Exploration of For-Purpose Decentralized Algorithmic Cyber Attacks in EV Charging Control

Mahan Fakouri Fard*, Xiang Huo†, Mingxi Liu‡
Department of Electrical & Computer Engineering
University of Utah
Salt Lake City, UT
{*mahan.fakourifard, †xiang.huo, ‡mingxi.liu}@utah.edu

2023 IEEE 32nd International Symposium on Industrial Electronics (ISIE) | 979-8-3503-9971-4/23/$31.00 ©2023 IEEE | DOI: 10.1109/ISIE51358.2023.10227968

***Abstract*—Distributed and decentralized multi-agent optimization (DMAO) algorithms enable the control of large-scale grid-edge resources, such as electric vehicles (EVs), to provide power grid services. Despite its great scalability, DMAO is fundamentally prone to cyber attacks as it is highly dependent on frequent peer-to-peer communications. Existing cyber-security research in this regard mainly focuses on *broad-spectrum* attacks aiming at jeopardizing the entire control system while losing the possibility of achieving specific attacking purposes. This paper, for the first time, explores novel *for-purpose* algorithmic attacks that are launched by participating agents and interface with DMAO to achieve self-interest attack purposes. A decentralized EV charging control problem is formulated as an illustrative use case. Theoretical *for-purpose* attack vectors with and without the stealthy feature are devised. Simulations on EV charging control show the practicability of the proposed algorithmic *for-purpose* attacks and the impacts of such attacks on distribution networks.**

***Index Terms*—algorithmic cyber attack, cyber security, decentralized optimization, EV charging control.**

I. Introduction

The ever-growing electric vehicle (EV) penetration demands advanced control mechanisms to alleviate the negative impacts on distribution networks and increase power system flexibility [1]. Despite the related research progress, scalability and cyber security remain two major barriers to the large-scale deployment of EV charging control [2], [3]. Control scalability ensures a timely engagement of significant power flexibility for grid service participation, while cyber security ensures data integrity as well as reliability of the distribution network.

Centralized control structures, due to the curse of scalability, are not suitable for large-scale EV charging control. In contrast, distributed and decentralized multi-agent optimization (DMAO) has presented outstanding scalability [4], [5] and is capable of integrating privacy-preserving measures [6], thus are attracting growing attention. In [4], [7], [8], the alternating direction method of multipliers (ADMM) was used to construct scalable distributed EV charging control schemes. In another research line, authors of [5], [9] developed the shrunken-primal-dual subgradient (SPDS) algorithms to construct decentralized EV charging control frameworks. Represented by ADMM and SPDS, DMAO algorithms have undoubtedly achieved control scalability, however, must rely on iterative updates and frequent peer-to-peer communication, leading these algorithms prone to cyber attacks.

In the presence of malicious parties, once the transmitted information is obtained, altered, or jeopardized, cyber attackers can easily breach the entire operating system. Like other controllable grid-edge devices, EVs and their supply equipment are connected via the internet of things and are highly dependent on communication systems, leading EV charging control systems vulnerable to data manipulations [10]. Cyber security in DMAOs has recently attracted attention due to the vast use of decentralized and distributed control in industrial applications [11]. However, only a few works have attempted to investigate algorithmic cyber attacks that are integrated into DMAOs. The first attempt was made in [12], where the weaknesses of ADMM-based methods to various algorithmic attack vectors, including local problem distortion, noise injection, and coupling constraint distortion, were explored. However, only iterative noise injection attacks for convergence jeopardy were investigated through convexity-based methods. Du *et al.* in [13] investigated the impacts of data deception and denial of service (DoS) on ADMM-based smart grid state estimation. Unfortunately, the proposed attacks have noticeable impacts on the system, thus lacking stealthiness.

Besides the limited advancement in algorithmic cyber attacks, two practical issues remain untouched in general cyber-security research. First, most existing work only focuses on *broad-spectrum* attacks, e.g., DoS and noise injection, that aim at jeopardizing control stability [3], lowering the algorithm performance [14], and/or preventing convergence [15]. These attacks, unfortunately, cannot be adopted by internal attackers, i.e., algorithm participants, who want to achieve personal goals but still follow the algorithm. Second, most existing attack vectors have observable impacts on the system or the false data injected by attackers are noticeable [13], [16], making them easy to be detected by general detection methods [17], [18]. Very few attempts were made to develop stealthy algorithmic attacks that are capable of concealing their impacts. In [19], a reachability-based synthesis was developed to generate transient attacks that find attack parameters to avoid detection. Despite the detection avoidance performance, the proposed cyber-attack can only be used for overall system jeopardy rather than personal gain.

In this paper, we focus on the stealthy *for-purpose* algorith-

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

mic attack that targets the DMAO iterations and can be imposed by algorithm participants. The contribution of this paper is three-fold: (1) A novel *for-purpose* algorithmic cyber attack, which allows attackers to manipulate the DMAO algorithm to gain sophisticated personal benefits, is explored; (2) Two practical self-interest attack vectors in EV charging control are investigated. Their corresponding impacts on the distribution network are analyzed; (3) A novel mechanism is developed to grant stealthy features to the proposed algorithmic attacks. The proposed methods are rather general for DMAO algorithms – EV charging control is used in this paper for better illustration.

