CPS: Medium: Ensure Privacy and Truthfulness in Self-interested Multi-agent Cyber-physical Systems

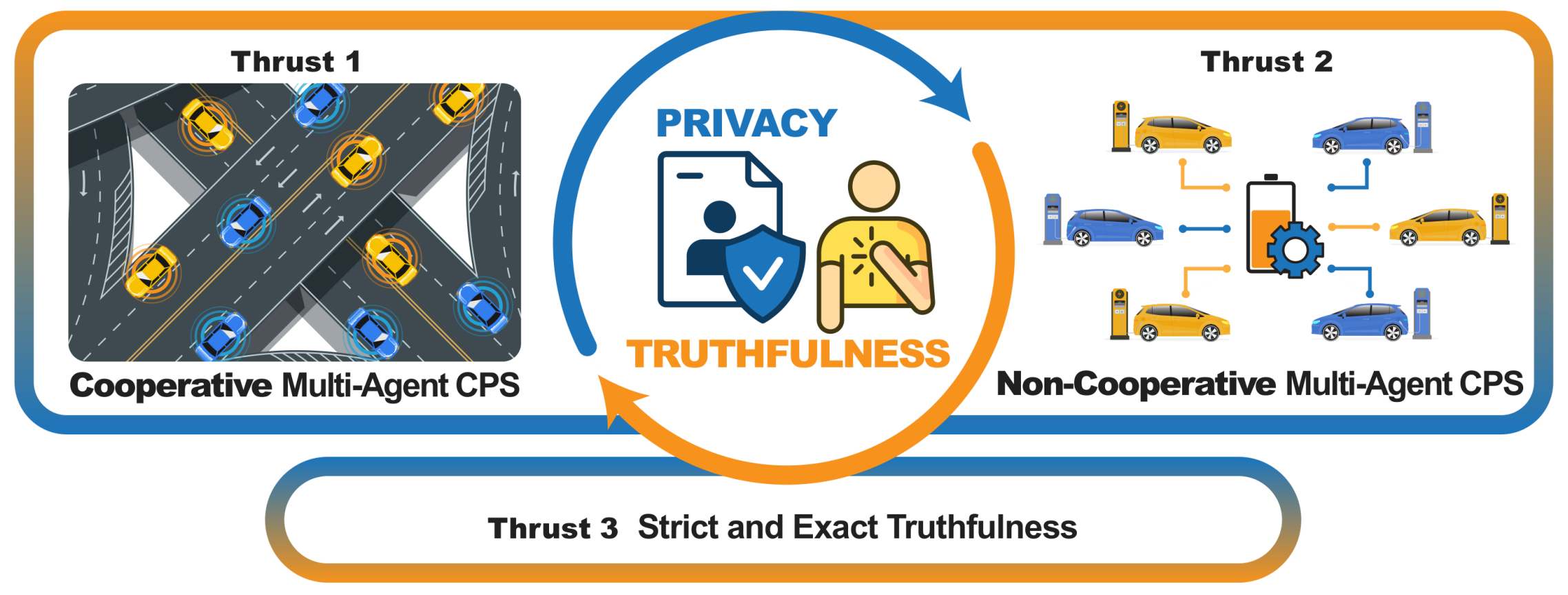
Yongqiang Wang[1] and Zhaojian Li[2]

1. Department of Electrical and Computer Engineering, Clemson University, Clemson, SC, 29634
2. Department of Mechanical Engineering, Michigan State University, East Lansing, MI 48824

