

Adversarially and Distributionally Robust Virtual Energy Storage Systems via the Scenario Approach

Georgios Pantazis, Nicola Mignoni, Raffaele Carli, Mariagrazia Dotoli, Sergio Grammatico

Abstract—We propose an optimization model where a parking lot manager (PLM) can aggregate parked EV batteries to provide virtual energy storage services that are provably robust under uncertain EV departures and state-of-charge caps. Our formulation yields a data-driven convex optimization problem where a prosumer community agrees on a contract with the PLM for the provision of storage services over a finite horizon. Leveraging recent results in the scenario approach, we certify out-of-sample constraint safety. Furthermore, we enable a tunable profit-risk trade-off through scenario relaxation and extend our model to account for robustness to adversarial perturbations and distributional shifts over Wasserstein-based ambiguity sets. All the approaches are accompanied by tight finite-sample certificates. Numerical studies demonstrate the out-of-sample and out-of-distribution constraint satisfaction of our proposed model compared to the developed theoretical guarantees, showing their effectiveness and potential in robust and efficient virtual energy services.

I. INTRODUCTION

Repurposing electric vehicle (EV) charging facilities in parking lots as *virtual energy storage systems* (VESS) allows the distribution system operator (DSO) to leverage EV aggregation for the provision of services to prosumers, which can enhance stability and reduce costs of purchasing physical storage facilities from the prosumers' side [1]–[3]. At the same time, recent advances in optimization under uncertainty can assist parking lot managers with making better informed decisions. Though early studies have shown that fleets of EVs can emulate dispatchable resources when state-of-charge dynamics and availability are respected, most rely on deterministic or parametric uncertainty models that do not take into account day-to-day variability in arrivals, departures, and user preferences [4]–[6]. This motivates the recent shift towards data-driven, distribution-free formulations with explicit finite-sample guarantees for out-of-sample feasibility and performance [7], [8].

Scenario optimization [9], [10], allows solving semi-infinite robust optimization problems by approximating them

with a tractable program built from sampled scenarios [11], [12]. Standard results provide *a priori* bounds on violation probabilities in terms of decision dimension and sample size, while more recent *a posteriori* bounds leverage the number of support constraints to tighten the provided guarantees [13], [14]. The approach adopted here builds mainly upon the *a posteriori* philosophy due to its potential to provide tighter guarantees, given that the training data is usually known. Providing guarantees for EV charging parking lots leveraging the scenario approach can be found in [15]–[18] where uncertain operating constraints are considered and probabilistic safety guarantees are provided for feasible deviations from the optimal solution. However, such solutions are robust in perturbations on the solution but not necessarily on distributional shifts of the probability distribution that the data follows. Furthermore, they do not consider EV parking lots interconnected with retailers and prosumer communities. In papers that focus more on the EV parking lot management for community services, models for parking lot arbitrage and flexibility scheduling have often imposed fixed capacity envelopes or known departure processes [6], [19]. Other methods may risk infeasibility or exhibit excessive conservatism. Only a few works model parking lots as virtual energy storage services. Specifically, [20] designs a three-stage energy management system that coordinates EV charging of fleets to maximize community benefits and operational efficiency. The works [21] and [22] focus mainly on the market participation of the EV parking lots, e.g., the interaction between EV storage services and retailers. To the best of our knowledge, this is the first time that adversarially and distributionally robust probabilistic guarantees are proposed as a tool to study the performance and safety of virtual storage services provided by stationary EV batteries.

A. Challenges and Main Contributions

This paper addresses two limitations that are crucial in virtual energy storage services of this type: i) the flexibility to trade off economic performance with robustness in constraint satisfaction; ii) our model interconnects prosumer communities with EV parking lots and a retailer. In this setting EV arrivals/departures, as well as EV users' choices are uncertain. Such uncertainty is quantified based on data measurements often affected by noise or prone to data poisoning from an adversarial entity. Furthermore, since they are heavily based on human behaviour, they can exhibit probabilistic shifts, i.e., changes in the probabilistic model followed. This can render the provided guarantees based

The work of N. Mignoni, R. Carli, and M. Dotoli was supported by the NRRP - Mission 4 Component 2 Investment 1.3 - Call for tender No. 341 of March 15, 2022 of MUR - project "NEST (Network 4 Energy Sustainable Transition)" (project no. PE00000021) and NRRP - Mission 4 Component 2 Investment 1.1 - Call for "Projects of significant national interest - Progetti di rilevante interesse nazionale (PRIN)" - Decree no. 104 of February 2, 2022 of MUR (project: CORRECT, code: 202248PWRY).

G. Pantazis and S. Grammatico are with the Delft Center for Systems and Control of the Technical University of Delft, Delft, the Netherlands (e-mail: {G.Pantazis, S.Grammatico}@tudelft.nl).

N. Mignoni, R. Carli, and M. Dotoli are with the Department of Electrical and Information Engineering of the Polytechnic of Bari, Italy (e-mail: {nicola.mignoni, raffaele.carli, mariagrazia.dotoli}@poliba.it).

on a nominal model inadequate for out-of-sample or out-of-distribution robustness. As such, resilience to adversarial perturbations of data (or distributional shifts) is of utmost importance.

Our main contributions with respect to the related literature are the following:

- 1) We propose a model for a virtual energy storage service provided to a community of prosumers that can be seamlessly integrated with the existing network. The role of the PLM is to aggregate the batteries of parked EVs into a *virtual* energy storage system with time-varying capacity and offer a requested capacity to the prosumers community under a contract. Thus, the PLM has a dual role, as a profit making entity and as a risk absorber. The model captures the uncertain virtual state-of-charge dynamics with losses induced by parked EV departures, uncertain virtual capacity bounds, as well as market actions with retailers, while still retaining convexity.
- 2) Because the distributions of losses and capacity caps often follow distributions difficult to model due to inherent behavioural aspects of EV users, we resort to data and formulate an approximated program based on scenarios over the defined horizon. We then provide distribution-free probabilistic robustness certificates on the probability that our solution will be robust against yet unseen vehicle departures and capacity caps. We offer a method for the PLM to tune the trade-off between constraint satisfaction and profit accompanied by tight safety guarantees.
- 3) We allow the PLM to tune the level of trust to the data by allowing each training sample to vary within a perturbation set chosen by the PLM. We show that such adversarially robust solutions can still be accompanied by distribution-free guarantees. We consider a distributionally robust optimization setting where the distribution during the training can differ from the probability distribution during the test period up to a risk-aversion radius chosen by the PLM. Leveraging recent results in the scenario approach [23], we show that robustness certificates on the violation of the test distributions can be obtained, thus certifying our decision against future shifts in the probabilistic models of EV departures and capacity caps.

Notation: Sets $\mathbb{R}$ and $\mathbb{R}_{\geq 0}$ denote the real and non-negative real numbers. The positive and *negative part* operators are defined as $[\cdot]_+ := \max\{0, \cdot\}$ and $[\cdot]_- := -\min\{0, \cdot\}$, respectively. Let $\mathcal{K} = \{1, \dots, K\}$ be a discrete time window of $K \in \mathbb{N}$ equally spaced time steps. $\mathfrak{N}(0, 1)$ denotes a Gaussian distribution with mean 0 and standard deviation 1. Given a set $\mathcal{A} \subseteq \mathbb{R}^n$, $\mathbb{1}_{\mathcal{A}} : \mathbb{R}^n \rightarrow \{0, 1\}$ is the indicator function associated with $\mathcal{A}$, so that $\mathbb{1}_{\mathcal{A}}(x) = 1$ if $x \in \mathcal{A}$ and 0 otherwise.