II. EV Charging Control Scheme

A. Distribution network and EV charging model

This paper adopts the LinDisFlow model [20] to represent a linear relationship between EV charging power and squared nodal voltage magnitudes. In a distribution network with n buses, at time t, the LinDistFlow model gives

$$\boldsymbol{V}(t) = \boldsymbol{V}_0 - 2\boldsymbol{R}\boldsymbol{P}(t) - 2\boldsymbol{X}\boldsymbol{Q}(t), \tag{1}$$

where $\boldsymbol{P}(t) \in \mathbb{R}^n$ and $\boldsymbol{Q}(t) \in \mathbb{R}^n$ denote the real and reactive power consumption of all buses, respectively, $\boldsymbol{V}(t) \in \mathbb{R}^n$ contains the squared voltage magnitudes of all buses, and $\boldsymbol{V}_0 = V_0^2\mathbf{1}_n \in \mathbb{R}^n$ denotes the slack constant voltage magnitude vector with V_0 being the voltage magnitude at the feeder head. $\boldsymbol{R}$ and $\boldsymbol{X}$ are the adjacency matrices defined as

$$\begin{aligned} \boldsymbol{R} \in \mathbb{R}^{n\times n}, \quad R_{\nu\kappa} &= \sum_{(\nu,\kappa)\in\mathbb{E}_\nu\cap\mathbb{E}_\kappa} r_{\nu\kappa}, \\ \boldsymbol{X} \in \mathbb{R}^{n\times n}, \quad X_{\nu\kappa} &= \sum_{(\nu,\kappa)\in\mathbb{E}_\nu\cap\mathbb{E}_\kappa} x_{\nu\kappa}, \end{aligned} \tag{2}$$

where $r_{\nu,\kappa}$ and $x_{\nu,\kappa}$ are the resistance and reactance of line (ν,κ), respectively, and $\mathbb{E}_\nu$ and $\mathbb{E}_\kappa$ are the line sets connecting the feeder head to bus ν and κ, respectively [21].

The power consumption at each node consists of the baseline and EV charging load. Assuming the EVs only consume real power, at node l, we have $p_l(t) = p_{l,b}(t) + p_{l,EV}(t)$ and $q_l(t) = q_{l,b}(t)$, where $p_{l,b}(t)$, $q_{l,b}(t)$, and $p_{l,EV}(t)$ denote the real baseline power, reactive baseline power, and EV charging power, respectively. Let $\boldsymbol{V}_b(t)$ denote the squared voltage drop caused by the baseline load, (1) can be rewritten as

$$\boldsymbol{V}(t) = \boldsymbol{V}_0 - \boldsymbol{V}_b(t) - 2\boldsymbol{R}p_{EV}(t), \tag{3}$$

where $p_{EV}(t) = [p_{1,EV}(t)\ p_{2,EV}(t)\ \cdots\ p_{n,EV}(t)]^\mathsf{T}$. Suppose s_l EVs are connected to node l, we have $p_{l,EV}(t) = \sum_{\hat{l}=1}^{s_l} \tilde{P}_{l,\hat{l}}c_{l,\hat{l}}(t)$, where $c_{l,\hat{l}}(t)$ and $\tilde{P}_{l,\hat{l}}$ denote the charging rate and maximum charging power of the $\hat{l}$th EV connected to node l. Re-indexing $c_{l,\hat{l}}$ and $\tilde{P}_{l,\hat{l}}$ with $i = 1,\dots,s$ by following the ascending orders of l and $\hat{l}$, and defining $\boldsymbol{G} = \oplus_{l=1}^n \boldsymbol{G}_l \in \mathbb{R}^{n\times s}$ and $\tilde{\boldsymbol{P}} = \oplus_{i=1}^s \tilde{P}_i \in \mathbb{R}^{s\times s}$, we have

$$\boldsymbol{V}(t) = \boldsymbol{V}_0 - \boldsymbol{V}_b(t) - 2\boldsymbol{R}\boldsymbol{G}\tilde{\boldsymbol{P}}\boldsymbol{C}(t), \tag{4}$$

where $\boldsymbol{G}_l = \mathbf{1}_{s_l}^\mathsf{T}$ is the charging power aggregation vector, $\boldsymbol{C}(t) = [c_1(t)\ c_2(t)\ \cdots\ c_s(t)]^\mathsf{T} \in \mathbb{R}^s$, and $\oplus$ denotes matrix direct sum. Further let $\boldsymbol{D} \in \mathbb{R}^{n\times s}$ denote $-2\boldsymbol{R}\boldsymbol{G}\tilde{\boldsymbol{P}}$, $\boldsymbol{y}_d(t)$ denote $\boldsymbol{V}_0 - \boldsymbol{V}_b(t)$ and $\boldsymbol{y}(t)$ denote $\boldsymbol{V}(t)$, we have

$$\boldsymbol{y}(t) = \boldsymbol{y}_d(t) + \boldsymbol{D}\boldsymbol{C}(t). \tag{5}$$

Let $SOC_{i,ini}$ and $SOC_{i,des}$ denote the initial and the desired SOC of the ith EV, respectively, and $\hat{E}_i$ denotes the battery capacity of ith EV. Then the total battery energy required by the ith EV is $E_{i,req} = \hat{E}_i(SOC_{i,des} - SOC_{i,ini})$.

B. Valley filling problem

The goal of valley filling is to use the aggregated EV charging power to fill the overnight electricity use valley. The valley-filling problem can be modeled as an optimal power flow problem that minimizes the variance of the aggregated total load. Let T be the valley filling period, then the charging profile of the ith EV is represented as $\boldsymbol{\mathcal{C}}_i = [c_i(t)\ c_i(t+1)\ \cdots\ c_i(t+T-1)]^\mathsf{T} \in \mathbb{R}^T$. In a centralized fashion, let $\boldsymbol{\mathcal{C}} = [\boldsymbol{\mathcal{C}}_1^\mathsf{T}\cdots\boldsymbol{\mathcal{C}}_s^\mathsf{T}]^\mathsf{T} \in \mathbb{R}^{sT}$ denote the collection of all EVs' charging profiles, the valley-filling problem is formulated as

$$\min_{\boldsymbol{\mathcal{C}}}\ \mathcal{F}(\boldsymbol{\mathcal{C}}) = \frac{1}{2}\left\|\boldsymbol{P}_b + \sum_{i=1}^s \tilde{P}_i\boldsymbol{\mathcal{C}}_i\right\|_2^2 \tag{6a}$$

$$\text{s.t.}\ \ \boldsymbol{\mathcal{C}}_i \in \mathbb{C}_i,\ \forall i \in 1,2,...,s, \tag{6b}$$

