EV) charging control has emerged as a key component in grid-edge resource (GER) management. However, customers' privacy remains a major barrier to large-scale implementation of EV charging control. In this paper, we develop a distributed privacy-preserving EV charging control protocol based on secret sharing (SS) that (1) achieves scalability over EV population size; (2) enjoys higher computation efficiency compared to homomorphic encryption (HE) based methods; and (3) secures the privacy of the participating EVs against honest-but-curious adversaries and external eavesdroppers. The cooperative EV charging control is formulated to achieve overnight valley filling and framed into the projected gradient algorithm (PGA) structure as a distributed optimization problem. SS is integrated into PGA to achieve secure updates of both primal and dual variables. Theoretical security analyses and simulations in a residential area are conducted to prove the privacy preservation guarantee as well as the efficacy and efficiency of the proposed privacy preservation method. Broadly, the proposed method can be readily extended to various GER control applications.

1. Introduction

The increasing penetration of electric vehicles (EV) has brought unprecedented challenges and opportunities to the power grid. EVs are more economic and environmental friendly owing to their petroleum independence and reduced greenhouse gas emissions [1]. Nevertheless, without proper coordination and control, the enormous EV charging loads can cause multiple detrimental impacts on the traditional distribution grid, such as stability, uncertainty, and scalability issues [2, 3]. On the other side, EV charging load coordination and regulation can provide a range of grid services [4], e.g., peak shaving and valley filling. Hence, a commensurate EV charging control framework is demanded to attenuate the impacts and promote the benefits.

To improve the scalability and resilience of the distribution grid, distributed controller and optimization strategies for large-scale EV charging problems are drawing more attentions. Faddel et al. in [5] focused on demand side management programs and designed a distributed controller to coordinate the charging behaviors of EVs. In [6], an optimization framework based on the alternating directions method of multipliers (ADMM) was proposed to achieve computational scalability of large-scale EV charging control. The proposed method can concurrently solve the valley filling and cost minimization optimization problems. Similarly, Shao et al. in [7] proposed a partial decomposition method based on the Lagrangian relaxation for EV charging control, aiming at reducing the total generation cost and alleviating the grid congestion. To deal with the high penetration of EVs, Ma et al. in [8] designed three distributed EV charging control algorithms and compared the trade-off between the feasibility and the optimality under power network capacity constraints.

However, the abovementioned distributed EV charging control algorithms as well as general distributed multi-agent optimization techniques require frequent communications between participants, which can lead to potential privacy breaches, e.g., the charging behavior of an EV can reveal the owner's driving patterns [9]. Therefore, privacy has emerged as a major blocking barrier to the implementation of distributed control. One popular tool that can be integrated into distributed control to achieve privacy preservation is homomorphic encryption (HE). HE enables secure arithmetic operations over encrypted data, and when decrypted, the result matches operations performed on the original plaintext. Li et al. in [10] designed a privacy-preserving demand response scheme based on HE, and an adaptive key evolution was proposed to balance the trade-off between the communication efficiency and security level. In [11], a privacy-preserving approach based on partial HE was proposed to solve consensus problems securely. The proposed approach leverages cryptography to protect each agent

☆ This work has been supported in part by National Science Foundation, USA Award: ECCS-2145408.
* Corresponding author.
E-mail addresses: xiang.huo@utah.edu (X. Huo), mingxi.liu@utah.edu (M. Liu).

https://doi.org/10.1016/j.epsr.2022.108357
Received 1 October 2021; Received in revised form 2 March 2022; Accepted 2 July 2022
Available online 13 July 2022

from disclosing its true states to the neighbors and guarantee the convergence to the consensus value. Brettschneider et al. in [12] proposed an HE scheme for distributed load adaption, where the complexity of the communicational and computational overhead was analyzed.

Though HE-based methods have guaranteed security and high accuracy, their industrial applicability is severely limited by the high computational complexity induced by encryption and decryption. In contrast to HE-based strategies, another lightweight cryptographic strategy to enabling privacy preservation is secret sharing (SS) which was firstly introduced by Shamir in [13]. SS is polynomial based and it deploys a manager to divide a secret message to multiple shares and distribute each share to an agent. In this manner, individuals learn nothing about the secret, but any set of agents that has a cardinality more than a threshold can reconstruct the secret. Compared to HE-based methods, SS-based strategies remove the computing burden caused by frequent encryption and decryption, and achieve improved efficiency by adopting share computation and secret reconstruction. In [14], a distributed cloud-based controller using SS was proposed to achieve encrypted linear state feedback, where the encryption scheme was modified by one-time pad to reduce the computational overhead. Li et al. in [15] developed a distributed privacy-preserving algorithm based on SS specifically for averaging consensus problems. In [16], a distributed privacy-preserving framework based on SS was proposed to protect the privacy of the customers. The designed framework can protect the readings of a smart meter from dedicated aggregators and the electrical utility.

However, none of the existing SS-based methods are applicable to EV charging control, as they either rely on the coordination of a third party or are designed for special problem formulations that are not suitable for EV charging control. This paper fills this gap by developing a novel SS-based distributed privacy-preserving EV charging control scheme that is third party free and concurrently achieves privacy preservation, scalability, high computing efficiency, and high accuracy.

The contribution of this paper is three-fold: (1) We, for the first time, integrate SS into distributed optimization algorithms to achieve scalable EV charging control for valley filling. (2) The proposed protocol enjoys high computing efficiency compared to HE-based methods. (3) We investigate the attacks from both internal and external adversaries, and provide theoretically sound proof of security. The proposed method can be extended to other grid-edge resource (GER) controls.