II. PROBLEM FORMULATION

An overview of the considered energy community setup is illustrated in Fig. 1. The virtual energy storage state-of-

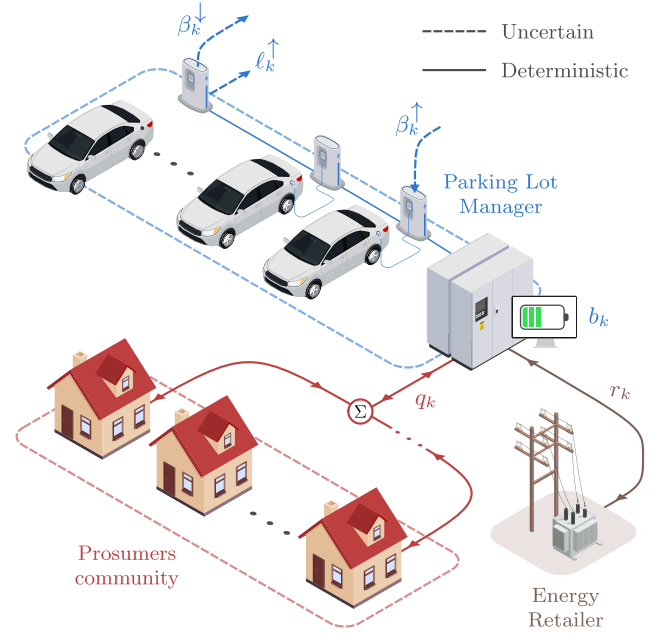


Fig. 1: The parking lot manager (PLM) leverages the available storage of the parked EVs, as agreed with the EV users, to provide virtual energy storage services to a community of prosumers. Furthermore, the PLM is allowed to trade energy with retailers.

charge $b_k \in \mathbb{R}$ satisfies the dynamics:

$$b_k = b_{k-1} + q_k + r_k - \ell_k, \quad \forall k \in \mathcal{K} \quad (1a)$$

$$b_k \in [0, \beta_k], \quad \forall k \in \mathcal{K}. \quad (1b)$$

Here, $q_k \in \mathbb{R}$ denotes the energy exchange as requested by the prosumer, which has to be met by the PLM. In particular, $q_k > 0$ ($q_k < 0$) denotes energy that the prosumers injected into (withdraw from) the virtual storage. Term $\ell_k \in \mathcal{L} \subset \mathbb{R}_{\geq 0}$ denotes the state of charge losses due to, e.g., EVs leaving the parking lot, or operational faults. Term $\beta_k \in \mathcal{B} \subset \mathbb{R}_{\geq 0}$ is the time-varying capacity: incoming EVs increase the battery capacity, while leaving EVs reduce it. Finally, $r_k \in \mathbb{R}$ is the PLM's decision to buy from ($r_k > 0$) or sell ($r_k < 0$) energy to the retailer. This decision is subject to the operational constraint $|r_k| \leq r_{\max}$.

The need for r_k serves two purposes: i) it allows the PLM to compensate state-of-charge drops due to EVs leaving, and ii) it provides a means for energy arbitrage. The second aspect is not strictly related to virtual storage markets, i.e., one could set $r_k \geq 0$. Nonetheless, we allow it for the sake of generality.

We denote the collection of the virtual state of charge over the horizon $k \in \mathcal{K}$ by $\mathbf{b} = \text{col}(b_k)_{k \in \mathcal{K}}$ and $\mathbf{r} = \text{col}(r_k)_{k \in \mathcal{K}}$, respectively. Being an economic actor, the PLM is interested in minimizing the sustained costs, i.e., maximizing its revenues. The objective $J : \mathbb{R}^K \rightarrow \mathbb{R}$ denotes such quantity, defined as

$$J(\mathbf{r}) = \sum_{k \in \mathcal{K}} (\pi_k^+ [r_k]_+ + \pi_k^- [r_k]_-) \quad (2)$$

where $\pi_k^+, \pi_k^- \in \mathbb{R}_{\geq 0}$ are the retailer's selling and buying

price, respectively. Note that the first sum term in (2) represents the costs sustained for buying energy from the retailer, while the second represents the revenues coming from arbitrage.

Assumption 1: For all time steps $k \in \mathcal{K}$, the buying price is larger than the selling price, i.e., $\pi_k^+ \geq \pi_k^-$. $\square$

Assumption 1 is aligned with the existing market structure as discussed in detail in [24]. The scheduling problem of the PLM then takes the form:

$$\begin{aligned} & \underset{\mathbf{r}, \mathbf{b}}{\text{minimize}} \quad J(\mathbf{r}) & (\text{PLM}_{\text{base}}) \\ & \text{subject to} \quad b_k = b_{k-1} + q_k + r_k - \ell_k, \quad \forall k \in \mathcal{K} & (3a) \\ & \quad b_k \in [0, \beta_k], \quad \forall k \in \mathcal{K} & (3b) \\ & \quad |r_k| \leq r_{\max}, \quad \forall k \in \mathcal{K}. & (3c) \end{aligned}$$

Remark 1: Based on Assumption 1, the objective $J(\cdot)$ is convex, and linear when $\pi_k^+ = \pi_k^-$, for all $k \in \mathcal{K}$. Moreover, since the constraints (3a)-(3c) are affine, the problem in $(\text{PLM}_{\text{base}})$ is convex.

We consider a general setting, where the loss vector associated with EV departures $\ell = \text{col}(\ell_k)_{k \in \mathcal{K}}$ and the upper bound on the virtual state of charge $\beta = (\beta_k)_{k \in \mathcal{K}}$ are uncertain. Since it is generally challenging to identify the underlying distribution (if it exists) of both parameters, an approach to deal with this problem is by considering a robust counterpart for $(\text{PLM}_{\text{base}})$ parameterized by the support sets $\mathcal{L}, \mathcal{B}$:

$$\begin{aligned} & \underset{\mathbf{r}, \mathbf{b}}{\text{minimize}} \quad J(\mathbf{r}) & (\text{PLM}_{\mathcal{L}, \mathcal{B}}) \\ & \text{subject to} \quad b_k \geq b_{k-1} + q_k + r_k - \max_{\ell \in \mathcal{L}} \ell, \quad \forall k \in \mathcal{K} & (4a) \\ & \quad 0 \leq b_k \leq \beta, \quad \forall k \in \mathcal{K} & (4b) \\ & \quad \quad \quad \forall \beta \in \mathcal{B} \\ & \quad |r_k| \leq r_{\max}, \quad \forall k \in \mathcal{K}. & (4c) \end{aligned}$$

Such formulation, however, can be overly conservative. Furthermore, a robust approach does not leverage the historical data trajectories of EV departures. To reduce the excessive conservatism imposed in the model $(\text{PLM}_{\mathcal{L}, \mathcal{B}})$ through traditional robust approaches, we adopt a data-driven perspective and obtain samples from previous values of β_k, ℓ_k obtained either from real measurements or data produced from a synthetic model. To this end, let $b_k^{(i)}$ and $\ell_k^{(i)}$ correspond to the i -th sample at time k from a collection of samples $\mathcal{N} = \{1, \dots, N\}$. We can then define the following scenario approximation of the original robust problem:

$$\begin{aligned} & \underset{\mathbf{r}, \mathbf{b}}{\text{minimize}} \quad J(\mathbf{r}) & (\text{PLM}_N) \\ & \text{subject to} \quad b_k \geq b_{k-1} + q_k + r_k - \max_{i \in \mathcal{N}} \ell_k^{(i)}, \quad \forall k \in \mathcal{K} & (5a) \\ & \quad 0 \leq b_k \leq \beta_k^{(i)}, \quad \forall i \in \mathcal{N} & (5b) \\ & \quad \quad \quad \forall k \in \mathcal{K} \\ & \quad |r_k| \leq r_{\max}, \quad \forall k \in \mathcal{K}. & (5c) \end{aligned}$$

