<http://www.diva-portal.org>

Postprint

This is the accepted version of a paper published in *IEEE Transactions on Smart Grid*. This paper has been peer-reviewed but does not include the final publisher proof-corrections or journal pagination.

Citation for the original published paper (version of record):

Avula, R R., Chin, J-X., Oechtering, T J., Hug, G., Månsson, D. (2021)
Design Framework for Privacy-Aware Demand-Side Management with Realistic Energy
Storage Model
IEEE Transactions on Smart Grid, : 1-1
<https://doi.org/10.1109/TSG.2021.3066128>

Access to the published version may require subscription.

N.B. When citing this work, cite the original published paper.

Permanent link to this version:

<http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-293101>

Design Framework for Privacy-Aware Demand-Side Management with Realistic Energy Storage Model

Ramana R. Avula, *Student Member, IEEE*, Jun-Xing Chin, *Member, IEEE*,

Tobias J. Oechtering, *Senior Member, IEEE*, Gabriela Hug, *Senior Member, IEEE*, and Daniel Månsson

Abstract—Demand-side management (DSM) is a process by which the user demand patterns are modified to meet certain desired objectives. Traditionally, DSM was utility-driven, but with an increase in the integration of renewable sources and privacy-conscious consumers, it also becomes a “consumer-driven” process. Promising theoretical studies have shown that privacy can be achieved by shaping the user demand using an energy storage system (ESS). In this paper, we present a framework for utility-driven DSM while considering the user privacy and the ESS operational cost due to its energy losses and capacity degradation. We propose an ESS model using a circuit-based and data-driven approach that can be used to capture the ESS characteristics in control strategy designs. We measure privacy leakage using the Bayesian risk of a hypothesis testing adversary and present a novel recursive algorithm to compute the optimal privacy control strategy. Further, we design an energy-flow control strategy that achieves the Pareto-optimal trade-off between privacy leakage, deviation of demand from a DSM target profile, and the ESS cost. With numerical experiments using real household data and an emulated lithium-ion battery, we show that the desired level of privacy and demand shaping performance can be achieved while reducing the ESS degradation.

Index Terms—Demand-side management, smart meter privacy, energy storage model, Bayesian hypothesis testing, lithium-ion battery degradation.

I. INTRODUCTION

ELECTRICITY demand in a power grid can vary significantly within short time frames, depending on weather and other common user patterns. Generally, a conventional power system responds to these fluctuations by increasing or decreasing the generation. During peak demand, the additional generation is supplied by standby generators, which incur additional costs and reduces the energy efficiency of the grid. As a consequence, the idea of demand-side management (DSM) has emerged. DSM is a process by which the users' energy demands are modified with various incentives to bring them closer to the desired demand pattern. To enable DSM in smart grids, smart meters (SMs) play a crucial role by facilitating two-way communication between the user and the utility provider. Based on cost-benefit analyses, the European

Manuscript received June 2, 2020; revised November 20, 2020 and March 02, 2021; accepted March 08, 2021. This work was supported in part by KTH graduate school on Digitalization of Swedish Electrical Engineering Industry and Swedish Energy Agency project STOMP under grant P43019-1.

R. R. Avula, T. J. Oechtering, and Daniel Mannsönd are with the School of Electrical Engineering and Computer Science, KTH Royal Institute of Technology, Stockholm 10044, Sweden (e-mail: {avula, oech.mannsönd}@kth.se).

J. Chin is with the Singapore-ETH Centre, ETH Zürich, Singapore 138602 (e-mail: jack.chin@sec.ethz.ch).

G. Hug is with the Power Systems Laboratory, ETH Zürich, 8092 Zürich, Switzerland (e-mail: hug@eeh.ee.ethz.ch).

Fig. 1. The smart metering system which enables the privacy-aware DSM by altering the user demand from the grid Y_k using an ESS so that the deviation from the reference signal $\bar{Y}_k$ is minimized while reducing the privacy leakage and losses in the ESS. Here, the solid lines denote the energy flow and the dotted lines denote the information flow.

Commission Electricity Directive (2009/72/EC) mandates that its member countries should have at least 80% of users equipped with SMs by 2020 [1].

However, the large-scale roll-out of SMs triggered public opposition in several countries due to concerns about privacy [2]. Non-intrusive load monitoring (NILM) techniques have become quite effective in dis-aggregating the household energy consumption data and thereby detecting the states of most of the general types of household appliances [3]. In contrast to the data security problem, where traditional encryption techniques may prevent unauthorized access, any legitimate receiver such as the utility provider or a third-party agent can be an adversary in the SM privacy problem. The General Data Protection Regulation (GDPR) in Europe defines strict rules when dealing with data that contain sensitive personal information. In particular, the GDPR prohibits the processing of data that may reveal, for example, health status, religious beliefs, etc., without the users' informed consent. Therefore, when using SM data one should *not be able* to infer information about health-related appliances or appliance usage patterns during specific days that may reveal the religious beliefs of consumers without consent.