2. Main results & methodologies

2.1. Problem formulation

In a distribution feeder, the high electricity demand during daytime and the low electricity demand at night create a valley in the demand profile. Such valley can increase the grid operation cost like shutting down or restarting large power plants [17]. In this section, we formulate an EV charging control optimization problem to fill the overnight demand valley. Suppose n EVs need to be charged during the valley-filling period $\tilde{T} = [1 : T]$ of length $T\Delta T$ where ΔT is the sampling period. We denote the charging profile of the ith EV by $\boldsymbol{x}_i = [x_i(1), \dots, x_i(T)]^\mathsf{T} \in \mathbb{R}^T$ where $x_i(t)$ is a scalar representing its charging rate at time t. For the ith EV, its charging rate is constrained by

$$\mathbf{0} \le \boldsymbol{x}_i \le \boldsymbol{r}_i^u, \tag{1}$$

where $\boldsymbol{r}_i^u$ denotes the maximum charging rate of the ith EV.

To guarantee all EVs can be charged to the desired energy level by the end of valley-filling period, the summation of the charging loads of the ith EV during period $\tilde{T}$ should satisfy

$$\boldsymbol{G}\boldsymbol{x}_i = d_i, \tag{2}$$

where $\boldsymbol{G} = [\Delta T, \dots, \Delta T] \in \mathbb{R}^{1\times T}$ denotes the aggregation vector and d_i denotes the charging demand of the ith EV.

Filling the overnight demand valley is equivalent to flattening the total demand curve by exploiting the EV charging loads [18]. Therefore, the valley-filling optimization problem can be formulated into a quadratic programming problem with the abovementioned constraints as

$$\begin{aligned} \min_{\boldsymbol{x}} \quad & \frac{1}{2}\left\| \boldsymbol{P}_b + \sum_{i=1}^{n} \boldsymbol{x}_i \right\|_2^2 \\ \text{s.t.} \quad & \mathbf{0} \le \boldsymbol{x}_i \le \boldsymbol{r}_i^u, \quad \forall i = 1, 2, \dots, n, \\ & \boldsymbol{G}\boldsymbol{x}_i = d_i, \quad \forall i = 1, 2, \dots, n, \end{aligned} \tag{3}$$

where $\boldsymbol{P}_b$ denotes the baseline load. Other network constraints, e.g., the voltage limits of the distribution network, can also be included in problem (3) and have no impact on privacy preservation. In this paper, to better illustrate the design of the privacy preservation method, we avoid over-complicating the optimization problem by omitting those network constraints.

To solve the valley-filling problem in (3), n agents (EVs) can work corporately using projected gradient algorithms (PGA) [19]. The PGA based method is widely adopted in distributed and decentralized optimization, e.g., multiuser optimization problem [20], decentralized EV charging control [21], and convex games [22]. Using PGA, agent i updates its decision variable by following

$$\boldsymbol{x}_i^{\ell+1} = \mathbb{P}_{X_i}[\boldsymbol{x}_i^{\ell} - \gamma_i^{\ell}\boldsymbol{\Phi}_i(\boldsymbol{x}^{\ell})], \tag{4}$$

where ℓ denotes the iteration index, $\boldsymbol{x} \triangleq [\boldsymbol{x}_1^\mathsf{T}, \dots, \boldsymbol{x}_n^\mathsf{T}]^\mathsf{T}$, X_i denotes the feasible set of $\boldsymbol{x}_i$, γ_i^{ℓ} is the step size length of agent i, $\boldsymbol{\Phi}_i(\cdot)$ is the first-order gradient of the Lagrangian function *w.r.t.* $\boldsymbol{x}_i$, and $\mathbb{P}_{X_i}[\cdot]$ denotes the Euclidean projection operation onto set X_i.

To solve (3) with any projection-based method, we firstly calculate the relaxed Lagrangian of (3) as

$$\mathcal{L}(\boldsymbol{x}, \lambda) = \frac{1}{2}\left\| \boldsymbol{P}_b + \sum_{i=1}^{n} \boldsymbol{x}_i \right\|_2^2 + \sum_{i=1}^{n} \lambda_i(\boldsymbol{G}\boldsymbol{x}_i - d_i), \tag{5}$$

where $\lambda \triangleq [\lambda_1, \dots, \lambda_n]^\mathsf{T}$ and λ_i is the dual variable associated with the ith equality constraint. Therefore, the subgradients of $\mathcal{L}(\boldsymbol{x}, \lambda)$ *w.r.t.* $\boldsymbol{x}_i$ and λ_i can be readily obtained as

$$\nabla_{x_i}\mathcal{L}(\boldsymbol{x}, \lambda) = \boldsymbol{P}_b + \sum_{i=1}^{n} \boldsymbol{x}_i + \lambda_i \boldsymbol{G}^\mathsf{T}, \tag{6a}$$

$$\nabla_{\lambda_i}\mathcal{L}(\boldsymbol{x}, \lambda) = \boldsymbol{G}\boldsymbol{x}_i - d_i. \tag{6b}$$

Then, the decision variable (primal variable) and the dual variable can be updated using the PGA. Herein, we derive the update rule (7a) for the primal variable using the subgradient in (6a) and PGA equation in (4). The dual variable can be updated using subgradient ascent with the subgradient in (6b). Consequently, we have

$$\boldsymbol{x}_i^{\ell+1} = \Pi_{\mathbb{X}_i}\left(\boldsymbol{x}_i^{\ell} - \gamma_i \nabla_{x_i}\mathcal{L}\left(\boldsymbol{x}^{\ell}, \lambda^{\ell}\right)\right), \tag{7a}$$

$$\lambda_i^{\ell+1} = \lambda_i^{\ell} + \beta \nabla_{\lambda_i}\mathcal{L}\left(\boldsymbol{x}^{\ell}, \lambda^{\ell}\right), \tag{7b}$$

where $\mathbb{X}_i \triangleq \{\boldsymbol{x}_i \mid \mathbf{0} \le \boldsymbol{x}_i \le \boldsymbol{r}_i^u\}$ denotes the feasible set of the charging rate limits, and γ_i and β denote the primal and dual step sizes, respectively. Note that $\mathbb{X}_i$ assumes the ith EV's charging rate can vary continuously between $\mathbf{0}$ and $\boldsymbol{r}_i^u$. This is an assumption commonly made in EV charging control algorithm designs [18,23]. Discrete local constraint sets that accommodate positive lower bounded charging power will be considered in our future work.