$$\boldsymbol{\mathcal{Y}}_b - \sum_{i=1}^n \boldsymbol{\mathcal{D}}_i\boldsymbol{\mathcal{C}}_i \le \mathbf{0}, \tag{6c}$$

where $\boldsymbol{P}_b = [P_b(t)\ P_b(t+1)\ \cdots\ P_b(t+T-1)]^\mathsf{T} \in \mathbb{R}^T$ is the aggregated baseline load profile of the entire distribution network. The constraint set $\mathbb{C}_i$ guarantees the ith EV can be charged to the desired SOC by the end of the valley filling period, which takes the form of

$$\mathbb{C}_i := \{\boldsymbol{\mathcal{C}}_i | \mathbf{0} \le \boldsymbol{\mathcal{C}}_i \le \mathbf{1}, E_{i,req} - \hat{\boldsymbol{B}}_{i,l}\boldsymbol{\mathcal{C}}_i = 0\}, \tag{7}$$

where $\hat{\boldsymbol{B}}_{i,l} = \mathbf{1}_s\boldsymbol{B}_{i,l}$, $\boldsymbol{B}_{i,l} = [\boldsymbol{B}_{i,c}\ \boldsymbol{B}_{i,c}\ \cdots\ \boldsymbol{B}_{i,c}] \in \mathbb{R}^{s\times T}$, $\boldsymbol{B}_{i,c} \in \mathbb{R}^s$ denotes the the ith column of the matrix $\boldsymbol{B} = \oplus_{i=1}^s B_i$, $B_i = -\eta_i\Delta t\tilde{P}_i$, η_i is the charging efficiency, Δt is the sampling time, and $\mathbf{1}_s = [1\cdots1] \in \mathbb{R}^{1\times s}$. Eqn. (6c) ensures all nodal voltage magnitudes stay above the lower bound, where $\boldsymbol{\mathcal{Y}}_b$ denotes $\underline{v}^2\boldsymbol{V_0} - \boldsymbol{\mathcal{Y}}_d$, $\boldsymbol{\mathcal{Y}}_d = [y_d(t)\ y_d(t+1)\ \cdots\ y_d(t+T-1)]^\mathsf{T} \in \mathbb{R}^{nT}$, $\underline{v}$ is the bus voltage magnitude lower bound, $\boldsymbol{\mathcal{D}_i} = D_i \oplus D_i\cdots\oplus D_i \in \mathbb{R}^{sT\times T}$ denotes the mapping between EV charging power and the nodal voltage magnitudes, and $\boldsymbol{D} = [D_1\ D_2\ \cdots\ D_s]$.

C. Decentralized EV charging control

To achieve control scalability, we adopt SPDS [5] to solve (6) in a decentralized way. With the relaxed Lagrangian of problem (6) defined as

$$\mathcal{L}(\boldsymbol{\mathcal{C}},\boldsymbol{\lambda}) = \mathcal{F}(\boldsymbol{\mathcal{C}}) + \boldsymbol{\lambda}^\mathsf{T}\big(\boldsymbol{\mathcal{Y}}_b - \sum_{i=1}^n \boldsymbol{\mathcal{D}}_i\boldsymbol{\mathcal{C}}_i\big), \tag{8}$$

each EV iteratively updates the primal variable by following

$$\boldsymbol{\mathcal{C}}_i^{(k+1)} = \Pi_{\mathbb{C}_i}\left(\frac{1}{\tau_{\mathcal{C}}}\Pi_{\mathbb{C}_i}\left(\tau_{\mathcal{C}}\boldsymbol{\mathcal{C}}_i^{(k)} - \alpha_{i,k}\nabla_{\boldsymbol{\mathcal{C}}_i}\mathcal{L}(\boldsymbol{\mathcal{C}}^{(k)},\boldsymbol{\lambda}^{(k)})\right)\right), \tag{9}$$

where $\tau_{\mathcal{C}}$ is the primal shrinking parameter and $\alpha_{i,k}$ is the primal update step size. Similarly, SPDS iteratively updates the dual variable by following

$$\boldsymbol{\lambda}^{(k+1)} = \Pi_{\mathbb{D}}\left(\frac{1}{\tau_\lambda}\Pi_{\mathbb{D}}\left(\tau_\lambda \boldsymbol{\lambda}^{(k)} + \beta_k \nabla_\lambda \mathcal{L}(\boldsymbol{\mathcal{C}}^{(k)}, \boldsymbol{\lambda}^{(k)})\right)\right), \quad (10)$$

where $\boldsymbol{\lambda} \in \mathbb{R}^{nT}$ is the dual variable associated with (6c), τ_λ is the dual shrinking parameter, and $\beta_{i,k}$ is the dual update step size. Under Slater condition, $\mathbb{D}$ is non-empty [22].

By implementing SPDS in EV charging control, individual EV chargers only need to share their own $\boldsymbol{\mathcal{C}}_i^{(k)}$ with the system operator. The system operator computes the Lagrange gradient and $\boldsymbol{\lambda}^{(k)}$ and broadcasts them to all EVs. This process will continue until the tolerance $\|\boldsymbol{\mathcal{C}}^{(k+1)} - \boldsymbol{\mathcal{C}}^{(k)}\|_2$ drops below a threshold. The convergence of SPDS is proved in [5].

III. For-Purpose Algorithmic Cyber Attacks

As aforementioned, one common issue of existing cyber-attack studies is that the goals of the attackers are not self-beneficial or rather realistic, and because of the noticeable impacts, they are more likely detectable. To resolve this issue, we will devise a new algorithmic attack – *for-purpose* cyber attack, where the attacker injects deliberate data into the DMAO iterations to gain self-beneficial results without affecting algorithm convergence or making noticeable changes. The presented cyber attack enables multiple attack scenarios. Specifically, in EV charging control, EVs can inject sophisticated data into their own and/or others' communication channels to achieve personal benefits without affecting algorithm convergence. Due to the page limit, we only consider the scenario where attackers manipulate their own data.