Addressing the SM privacy problem, several privacy-by-design techniques have been proposed in the literature [4]–[25], which can be classified into two main categories: *data manipulation* techniques that directly alter the SM data; and *user demand shaping* techniques that physically alter the user demand from the grid using energy storage systems (ESSs), flexible loads such as heating systems, and renewable energy sources. Although data manipulation techniques may succeed in protecting privacy in the measured SM data, they result in a mismatch between the reported and the real energy consumption values (quantity or timing or both). More importantly, these techniques would fail if an adversary gathers high-

frequency energy consumption data using an additional meter outside a household [4]. So, we consider the physical layer privacy problem in the system shown in Fig. 1 where the user demand from the grid Y_k is altered using an ESS so that the deviation from a reference signal $\bar{Y}_k$ is minimized while reducing the privacy leakage in the smart meter measurements and losses in the ESS. Here, we envision a future smart grid where the DSM operator generates the reference signal $\bar{Y}_k$ for each user to actively control the grid in real-time. Alternatively, the reference signal $\bar{Y}_k$ may be generated by a local controller based on a demand response incentive signal from the DSM operator such as time-of-use electricity price.

Although several user demand shaping techniques have been proposed in the literature, the physical ESS operating limitations on the energy management unit (EMU) strategy design, the effects of privacy-preserving control actions on the ESS, and the utility-driven DSM are not well understood. To the best of our knowledge, [22] is the first attempt to consider a deterministic ESS model characterizing energy losses due to privacy control actions of a one-step-ahead sub-optimal EMU strategy. Further, [23] considers capacity and energy loss degradation aspects in the privacy controller design using a deterministic energy storage model based on degradation maps. Extending [22] and [23], in this work, we propose a stochastic ESS model that is circuit-based as well as data-driven, characterizes important ESS aspects such as energy losses and capacity degradation, and can be used for general storage technologies such as electrochemical batteries, flywheels, and pumped hydro storage.

Compared to other privacy metrics such as mutual information [10]–[17]; conditional entropy [6], [20]; Kullback-Leibler divergence in [18]; and load variance [9], Bayesian risk [21]–[24] has an operational meaning as it explicitly captures the detection performance of an adversary. Hence, using the Bayesian risk metric, we model the adversary using the Bayesian hypothesis testing framework [26] and present the design of an EMU strategy that *optimally* trades-off privacy risk, deviation from the DSM target profile, and the ESS cost. With the same system model and optimization objective, our preliminary work [24] briefly presents the strategy design and initial numerical simulation results. We note that this work significantly extends [24] by deriving the stochastic modeling approach to capture crucial ESS aspects as well as deriving the optimal EMU control strategy. Moreover, in this work, the numerical experiments have been significantly extended, including a comparative study that demonstrates the value of the stochastic modeling approach. In summary, this paper introduces a novel and comprehensive design framework for privacy-preserving DSM that includes crucial ESS aspects, which enhances the technology readiness of these approaches. The key contributions are as follows:

- We propose a realistic ESS model that is both circuit-based and data-driven, which captures the steady-state energy losses and slow degradation in ESS capacity. This model can be used to capture the ESS characteristics in control strategy designs with sufficient accuracy.
- We present a framework for privacy-aware DSM and an EMU strategy that optimally trades-off privacy risk,

deviation from the DSM target profile, and ESS cost. We also present a recursive approach to optimally control the risk against a hypothesis testing adversary.

- We validate our design approach with numerical simulations using real household consumption data and an emulated battery. Using the numerical study, we illustrate the need for using accurate ESS models in EMU strategy designs to achieve close-to-optimal privacy-preserving and DSM performance.

Notations: Throughout the paper, we denote random variables by capital letters, their realizations by lower-case letters, and their alphabets, i.e., range spaces by calligraphic letters. We use $A_{k:k+i}$ to denote the row vector $[A_k, A_{k+1}, \dots, A_{k+i}]$; $\mathbb{E}[\cdot]$ to denote the expectation operator; $(\cdot)^\top$ to denote the matrix transpose; $P_A(a)$ to denote a probability distribution function; $\mathbb{1}$ to denote an indicator function for which $\mathbb{1}\{a\} = 1$ if a is true, and 0 otherwise; $\mathbf{1}_n$ is an n dimensional vector with all entries equal to one; and Δ_n to denote an $(n-1)$ dimensional simplex. If not specified, the domain of a variable in summations and integrals is its alphabet. The nomenclature used in the paper is given in Table I.

II. SYSTEM MODEL

A. Preliminaries

In the presented design framework, the user demand is controlled by an EMU using a strategy that is pre-computed for a discrete-time finite-horizon $\mathcal{K} := \{1, \dots, N\}$. Within $\mathcal{K}$, let k denote the index of the time-slot with a fixed duration T . Let $x_{\max}$, $y_{\max}$, and $\tilde{z}_r$ denote the maximum power demand of the user, maximum power drawn from the grid, and the rated energy capacity of the ESS respectively. Further, we denote the rated discharge and charge powers by $d_{r,d}$ and $d_{r,c}$ respectively.

For each $k \in \mathcal{K}$, we model the consumer's power demand, the SM measurement, and the operating power of the ESS using discrete random variables denoted by X_k , Y_k , and D_k respectively, which are defined on finite alphabets $\mathcal{X}$, $\mathcal{Y}$, and $\mathcal{D}$. Let $\tilde{Z}_k$ denote the continuous random variable defined on $[0, \tilde{z}_r]$, which represents the available energy in the ESS. Further, let Z_k denote the quantized value of the energy state $\tilde{Z}_k$, which is defined on a finite alphabet $\mathcal{Z}$. Further, we design an ancillary service provided by the user for the DSM. At each k , the EMU receives a target demand signal from the grid operator, which is modeled using a discrete random variable $\bar{Y}_k$ defined on $\mathcal{Y}$. We assume that the probability distribution of the target signal $P_{\bar{Y}_k}$ is available to the EMU before the horizon $\mathcal{K}$ starts, which can be empirically computed by the EMU or publicly broadcasted by the grid operator for DSM.