Remark 1. $\mathbb{X}_i$ is chosen to only include (1) so that (2) can mimic the global network constraints in $\mathcal{L}(\boldsymbol{x}, \lambda)$. □

Note that in (6a), the calculation of $\nabla_{x_i}\mathcal{L}(\boldsymbol{x}, \lambda)$ depends on $\boldsymbol{x}_i$'s from all the agents. Therefore, the update in (7a) requires decision variable exchanges between agents, which can lead to potential privacy breaches [24]. To overcome this privacy challenge, we aim at

designing a novel protocol based on SS that can protect agents' privacy, in which the agents aggregate and distribute information privately without exposing privacy to others. In the following, we first illustrate the standard steps of SS, then develop the SS-based privacy-preserving protocol.

2.2. Shamir's secret sharing scheme

The essential idea of SS is Lagrange polynomial interpolation, i.e., given k points $(a_1, b_1), \dots, (a_k, b_k)$ with distinct a_i's on the 2-D plane, there exists a unique polynomial $q(z)$ of degree $k-1$ such that $q(a_i) = b_i, \forall i = 1, \dots, k$. Any number of points that are strictly smaller than k will not reveal any information about the polynomial, and at least k points are required to reconstruct the polynomial.

In the following, we present a case where a manager wants to distribute an integer secret s to n agents, and at least k agents are required to cooperatively retrieve the secret. The secret is randomized via a polynomial and sent to the agents in the form of shares. Any $\hat{k}$ agents, where $k \le \hat{k} \le n$, can reconstruct the secret, otherwise no information about the secret can be revealed. This is called a (k, n)-threshold SS which comprises of three steps as

(1) *Polynomial generation:* The manager constructs a random polynomial

$$f(z) = s + c_1 z + \cdots + c_{k-1} z^{k-1}, \tag{8}$$

where s denotes the secret, the coefficients $c_1, \dots, c_{k-1}$ are randomly chosen from a uniform distribution in the integer field $\mathbb{E} \triangleq [0, e)$, where e denotes a prime number that is larger than s.

(2) *Share distribution:* The manager computes the shares with a non-zero integer input and the corresponding output, e.g., set $i = 1, \dots, n$ to retrieve $(i, f(i))$. Then, it distributes the share f_i to the ith agent, where

$$f_i = f(i) \bmod e, \tag{9}$$

and mod denotes the modular operation.

(3) *Secret reconstruction:* Since each agent is given a point and k points are sufficient to reconstruct the polynomial using Lagrange interpolation, any $\hat{k}$ agents, where $k \le \hat{k} \le n$, can calculate the secret s using interpolation as

$$s = \sum_{i=1}^{k} f_i \prod_{\substack{j=0 \\ j \neq i}}^{k} \frac{j}{j-i}. \tag{10}$$

Note that the constant term s in (8) is exactly the secret that can be calculated by $f(0) = s$. The Shamir's SS scheme requires integers and finite field arithmetic to guarantee the perfect security, i.e., the coefficients $c_1, \dots, c_{k-1}$ and the secret s have to be within the field $\mathbb{E}$. Besides, the modular operation in (9) also guarantees that the outputs of the polynomials are within the field $\mathbb{E}$. In (10), though we only calculate the secret s, it is also possible to reconstruct (8). But since we are only interested in retrieving the secret, (10) is adopted to reduce the unnecessary computing cost.

2.3. Real number and integer transformation

Note that the SS scheme requires modular arithmetic within the field $\mathbb{E}$. However, distributed optimization genetically requires real decision variables and parameters. Therefore, to integrate SS into distributed optimization, a real number needs to be transformed into an integer. Herein, we formulate the real number to integer transformation rule as

$$z_e = \lfloor 10^{\delta} \theta \rfloor, \tag{11}$$

where θ denotes any real number, δ denotes the preserved decimal fraction digits, $\lfloor \cdot \rfloor$ denotes the floor operation, and z_e is the transformed integer. To proceed with the SS, we further need to map z_e to the field $\mathbb{E}$, which can be achieved by

$$z_e^+ = z_e \bmod e, \tag{12}$$

where $z_e^+ \in \mathbb{E}$ denotes the integer that is mapped to the field $\mathbb{E}$. To transform an integer back to the real number, we employ the inverse function $\phi(\cdot)$ that is defined as

$$\phi(z) = \begin{cases} z - e, & \text{if } z \ge \frac{e}{2}, \\ z, & \text{otherwise.} \end{cases} \tag{13}$$

Therefore, a number in the field $\mathbb{E}$ can be transformed to the original signed integer. Finally, we can simply divide the signed integer by 10^{δ} to convert it to the original real number.

2.4. Proposed privacy-preserving algorithm

In this section, we develop a novel privacy-preserving protocol based on SS. During the iterative computations, agents update their primal and dual variables by following (7). The agents can perform the dual update in (7b) independently without having to communicate with each other. Therefore, the dual variables λ_i's can be kept private to the ith agents directly. However, the primal update in (7a) requires the aggregation $\sum_{i=1}^{n} \boldsymbol{x}_i$ in (6a), leading to mandatory exchange of decision variables between all the agents. To eliminate the potential decision variable leakage caused by the information exchange, we integrate SS into (7) to achieve the secure message aggregation. To clearly state the privacy issues concerned in this paper, we herein define the privacy as follows.