Note that, by introducing the scalar auxiliary decision variable $u_k \in \mathbb{R}_{\geq 0}$, with $\mathbf{u} = \text{col}(u_k)_{k \in \mathcal{K}}$, the scenario program

(PLM_N) can be written in the form:

$$\begin{aligned} & \underset{\mathbf{r}, \mathbf{b}, \mathbf{u}}{\text{minimize}} \quad J(\mathbf{r}) & (\text{PLM}'_N) \\ & \text{subject to} \quad b_k \geq b_{k-1} + q_k + r_k - u_k, \quad \forall k \in \mathcal{K} & (6a) \\ & \quad u_k \geq \ell_k^{(i)}, \quad \forall i \in \mathcal{N} & (6b) \\ & \quad \quad \quad \forall k \in \mathcal{K} \\ & \quad 0 \leq b_k \leq \beta_k^{(i)}, \quad \forall i \in \mathcal{N} & (6c) \\ & \quad \quad \quad \forall k \in \mathcal{K} \\ & \quad |r_k| \leq r_{\max}, \quad \forall k \in \mathcal{K}. & (6d) \end{aligned}$$

Remark 2: If $(\mathbf{r}_{\mathcal{N}}^*, \mathbf{b}_{\mathcal{N}}^*, \mathbf{u}_{\mathcal{N}}^*)$ is the optimal solution of (PLM'_N) then $(\mathbf{r}_{\mathcal{N}}^*, \mathbf{b}_{\mathcal{N}}^*)$ is an optimal decision for (PLM_N) .

Note that the data trajectories are considered as an independent and identically distributed (i.i.d.) sample vector from an unknown probability distribution $\mathbb{P}$. This is a reasonable assumption, as in practice the pattern of vehicle departures on a given day shows very little correlation with departures on the same weekday in subsequent weeks or even in the same period of the following year. However, correlations between components of the data trajectory can be taken into account without violating the i.i.d. assumption. Given the program above, we now define the probability of violation of the PLM constraints as follows:

$$\mathbb{V}(\mathbf{r}, \mathbf{b}) := \left\{ \mathbb{P}(\tilde{\ell}, \tilde{\beta}) : \begin{aligned} & b_k < b_{k-1} + r_k - \tilde{\ell}_k, \\ & b_k > \tilde{\beta}_k \\ & \forall k \in \mathcal{K} \end{aligned} \right\} \quad (7)$$

where $\tilde{\ell} = (\tilde{\ell}_k)_{k \in \mathcal{K}}$ and $\tilde{\beta} = (\tilde{\beta}_k)_{k \in \mathcal{K}}$. Although not present on the right-hand side, r_k implicitly affects the decision variables u_k, b_k via (6a). The probability of violation quantifies the probability that the PLM's decision $\mathbf{r}, \mathbf{b}$ will violate constraints for future yet unseen data trajectories $\tilde{\ell}, \tilde{\beta}$. The probability of violation and its extensions will be used in the subsequent developments as a risk measure for the provision of theoretical safety guarantees for the PLM model.

III. ROBUST VIRTUAL ENERGY STORAGE SERVICES

Based on Remark 1, the problem in (PLM_N) is convex. Assuming feasibility, convexity alone does not ensure the uniqueness of the minimizer. To this end, we impose the following standing assumption for PLM_N .

Assumption 2 (Uniqueness): For any number of samples $N \in \mathbb{N}$ and for every sample $\ell^{(i)} = \text{col}(\ell_k^{(i)})_{k \in \mathcal{K}}$ and $\beta^{(i)} = \text{col}(\beta_k^{(i)})_{k \in \mathcal{K}}$, with $i \in \mathcal{N}$, the solution is unique.

If more than one solution exist, a unique solution can be singled out using a convex tie-break rule [14]. We denote the unique optimal solution of (PLM_N) returned by the optimization algorithm by $(\mathbf{r}_{\mathcal{N}}^*, \mathbf{b}_{\mathcal{N}}^*, \mathbf{u}_{\mathcal{N}}^*)$. Upon computing such an optimal solution, the PLM is interested in knowing what safety guarantees this solution admits against unseen uncertainties. Such certificates are fundamentally connected with the concept of support constraints/ support samples. Considering the reformulation (PLM'_N) , each sample $i \in \mathcal{N}$ gives rise to the randomized constraint:

$$\mathcal{C}_i = \left\{ \begin{bmatrix} \mathbf{r} \\ \mathbf{b} \\ \mathbf{u} \end{bmatrix} \in \mathbb{R}^{3K} : u_k \geq \ell_k^{(i)}, b_k \leq \beta_k^{(i)}, \forall k \in \mathcal{K} \right\}. \quad (8)$$

The concept of support constraints and support samples lies at the heart of out-of-sample generalization of scenario programs [11] and is defined as follows:

Definition 1 (Support constraints/ samples): A constraint $\mathcal{C}_i$, with $i \in \mathcal{N}$, is a *support constraint* if its removal changes the optimal solution, i.e., $(\mathbf{r}_{\mathcal{N}}, \mathbf{b}_{\mathcal{N}}^*, \mathbf{u}_{\mathcal{N}}^*) \neq (\mathbf{r}_{\mathcal{N} \setminus \{i\}}, \mathbf{b}_{\mathcal{N} \setminus \{i\}}^*, \mathbf{u}_{\mathcal{N} \setminus \{i\}}^*)$, where $(\mathbf{r}_{\mathcal{N} \setminus \{i\}}, \mathbf{b}_{\mathcal{N} \setminus \{i\}}^*, \mathbf{u}_{\mathcal{N} \setminus \{i\}}^*)$ denotes the optimal solution obtained after removing the constraint $\mathcal{C}_i$ from program $\text{PLM}_{\mathcal{N}}$. The sample that corresponds to a support constraint $\mathcal{C}_i$ is called a *support sample*.

In practice, support constraints/samples encode which samples of the data are required to reconstruct the optimal solution. However, there can be ill-defined cases where multiple copies of the same constraint accumulate on top of each other. To exclude such degenerate cases, we impose the following assumption:

Assumption 3: (Non-degeneracy [11]) For every sample $(\tilde{\ell}, \tilde{\beta})$ of size N , the solution $(\mathbf{r}_{\mathcal{N}}^*, \mathbf{b}_{\mathcal{N}}^*, \mathbf{u}_{\mathcal{N}}^*)$ of $(\text{PLM}_{\mathcal{N}})$ coincides with probability 1 with the solution that is obtained after eliminating all the constraints that are not of support.

Assumption 3 ensures that there are no multiple copies of the same constraint for different samples, since if that were the case, the solutions calculated only using the support constraints would differ from the original randomized solution. Consider now the probability of violation $\mathbb{V}(\mathbf{r}_{\mathcal{N}}^*, \mathbf{b}_{\mathcal{N}}^*)$ and the cardinality of support constraints or support samples defined as:

$$s_{\mathcal{N}} = |\{i \in \mathcal{N} : \mathcal{C}_i \text{ is a support constraint}\}|. \quad (9)$$

Then, the following result provides *a priori* robustness certificates for constraint satisfaction:

Lemma 1: Consider the data-driven program $(\text{PLM}_{\mathcal{N}})$ with $N > 2K$. Then, the following holds:

$$\mathbb{P}^N\{\mathbb{V}(\mathbf{r}_{\mathcal{N}}^*, \mathbf{b}_{\mathcal{N}}^*) \leq \varepsilon\} \geq 1 - \delta \quad (10a)$$

$$\delta = \sum_{i=0}^{2K-1} \binom{N}{i} \varepsilon^i (1 - \varepsilon)^{N-i} \quad (10b)$$

with $\varepsilon \in [0, 1]$ being a violation level upper bound set by the PLM.