A. Self-interest algorithmic attack vectors

Suppose the ith EV wants to pursue a self-interest objective represented as $\omega_1 \mathcal{G}(\boldsymbol{\mathcal{C}}_i)$, where $\omega_1 > 0$ denotes the power of the self-interest attack. We have the following theorems.

Theorem 1: An internal attacker who follows SPDS algorithm can deviate the optimal solution of the problem in (6) towards its convex interest function $\mathcal{G}(\boldsymbol{\mathcal{C}}_i)$ by only modifying its local primal update direction by $\omega_1 \nabla_{\boldsymbol{\mathcal{C}}_i} \mathcal{G}(\boldsymbol{\mathcal{C}}_i)$, i.e.,

$$\boldsymbol{\mathcal{C}}_i^{(k+1)} = \Pi_{\mathbb{C}_i}\left(\frac{1}{\tau_{\mathcal{C}}}\Pi_{\mathbb{C}_i}\left(\tau_{\mathcal{C}} \boldsymbol{\mathcal{C}}_i^{(k)} - \alpha_{i,k} \nabla_{\boldsymbol{\mathcal{C}}_i} \tilde{\mathcal{L}}(\boldsymbol{\mathcal{C}}^{(k)}, \boldsymbol{\lambda}^{(k)})\right)\right), \quad (11)$$

where $\tilde{\mathcal{L}}(\boldsymbol{\mathcal{C}}^{(k)}, \boldsymbol{\lambda}^{(k)}) = \mathcal{L}(\boldsymbol{\mathcal{C}}^{(k)}, \boldsymbol{\lambda}^{(k)}) + \omega_1 \mathcal{G}(\boldsymbol{\mathcal{C}}_i)$ while the algorithm convergence is guaranteed. ■

Proof: Locally modifying the ith EV's primal update as in (11) is equivalent to modifying the problem in (6) to

$$\min_{\boldsymbol{\mathcal{C}}} \ \mathcal{F}(\boldsymbol{\mathcal{C}}) + \omega_1 \mathcal{G}(\boldsymbol{\mathcal{C}}_i) \quad (12a)$$

$$\text{s.t.} \ \ (6b), \ (6c). \quad (12b)$$

Therefore, following the convergence proof of SPDS [5], as long as $\mathcal{G}(\boldsymbol{\mathcal{C}}_i)$ is convex and $\omega_1 > 0$, the algorithm convergence is guaranteed. Because the voltage constraints remain unchanged, the converged results satisfy the global voltage requirements. Since, in each iteration, the ith EV's primal update is re-directed to honor the descending direction of $\mathcal{G}(\boldsymbol{\mathcal{C}}_i)$, the converged results are in favor of the ith EV. □

Theorem 2: Given $\mathcal{G}(\boldsymbol{\mathcal{C}}_i) \geq 0$ for all feasible $\boldsymbol{\mathcal{C}}_i$, the optimal solution for the problem in (12) differs from the optimal solution for problem (6) and the difference is bounded by $\omega_1 \max\{\mathcal{G}(\boldsymbol{\mathcal{C}}), \forall \boldsymbol{\mathcal{C}_i} \in \mathbb{S}\}$. ■

Proof: Let $\boldsymbol{\mathcal{C}}^* \in \mathbb{R}^{sT\times 1}$ denote the optimal solution of the attack-free problem in (6) with feasible region $\mathbb{S}$, then

$$\mathcal{F}(\boldsymbol{\mathcal{C}}^*) \leq \mathcal{F}(\boldsymbol{\mathcal{C}}), \ \forall \boldsymbol{\mathcal{C}} \in \mathbb{S}. \quad (13)$$

Further, let $\hat{\boldsymbol{\mathcal{C}}}$ be the optimal solution of the attacked problem (12) with the same feasible region $\mathbb{S}$. Since for all feasible $\boldsymbol{\mathcal{C}}_i$, $\mathcal{G}(\boldsymbol{\mathcal{C}}_i) \geq 0$ and $\omega_1 > 0$, it follows that

$$\mathcal{F}(\hat{\boldsymbol{\mathcal{C}}}) \leq \mathcal{F}(\hat{\boldsymbol{\mathcal{C}}}) + \omega_1 \mathcal{G}(\hat{\boldsymbol{\mathcal{C}}}_i). \quad (14)$$

Therefore, it can be readily derived that

$$\mathcal{F}(\boldsymbol{\mathcal{C}}^*) \leq \mathcal{F}(\hat{\boldsymbol{\mathcal{C}}}) \leq \mathcal{F}(\hat{\boldsymbol{\mathcal{C}}}) + \omega_1 \mathcal{G}(\hat{\boldsymbol{\mathcal{C}}}_i), \quad (15)$$

indicating that the optimal value of the attack-free problem (6) is always no greater than the optimal value of the attacked problem (12). According to multi-objective optimization theories, a Pareto-optimal set is the set of all optimal solutions such that no other solution can improve one objective function without deteriorating another [23]. Therefore, based on (15), the Pareto-optimal set for $\mathcal{F}(\boldsymbol{\mathcal{C}}) + \omega_1 \mathcal{G}(\boldsymbol{\mathcal{C}}_i)$ will always contain the Pareto-optimal set for $\mathcal{F}(\boldsymbol{\mathcal{C}})$. Hence, $\boldsymbol{\mathcal{C}}^*$ and $\hat{\boldsymbol{\mathcal{C}}}$ cannot belong to the same Pareto-optimal set, and they must be different. Note that the upper bound for the total deviation from the original optimal solution after the attack is dependent on the attack function and power, $\mathcal{G}(\boldsymbol{\mathcal{C}}_i)$ and ω_1. Generally, based on (15), this upper bound can be calculated as

$$\mathcal{F}(\boldsymbol{\mathcal{C}}^*) - \mathcal{F}(\hat{\boldsymbol{\mathcal{C}}}) \leq \omega_1 \mathcal{G}(\hat{\boldsymbol{\mathcal{C}}}_i) \leq \omega_1 \max\{\mathcal{G}(\boldsymbol{\mathcal{C}}_i), \forall \boldsymbol{\mathcal{C}} \in \mathbb{S}\}. \quad (16)$$

□

The assumption of non-negative self-interest objective in **Theorem 2** is generally true for most attacking purposes. In what follows, we present two possible scenarios. Linear $\mathcal{G}(\boldsymbol{\mathcal{C}}_i)$ that may violate this assumption will be studied in future work.