Background and motivation

In many multi-agent CPS, the agents are self-interested and have individual costs and priorities that are not fully aligned with the global objective. For example, in distributed optimization based smart grid control, the network-level optimization goal is to minimize the cost of imbalance between power generation and the aggregate load while individual agents (customers) prioritize minimizing their own power usage costs. Similarly, in coordinated charging of electric vehicles (EV), network-level objectives usually focus on avoiding peak overload and filling the overnight valley in background power demand while individual EVs prioritize personal charging costs and completion times. Therefore, an opportunistic self-interested agent may be tempted to lie in information sharing to reduce its local cost. However, prevailing CPS models typically presume that all agents consistently share accurate and truthful information with one another, both in cooperative multi-agent optimization and noncooperative games, which could potentially result in suboptimal performance in practical scenarios. In this project, we delve into novel frameworks to simultaneously enforce privacy and truthfulness in self-interested multi-agent CPS. We study privacy and truthfulness together because 1) privacy needs truthfulness: privacy of data only makes sense under truthfulness as protecting the privacy of false data is superfluous; and 2) truthfulness also needs privacy: privacy is an important approach to promoting truthfulness since without privacy protection, agents are disinclined to truthfully share sensitive information.

Research Goal


Thrust 1
Cooperative Multi-Agent CPS
PRIVACY
TRUTHFULNESS
Thrust 2
Non-Cooperative Multi-Agent CPS
Thrust 3 Strict and Exact Truthfulness

Thrusts

1) We will develop a novel privacy scheme to ensure DP and promote truthfulness in general distributed constrained optimization without compromising accuracy
2) We will consider non-cooperative multi-agent CPS and develop novel privacy-preserving and truthfulness-promoting schemes for Nash equilibrium seeking in constrained multi-agent games.
3) We will also leverage the relation between DP and truthfulness to promote truthful behaviors of agents

Research Description

Private and Truthful Distributed Optimization for Multi-agent CPS

Background and state-of-the-art:

1. Privacy has become a primary concern in many multi-agent CPS. For example, in power systems, the shared real-time usage data can expose consumers' personal habits. The problem is more acute in multi-agent learning, where using shared model updates/gradients, adversaries have been proven able to precisely recover the raw training data (pixel-wise accurate for images). While numerous DP solutions have been proposed for distributed optimization and learning, all these findings necessitate a compromise on convergence accuracy to uphold privacy in the infinite time horizon (ensuring a finite privacy budget as the number of iterations tends towards infinity), a trade-off unsuitable for many CPS demanding high accuracy and performance.
2. Truthfulness considers the problem where agents are opportunistic and can be dishonest when sharing information. Having been intensively studied in game theory, it is also receiving increased attention in multi-agent CPS. A typical application example is in EV charging, where a user may untruthfully report its specifications and/or deviate from the prescribed charging schedule due to potential to reduce its own cost or concerns on privacy.

Outline of the proposed research:

$$\min J(x_1,\ldots,x_m) \quad \text{s.t.} \quad x_i \in \mathcal{X}_i \quad \text{and} \quad \textstyle\sum_{i=1}^{m} g_i(x_i) \leq 0$$

The key idea of our approach to successfully ensure both accurate convergence and rigorous DP in distributed unconstrained optimization is to incorporate a decaying factor in inter-agent interaction to gradually attenuate the influence of DP noises.

$$y_i^{k+1}=(1-\theta^k)y_i^k+\chi^k\textstyle\sum_{j\in\mathbb{N}_i}w_{ij}(y_j^k+\xi_j^k-y_i^k)+f_i(x_i^{k+1})-(1-\theta^k)f_i(x_i^k),$$
$$z_i^{k+1}=(1-\theta^k)z_i^k+\chi^k\textstyle\sum_{j\in\mathbb{N}_i}w_{ij}(z_j^k+\upsilon_j^k-z_i^k)+g_i(x_i^{k+1})-(1-\theta^k)g_i^k(x_i^k).$$

Private and Truthful Games for Multi-agent CPS

Background and state-of-the-art:

1. In many self-interested multi-agent CPS, agents are not interested in optimizing a network-level objective function. Instead, individual agents have their own cost functions and are only interested in minimizing their respective cost functions. In general, not only does the cost function of an agent depend on its own action, it is also affected by the actions of other agents. Therefore, the behaviors of agents naturally fall within the framework of a game and the goal of network design becomes the computation of a Nash equilibrium (NE). Typical examples include allocation of EVs to charging stations, coordination of mobile sensor networks, power control of optical networks, and many others.