Further, let $\tilde{E}_k$ and $\tilde{B}_k$ denote continuous random variables defined on $\mathbb{R}_+$, which represent the operational energy loss and the charge-capacity loss of an ESS. Let $l \in \mathbb{N}$ denote the time index starting when the ESS is new and let $\phi_l \in [0, 1]$ denote the *age* of an ESS given by

$$\phi_l = \frac{1}{(\tilde{z}_r - \tilde{z}_{\text{eol}})} \sum_{m=1}^l \tilde{b}_m, \quad \forall l \geq 1,$$

where $\tilde{z}_{\text{eol}}$ denotes the ESS capacity at its end of life.

TABLE I. NOMENCLATURE

Parameters	
T, N	Duration and the number of time-slots in finite horizon
$\tilde{z}_r, \tilde{z}_{eol}$	ESS energy capacity at its beginning and end of life
$d_{r,c}, d_{r,d}$	Maximum charging and discharging power of the ESS
$x_{\max}, y_{\max}$	Maximum user demand and max. power drawn from grid
$\theta, \hat{\theta}$	Sets of HMM parameters of EMU and modeled adversary
$\bar{c}(h, \hat{h})$	Reward of an adversary in Bayesian hypothesis testing
ω_u, ω_c	Trade-off parameters of the objectives in $[0, 1]$
ρ, λ_k	Price of unit charge-capacity loss of ESS and unit energy
r_l^{sd}, c_l^{sd}	Self-dissipation circuit parameters of the ESS
r_l, v_l	Internal resistance and terminal voltage of the ESS
σ_l	Efficiency factor of the ESS power converter
Deterministic variables	
k	Time-slot index in the horizon $\mathcal{K}$
l	Time-slot index starting from when the ESS is new
ϕ_l	Age of the ESS at time-slot l , represented in $[0, 1]$
$\bar{r}_k$	Bayesian risk of the user
w_k	Mean square demand deviation from the target signal $\bar{Y}_k$
c_k	Average ESS operational cost due to losses
Random variables and their realizations	
H_k, h_k	Hypothesis state of user
$\hat{H}_k, \hat{h}_k$	Hypothesis state guessed by the modeled adversary
X_k, x_k	Actual power consumption of user
Y_k, y_k	Power drawn from grid (and measured by SM)
$\bar{Y}_k, \bar{y}_k$	Target signal from grid for DSM
D_k, d_k	ESS power consumption
$\tilde{Z}_k, \tilde{z}_k$	ESS energy state defined on $\mathbb{R}_+$
Z_k, z_k	Quantized ESS energy state defined on $\mathcal{Z}$
$\tilde{E}_k, \tilde{e}_k$	ESS energy loss
$\tilde{B}_k, \tilde{b}_k$	ESS charge-capacity loss
Ψ_l, ψ_l	Three-circuit model parameters set of the ESS
$\hat{\Pi}_k, \hat{\pi}_k$	Belief state of the modeled adversary
S_k, s_k	EMU state vector
I_k, i_k	Information state of EMU
Sets and state-spaces	
$\mathbb{R}_+, \mathbb{N}$	Sets of non-negative real numbers and positive integers
$\mathcal{K}$	Discrete time-horizon in the EMU strategy design
$\mathcal{H}, \mathcal{X}, \mathcal{Y}, \mathcal{Z}$	Discrete space of random variables H_k, X_k, Y_k, Z_k
$\mathcal{D}, \mathcal{I}_k$	Discrete space of D_k, I_k
$\mathcal{G}_k$	Set of polyhedrons within $\Delta_{ \mathcal{H} }$
$\mathcal{U}_k$	Set of randomized strategies of EMU
Functions	
$f_{act}^{(l)}$	function that accurately describes relation between the variables in the sequence $[\tilde{z}_{1:l+1}, \tilde{b}_{1:l}, \tilde{e}_{1:l}, d_{1:l}]$
f_3	a deterministic ESS model based on electrical circuits
$\mathbf{M}_{\hat{\pi}}$	function that outputs matrices for belief state transformation
ζ_k	Randomized strategy of modeled adversary, which outputs a probability distribution of hypothesis guess $\hat{H}_k$
μ_k	Randomized strategy of the EMU, which outputs a probability distribution of control actions D_k

B. Energy storage system model

In practice, with repeated charge and discharge operations of an ESS, the energy losses increase and the usable capacity decreases due to physical degradation processes, which is known as *cycle aging*. Further, an ESS undergoes *calendar aging* whereby the ESS capacity degrades even when it is not being used [27]. Let $f_{act}^{(l)}$ denote a deterministic function that accurately models these physical processes considering the complete history of the ESS states starting with a new battery, represented as

$$(\tilde{z}_{l+1}, \tilde{b}_l, \tilde{e}_l, \tilde{\psi}_l) = f_{act}^{(l)}(\tilde{z}_{1:l}, d_{1:l}, \tilde{b}_{1:l-1}, \tilde{e}_{1:l-1}, \tilde{\psi}_{1:l-1}), \quad (1)$$

where $\tilde{\psi}_l$ represents a set of parameters of a specific ESS. To achieve truly *optimal* control, we need to consider $f_{act}^{(l)}$ in the control strategy design. However, in general, it is difficult to specify $f_{act}^{(l)}$ since the relationships between the variables are too complex and highly depend on the storage technology. Even if there exist high fidelity deterministic models that approximate $f_{act}^{(l)}$, such as in [28], [29] for lithium-ion battery systems, the dimensionality of $\tilde{\psi}_l$ is generally big and hence these high fidelity models are computationally too complex to be used in system-level optimization problems. In such situations, using a stochastic model has been a successful approach in other engineering problems¹. We therefore propose an ESS model using a simplified deterministic model to describe energy losses and a stochastic model to capture the remaining effects such as temperature dependence, capacity fading, etc.