Definition 1 (*Privacy*)**.** For the ith EV, the private information includes its charging profile $\boldsymbol{x}_i$, dual variable λ_i, the maximum charging rates $\boldsymbol{r}_i^u$, demand d_i, and the primal and dual step sizes γ_i and β. ■

The privacy in Definition 1 can be categorized into three aspects: (1) private parameters of the EVs (agents), i.e., $\boldsymbol{r}_i^u$ and d_i; (2) intermediate iteration variables of the agents, i.e., $\boldsymbol{x}_i^\ell$ and λ_i^ℓ; and (3) the parameters used by the PGA, i.e., γ_i and β. Though Definition 1 specifically targets at EV charging control problem, it can also be extended to various optimization problems in other fields (as illustrated in Remark 3). Besides, the private parameters of the agents can be extended as well, e.g., constraints on charging ramp rate.

To proceed with the protocol design, the following assumption is required for the network communication.

Assumption 1. The network is interconnected through communication channels. ■

Under Assumption 1, each agent is able to communicate with any other agents. This interconnected communication network can be easily set up, e.g., EVs can communicate in the cloud or on a specific server with internet access [25]. In the following proposed framework, we admit that Assumption 1 may introduce an overall high communication load between agents, so our future research direction will target at lifting Assumption 1 to reduce the communication cost, e.g., using a spanning-tree communication network.

Recall that in the SS scheme, a manager is required to generate the polynomial and distribute the shares. To eliminate the need of a manager, we empower each agent to act as both manager and agent. Each agent can construct polynomials, distribute shares, and receive messages from others. The ith agent firstly generates a set of random parameters $c_{i1}^\ell, \dots, c_{ik}^\ell \in \mathbb{E}$, then constructs a polynomial as

$$p_i^\ell(z) = s_i^\ell + c_{i1}^\ell z + \cdots + c_{ik}^\ell z^k, \tag{14}$$

where s_i^ℓ is the secret held by the ith agent, i.e., the charging profile $\boldsymbol{x}_i^\ell$. Note that the charging profiles $\boldsymbol{x}_i^\ell$'s are real number vectors, while s_i^ℓ's need to be integers. To resolve this issue, agents should firstly transform

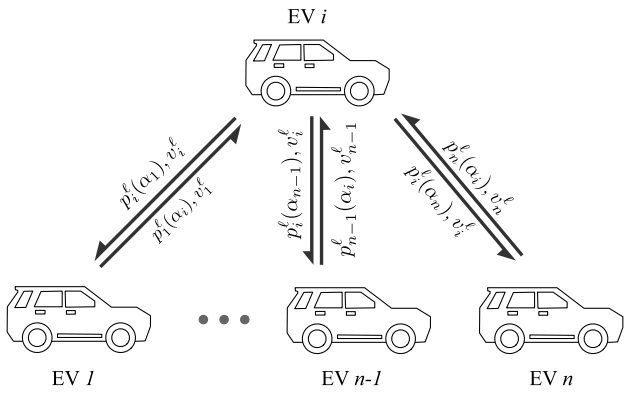

Fig. 1. The information exchange between the ith EV and other EVs.

secret $\boldsymbol{x}_i^\ell$ into integer vectors using (11), then deal with the integer vectors elementwisely.

Having the polynomial constructed, the ith agent then evaluates $p_i^\ell(\alpha_j), \forall j = 1, \dots, n$ where α_j's are the shared input knowledge among all the agents. Following that, the ith agent sends $p_i^\ell(\alpha_j), j \neq i$, to the jth agent and keeps $p_i^\ell(\alpha_i)$ to itself. After receiving all the messages, agent i is ready to compute the summation of the received messages as

$$v_i^\ell = \sum_{l=1}^{n} p_l^\ell(\alpha_i). \tag{15}$$

Following the summation, agent i broadcasts v_i^ℓ to other agents without revealing any true self-relevant information. Note that the summation v_i^ℓ's calculated by the agents in (15) correspond to the outputs of the polynomial

$$\tilde{p}_i^\ell(z) = \sum_{l=1}^{n} s_l^\ell + \sum_{j=1}^{k}\left(\sum_{l=1}^{n} c_{lj}^\ell\right) z^j, \tag{16}$$

at $z = \alpha_l, \forall l = 1, \dots, n$. The polynomial $\tilde{p}_i^\ell(z)$ has a degree of k, affiliated with the constant term $\sum_{l=1}^{n} s_l^\ell$ and the coefficients $\sum_{l=1}^{n} c_{lj}^\ell, j = 1, \dots, k$.

Therefore, the ith agent can collect in total n points, i.e., $(\alpha_l, v_l^\ell), \forall l = 1, \dots, n$, that correspond to the input and output pairs of the polynomial in (16). In the following, each agent is ready to reconstruct the constant term $\sum_{l=1}^{n} s_l^\ell$ according to the secret reconstruction step in (10). After obtaining the summation of the secrets $\sum_{l=1}^{n} s_l^\ell$, one can apply the inverse function $\phi(\cdot)$ defined in (13) to acquire the signed integer summation $10^\delta \sum_{l=1}^{n} \hat{\boldsymbol{x}}_l^\ell$ elementwisely. Note that $\hat{\boldsymbol{x}}_l^\ell$ is a real vector that is approximated by keeping δ digits of $\boldsymbol{x}_l^\ell$. Then, the signed integer summation $\sum_{l=1}^{n} \hat{\boldsymbol{x}}_l^\ell \cdot 10^\delta$ can be transformed back to the real vectors by the division of 10^δ.