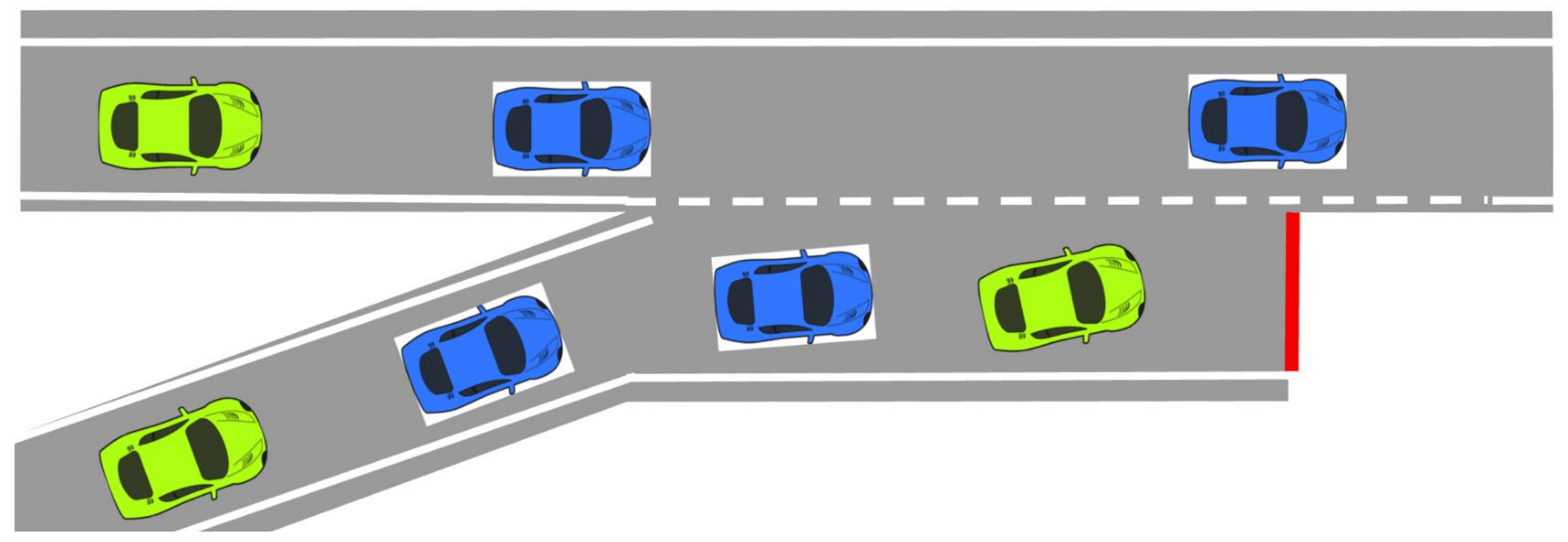
Outline of the proposed research:

$$\min_{x_i} J_i(x_i,x_{-i}) \quad \text{s.t.} \quad x_i \in \Omega_i \text{ and } C_i x_i - c_i \leq \textstyle\sum_{j\neq i, j\in[m]} c_j - C_j x_j$$