1) Smooth-charging attack: In this case, the ith EV aims to converge to a relatively smoother charging profile to preserve the battery's state of health (SOH). To this end, the ith EV can modify its local primal update to

$$\boldsymbol{\mathcal{C}}_i^{(k+1)} = \Pi_{\mathbb{C}_i}\Bigg(\frac{1}{\tau_{\mathcal{C}}}\Pi_{\mathbb{C}_i}\big(\tau_{\mathcal{C}} \boldsymbol{\mathcal{C}}_i^{(k)} - \alpha_{i,k} \nabla_{\boldsymbol{\mathcal{C}}_i} \mathcal{L}(\boldsymbol{\mathcal{C}}^{(k)}, \boldsymbol{\lambda}^{(k)}) - 2\alpha_{i,k}\omega_1 \boldsymbol{\mathcal{C}}_i^{(k)}\big)\Bigg). \quad (17)$$

As shown in the proof of **Theorem 1**, if the ith EV injects $2\omega_1 \boldsymbol{\mathcal{C}}_i^{(k)}$ in every iteration, the overall EV charging control problem is equivalent to adding $\omega_1 \|\boldsymbol{\mathcal{C}}_i\|_2^2$ to the objective function to flatten the ith EV's charging profile. The impacts of the charging profile change of the ith EV on the valley-filling performance will be compensated for by other EVs.

2) Rush-charging attack: In this scenario, the ith EV aims to charge as soon as possible. To this end, it needs to inject $2\omega_1 \boldsymbol{A}^\top \boldsymbol{A}\boldsymbol{\mathcal{C}}_i^{(k)}$ at each primal update iteration, where $\boldsymbol{A} \in \mathbb{R}^{T\times T}$ is a diagonal matrix with each element

$$A_{\hat{t},\hat{t}} = \begin{cases} m, & \text{if } \hat{t} \le t_d \\ M, & \text{otherwsie} \end{cases} \tag{18}$$

Herein, $0 < m \ll M$ and t_d denotes the attacker's desired termination time to reach $SOC_{i,des}$. According to **Theorem 1**, this is equivalent to adding $\omega_1 \|\boldsymbol{A}\boldsymbol{\mathcal{C}}_i\|_2^2$ to the objective function of problem (6). Entries in $\boldsymbol{A}$ with smaller values will force the corresponding elements in $\boldsymbol{\mathcal{C}}_i$ to be maximized, and *vice versa*, to achieve the rush-charging goal.

B. Stealthy for-purpose algorithmic attack vector

Though the attack vectors developed in Section III-A can assist individual EVs to attain self-interest objectives, according to **Theorem 2**, the deviations in the objective value, reflected by the impaired valley filling performance, may inform the system operator about the existence of cyber attacks. Therefore, in order to remain stealthy, it is critical to develop an attacking mechanism to minimize the deviation of the post-attack results from the true optimal solution. To this end, it is ideal for the ith EV to launch an attack that equivalently converts the EV charging control problem (6) to

$$\min_{\boldsymbol{\mathcal{C}}} \ \mathcal{F}(\boldsymbol{\mathcal{C}}) + \omega_1 \mathcal{G}(\boldsymbol{\mathcal{C}}_i) + \omega_2 \|\boldsymbol{\mathcal{C}} - \boldsymbol{\mathcal{C}}^*\|_2^2 \tag{19a}$$

$$\text{s.t. (6b), (6c),} \tag{19b}$$

where $\boldsymbol{\mathcal{C}}^*$ denotes the true optimal solution of problem (6).

To realize this, the ith EV needs to inject $\omega_1 \nabla_{\boldsymbol{\mathcal{C}}_i} \mathcal{G}(\boldsymbol{\mathcal{C}}_i^{(k)}) + 2\omega_2 \boldsymbol{I}_i^\top (\boldsymbol{\mathcal{C}}^{(k)} - \boldsymbol{\mathcal{C}}^{(\ell)})$ into its primal update, where $\boldsymbol{I}_i \in \mathbb{R}^{sT\times T}$ denotes a block matrix whose ith block is an identity matrix $\boldsymbol{I} \in \mathbb{R}^{T\times T}$ and others are zeros. Two challenges exist: First, the attacker is not able to obtain $\boldsymbol{\mathcal{C}}^*$ after launching the attacks. Second, the second term in the injected malicious data requires knowledge of other EVs' intermediate decision variables. Herein, for the purpose of exploring the existence of stealthy algorithmic attacks, we assume that an attacker is capable of wiretapping the communication channels between other EVs and the system operator, which resolves the second challenge. This assumption will be lifted in future work.