Proof: The reformulation $(\text{PLM}'_{\mathcal{N}})$ has two uncertain constraints, i.e., (6c) and (6b), while (6a) does not depend on the uncertainty, but only on the decision variables. Note that in $(\text{PLM}'_{\mathcal{N}})$, there are K unconstrained directions in the feasible space constructed by (6c) and (6b). As such, based on [25, Def. 3.3], we can replace the original bound on the total dimension with the support rank $d_{sr} = 2K$ and apply [25, Lemma 3.8] and [25, Thm. 4.1] on problem $(\text{PLM}_{\mathcal{N}})$ to obtain:

$$\begin{aligned} \mathbb{P}^N\{\mathbb{V}(\mathbf{r}_{\mathcal{N}}^*, \mathbf{b}_{\mathcal{N}}^*) \leq \varepsilon\} &= \mathbb{P}^N \left\{ \mathbb{P} \left\{ \begin{array}{l} u_k^* < \tilde{\ell}_k \\ (\tilde{\ell}, \tilde{\beta}) : b_k^* > \tilde{\beta}_k \\ \forall k \in \mathcal{K} \end{array} \right\} \leq \varepsilon \right\} \\ &\geq 1 - \delta \end{aligned}$$

where δ satisfies (10b). $\blacksquare$

As such, the PLM ensures that, with high confidence $1 - \delta$, the probability that the state-of-charge of the virtual battery

will be enough for most future EV departures and state of charge caps is bounded by a quantity ϵ that improves with the data size and is given by (10b). Note that for a longer horizon K , the bound on ϵ becomes looser. This implies that the PLM requires more data to ensure the safety of the constraint up to this violation level if it plans further into the future. The result of Lemma 1 is *a priori* in the sense that to guarantee these safety margins, the PLM is not required to know the samples beforehand. However, *a priori* results often correspond to a worst-case bound and are thus conservative.

A. Profit vs Risk in EV Parking Lot Management

The results established in the previous subsection do not take into account that the PLM, as a service provider and profit-driven entity, might wish to decide for itself on the trade-off between constraints' satisfaction and profit. We thus grant this flexibility for the PLM by extending the problem in $(\text{PLM}_{\mathcal{N}})$ as follows:

$$\begin{aligned} &\underset{\mathbf{r}, \mathbf{b}, \boldsymbol{\xi}}{\text{minimize}} \quad J(\mathbf{r}) + \rho \sum_{i \in \mathcal{N}} \xi_i & (\text{PLM}_{\mathcal{N}, \rho}) \end{aligned}$$

$$\begin{aligned} &\text{subject to } \xi_i + b_k \geq b_{k-1} + q_k \\ &\quad \quad \quad + r_k - \max_{i \in \mathcal{N}} \ell_k^{(i)}, \quad \forall k \in \mathcal{K} \end{aligned} \quad (11a)$$

$$0 \leq b_k \leq \beta_k^{(i)} + \xi_i, \quad \forall i \in \mathcal{N}, \quad \forall k \in \mathcal{K} \quad (11b)$$

$$|r_k| \leq r_{\max}, \quad \forall k \in \mathcal{K} \quad (11c)$$

with $\boldsymbol{\xi} = \text{col}(\xi_i)_{i \in \mathcal{N}}$. In this setting, the PLM has an additional penalty term in the cost function that is responsible for tightening or relaxing the safety constraints depending on the value of the weight $\rho \in \mathbb{R}_{\geq 0}$. Note that $(\text{PLM}_{\mathcal{N}, \rho}) \rightarrow (\text{PLM}_{\mathcal{N}})$ as $\rho \rightarrow \infty$. A positive ξ_i generates the *regret* associated with non-exact satisfaction of the associated i -th constraint of program $(\text{PLM}_{\mathcal{N}, \rho})$. Thus, the following program reformulation can then be obtained:

$$\begin{aligned} &\underset{\mathbf{r}, \mathbf{b}, \boldsymbol{\xi}, \mathbf{u}}{\text{minimize}} \quad J(\mathbf{r}) + \rho \sum_{i \in \mathcal{N}} \xi_i & (\text{PLM}'_{\mathcal{N}, \rho}) \end{aligned}$$

$$\text{subject to } \xi_i + b_k \geq b_{k-1} + q_k \quad (12a)$$

$$\quad \quad \quad + r_k - u_k, \quad \forall k \in \mathcal{K} \quad (12b)$$

$$u_k \geq \ell_k^{(i)}, \quad \forall i \in \mathcal{N}, \quad \forall k \in \mathcal{K} \quad (12c)$$

$$0 \leq b_k \leq \beta_k^{(i)} + \xi_i, \quad \forall i \in \mathcal{N}, \quad \forall k \in \mathcal{K} \quad (12d)$$

$$|r_k| \leq r_{\max}, \quad \forall k \in \mathcal{K}. \quad (12e)$$

Note again that for any optimal solution of $(\text{PLM}'_{\mathcal{N}, \rho})$, $(\mathbf{r}_{\rho}^*, \mathbf{b}_{\rho}^*, \mathbf{u}_{\rho}^*)$, the pair $(\mathbf{r}_{\rho}^*, \mathbf{b}_{\rho}^*)$ is the optimizer of $(\text{PLM}_{\mathcal{N}, \rho})$.

Given that the data on vehicle arrivals and departures and the virtual state of charge bounds are available to the PLM, one can indeed obtain (possibly) tighter guarantees by leveraging the so-called *a posteriori* bounds. To this end, we impose the following assumption:

Assumption 4 (Non-accumulation): For every decision $(\mathbf{r}, \mathbf{b}, \mathbf{u})$ we have that:

$$\mathbb{P}[\exists k \in \mathcal{K} \mid b_k = b_{k-1} + r_k - \ell_k \text{ or } b_k = \beta_k] = 0 \quad (13)$$

Assumption 4 avoids degenerate cases, where different samples lead to constraints that overlap at the solution. Choosing different weight parameters ρ , the PLM can assess the trade-off between performance and the state-of-charge constraints violation based on the following result:

Proposition 1: Consider Assumptions 2 and 4. Let $(\mathbf{r}_\rho^*, \mathbf{b}_\rho^*)$ be the solution of $(\text{PLM}_{N,\rho})$. Given a confidence parameter $\delta \in (0, 1)$, for any $m = 0, \dots, N-1$, $m < N$, consider the polynomial equation

$$\binom{N}{m} t^{N-m} - \frac{\delta}{2N} \sum_{i=m}^{N-1} \binom{i}{m} t^{i-m} - \frac{\delta}{6N} \sum_{i=N+1}^{4N} \binom{i}{m} t^{i-m} = 0 \quad (14)$$

with respect to t . For $k = N$, consider instead the polynomial equation

$$1 - \frac{\delta}{6N} \sum_{i=N+1}^{4N} \binom{i}{N} t^{i-N} = 0. \quad (15)$$

For any $m = 0, \dots, N-1$, equation (14) has exactly two solutions in $[0, +\infty)$, which we denote by $t^{(m)}$ and $\bar{t}^{(m)}$, with $t^{(m)} \leq \bar{t}^{(m)}$. Instead, equation (15) has only one solution in $[0, +\infty)$, which we denote by $\bar{t}^{(N)}$, while we define $t^{(N)} := 0$. Let $\underline{\epsilon}(m) := \max\{0, 1 - t^{(m)}\}$, $\bar{\epsilon}(m) := 1 - \bar{t}^{(m)}$, for $m = 0, \dots, N$. Then, with confidence at least $1 - \delta$, it holds that

$$\underline{\epsilon}(\tilde{s}_N^*) \leq V(\mathbf{r}_\rho^*, \mathbf{b}_\rho^*) \leq \bar{\epsilon}(\tilde{s}_N^*)$$

where $\tilde{s}_N^*$ is the cardinality of samples $(\ell^{(i)}, \beta^{(i)})$ for which $b_k^* \leq b_{k-1}^* + q_k + r_k^* - \ell_k^*$ or $b_k^* \geq \beta_k^{(i)}$.