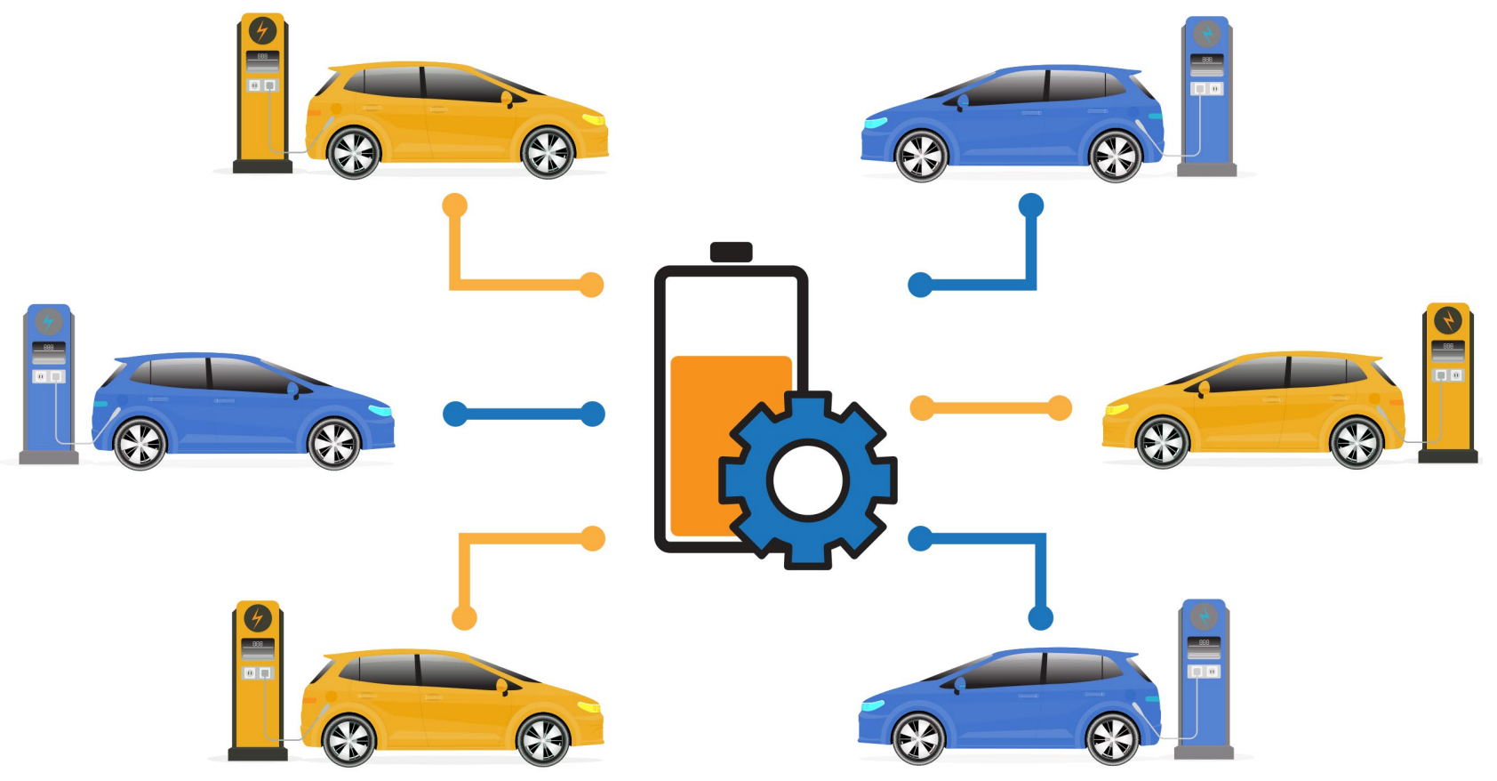
We will investigate how to ensure DP in the proposed GNE seeking problem. Compared with NE seeking in the absence of coupling constraints, the shared coupling constraints in GNE seeking increase attack surfaces, and hence, pose additional challenges to privacy protection. Since the key of our approach to retain provable convergence is to leverage a decaying factor in inter-agent interaction to gradually eliminate the influence of DP noises, we will investigate incorporating a decaying factor in the inter-agent interaction of existing GNE seeking algorithms.