Though it is impossible to obtain $\boldsymbol{\mathcal{C}}^*$ of the attack-free problem, it is possible for the ith EV to make an estimation. In the convergence of DMAO algorithms, with an overwhelming possibility, all decision variables converge or meet the stopping criterion at the same time. Based on this, the ith EV (the attacker) first pre-determines a threshold ϵ_{att}^* for the difference between two consecutive iterations $\epsilon_{att}^{(\ell)} = \|\boldsymbol{\mathcal{C}}_i^{(\ell+1)} - \boldsymbol{\mathcal{C}}_i^{(\ell)}\|_2$. At the beginning of valley filling, the ith EV allows the algorithm to run normally without launching any attack. As the iteration goes, once $\epsilon_{att}^{(\ell)}$ drops below ϵ_{att}^* in the ℓth iteration, the ith EV regards the algorithm "converged" and wiretaps other EVs' communication channels to obtain $\boldsymbol{\mathcal{C}}^{(\ell)}$ which will be used as an approximation of $\boldsymbol{\mathcal{C}}^*$. At any iteration k after the $(\ell+1)$th iteration, the ith EV launches the stealthy attack by injecting $\omega_1 \nabla_{\boldsymbol{\mathcal{C}}_i} \mathcal{G}(\boldsymbol{\mathcal{C}}_i^{(k)}) + 2\omega_2 \boldsymbol{I}_i^\top (\boldsymbol{\mathcal{C}}^{(k)} - \boldsymbol{\mathcal{C}}^{(\ell)})$ into its primal update.

By implementing this stealthy attacking mechanism, the attacker can achieve personal benefit while manipulating the post-attack converged solution to be close enough to the original optimal solution that the system operator is hard to detect any unusual anomaly. The attackers could tune the stealthy level ω_2 in addition to their personal benefit attack power ω_1 to balance the trade-off between gaining extra personal benefits and being more stealthy.

Remark 1: ϵ_{att}^* should not be too small, i.e., the approximation cannot be too accurate; otherwise, the algorithm would stop at full convergence before the ith EV launches the attack.

Remark 2: The attacker must continuously wiretap other EVs' communication channels after the ℓth iteration.

IV. Simulation Results

The performance of different *for-purpose* attacks will be demonstrated through simulations of controlling 500 EVs connected to a modified IEEE 13-bus test feeder [5]. Note that, Nodes 1 and 6 have no EV connected, and each of the other nodes is connected with 50 EVs equipped with level-2 chargers, i.e., $\tilde{P}_i = 6.6$ kW. Battery capacities are uniformly distributed in $[18, 20]$ kWh. Initial and designated SOCs are uniformly distributed in $[0.3, 0.5]$ and $[0.7, 0.9]$, respectively. Primal and dual step sizes are empirically tuned to $\alpha_{i,k} = 2.8 \times 10^{-10}$ and $\beta_k = 1.8$, respectively. The shrinking parameters are empirically chosen as $\tau_{\boldsymbol{\mathcal{C}}} = \tau_{\boldsymbol{\lambda}} = 0.974$. The maximum iteration number is set to $k_{max} = 25$. The convergence tolerance is chosen as $\epsilon = 1 \times 10^{-4}$. The voltage lower bound is set to 0.954 p.u. The valley-filling period is from 19:00 to 8:00 the next day, which has been divided into 52 time periods with 15-minute lengths. The baseline load data is scaled while collected from Southern California Edison [24].

A. Attack-free scenario

By running SPDS to solve the attack-free problem in (6), the charging profiles of all 500 EVs are shown in Fig. 1. It can be

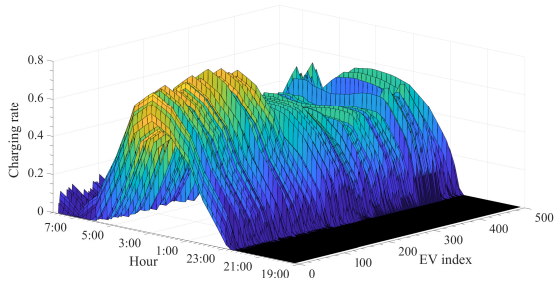

Fig. 1. Charging profiles of all EVs in the attack-free scenario.

readily observed that all EVs stay idle before 22:30 and start charging after that to fill the valley. If EVs are grouped into four groups, i.e., Group 1 (1-200), Group 2 (201-300, 451-500), Group 3 (301-400), and Group 4 (401-450), according to their geographic locations, we can notice that the charging profiles of EVs in the same group have the same trend. The valley filing performance and the nodal voltage magnitudes

under the attack-free scenario are shown in Fig. 2 and Fig. 3, respectively. It can be observed that the total load profile

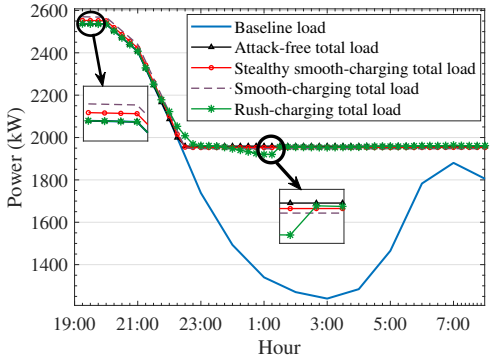

Fig. 2. Baseline load and total load under different attacks.

becomes flat and stays at $1,958$ kW after 22:30, and all nodal voltage magnitudes are maintained above 0.954 p.u.

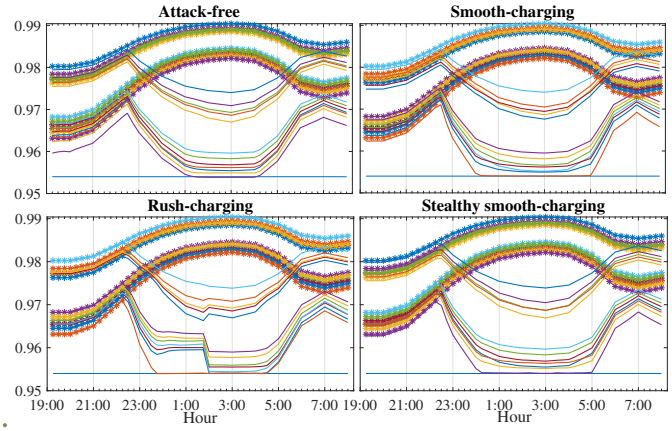

Fig. 3. Nodal voltage magnitudes. Star-marked lines represent the baseline case, and solid lines represent the case with controlled EV charging loads.