Proof: Consider the unique optimizers of $(\mathbf{r}_\rho^*, \mathbf{b}_\rho^*, \xi_\rho^*)$ and $(\mathbf{r}_\rho^*, \mathbf{b}_\rho^*, \xi_\rho^*, \mathbf{u}_\rho^*)$ of $(\text{PLM}_{N,\rho})$ and $(\text{PLM}'_{N,\rho})$, respectively. Then, the following equality holds:

$$\begin{aligned} & \mathbb{P}^N \{ \mathbb{V}(\mathbf{r}_\rho^*, \mathbf{b}_\rho^*) \in [\underline{\epsilon}(\tilde{s}_N^*), \bar{\epsilon}(\tilde{s}_N^*)] \} \\ &= \mathbb{P}^N \left\{ \mathbb{P} \left\{ \begin{array}{l} u_{k,\rho}^* < \tilde{\ell}_k \\ (\tilde{\ell}, \tilde{\beta}) : b_{k,\rho}^* > \tilde{\beta}_k \\ \forall k \in \mathcal{K} \end{array} \right\} \in [\underline{\epsilon}(\tilde{s}_N^*), \bar{\epsilon}(\tilde{s}_N^*)] \right\}. \end{aligned}$$

Calculating $\tilde{s}_N^*$ for $(\text{PLM}'_{N,\rho})$ and applying Theorem 2 in [14] concludes the proof. ■

Note that in Proposition 1, the constraints that are important and affect the quality of the generalization guarantees are the active constraints and violating constraints. The smaller the cardinality $\tilde{s}_N^*$, the tighter the lower and upper violation levels on the true probability risk.

In practice, the data used by the PLM can be subject to manipulations either by noise or by adversarial entities. With the advent of cyber-physical systems, cyber-attacks on subsystems of the electricity grid have become increasingly more common. Furthermore, even after appropriate pre-processing, the PLM might not be sure how much trust to put into their data. In the following Section, we aim to address this issue by proposing a distributionally and adversarially robust virtual energy storage methodology for the PLM with tunable guarantees.

IV. DISTRIBUTIONALLY ROBUST VIRTUAL STORAGE SERVICES

In the first part of this Section, we design the PLM such that it is robust against adversarial or noisy changes in the data. Specifically, we consider the case where the PLM may trust the data up to a certain threshold that defines a *trust-region*. Specifically, we consider that each sample (ℓ, β) lies within an adversarial region $\mathcal{A}_{\ell,\beta} \subseteq \mathbb{R}^{2K}$ defined as

$$\mathcal{A}_{\ell,\beta} = \{(\ell + \Delta\ell, \beta + \Delta\beta) : (\Delta\ell, \Delta\beta) \in \mathcal{A}\}, \quad (16)$$

where $\mathcal{A} \subset \mathbb{R}^{2K}$ is considered to be a set of possible data deviations considered by the PLM as design choices. As data perturbations can alter the resulting decision and thus its associated robustness certificates, the notion of the probability of violation of the virtual SoC constraints has to be redefined to account for a risk function robust against not only the drawn sample but also a region around it. If mistrust is high, the region is larger, while if the PLM trusts the measurements, the region is smaller. Consider the adversarial region $\mathcal{A}_{\ell,\beta}$ around sample (ℓ, β) and that $(\mathbf{r}, \mathbf{b})$ is the PLM's decision. Then, the risk measure is defined as

$$\begin{aligned} \mathbb{V}_A(\mathbf{r}, \mathbf{b}) = & \mathbb{P} \left\{ (\ell, \beta) : \exists (\tilde{\ell}, \tilde{\beta}) \in \mathcal{A}_{\ell,\beta}, k \in \mathcal{K} : \right. \\ & \left. b_k < b_{k-1} + q_k + r_k - \tilde{\ell}_k \text{ or } b_k > \tilde{\beta}_k \right\} \end{aligned}$$

is called the adversarial probability of violation. Such a risk measure does not consider only the particular points to account for violations, but an entire set of perturbations around the data belonging to $\mathcal{A}_{\ell,\beta}$. In this paper, we consider a finite approximation of $\mathcal{A}_{\ell,\beta}$ obtained as the convex hull of $M \in \mathbb{N}$ points in $\mathcal{A}$ and denoted by $\hat{\mathcal{A}} \subseteq \mathcal{A}$. For ease of notation, we denote $\mathcal{M} = \{1, \dots, M\}$. Then, the adversarially robust optimization program that the PLM aims to solve takes the form:

$$\underset{\mathbf{r}, \mathbf{b}, \xi}{\text{minimize}} \quad J(\mathbf{r}) + \rho \sum_{i \in \mathcal{N}} \xi_i \quad (\text{PLM}_{N,\rho,\hat{\mathcal{A}}})$$

$$\text{subject to } \xi_i + b_k \geq b_{k-1} + q_k$$

$$+ r_k - \max_{i \in \mathcal{N}, j \in \mathcal{M}} \ell_k^{(i,j)}, \quad \forall k \in \mathcal{K} \quad (17a)$$

$$0 \leq b_k \leq \beta_k^{(i,j)} + \xi_i, \quad \forall i \in \mathcal{N}, \forall k \in \mathcal{K} \quad (17b)$$

$$|r_k| \leq r_{\max}, \quad \forall k \in \mathcal{K} \quad (17c)$$

where $\mathcal{M}$ is the set of points of $\mathcal{A}$ used to approximate $\mathcal{A}_{\ell,\beta}$. Note that $(\text{PLM}_{N,\rho,\hat{\mathcal{A}}})$ coincides with $(\text{PLM}_{N,\rho})$, when $\hat{\mathcal{A}} = \emptyset$. The following program reformulation can then be obtained:

$$\underset{\mathbf{r}, \mathbf{b}, \mathbf{u}}{\text{minimize}} \quad J(\mathbf{r}) + \rho \sum_{i \in \mathcal{N}} \xi_i \quad (\text{PLM}'_{N,\rho,\hat{\mathcal{A}}})$$

$$\text{subject to } \xi_i + b_k \geq b_{k-1} + q_k$$

$$+ r_k - u_k, \quad \forall k \in \mathcal{K} \quad (18a)$$

$$u_k \geq \ell_k^{(i,j)}, \quad \forall i \in \mathcal{N} \quad (18b)$$

$$0 \leq b_k \leq \beta_k^{(i,j)} + \xi_i, \quad \forall m \in \mathcal{M} \quad (18c)$$

$$|r_k| \leq r_{\max}, \quad \forall k \in \mathcal{K} \quad (18d)$$

Note that the data points of the adversarial set that violate the constraints would correspond to the empirical adversarial risk of the PLM. However, considering only those samples as support samples would not be enough to assess the data-driven decision's out-of-sample performance. To account for potential overfitting issues, we also need to consider the points that lead to active constraints on the boundary of the PLM's feasible set formed by sampled constraints. In accordance with [23, Def. 5],

a sample $(\ell^{(i)}, \beta^{(i)})$ is an *adversarial support sample* or contributes to the *adversarial complexity* for problem $(\text{PLM}_{N,\rho,\hat{\mathcal{A}}})$ for some time step $k \in \mathcal{K}$ if one of the following conditions holds:

$$\begin{aligned} \exists(\tilde{\ell}^{(i)}, \tilde{\beta}^{(i)}) \in \mathcal{A}_{\ell^{(i)}, \beta^{(i)}} : u_{k,\hat{\mathcal{A}}}^* < \tilde{\ell}_k^{(i)} \text{ or } b_{k,\hat{\mathcal{A}}}^* > \tilde{\beta}_k^{(i)} \\ \exists(\tilde{\ell}^{(i,j)}, \tilde{\beta}^{(i,j)}) \in \mathcal{A}_{\ell^{(i,j)}, \beta^{(i,j)}} : u_{k,\hat{\mathcal{A}}}^* = \tilde{\ell}_k^{(i,j)} \text{ or } b_{k,\hat{\mathcal{A}}}^* = \tilde{\beta}_k^{(i,j)} \\ \exists(\tilde{\ell}^{(i,j)}, \tilde{\beta}^{(i,j)}) \in \mathcal{A}_{\ell^{(i,j)}, \beta^{(i,j)}} : u_{k,\hat{\mathcal{A}}}^* < \tilde{\ell}_k^{(i,j)} \text{ or } b_{k,\hat{\mathcal{A}}}^* > \tilde{\beta}_k^{(i,j)} \end{aligned}$$

where $u_{k,\hat{\mathcal{A}}}^*$ denotes the optimal value of the auxiliary variable of $(\text{PLM}_{N,\rho,\hat{\mathcal{A}}})$.