We first present a circuit-based deterministic ESS model to describe the steady-state energy losses, as shown in Fig. 2, which has been studied in the literature in different variations [30]–[33], but in deterministic settings. The circuit in Fig. 2(a) models the self-dissipation phenomenon using an RC network of capacitance c_l^{sd} and resistance r_l^{sd} . Fig. 2(b) shows the circuit that models the internal resistive losses using a resistor r_l , and the circuit in Fig. 2(c) models the power converter losses using an efficiency factor $\sigma_l \in [0, 1]$. The charge content on the capacitor is updated through a current source controlled by the current i_l flowing through the circuit in Fig. 2(b). Further, let v_l denote the open-circuit voltage across the converter, which is modeled using a voltage source controlled by the charge content on the capacitor. Here, we assume that the circuit parameters and the circuit current remain unchanged within the duration of the time slot. By solving the circuit equations, the energy state $\tilde{z}_{l+1}$ is given by

$$\tilde{z}_{l+1} = (1 - \gamma_l)\tilde{z}_l + \frac{\gamma_l \tau_l v_l}{2r_l} \left[\sqrt{v_l^2 + 4r_l \sigma_l d_l} - v_l \right], \quad (2)$$

$$=: f_3(\tilde{z}_l, d_l, \psi_l), \quad (3)$$

where $\psi_l = \{v_l, r_l, \gamma_l, \sigma_l\}$ denotes the set of parameters of the three-circuit model, $\gamma_l = 1 - \exp(-T/\tau_l)$, $\tau_l = r_l^{sd} c_l^{sd}$, and f_3 is a deterministic function given on the right-hand side of (2). In this work, we use the energy state estimate of the three-circuit model as the actual energy state of an ESS. The steady-state energy loss estimate obtained by balancing the energy flow is given by

$$\tilde{e}_l = \tilde{z}_l + d_l T - f_3(\tilde{z}_l, d_l, \psi_l). \quad (4)$$

In this work, we extend the three-circuit deterministic model by considering the circuit parameters ψ_l and the ESS capacity loss $\tilde{b}_l$ as random variables whose characteristics are learnt using a data driven approach. In practice, the data samples can either be obtained using system-identification methods such as in [34], [35] or using existing high-fidelity models [28], [29]. Assuming that sufficient data of $[\tilde{b}_{1:l}, \psi_{1:l}, \tilde{z}_{1:l}, d_{1:l}]$ is available, we characterize the dependency between these

¹In wireless communications, the ray-tracing approach provides a high-fidelity model. However, transmission strategies are often designed using simple stochastic models such as Rayleigh fading and more realistic simulations are done using detailed stochastic models such as COST 2100 or COST 259.

Fig. 2. Three-circuit ESS model that characterizes the energy losses.

variables using empirically estimated conditional probability density function (PDF) $P_{\tilde{B}_l, \Psi_l | \tilde{Z}_{1:l}, D_{1:l}, \tilde{B}_{1:l-1}, \Psi_{1:l-1}}$, where Ψ_l denotes the random variable that represents the set of parameters of the three-circuit model. To limit the increasing dimensionality of this conditional PDF, we partition the age interval $[0, 1]$ into a finite number of intervals within which we assume that the variables in $[\tilde{B}_{1:l}, \Psi_{1:l}, \tilde{Z}_{1:l}, D_{1:l}]$ follow a time-invariant Markov chain

$$(\tilde{B}_l, \Psi_l) - (\tilde{Z}_l, D_l) - (\tilde{Z}_{l-1}, D_{l-1}, \tilde{B}_{l-1}, \Psi_{l-1}). \quad (5)$$

Further, assuming that the circuit based model represented by (3) and (4) accurately captures the energy state transition and energy loss, we arrive at the simplified stochastic representation of the ESS model $P_{\tilde{Z}_{l+1}, \tilde{B}_l, \tilde{E}_l | \tilde{Z}_l, D_l}$ in (6). The first term in the integral in (6) can be empirically estimated using the available data. Whereas, the second term can be obtained using (2) and (4), i.e.,

$$P_{\tilde{Z}_{l+1}, \tilde{E}_l | \tilde{Z}_l, D_l, \Psi_l}(\tilde{z}_{l+1}, \tilde{e}_l | \tilde{z}_l, d_l, \psi_l) = \mathbb{1}\{\tilde{z}_{l+1} = f_3(\tilde{z}_l, d_l, \psi_l)\} \times \mathbb{1}\{\tilde{e}_l = \tilde{z}_l + d_l T - f_3(\tilde{z}_l, d_l, \psi_l)\}. \quad (7)$$

In (6) we marginalize the circuit parameters Ψ_l since, in this work, the objective functions in the control strategy design do not depend on the circuit parameters directly. To reduce the computational complexity of the control strategy design, we did not consider circuit parameter ψ_l as a state variable. However, it is measured and used in the estimation of the conditional PDF $P_{\tilde{Z}_{l+1}, \tilde{B}_l, \tilde{E}_l | \tilde{Z}_l, D_l}$ and in the real-time computation of the energy state $\tilde{z}_{l+1}$.