B. Smooth-charging attack

To better illustrate the smooth-charging attack, the first 50 EVs are selected as attackers. The self-interest attack power is set to $\omega_1 = 1 \times 10^5$ to make attacking impacts observable. Fig. 4 shows the charging profiles of all EVs, where the attackers

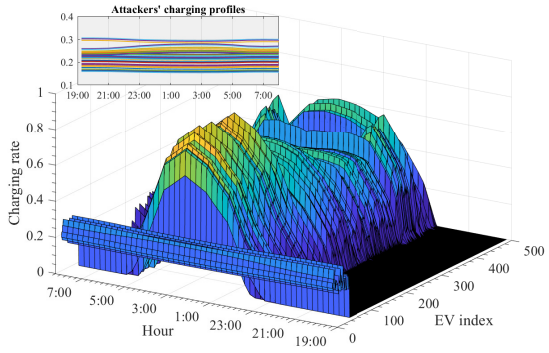

Fig. 4. Charging profile of all EVs under smooth-charging attacks.

charge for all the time periods at almost a constant charging rate between 0.15 to 0.3. Meanwhile, the charging profiles of other EVs have no significant changes. Non-attacker EVs in the first Group charge at higher rates from 00:00 to 4:00 in contrast to the attack-free scenario as they need to compensate for the 50 attackers in achieving valley filling.

As shown in Fig. 2, the valley filling objective can still be fulfilled under smooth-charging attacks. However, unlike the attack-free scenario, the controlled total load is slightly higher than the baseline load before 22:15 as the attackers start charging from the beginning. The flat value of the total load after 22:30 is 0.5% lower than that of the attack-free scenario. The voltage behaviors under smooth-charging attacks are similar to those in the attack-free scenario, which can be found in Fig. 3. If the system operator only monitors the nodal voltages, this attack is not making any suspicious impact.

C. Rush-charging attack

To better illustrate the rush-charging attack, 50 EVs in Group 4 are selected as attackers. The self-interest attack power is set to $\omega_1 = 1$, while $t_d = 25$, $m = 0.2$, and $M = 1 \times 10^5$. Fig. 5 shows the charging profiles of all EVs

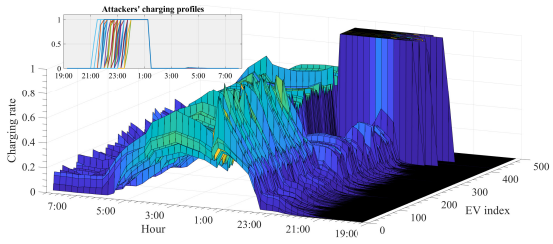

Fig. 5. Charging profile of all EVs under rush-charging attacks.

in this scenario. It can be observed that the attackers in Group 4 start to charge at full power starting from 21:00 until they reach their SOC_{des} before 2:00. The spike increase in the charging profiles of these 50 EVs led to lower EV charging rates in Groups 2 and 3 during the attacking period.

The valley-filling performance under rush-charging attack can be found in Fig. 2, which presents the impaired performance. The total load is not entirely flattened, with the maximum value hitting $1,920$ kW while the final value being $1,961$ kW. Unlike the smooth-charging attack, the voltage behaviors are very distinguishable in this case, as shown in Fig. 3. Though all the nodal voltages are still above 0.954 p.u., sudden drops and increases exist due to the rush charging.

D. Stealthy smooth-charging attack

In this case, ϵ^*_{att} is set to 1.1×10^{-4}, leading the attacker to choose $\boldsymbol{c}^{(19)}$ as the approximated optimal solution. We adopt the same setup for the smooth-charging attack of the first 50 EVs and set the stealthy attack power to $\omega_2 = 100$. The charging profiles of all EVs in this scenario can be found in Fig. 6, which shows smooth charging is realized for the first 50 EVs. The charging profiles of the attackers also follow the trend of other EVs in Group 1, which differentiates from the results shown in Fig. 4.

The optimal values, i.e., the value of $\mathcal{F}(\cdot)$, under the attack-free, non-stealthy smooth-charging attack, and stealthy

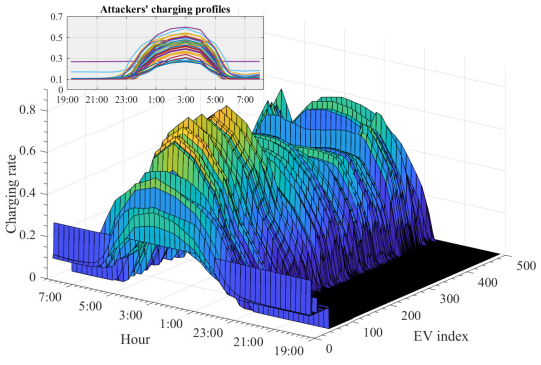

Fig. 6. Charging profiles of all EVs under stealthy smooth-charging attacks.

smooth-charging attack scenarios are 8.48866×10^6, 8.5089×10^6, and 8.5022×10^6, respectively, where the differences are unnoticeable. Let $\boldsymbol{\mathcal{C}}^*$ denote the attack-free optimal solution and define $\zeta = \|\hat{\boldsymbol{\mathcal{C}}} - \boldsymbol{\mathcal{C}}^*\|_2$ as an indicator for stealthiness where $\hat{\boldsymbol{\mathcal{C}}}$ is the optimal solution under attacks. The values of ζ under the non-stealthy smooth-charging attack and stealthy smooth-charging attack scenarios are 13.02 and 6.44, respectively, indicating 49% improvement in stealthiness.

The valley filling performance and nodal voltage behaviors are shown in Fig. 2 and Fig. 3, respectively. Compared with the non-stealthy case, less total load deviation at the beginning can be observed. At 21:30, the total loads of the non-stealthy and stealthy scenarios are $2,570$ kW and $2,553$ kW, respectively, while the baseline load is $2,537$ kW, indicating 48% lower load deviation. Compared to that of the non-stealthy case, the nodal voltages in the stealthy case have around 57% less deviation from the attack-free case. These results imply that the proposed stealthy attacking mechanism can effectively reduce the deviations from the truly optimal operation, thus improving attacking stealthiness.