Finally, the agents can update the primal and dual variables according to (7). The agents firstly calculate the subgradients defined in (6) using the summation $\sum_{l=1}^{n} \hat{\boldsymbol{x}}_l^\ell$. The ith agent then updates its primal variable $\boldsymbol{x}_i^\ell \to \boldsymbol{x}_i^{\ell+1}$ and dual variable $\lambda_i^\ell \to \lambda_i^{\ell+1}$. The convergence error ϵ_i^ℓ can be calculated as the summation of the Euclidean distances of the primal and dual variables in two consecutive iterations as

$$\epsilon_i^\ell = \|\boldsymbol{x}_i^{\ell+1} - \boldsymbol{x}_i^\ell\|_2^2 + \|\lambda_i^{\ell+1} - \lambda_i^\ell\|_2^2. \tag{17}$$

EV i can stop the iterations and keep the previous values if $\epsilon_i^\ell \leq \epsilon_0$ where ϵ_0 denotes the error tolerance.

The detailed procedure of the proposed method is presented via Protocol 1. The information exchange between the ith EV and other EVs is shown in Fig. 1.

Theorem 1 (*Correctness*). *Within the precision range δ, the results calculated by Protocol 1 are exactly the same as those calculated without privacy preservation.* ■

Protocol 1 Distributed SS-based privacy-preserving EV charging control protocol

1: The ith EV is associated with an integer α_i, and $\alpha_j, \forall j = 1, \dots, n$, are common knowledge among all EVs.
2: All EVs initialize primal and dual variables, tolerance ϵ_0, iteration counter $\ell = 0$, and maximum iteration ℓ_{max}.
3: **while** $\epsilon_i^\ell > \epsilon_0$ and $\ell < \ell_{max}$ **do**
4: EV i generates a set of random parameters satisfying $c_{i1}^\ell, \dots, c_{ik}^\ell \in \mathbb{E}$, then constructs the polynomial in (14).
5: The ith EV calculates $p_i^\ell(\alpha_j), \forall j = 1, \dots, n$, and sends $p_i^\ell(\alpha_j), j \neq i$ to the jth EV and keeps $p_i^\ell(\alpha_i)$ to itself.
6: EV i computes the summation of the received messages v_i^ℓ defined in (15) and broadcasts it to other agents.
7: Each EV collects in total n points, i.e., $(\alpha_l, v_l^\ell), \forall l = 1, \dots, n$, then reconstructs the constant term of the polynomial in (16) based on the secret reconstruction method introduced in (10).
8: The ith EV updates the primal variable $\boldsymbol{x}_i^\ell$ by (7a) and the dual variable λ_i^ℓ by (7b).
9: Each agent i calculates the error ϵ_i^ℓ.
10: $\ell = \ell + 1$.
11: **end while**

Theorem 1 states that the proposed privacy-preserving protocol does not jeopardize the accuracy of the PGA except for the rounding error introduced by real to integer number transformation. In fact, Protocol 1 can achieve arbitrarily higher precision level by increasing the decimal digits δ at the cost of computing load.

Theorem 2 (*Privacy-preservation against honest-but-curious agents and external eavesdroppers*). *Privacy of all agents are guaranteed if the number of agents is larger than two and each agent carries out the proposed protocol accordingly.* ■

Theorem 2 provides that the participants' privacy preservation can be guaranteed under Protocol 1 against both internal and external attacks. The internal attacks are launched by the *honest-but-curious agent* who follows the protocol but may observe the intermediate data to infer the private information of other participants. The *external eavesdropper* can launch external attacks by wiretapping and intercepting exchanged messages from the communication channels to invade the privacy of the agents. The detailed privacy analysis will be presented in Section 2.5.

Remark 2. The polynomial in (16) is of degree k, hence at least $k + 1$ points are required to reconstruct the polynomial. According to Protocol 1, each agent can have access to n points on the 2-D plane corresponding to the inputs and outputs of (16). To guarantee a successful secret reconstruction, the number of agents n and the degree k of the polynomials need to satisfy $n \geq k + 1$. Note that increasing the degree k does not improve the security level of Protocol 1 against honest-but-curious agents or external eavesdroppers. However, a larger k could potentially prevent the information leakage caused by the collaboration between honest-but-curious agents. Please refer to Section 2.5.3 for the extended discussion on the collaboration between honest-but-curious agents. □

Remark 3. Protocol 1 is not limited to the specific valley-filling optimization problem in (3). We use this EV charging control example to illustrate the grid-level applications. The proposed protocol can be applied to a variety of different areas, e.g., controlling heterogeneous GERs for grid-level services [26], energy management optimization where the neighbors are required to exchange information [27], and the general cooperative optimization problem in [28]. □

2.5. Privacy analysis

2.5.1. Security analysis against honest-but-curious agents

An *honest-but-curious agent* can use the private information belonging to itself, the common knowledge between all the agents, and the received messages from others to infer the privacy of certain agents. To analyze the attacks from honest-but-curious agents, we simulate its behaviors to prove that no private information can be obtained under the proposed protocol. Let EV i be an honest-but-curious agent. Then during the ℓth iteration, EV i can have access to

$$\mathbb{I}_{hi}^{\ell} = \{\alpha_j, p_i^{\ell}(\alpha_j), v_j^{\ell}, \forall j = 1, \dots, n, s_i^{\ell}, p_j^{\ell}(\alpha_i), \forall j \neq i\}, \tag{18}$$

where $\mathbb{I}_{hi}^{\ell}$ denotes the accessible information to EV i. Suppose EV i is interested in finding the secret s_m^{ℓ} that belongs to EV m. The information EV i can use includes α_m, $p_i^{\ell}(\alpha_m)$, and the message $p_m^{\ell}(\alpha_i)$ received from EV m. To reconstruct the secret s_m^{ℓ} contained in $p_m^{\ell}(\cdot)$, EV i needs to obtain at least k points on the 2-D plane. However, EV i only has access to a single point $(\alpha_i, p_m^{\ell}(\alpha_i))$. Therefore, it is impossible for EV i to reconstruct the secret s_m^{ℓ}. Another useful information for EV i is the collected points $(\alpha_l, v_l^{\ell}), \forall l = 1, \dots, n$, from which it can deduce the summation of secrets $\sum_{l=1}^{n} s_l^{\ell}$ from all the agents. However, when there exist other EVs other than EV i and EV m, having the summation $\sum_{l=1}^{n} s_l^{\ell}$ is still insufficient for EV i to infer any private information of EV m.