Furthermore, when using discrete energy states Z_l in the EMU strategy design, we characterize the ESS using a conditional PDF $P_{\tilde{Z}_{l+1}, \tilde{B}_l, \tilde{E}_l | Z_l, D_l}$ that is induced by (6) as a result of the quantization of continuous state $\tilde{Z}_l$. To achieve

optimal control, the data samples $[\tilde{b}_{1:l}, \psi_{1:l}, \tilde{z}_{1:l}, d_{1:l}]$ used for estimating $P_{\tilde{Z}_{l+1}, \tilde{B}_l, \tilde{E}_l | Z_l, D_l}$ should ideally be generated using the distribution P_{Z_l, D_l} corresponding to the optimal control strategy, which in turn depends on $P_{\tilde{Z}_{l+1}, \tilde{B}_l, \tilde{E}_l | Z_l, D_l}$. Given this circular dependency, we propose to use an iterative approach where an initial distribution P_{Z_l, D_l} is used to generate the data samples. Then $P_{\tilde{Z}_{l+1}, \tilde{B}_l, \tilde{E}_l | Z_l, D_l}$, the EMU strategy, and P_{Z_l, D_l} are updated iteratively.

C. Adversarial model

Generally, the user demands are associated with events of appliance usage, user presence or absence in the house during certain hours, etc., which in turn depend on user behavioral patterns. We call these events, which are privacy-sensitive to a user, as *hypothesis states*, denoted by a discrete random variable H_k . Let $\mathcal{H}$ denote a finite alphabet of H_k . Further, we model the dependency between the sequence of user demands and hypothesis states $(H_{1:N}, X_{1:N})$ corresponding to the finite-horizon $\mathcal{K}$ using a first-order hidden Markov model (HMM), which simplifies their joint distribution as:

$$P_{H_{1:N}, X_{1:N}}(h_{1:N}, x_{1:N}) = \prod_{k=1}^N P_{X_k | H_k}(x_k | h_k) \times P_{H_k | H_{k-1}}(h_k | h_{k-1}), \quad (8)$$

where $P_{X_k | H_k}$ and $P_{H_k | H_{k-1}}$ are the time-dependent observation and transition probabilities and the HMM is initialized by a prior probability P_{H_1} , which denotes $P_{H_1 | H_0}$. The HMM can be characterized using the set of parameters

$$\theta := \{P_{X_k | H_k}, P_{H_k | H_{k-1}}; \forall k \in \mathcal{K}\}.$$

In practice, the HMM θ can be learned by the EMU using private historical data of the user. Let $\hat{\theta}$ be the adversarial estimate of θ that can be obtained either by using publicly available datasets or by using the historical data of the specific user. In this work, we model the adversary using the Bayesian hypothesis testing framework [26]. We consider an adversary who is unaware of the energy manipulation, and makes a guess on the hypothesis state h_k using the causal SM data $y_{1:k}$ and HMM $\hat{\theta}$. Let $\hat{H}_k$ denote the adversarial hypothesis guess on H_k , which is a discrete random variable defined on $\mathcal{H}$. In Bayesian hypothesis testing, each of the test outcomes $(h, \hat{h}) \in \mathcal{H}^2$ is assigned a reward, denoted by $\bar{c}(h, \hat{h}) \geq 0$, and an optimal detection strategy is designed by optimizing the expected cumulative reward. Let $\bar{r}_k$ denote the expected privacy cost of the user (or the expected detection reward of the adversary), known as the *Bayesian risk* of the user (or the *Bayesian reward* of the adversary), given by

$$\bar{r}_k = \mathbb{E}[\bar{c}(H_k, \hat{H}_k)] = \sum_{h, \hat{h} \in \mathcal{H}^2} \bar{c}(h, \hat{h}) P_{H_k, \hat{H}_k}(h, \hat{h}). \quad (9)$$

$$P_{\tilde{Z}_{l+1}, \tilde{B}_l, \tilde{E}_l | \tilde{Z}_{1:l}, D_{1:l}, \tilde{B}_{1:l-1}, \Psi_{1:l-1}}(\tilde{z}_{l+1}, \tilde{b}_l, \tilde{e}_l | \tilde{z}_{1:l}, d_{1:l}, \tilde{b}_{1:l-1}, \psi_{1:l-1}) \\ = \int_{\psi_l} P_{\tilde{B}_l, \Psi_l | \tilde{Z}_l, D_l}(\tilde{b}_l, \psi_l | \tilde{z}_l, d_l) P_{\tilde{Z}_{l+1}, \tilde{E}_l | \tilde{Z}_l, D_l, \Psi_l}(\tilde{z}_{l+1}, \tilde{e}_l | \tilde{z}_l, d_l, \psi_l) d\psi_l = P_{\tilde{Z}_{l+1}, \tilde{B}_l, \tilde{E}_l | \tilde{Z}_l, D_l}. \quad (6)$$

We consider $\bar{c}(h, \hat{h})$ with a structure where the reward for a correct guess is higher compared to that of the wrong guess so that the adversary aims to maximize the cumulative reward, while the EMU aims to minimize it. In a special case with $\bar{c}(h, \hat{h}) = 1$ for a correct guess and $\bar{c}(h, \hat{h}) = 0$ for a wrong guess, the Bayesian risk $\bar{r}_k$ represents the successful detection probability of the adversary. Due to this operational meaning, we use the Bayesian risk metric to measure privacy leakage.