V. Conclusion

This paper inaugurated *for-purpose* algorithmic attacks that target general DMAO algorithms. By utilizing the *for-purpose* algorithmic attacks, algorithm participants can achieve self-interest purposes without affecting the algorithm convergence. Attack vectors with and without the stealthy feature were theoretically investigated and illustrated through a decentralized EV charging control problem. The efficacy of the proposed *for-purpose* algorithmic attack was verified through EV charging control simulations. This paper is one of the first steps in bringing awareness of cyber attacks launched by DMAO participants and integrated into the algorithms. Comprehensive theoretical analyses will be provided in future work.

References

[1] C. Jin, J. Tang, and P. Ghosh, "Optimizing electric vehicle charging: A customer's perspective," *IEEE Transactions on Vehicular Technology*, vol. 62, no. 7, pp. 2919–2927, 2013.

[2] 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.

[3] Y. Cao, O. Kaiwartya, R. Wang, T. Jiang, Y. Cao, N. Aslam, and G. Sexton, "Toward efficient, scalable, and coordinated on-the-move EV charging management," *IEEE Wireless Communications*, vol. 24, no. 2, pp. 66–73, 2017.

[4] X. Zhou, S. Zou, P. Wang, and Z. Ma, "ADMM-based coordination of electric vehicles in constrained distribution networks considering fast charging and degradation," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 1, pp. 565–578, 2021.

[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] C. Zhang, M. Ahmad, and Y. Wang, "ADMM based privacy-preserving decentralized optimization," *IEEE Transactions on Information Forensics and Security*, vol. 14, no. 3, pp. 565–580, 2018.

[7] B. Khaki, C. Chu, and R. Gadh, "Hierarchical distributed framework for EV charging scheduling using exchange problem," *Applied Energy*, vol. 241, pp. 461–471, 2019.

[8] H. Fan, C. Duan, C.-K. Zhang, L. Jiang, C. Mao, and D. Wang, "ADMM-based multiperiod optimal power flow considering plug-in electric vehicles charging," *IEEE Transactions on Power Systems*, vol. 33, no. 4, pp. 3886–3897, 2018.

[9] 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.

[10] C. Chen, K. Zhang, K. Yuan, L. Zhu, and M. Qian, "Novel detection scheme design considering cyber attacks on load frequency control," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 5, pp. 1932–1941, 2018.

[11] A. H. Sodhro, S. Pirbhulal, M. Muzammal, and L. Zongwei, "Towards blockchain-enabled security technique for industrial internet of things based decentralized applications," *Journal of Grid Computing*, vol. 18, pp. 615–628, 2020.

[12] E. Munsing and S. Moura, "Cybersecurity in distributed and fully-decentralized optimization: Distortions, noise injection, and ADMM," *arXiv preprint arXiv:1805.11194*, 2018.

[13] D. Du, X. Li, W. Li, R. Chen, M. Fei, and L. Wu, "ADMM-based distributed state estimation of smart grid under data deception and denial of service attacks," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 49, no. 8, pp. 1698–1711, 2019.

[14] Y. Liu, O. Ardakanian, I. Nikolaidis, and H. Liang, "False data injection attack on electric vehicle-assisted voltage regulation," *arXiv preprint arXiv:2203.05087*, 2022.

[15] X. Liu, Z. Li, and Z. Li, "Optimal protection strategy against false data injection attacks in power systems," *IEEE Transactions on Smart Grid*, vol. 8, no. 4, pp. 1802–1810, 2017.

[16] J. Su, C. Xie, P. Dehghanian, and S. Mehrani, "Optimal defense strategy against load redistribution attacks under attacker's resource uncertainty: A trilevel optimization approach," in *2023 IEEE PES Grid Edge Technologies Conference & Exposition*, San Diego, CA, USA, Apr. 10-13 2023, pp. 1–5.

[17] K. Chatterjee, V. Padmini, and S. A. Khaparde, "Review of cyber attacks on power system operations," in *Proceedings of IEEE Region 10 Symposium*, Cochin, India, July 14-16 2017, pp. 1–6.

[18] I. A. Khan, D. Pi, Z. U. Khan, Y. Hussain, and A. Nawaz, "HML-IDS: A hybrid-multilevel anomaly prediction approach for intrusion detection in SCADA systems," *IEEE Access*, vol. 7, pp. 89 507–89 521, 2019.

[19] Z. Huang, S. Etigowni, L. Garcia, S. Mitra, and S. Zonouz, "Algorithmic attack synthesis using hybrid dynamics of power grid critical infrastructures," in *Proceedings of the Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, Luxembourg, Luxembourg, June 25-28 2018, pp. 151–162.

[20] M. Baran and F. Wu, "Optimal capacitor placement on radial distribution systems," *IEEE Transactions on Power Delivery*, vol. 4, no. 1, pp. 725–734, 1989.

[21] M. Farivar, L. Chen, and S. Low, "Equilibrium and dynamics of local voltage control in distribution systems," in *Proceedings of the IEEE Conference on Decision and Control*, Firenze, Italy, Dec. 10-13 2013, pp. 4329–4334.

[22] J. Koshal, A. Nedić, and U. V. Shanbhag, "Multiuser optimization: Distributed algorithms and error analysis," *SIAM Journal on Optimization*, vol. 21, no. 3, pp. 1046–1081, 2011.

[23] P. Ngatchou, A. Zarei, and A. El-Sharkawi, "Pareto multi objective optimization," in *Proceedings of the International Conference on, Intelligent Systems Application to Power Systems*, Arlington, VA, USA, Nov. 06-10 2005, pp. 84–91.

[24] Southern California Edison, 2011. [Online]. Available: https://www.sce.com/005_regul_info/eca/DOMSM11.DLP