We next consider a special case where only two EVs exist, i.e., EV i and EV m, and EV i tries to infer the secret s_m^{ℓ} that belongs to EV m. Since EV i knows its own secret s_i^{ℓ} and the summation $\sum_{l=1}^{n} s_l^{\ell}$, s_m^{ℓ} can be easily compromised. We argue that this rarely happens in real EV charging control cases as well as other large-scale networked optimization problems because of the large agent population size. To address this concern, Theorem 2 states the requirement that more than two agents should be involved during the execution of Protocol 1.

2.5.2. Security analysis against external eavesdroppers

Another principal adversary is the *external eavesdropper*. For general SS-based schemes (presented in Section 2.2), the shares are distributed by the manager, and k shares can expose the secret. In those cases, an external eavesdropper can easily wiretap and collect all the transmitted messages, thus revealing the secret. We next simulate the behaviors of the external eavesdroppers and prove the security of Protocol 1.

Suppose an external eavesdropper wiretaps all communication channels in Protocol 1. Then the external eavesdropper can have access to the following transmitted messages

$$\mathbb{I}_{e}^{\ell} = \{p_i^{\ell}(\alpha_j), \forall i \neq j, v_i^{\ell}, \forall i, j = 1, \dots, n\}, \tag{19}$$

where $\mathbb{I}_{e}^{\ell}$ denotes the accessible information to the external eavesdropper. The message $p_i^{\ell}(\alpha_i), i = 1, \dots, n$, is kept private to the ith EV, therefore this message cannot be directly overheard by the external eavesdroppers. However, the external eavesdropper can deduce the value of $p_i^{\ell}(\alpha_i)$ by wiretapping the value of v_i^{ℓ} due to the summation operation in (15). Therefore, the external eavesdropper can have access to $\{p_i^{\ell}(\alpha_j), \forall i, j = 1, \dots, n\}$. In summary, the external eavesdropper can have access to the outputs of the polynomials in (14) and the polynomial in (16). In order to derive the secrets of the agents, the external eavesdropper also need to know the inputs of those polynomials. Instead of distributing the shares in the form of both the inputs and outputs of a polynomial, the proposed protocol keeps the inputs $\alpha_i, \forall i = 1, \dots, n$, private to the agents. Hence, any external eavesdropper cannot reconstruct agents' secrets with only outputs of those polynomials.

2.5.3. Collusion between honest-but-curious agents

Honest-but-curious agents may collude to infer the privacy of other agents. However, few research has addressed the collusion between honest-but-curious agents. In this paper we extend the privacy analysis against this type of attacks to achieve enhanced security. The degree of the polynomial in (14) is k, hence at least k honest-but-curious agents need to collude to infer the privacy of one specific agent. To prevent from this collusion, it is possible to increase the degree k within the limit of $k \leq n-1$. By increasing k, more honest-but-curious agents are required to work together in order to infer the privacy, which is more demanding for the honest-but-curious agents. Consequently, a higher security level towards colluding honest-but-curious agents can be achieved.

Note that when k is at the maximum, i.e., $k = n-1$, the received shares from all n agents are needed to reconstruct a secret. In this scenario, all agents have to be honest-but-curious so as to retrieve the secret. However, it is trivial to discuss the case where all agents are honest-but-curious and trying to collaborate with each other, because they share information with each other through collusion and secrets do not exist.

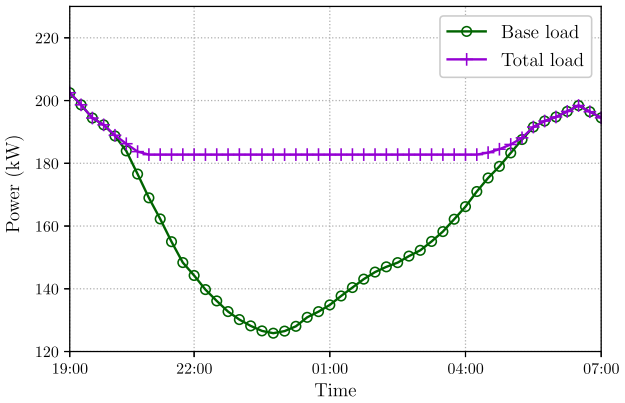

Fig. 2. The baseline load profile and the total load profile under the proposed privacy-preserving EV charging control protocol.

3. Simulation results

In this section, we conduct valley-filling simulations with 20 EVs for an apartment complex in the residential area. Assume this complex is equipped with a 20 level-2 electric vehicle supply equipment (maximum 6.6 kW). All EVs need to be charged to the desired levels by the end of the valley-filling period. The net demand profile (system demand minus wind and solar) was taken from California Independent System Operator on 07/21/2021 and 07/22/2021 [29]. We scale the demand profile by 200 to simulate the daily residential load profile of the complex. The valley filling starts at 19:00 in the evening and ends at 7:00 in the morning next day. Herein, we have in total 48 time slots by sampling every 15 min within 12 h. The preserved decimal fraction digits is set as $\delta = 3$. The primal step sizes are uniformly chosen as $\gamma_i = 0.01, \forall i = 1, \dots, n$, and the dual step size is $\beta = 1$. For the ith EV, the input α_i is chosen to be i. Initial values of $\boldsymbol{x}_i$ and λ_i are set to be zeros. The maximum charging rates of all EVs are uniformly set as $r_u = 6.6$ kW. The charging demands d_i's of the EVs are randomly distributed in $[10, 20]$ kWh. The degree of all polynomials are set as $k = 3$ and the integer field is chosen as $\mathbb{E} = [0, 2^{31} - 1)$.