III. OPTIMAL ENERGY MANAGEMENT STRATEGY DESIGN

In the smart-metering system shown in Fig. 1, the EMU schedules charge and discharge operations of an ESS that achieve desired levels of privacy and demand shaping by following a DSM target profile, while also considering the ESS operational costs. In the following, we first design optimal energy management strategies separately and then present a randomized control strategy to trade-off between optimal values of the multiple objectives.

In this work, we assume that the EMU has access to all the causal information of the system states and formulate Markov decision processes (MDPs) to design an optimal control strategy with respect to each objective. Let $S_k := [X_k, Z_k, H_k, \bar{Y}_k]$ denote the EMU state vector, which is defined on the discrete space $\mathcal{S} := \mathcal{X} \times \mathcal{Z} \times \mathcal{H} \times \mathcal{Y}$. Further, let $I_k := [S_{1:k}, D_{1:k-1}, Y_{1:k-1}]$ denote the information available to the EMU, which is defined on $\mathcal{I}_k := \mathcal{S}^k \times \mathcal{D}^{k-1} \times \mathcal{Y}^{k-1}$. Let $\mu_k : \mathcal{I}_k \rightarrow \Delta_{|\mathcal{D}|}$ denote a randomized EMU strategy, which is characterized by a conditional PDF $P_{D_k|I_k}$. Thus, for each $i_k \in \mathcal{I}_k$, the EMU strategy μ_k specifies a probability distribution of D_k , which can be represented by some vector $\beta_k \in \Delta_{|\mathcal{D}|}$, i.e., $\mu_k(i_k) = \beta_k$. Let $\mathcal{U}_k$ denote the set of all mappings from $\mathcal{I}_k$ to $\Delta_{|\mathcal{D}|}$. Let w_k denote the mean square demand deviation (MSDD) from the DSM target signal $\bar{Y}_k$, given by

$$w_k(i_k, \beta_k) = \mathbb{E}[(\bar{Y}_k - Y_k)^2 | I_k = i_k] = \sum_{d \in \mathcal{D}} (\bar{y}_k - (x_k + d))^2 P_{D_k|I_k}(d|i_k) \quad (10)$$

$$=: \beta_k^\top \cdot \mathbf{f}_w(s_k), \quad (11)$$

where $\mathbf{f}_w : \mathcal{S} \rightarrow \mathbb{R}_+^{|\mathcal{D}|}$ is a deterministic vector function which can be obtained from (10). Further, let ρ be the price of unit charge-capacity loss and λ_k be the price of unit energy drawn from the grid. Then, the average ESS operational cost denoted by c_k is given by

$$c_k(i_k, \beta_k) = \mathbb{E}[\rho \check{B}_k + \lambda_k \check{E}_k | I_k = i_k] = \sum_{d \in \mathcal{D}} \int_{\check{b}} \int_{\check{e}} (\rho \check{b}_k + \lambda_k \check{e}_k) P_{D_k|I_k}(d|i_k) \times P_{\check{B}_k, \check{E}_k | Z_k, D_k}(\check{b}_k, \check{e}_k | z_k, d) d\check{b} d\check{e} \quad (12)$$

$$=: \beta_k^\top \cdot \mathbf{f}_c(s_k, k), \quad (13)$$

where $\mathbf{f}_c : \mathcal{S} \times \mathcal{K} \rightarrow \mathbb{R}_+^{|\mathcal{D}|}$ is a deterministic vector function which can be obtained from (12).

A. Optimal control of the MSDD and the ESS cost objectives

Let $\mu_{w,1:N}^*$ and $\mu_{c,1:N}^*$ denote the optimal strategies among all $\mathcal{U}_k$ that minimize the expected cumulative values of $w_k(I_k, \beta_k)$ and $c_k(I_k, \beta_k)$, respectively over the horizon $\mathcal{K}$. Then, $\mu_{w,1:N}^*$ and $\mu_{c,1:N}^*$ can be characterized as follows.

Proposition 1. *For each $k \in \mathcal{K}$, the optimal strategies $\mu_{w,k}^*$ and $\mu_{c,k}^*$ specify deterministic control actions $d_{w,k}^*$ and $d_{c,k}^*$ which can be obtained by solving the recursive Bellman's equations:*

$$\begin{aligned} \tilde{w}_k(s) &= \min_{d \in \mathcal{D}} \left\{ [\mathbf{f}_w(s)]_d + \sum_{s' \in \mathcal{S}} \tilde{w}_{k+1}(s') P_{S_{k+1}|S_k, D_k}(s'|s, d) \right\}, \\ \tilde{c}_k(s) &= \min_{d \in \mathcal{D}} \left\{ [\mathbf{f}_c(s, k)]_d + \sum_{s' \in \mathcal{S}} \tilde{c}_{k+1}(s') P_{S_{k+1}|S_k, D_k}(s'|s, d) \right\}, \end{aligned}$$

where $\tilde{w}_k$ and $\tilde{c}_k$ represent the backward cumulative values of w_k and c_k , respectively from k to N due to the optimal strategies $\mu_{w,k:N}^*$ and $\mu_{c,k:N}^*$, and the conditional PDF $P_{S_{k+1}|S_k, D_k}$ is given by $P_{Z_{k+1}|Z_k, D_k}$, $P_{\bar{Y}_k}$, and the HMM θ .