Proposition 2: Under Assumptions 2 and 4 and the condition $\hat{\mathcal{A}}_{\ell,\beta} \subseteq \mathcal{A}_{\ell,\beta}$ for all $(\ell, \beta) \in (\mathcal{L} \times \mathcal{B})^K$, it holds that with high confidence at least $1 - \beta$:

$$\mathbb{V}_{\mathcal{A}}(\mathbf{r}_{\hat{\mathcal{A}}}^*, \mathbf{b}_{\hat{\mathcal{A}}}^*) \in [\underline{\epsilon}(s_{\mathcal{A},\hat{\mathcal{A}}}^*), \bar{\epsilon}(s_{\mathcal{A},\hat{\mathcal{A}}}^*)], \quad (19)$$

where $s_{\mathcal{A},\hat{\mathcal{A}}}^*$ denotes the number of adversarial support samples of $(\text{PLM}_{N,\rho,\hat{\mathcal{A}}})$ and $\underline{\epsilon}(m)$ and $\bar{\epsilon}(m)$ are obtained by solving the polynomial equations of Proposition 1 and then setting $m = s_{\mathcal{A},\hat{\mathcal{A}}}^*$.

Proof: The following equalities hold:

$$\begin{aligned} \mathbb{V}_{\mathcal{A}}(\mathbf{r}, \mathbf{b}) &= \mathbb{P}\{(\ell, \beta) : \exists \tilde{\ell}, \tilde{\beta} \in \mathcal{A}_{\ell,\beta}, k \in \mathcal{K} : \\ &\quad b_k > \tilde{\beta}_k \text{ or } b_k^* < b_{k-1}^* + q_k + r_k - \tilde{\ell}_k\} \\ &= \mathbb{P}\{(\ell, \beta) : \exists \tilde{\ell}, \tilde{\beta} \in \mathcal{A}_{\ell,\beta} : \\ &\quad \max_{k \in \mathcal{K}} \max\{u_k^* - \tilde{\ell}_k, b_k^* - \tilde{\beta}_k\} > 0\} \\ &= \mathbb{P}\{(\ell, \beta) : \exists \tilde{\ell} \in \mathcal{A}_{\ell,\beta} : f(\mathbf{r}, \mathbf{b}, \mathbf{u}, \tilde{\ell}, \tilde{\beta}) > 0\} \end{aligned}$$

where function f in the last equality is defined as

$$f(\mathbf{r}, \mathbf{b}, \mathbf{u}, \tilde{\ell}, \tilde{\beta}) = \max_{k \in \mathcal{K}} \max\{u_k - \tilde{\ell}_k, b_k - \tilde{\beta}_k\} \quad (20)$$

Then, the result follows by [23, Thm. 3]. $\blacksquare$

A. EV Departures and Capacity Distributional Shifts

The training set $\{\ell^{(i)}, \beta^{(i)}\}_{i \in \mathcal{N}}$ can originate from, e.g., synthetic models or real-world measurements/historical data. However, due to distributional shifts, the data used for training might not follow the same distribution as the data

Algorithm 1 Tunable Distributionally Robust VESS

Require: $r_{\max}; \ell^{(i)}, \beta^{(i)}$ for $i = 1, \dots, N, j = 1, \dots, M$;
 $\mu, R, M, \delta, N^+, \rho^+, \hat{k}$

- 1: *Retailer-PLM:* Contract agreement on selling and buying price (π_k^+, π_k^-) per time step $k \in \mathcal{K}$.
- 2: *PLM-Prosumers:* Contract agreement on energy request q_k per time step $k \in \mathcal{K}$.
- 3: *PLM:* $\epsilon_{\text{goal}}, \epsilon \leftarrow 0$
- 4: **while** $\epsilon > \epsilon_{\text{goal}}$ **do**
- 5: Solve $(\text{PLM}_{N,\rho,\hat{\mathcal{A}}})$ and obtain $(\mathbf{r}_{\hat{\mathcal{A}}}^*, \mathbf{b}_{\hat{\mathcal{A}}}^*)$
- 6: Compute the adversarial complexity $s_{\mathcal{A},\hat{\mathcal{A}}}^*$
- 7: Compute $\bar{\epsilon}(s_{\mathcal{A},\hat{\mathcal{A}}}^*)$ based on Proposition 1
- 8: $\epsilon \leftarrow \bar{\epsilon}(s_{\mathcal{A},\hat{\mathcal{A}}}^*)$
- 9: $(\mathbf{r}_{\text{safe}}^*, \mathbf{b}_{\text{safe}}^*) \leftarrow (\mathbf{r}_{\hat{\mathcal{A}}}^*, \mathbf{b}_{\hat{\mathcal{A}}}^*)$
- 10: $N \leftarrow N + N^+$
- 11: $\rho \leftarrow \rho + \rho^+$
- 12: **end while**
- 13: **return** $(\mathbf{r}_{\text{safe}}^*, \mathbf{b}_{\text{safe}}^*, \epsilon)$

collected after deployment. In our setting, the PLM has collected data on the losses incurred from vehicle departures and data of imposed upper bounds in the state of charge of the virtual storage. However, the PLM wishes to have safety certificates against yet unseen realizations of these quantities that might follow a different distribution $\mathbb{P}'$. Unfortunately, without some connection between the probability distributions $\mathbb{P}$ and $\mathbb{P}'$, it is extremely challenging to provide any provable guarantees. To establish such results, a metric of similarity among distributions is often considered. An often used measure, due to its intuitive interpretation based on optimal transport, is the so-called Wasserstein distance defined as follows:

Definition 2: Consider the uncertain parameters (ℓ, β) and $(\tilde{\ell}, \tilde{\beta})$ following the probability distributions $\mathbb{P}$ and $\mathbb{P}'$. Then, the Wasserstein metric is given by:

$$d_W(\mathbb{P}, \mathbb{P}') = \inf_{\mathbb{Q}} \mathbb{E}_{\mathbb{Q}}[\|\ell - \tilde{\ell}\|_2^2 + \|\beta - \tilde{\beta}\|_2^2], \quad (21)$$

where $\mathbb{Q}$ denotes a joint probability distribution of random variables with marginals $\mathbb{P}$ and $\mathbb{P}'$. $\square$

Based on the Wasserstein distance, we can then define the ambiguity set that the PLM selects to account for risk aversion against probabilistic shifts with respect to this metric. To achieve this, the PLM needs to decide on a radius, which determines the size of the ambiguity set. As such, we assume that the distance between the training data distribution $\mathbb{P}$ and the test data distribution $\mathbb{P}'$ is coupled via the inequality:

$$d_W(\mathbb{P}, \mathbb{P}') \leq \mu,$$

for some PLM defined Wasserstein radius $\mu > 0$. The ambiguity set defined based on d_W , is defined as:

$$\mathbb{B}_{\mu}(\mathbb{P}) = \{\mathbb{P}' : d_W(\mathbb{P}, \mathbb{P}') \leq \mu\}. \quad (22)$$