Fig. 2 presents the valley-filling results where the baseline load is flattened into the total load by controlling the EVs' charging loads. The final charging profiles of the 20 EVs are shown in Fig. 3. All the EVs charge at the fastest rates ranging from 1 kW to 4.5 kW at around $00:00$ to fill the midnight deep valley. Without the loss of generality, we present the messages sent by two EVs in Fig. 4, i.e., $p_1^{\ell}(\alpha_2)$ and v_1^{ℓ} sent by EV 1, and $p_2^{\ell}(\alpha_1)$ and v_2^{ℓ} sent by EV 2 within 100 iterations. As can be readily observed, all the transmitted messages are randomized to achieve privacy preservation. Fig. 5 gives the polynomials generated by EV 1 that are of degree 3 and aim at randomizing and protecting the first element of the decision variable $\boldsymbol{x}_i$. In total 300 polynomials $p_1^{\ell}(z), \ell = 1, \dots, 300$ are presented in the upper plot of Fig. 5, and the polynomials from the first two iterations are shown in the lower plot for clear presentation. All other coefficients, i.e., c_{11}, c_{12}, and c_{13}, are randomized and vary in each iteration as well.

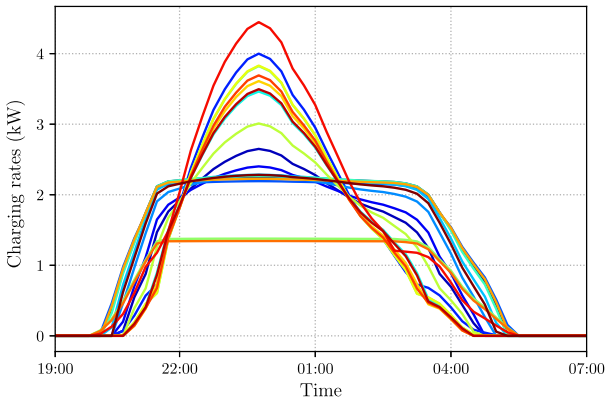

Fig. 3. Charging profiles of all EVs after 300 iterations during the valley-filling period.

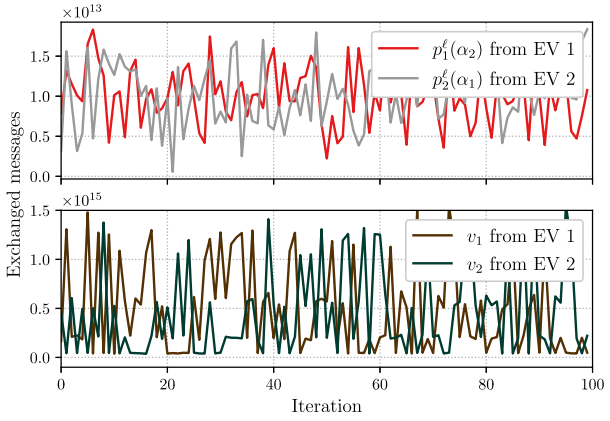

Fig. 4. Messages sent from EV 1 and EV 2.

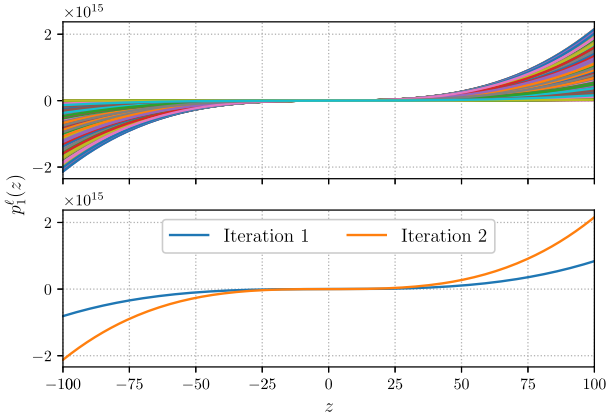

Fig. 5. Polynomials generated by EV 1 *w.r.t* the secret $\boldsymbol{x}_1(1)$.

4. Conclusion and future research

In this paper, we proposed a novel distributed SS-based privacy-preserving EV charging control protocol. We integrated SS into PGA to secure the privacy of the EVs where only secret shares were transmitted between EVs. Through theoretical security analyses, privacy of all EVs are guaranteed against individual and colluding honest-but-curious agents as well as external eavesdroppers. The proposed protocol enjoys lower computing cost compared to HE-based methods and achieves scalability through its distributed setting. Simulation results of a valley-filling problem show the efficiency and efficacy of the proposed privacy-preserving protocol. Some limitations of the proposed method were identified, and those limitations motivate future research directions including reducing the communication loads between EVs, considering discrete local constraint sets that accommodate positive lower bounded charging power, and targeting at broader grid-level services besides valley filling.