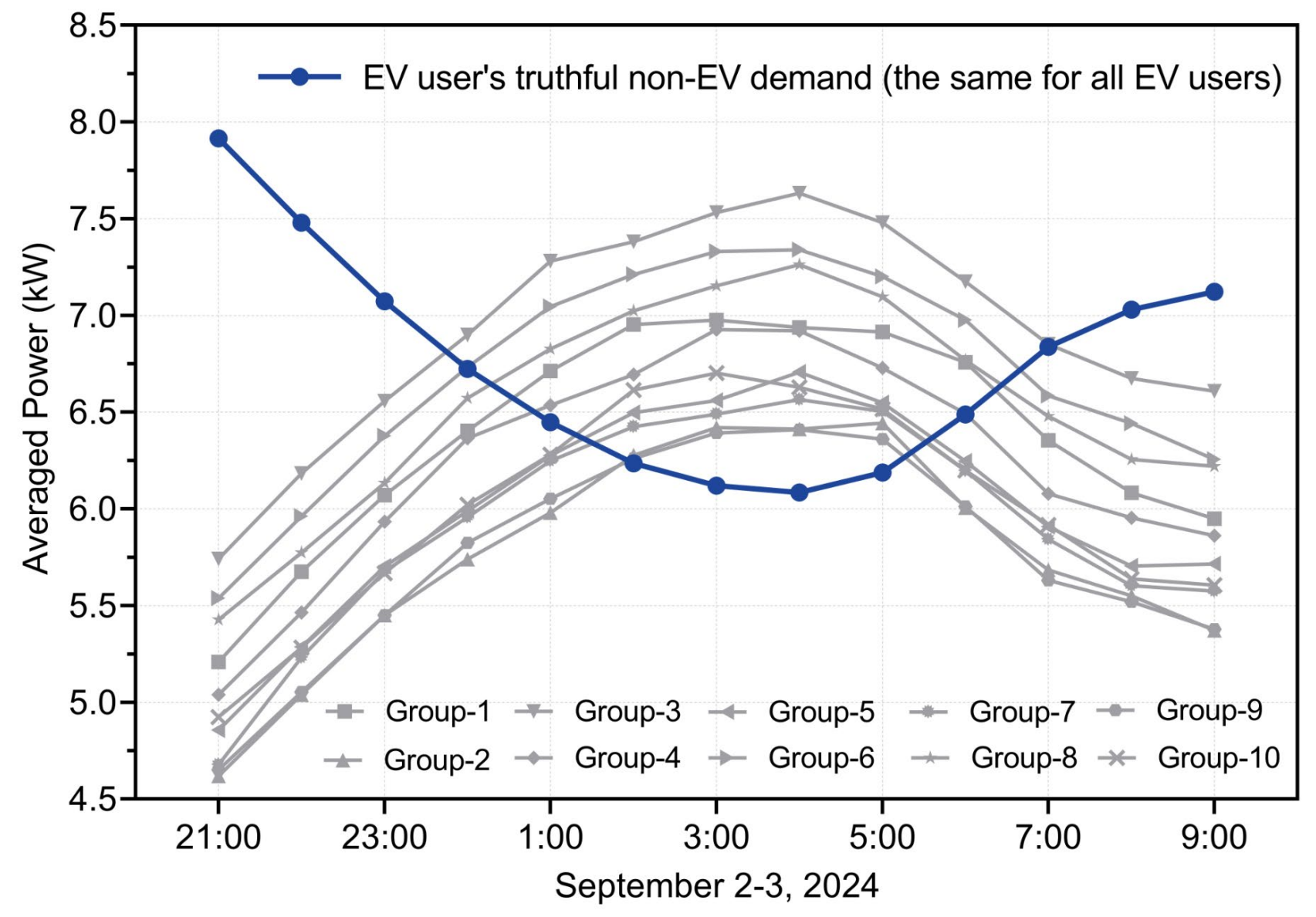
Evalutions

Cooperative CAV ramp merging

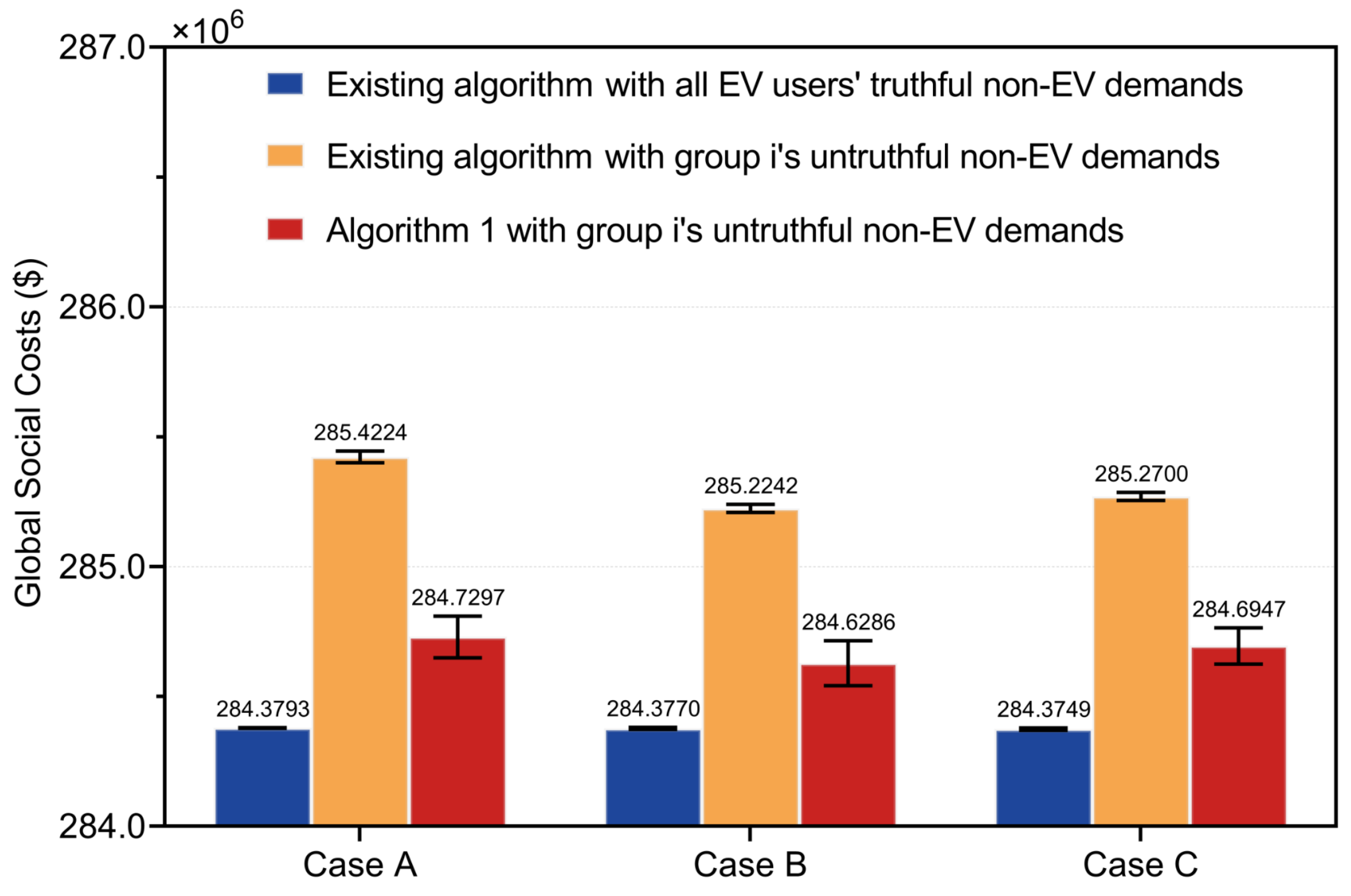


Coordinated EV charging





Some Results



(d) The global social costs after $4,000$ iterations