We define the probability of violation for a distribution $\mathbb{P}' \in \mathbb{B}_\mu(\mathbb{P})$ as:

$$\mathbb{V}'_{\mathcal{A}}(\mathbf{r}, \mathbf{b}) := \mathbb{P}'\{(\ell', \beta') : f(\mathbf{r}, \mathbf{b}, \mathbf{u}, \ell', \beta') > 0\} \quad (23)$$

Furthermore, we assume that $\|\ell_K - \tilde{\ell}_K\|_2^2 \leq R_\ell$ and $\|\beta_K - \tilde{\beta}_K\|_2^2 \leq R_\beta$, where $R_\ell, R_\beta \in \mathbb{R}_{\geq 0}$ are choices of the designer that determine how much they trust the possible realizations of the uncertainty obtained from distributions within the ambiguity set. In this setting, the following holds:

Theorem 1: Consider Assumption 4 and $\mathbb{P}' \in \mathbb{B}_\mu(\hat{\mathbb{P}})$. Then, we have that with confidence at least $1 - \beta$:

$$\mathbb{V}'_{\mathcal{A}}(\mathbf{r}_{\hat{\mathcal{A}}}^*, \mathbf{b}_{\hat{\mathcal{A}}}^*) \leq \bar{\epsilon}(s_{\mathcal{A}, \hat{\mathcal{A}}}^*) + \frac{\mu}{R} \quad (24)$$

where $R = R_\beta + R_\ell$ and $s_{\mathcal{A}, \hat{\mathcal{A}}}^*$ is the adversarial complexity.

Proof: The proof follows by the equivalence of the out-of-distribution risks of $(\text{PLM}_{N, \rho, \hat{\mathcal{A}}})$ and $(\text{PLM}'_{N, \rho, \hat{\mathcal{A}}})$ and the application of Theorem 5 in [9] on $(\text{PLM}'_{N, \rho, \hat{\mathcal{A}}})$. ■

Note that being more risk-averse towards probabilistic shifts by increasing μ results in a looser bound. While a larger R would seemingly improve the bound, this is not necessarily the case, as a larger R can lead to a larger number of adversarial support samples, which can then worsen the guarantees. As such, the risk-aversion of the PLM will have a direct effect on the quality of the theoretical guarantees they can provide. In the following, we test these bounds by calculating the solutions to a stochastic PLM problem and comparing them with the empirical out-of-sample and out-of-distribution results as obtained by running Algorithm 1.

Based on the result of Theorem 1, our proposed Algorithm 1 provides an optimal planning solution $(\mathbf{r}_{\hat{\mathcal{A}}, \text{safe}}^*, \mathbf{b}_{\hat{\mathcal{A}}, \text{safe}}^*)$ for the PLM that enjoys distributionally robust safety guarantees. The PLM sets the desired theoretical violation level and then, depending on whether such a level is satisfied or not, the PLM uses more samples $N + N^+$ (if available) or a larger penalty $\rho + \rho^+$ until the desired level of violation is achieved.

V. NUMERICAL STUDY

To simulate our methodology, we consider additive perturbations to each sample component of $(\ell^{(i)}, \beta^{(i)})$. The perturbation is of magnitude $0.05p$, where $p \sim \mathcal{N}(0, 1)$. Based on this, we construct $M = 6$ samples per original sample to use for adversarial training. The objective function of the PLM and the probability of violation for sample sizes $N \in \{500, 1000\}$ and varying values of the adversarial radius R is shown in Figure 2. The horizon is fixed at $K = 12$ time steps. Furthermore, for each time step $k \in \{1, \dots, K\}$ we fix $R = 0.01$. The energy r_k bought/sold from/to the retailer at each time step k , is bounded by $r_{\max} = 5$. The vectors $(\mathbf{b}^*, \mathbf{r}^*)$ denote the unique optimizer of $(\text{PLM}_{N, \rho, \hat{\mathcal{A}}})$ after the application of a convex tie-break rule. Figures 3 and 4 illustrate the virtual state of charge b_k of the PLM's energy buffer and the energy r_k sold to the retailer at each time step k for different multi-samples.

Furthermore, we consider that distribution shifts can occur with the 1-Wasserstein ball of radius $\mu = 10^{-3}$ around

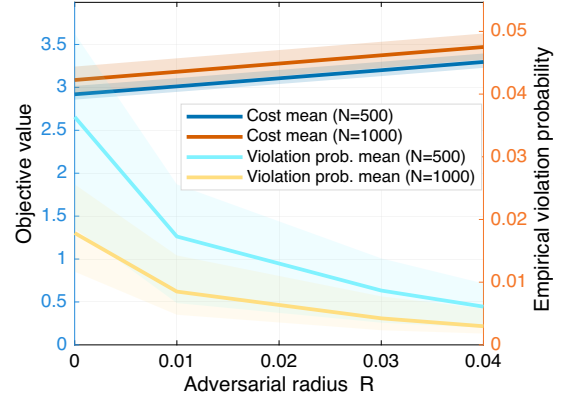


Fig. 2: Trade-off study between adversarially robust empirical probability of violation vs the profit of the PLM for varying values of R .

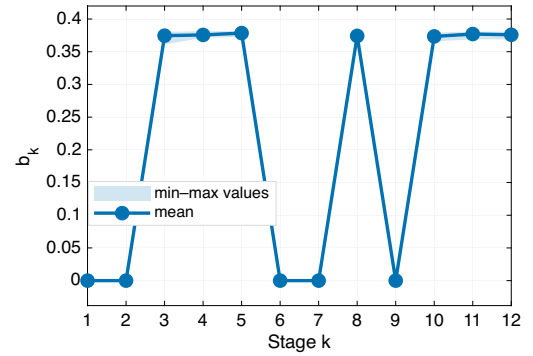


Fig. 3: Optimal virtual state of charge b_k of the PLM's energy buffer at each time step k .

the empirical probability distribution. To evaluate the out-of-distribution (OOD) performance we consider a test data set $(\ell^{(i)}, \beta^{(i)})$, $i \in \{1, \dots, N\}$. The samples are obtained each time from N' different probability distributions $\mathbb{P}_v$, $v \in \{1, \dots, N'\}$ obtained by perturbing the nominal probability distribution in different ways and then scaling them down such that they belong to the considered ambiguity set. We then wish to test the OOD violation level for each of those perturbed probability distributions. To do this, we calculate the corresponding empirical probability of violation defined as:

$$\hat{\mathbb{V}}_v(\ell, \beta) = \frac{1}{N_{\text{test}}} \sum_{i=1}^{N_{\text{test}}} \mathbb{1}_{\{b_k^* < b_{k-1}^* + q_k + r_k^* - \ell_k^{(i)} \text{ or } b_k^* > \beta_k^{(i)}\}}.$$

To see how well our model performs against probabilistic shifts, we use three metrics: i) an empirical mean across the empirical probabilities of violation of $N' = 40$ distributions within the considered ambiguity set, ii) a worst-case, and iii) a best-case probability of violation among these distributions. The results are summarized in Figure 5, where $\beta = 10^{-5}$ and a different number of samples $N \in \{500, 1000, 2000\}$ is used. Note that the out-of-distribution violation is at all times bounded by the theoretical violation level of Theorem 1. In case stricter out-of-distribution guarantees are required, the PLM can increase the penalty ρ , the deviation parameter

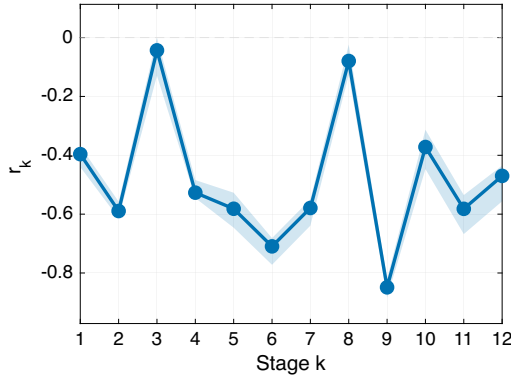


Fig. 4: Optimal energy r_k sold to the retailer at each time step k .