CRediT authorship contribution statement

Xiang Huo: Conceptualization, Methodology, Software, Data curation, Validation, Writing – original draft. **Mingxi Liu:** Conceptualization, Supervision, Funding acquisition, Writing – review & editing.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

[1] E.A. Nanaki, C.J. Koroneos, Comparative economic and environmental analysis of conventional, hybrid and electric vehicles – the case study of Greece, J. Cleaner Prod. 53 (2013) 261–266.
[2] A. Ovalle, A. Hably, S. Bacha, Optimal management and integration of electric vehicles to the grid: Dynamic programming and game theory approach, in: Proceedings of the IEEE International Conference on Industrial Technology, 2015, pp. 2673–2679, Seville, Spain.
[3] S. Yu, F. Fang, Y. Liu, J. Liu, Uncertainties of virtual power plant: Problems and countermeasures, Appl. Energy 239 (2019) 454–470.
[4] Z. Wang, S. Wang, Grid power peak shaving and valley filling using vehicle-to-grid systems, IEEE Trans. Power Deliv. 28 (3) (2013) 1822–1829.
[5] S. Faddel, O.A. Mohammed, Automated distributed electric vehicle controller for residential demand side management, IEEE Trans. Ind. Appl. 55 (1) (2018) 16–25.
[6] J. Rivera, C. Goebel, H.-A. Jacobsen, Distributed convex optimization for electric vehicle aggregators, IEEE Trans. Smart Grid 8 (4) (2017) 1852–1863.
[7] C. Shao, X. Wang, M. Shahidehpour, X. Wang, B. Wang, Partial decomposition for distributed electric vehicle charging control considering electric power grid congestion, IEEE Trans. Smart Grid 8 (1) (2017) 75–83.
[8] W.-J. Ma, V. Gupta, U. Topcu, On distributed charging control of electric vehicles with power network capacity constraints, in: Proceedings of the American Control Conference, 2014, pp. 4306–4311, Portland, OR, USA.
[9] F. Yucel, K. Akkaya, E. Bulut, Efficient and privacy preserving supplier matching for electric vehicle charging, Ad Hoc Netw. 90 (2019) 101730.
[10] H. Li, X. Lin, H. Yang, X. Liang, R. Lu, X. Shen, EPPDR: An efficient privacy-preserving demand response scheme with adaptive key evolution in smart grid, IEEE Trans. Parallel Distrib. Syst. 25 (8) (2013) 2053–2064.
[11] M. Ruan, H. Gao, Y. Wang, Secure and privacy-preserving consensus, IEEE Trans. Automat. Control 64 (10) (2019) 4035–4049.
[12] D. Brettschneider, D. Hölker, R. Tönjes, A. Scheerhorn, On homomorphic encryption for privacy-preserving distributed load adaption in smart grids, in: Proceedings of the IEEE International Conference on Communications, 2016, pp. 1–6, Kuala Lumpur, Malaysia.
[13] A. Shamir, How to share a secret, Commun. ACM 22 (11) (1979) 612–613.
[14] M.S. Daru, T. Jager, Encrypted cloud-based control using secret sharing with one-time pads, in: Proceedings of the IEEE Conference on Decision and Control, 2019, pp. 7215–7221, Nice, France.
[15] Q. Li, M.G. Christensen, A privacy-preserving asynchronous averaging algorithm based on Shamir's secret sharing, in: Proceedings of the European Signal Processing Conference, 2019, pp. 1–5, A Coruña, Spain.
[16] G.S. Wagh, S. Gupta, S. Mishra, A distributed privacy preserving framework for the smart grid, in: Proceedings of the IEEE Power & Energy Society Innovative Smart Grid Technologies Conference, 2020, pp. 1–5, Washington, D.C., USA.
[17] L. Zhang, F. Jabbari, T. Brown, S. Samuelsen, Coordinating plug-in electric vehicle charging with electric grid: Valley filling and target load following, J. Power Sources 267 (2014) 584–597.
[18] L. Gan, U. Topcu, S.H. Low, Optimal decentralized protocol for electric vehicle charging, IEEE Trans. Power Syst. 28 (2) (2012) 940–951.
[19] D. Bertsekas, J. Tsitsiklis, Parallel and Distributed Computation: Numerical Methods, Athena Scientific, 2015.
[20] J. Koshal, A. Nedić, U.V. Shanbhag, Multiuser optimization: Distributed algorithms and error analysis, SIAM J. Optim. 21 (3) (2011) 1046–1081.
[21] M. Liu, P.K. Phanivong, Y. Shi, D.S. Callaway, Decentralized charging control of electric vehicles in residential distribution networks, IEEE Trans. Control Syst. Technol. 27 (1) (2019) 266–281.

[22] M. Zhu, E. Frazzoli, Distributed robust adaptive equilibrium computation for generalized convex games, Automatica 63 (2016) 82–91.
[23] Z.J. Lee, D. Chang, C. Jin, G.S. Lee, R. Lee, T. Lee, S.H. Low, Large-scale adaptive electric vehicle charging, in: Proceedings of the IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids, 2018, pp. 1–7, Portland, OR, USA.
[24] C. Zhang, Y. Wang, Enabling privacy-preservation in decentralized optimization, IEEE Trans. Control Netw. Syst. 6 (2) (2018) 679–689.
[25] J. Chynoweth, C.-Y. Chung, C. Qiu, P. Chu, R. Gadh, Smart electric vehicle charging infrastructure overview, in: Proceedings of the IEEE PES Innovative Smart Grid Technologies Conference, 2014, pp. 1–5, Washington, DC, USA.
[26] X. Zhou, E. Dall'Anese, L. Chen, A. Simonetto, An incentive-based online optimization framework for distribution grids, IEEE Trans. Automat. Control 63 (7) (2017) 2019–2031.
[27] N. Rahbari-Asr, U. Ojha, Z. Zhang, M.-Y. Chow, Incremental welfare consensus algorithm for cooperative distributed generation/demand response in smart grid, IEEE Trans. Smart Grid 5 (6) (2014) 2836–2845.
[28] X. Huo, M. Liu, Privacy-preserving distributed multi-agent cooperative optimization—Paradigm design and privacy analysis, IEEE Control Syst. Lett. 6 (2022) 824–829.
[29] California Independent System Operator: Net demand trend, URL https://www.caiso.com/TodaysOutlook/Pages/default.aspx.