The proof of Prop. 1 follows from the Bellman's principle of optimality [36, Section 6.2] and the fact that the objective functions of the MSDD and the ESS cost in (11) and (13) depend on i_k only through the EMU state s_k .

B. Optimal control of risk due to hypothesis testing adversary

For the design of the optimal Bayesian risk control strategy, we first derive the worst-case adversarial detection strategy that maximizes the average cumulative reward. Since the adversary is assumed to be unaware of the energy manipulation, the optimal sequential detection strategy of the adversary can be obtained by formulating a HMM filter [36, Section 3.5]. In this case, the unaware adversary considers the likelihood of the SM measurement y_k given a hypothesis $h_k \in \mathcal{H}$ to be $P_{X_k|H_k}(y_k|h_k)$. Further, the posterior distribution of the hypothesis state H_k given the sequence $y_{1:k}$ is given by $\Pr(H_k | X_{1:k} = y_{1:k})$, known as the *belief state* and denoted by $\hat{\Pi}_k$. Let $\hat{\pi}_k$ be its realization which lies on the simplex $\Delta_{|\mathcal{H}|}$. Using Bayes' rule, each element of $\hat{\pi}_k$ is given by

$$\begin{aligned} [\hat{\pi}_k(y_{1:k})]_h &= P_{H_k | X_{1:k}}(h | y_{1:k}) \\ &= \frac{\sum_{h'} P_{X_k, H_k | H_{k-1}}(y_k, h | h') [\hat{\pi}_{k-1}(y_{1:k-1})]_{h'}}{\sum_{\tilde{h}, \tilde{h}'} P_{X_k, H_k | H_{k-1}}(y_k, \tilde{h} | \tilde{h}') [\hat{\pi}_{k-1}(y_{1:k-1})]_{\tilde{h}'}}. \end{aligned}$$

Therefore, the belief state evolution follows a linear-fractional transformation given by

$$\hat{\pi}_k(y_k, \hat{\pi}_{k-1}) = \frac{\mathbf{M}_{\hat{\pi}}(y_k, k) \cdot \hat{\pi}_{k-1}}{\mathbf{1}_{|\mathcal{H}|}^\top \cdot \mathbf{M}_{\hat{\pi}}(y_k, k) \cdot \hat{\pi}_{k-1}}, \quad (14)$$

where $\mathbf{M}_{\hat{\pi}}$ is a deterministic function of *belief generating matrices* with its elements given by the HMM $\hat{\theta}$ as

$$[\mathbf{M}_{\hat{\pi}}(y_k, k)]_{h, h'} = P_{X_k | H_k}(y_k | h) P_{H_k | H_{k-1}}(h | h').$$

For each $k \in \mathcal{K}$, let ζ_k denote a randomized detection strategy of the adversary that is characterized by the conditional probability distribution $P_{\hat{H}_k | Y_{1:k}}$, which can be represented by some vector $\delta_k \in \Delta_{|\mathcal{H}|}$ for each sequence $y_{1:k}$. Further, the

expected detection reward perceived by the adversary for a given $y_{1:k}$ and δ_k can be expressed as

$$\begin{aligned}\bar{r}_k(y_{1:k}, \delta_k) &= \mathbb{E} \left[\bar{c}(H_k, \hat{H}_k) | X_{1:k} = y_{1:k} \right] \\ &= \sum_{h, \hat{h} \in \mathcal{H}^2} \bar{c}(h, \hat{h}) P_{\hat{H}_k | Y_{1:k}}(\hat{h} | y_{1:k}) P_{H_k | X_{1:k}}(h | y_{1:k}) \\ &=: \delta_k^T \cdot \mathbf{C} \cdot \hat{\pi}_k(y_{1:k}),\end{aligned}\quad (15)$$

where $\mathbf{C}$ is a matrix with the adversarial reward $\bar{c}(h, \hat{h})$ as its elements. Then, the optimal detection strategy, denoted by ζ_k^* , that minimizes the expected cumulative reward $\bar{r}_k(Y_{1:k}, \delta_k)$ over the finite-horizon $\mathcal{K}$ can be characterized as follows.

Proposition 2. *For all $k \in \mathcal{K}$, the optimal strategy ζ_k^* specifies a deterministic hypothesis guess $\hat{h}_k^*$ based only on the belief state $\hat{\pi}_k$, and ζ_k^* can be characterized using a set of polyhedral decision regions in the simplex $\Delta_{|\mathcal{H}|}$.*

The proof of Prop. 2 follows from the fact that the objective function in (15) depends on $y_{1:k}$ only through $\hat{\pi}_k$, which evolves using the linear-fractional function in (14). Note that the characterization of the adversarial strategy using polyhedral regions is equivalent to the likelihood-ratio test where the linear constraints defining the polyhedral decision regions correspond to the thresholds of the likelihood-ratio test. Further, the Bayesian risk perceived by the user for a given information i_k and a randomized control action distribution β_k is given by

$$\begin{aligned}\bar{r}_k(i_k, \beta_k) &= \mathbb{E} \left[\bar{c}(H_k, \hat{H}_k) | I_k = i_k \right] \\ &= \sum_{d \in \mathcal{D}} \bar{c}(h_k, \zeta_k^*(\hat{\pi}_k(x_k + d, \hat{\pi}_{k-1}))) P_{D_k | I_k}(d | i_k) \\ &=: \beta_k^T \cdot \mathbf{f}_{\bar{r}}(s_k, \hat{\pi}_{k-1}),\end{aligned}\quad (16)$$

where $\mathbf{f}_{\bar{r}} : \mathcal{S} \times \Delta_{|\mathcal{H}|} \rightarrow \mathbb{R}_+^{|\mathcal{D}|}$ is a deterministic vector function with the adversarial reward due to optimal detection strategy ζ_k^* as its elements. Then, the optimal strategies denoted by $\mu_{\bar{r}, 1:N}^*$ that minimize the expected cumulative values of $\bar{r}_k(I_k, \beta_k)$ over the horizon $\mathcal{K}$ can be characterized as follows.