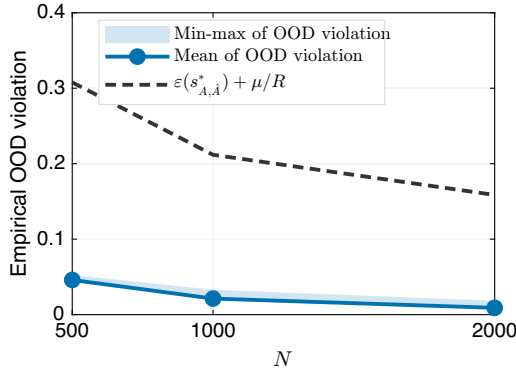


Fig. 5: Empirical distributional violations among $N' = 40$ different distribution perturbations from the ambiguity set.

R , or the number of samples N by trading some of the PLM's profit in return.

VI. CONCLUSION

This paper develops a distributionally robust framework based on scenario optimization that enables a parking-lot manager to operate aggregated EVs as a virtual energy storage system, providing profit/risk tuning flexibility and finite-sample guarantees under adversarial perturbations and Wasserstein distribution shifts. Numerical simulations on the proposed model show the alignment between empirical violation and theoretical bounds. Future work will involve integrating user-centric EV battery-health considerations into this scheme and modelling the EV users as active participants of the parking lot management system. Furthermore, this model can be extended for large-scale implementation by involving multiple interacting parking lots for market participation and incorporating network constraints.

REFERENCES

- [1] N. Mignoni, R. Carli, and M. Dotoli, "A noncooperative stochastic rolling horizon control framework for V1G and V2B scheduling in energy communities," in *2023 European Control Conference (ECC)*. IEEE, 2023, pp. 1–6.
- [2] K. Paridari, A. Parisio, H. Sandberg, and K. H. Johansson, "Demand response for aggregated residential consumers with energy storage sharing," pp. 2024–2030, 2015.
- [3] G. G. Zanvettor, M. Fochesato, M. Casini, J. Lygeros, and A. Vicino, "A stochastic approach for ev charging stations in demand response programs," *Applied Energy*, vol. 373, p. 123862, 2024.
- [4] W. Kempton and J. Tomić, "Vehicle-to-grid power fundamentals: Calculating capacity and net revenue," *Journal of Power Sources*, vol. 144, no. 1, pp. 268–279, 2005.
- [5] K. Sevdari, L. Calearo, P. B. Andersen, and M. Marinelli, "Ancillary services and electric vehicles: An overview from charging clusters and chargers technology perspectives," *Renewable and Sustainable Energy Reviews*, vol. 167, p. 112666, 2022.
- [6] G. G. Zanvettor, M. Casini, R. S. Smith, and A. Vicino, "Stochastic energy pricing of an electric vehicle parking lot," *IEEE Transactions on Smart Grid*, vol. 13, no. 4, pp. 3069–3081, 2022.
- [7] C. Duan, L. Jiang, W. Fang, and J. Liu, "Data-driven affinely adjustable distributionally robust unit commitment," *IEEE Transactions on Power Systems*, vol. 33, no. 2, pp. 1385–1398, 2018.
- [8] W. Wang and L. Wu, "A semi-decentralized real-time charging scheduling scheme for large ev parking lots considering uncertain ev arrival and departure," *IEEE Transactions on Smart Grid*, vol. 15, no. 6, pp. 5871–5884, 2024.
- [9] M. C. Campi, A. Carè, L. G. Crespo, S. Garatti, and F. A. Ramponi, "Risk analysis and design against adversarial actions," *arXiv:2505.01130*, 2025.
- [10] S. Garatti and M. C. Campi, "Risk and complexity in scenario optimization," *SIAM Journal on Optimization*, vol. 19, no. 3, pp. 1231–1258, 2008.
- [11] M. C. Campi and S. Garatti, "The exact feasibility of randomized solutions of uncertain convex programs," *SIAM Journal on Optimization*, vol. 19, no. 3, pp. 1211–1230, 2008. [Online]. Available: <https://epubs.siam.org/doi/10.1137/07069821X>
- [12] G. C. Calafiore and M. C. Campi, "The scenario approach to robust control design," *IEEE Transactions on Automatic Control*, vol. 51, no. 5, pp. 742–753, 2006.
- [13] M. C. Campi and S. Garatti, "Wait-and-judge scenario optimization," *Mathematical Programming*, vol. 167, no. 1, pp. 155–189, 2018.
- [14] S. Garatti and M. C. Campi, "Risk and complexity in scenario optimization," *Mathematical Programming*, 2019.
- [15] G. Pantazis, F. Fele, and K. Margellos, "A posteriori probabilistic feasibility guarantees for nash equilibria in uncertain multi-agent games," *IFAC-PapersOnLine*, vol. 53, no. 2, pp. 3403–3408, 2020.
- [16] —, "On the probabilistic feasibility of solutions in multi-agent optimization problems under uncertainty," *European Journal of Control*, vol. 63, pp. 186–195, 2022.
- [17] F. Fele and K. Margellos, "Probably approximately correct nash equilibrium learning," *IEEE Transactions on Automatic Control*, vol. 66, no. 9, pp. 4238–4245, 2021.
- [18] G. Pantazis, F. Fele, and K. Margellos, "A priori data-driven robustness guarantees on strategic deviations from generalised Nash equilibria," *Automatica*, vol. 167, p. 111746, 2024.
- [19] H. Mohsenian-Rad and M. Ghamkhari, "Optimal charging of electric vehicles with uncertain departure times: A closed-form solution," *IEEE Transactions on Smart Grid*, vol. 6, no. 2, pp. 940–942, 2015.
- [20] I. Chandra, N. K. Singh, P. Samuel, M. Bajaj, and I. Zaitsev, "Coordinated charging of ev fleets in community parking lots to maximize benefits using a three-stage energy management system," *Scientific Reports*, vol. 14, p. 32026, 2024.
- [21] Y. Zheng, Y. Wang, and Q. Yang, "Bidding strategy design for electric vehicle aggregators in the day-ahead electricity market considering price volatility: A risk-averse approach," *Energy*, vol. 283, p. 129138, 2023.
- [22] M. Tostado-Véliz, H. M. Hasanien, J. Carpio, and F. Jurado, "Risk-aware strategies for optimal participation of parking lots in day-ahead electricity markets," *Energy*, vol. 322, p. 135406, 2025.
- [23] M. C. Campi, A. Carè, L. G. Crespo, S. Garatti, and F. A. Ramponi, "Risk analysis and design against adversarial actions," *arXiv preprint*, 2025. [Online]. Available: <https://arxiv.org/abs/2505.01130>
- [24] W. Wei, F. Liu, and S. Mei, "Energy pricing and dispatch for smart grid retailers under demand response and market price uncertainty," *IEEE Transactions on Smart Grid*, vol. 6, pp. 1364–1374, 2015.
- [25] G. Schildbach, L. Fagiano, and M. Morari, "Randomized solutions to convex programs with multiple chance constraints," *SIAM Journal on Optimization*, vol. 23, no. 4, pp. 2315–2340, 2013.