Proposition 3. *For each $k \in \mathcal{K}$, the optimal strategy $\mu_{\bar{r}, k}^*$ specifies a deterministic control action $d_{\bar{r}, k}^*$, which can be obtained by solving the recursive Bellman's equation:*

$$\begin{aligned}\tilde{r}_k(s, \hat{\pi}_{k-1}) &= \min_{d_k \in \mathcal{D}} \left\{ [\mathbf{f}_{\bar{r}}(s, \hat{\pi}_{k-1})]_d + \right. \\ &\quad \left. \sum_{s' \in \mathcal{S}} \tilde{r}_{k+1}(s', \hat{\pi}_k(x + d, \hat{\pi}_{k-1})) P_{S_{k+1} | S_k, D_k}(s' | s, d) \right\},\end{aligned}\quad (17)$$

where $\tilde{r}_k$ represent the backward cumulative Bayesian risk from k to N due to the optimal strategies $\mu_{\bar{r}, k:N}^*$.

The proof of Prop. 3 follows from the Bellman's principle of optimality [36, Section 6.2] and the fact that the objective function in (16) depends on i_k only through the tuple $(s_k, \hat{\pi}_{k-1})$. Note that the backward recursion in (17) needs to be solved for all $\hat{\pi}_{k-1}$ in the continuous space $\Delta_{|\mathcal{H}|}$, similar to a partially observable Markov decision process (POMDP) control problem [36]. However, unlike a POMDP problem with a linear objective function where there exist algorithms to find the optimal control strategy, the objective in (17) depends non-linearly on $\hat{\pi}_{k-1}$. Nonetheless, the optimal

strategy $\mu_{\bar{r}, k}^*$ and the backward cumulative risk $\tilde{r}_k$ have the following structure.

Theorem 1. *At any $k \in \mathcal{K}$, if $\tilde{r}_{k+1}$ is piece-wise constant with respect to $\hat{\pi}_k$ in a set of polyhedral partitions, then the simplex $\Delta_{|\mathcal{H}|}$ can be partitioned into a finite set of polyhedrons $\mathcal{G}_k$ such that $\mu_{\bar{r}, k}^*$ is invariant and $\tilde{r}_k$ is constant with respect to $\hat{\pi}_{k-1}$ within each polyhedron of $\mathcal{G}_k$.*

Sketch of the proof: The constructive proof follows by showing the existence of polyhedral partitions $\mathcal{G}_k$, where $\tilde{r}_k$ is piece-wise constant, and they can be obtained using Algorithm 1. Further, Fig. 3 illustrates the transformations of a polyhedral partition with $|\mathcal{H}| = 3$. Here, $\mathcal{G}_k^{(m)}$ is the inverse image of $\mathcal{G}_{k+1}^{(n)}$ through (14), which can be constructed by taking the linear transformation of a polyhedral cone obtained by relaxing the equality constraint of $\mathcal{G}_{k+1}^{(n)}$ through the matrix $\mathbf{M}_{\hat{\pi}}^{-1}$. This backward transformation can be done for each partition in $\mathcal{G}_{k+1}$ using all non-singular belief generating matrices². If $\mathbf{M}_{\hat{\pi}}(y_k, k)$ is singular, then the forward propagation of $\hat{\pi}_{k-1}$ either becomes degenerate or lies in multiple partitions in $\mathcal{G}_{k+1}$. In this case, the control strategy depends on the adversarial model choice defining the forward propagation of $\hat{\pi}_{k-1}$. Generally, an unaware adversary may filter or ignore those SM measurement y_k which have very low likelihood $P_{X_k | H_k}$. In this case, the forward propagation of $\hat{\pi}_{k-1}$ can be modeled using only the transition probability $P_{H_k | H_{k-1}}$ or it can be reset to a priori distribution. Then, from (17), we have that $\tilde{r}_k$ is piece-wise constant with respect to $\hat{\pi}_{k-1}$. $\square$

Algorithm 1 Backward recursive belief state-space partitions.

- 1: **Initialization:** $\mathcal{M}(\hat{\theta})$, the set of belief generating matrices; $\mathcal{G}_{\zeta_k^*}$, the set of adversarial decision regions; $\mathcal{G}_{N+1} = \mathcal{G}_{\zeta_k^*}$.
- 2: **for** $i = N$ to 1 **do**
- 3: Set $\mathcal{G}_i = \mathcal{G}_{\zeta_k^*}$.
- 4: **for** $g_{i+1} = \{\hat{\pi} \in \Delta_{|\mathcal{H}|} : \mathbf{A}(g_{i+1}) \cdot \hat{\pi} \leq 0\} \in \mathcal{G}_{i+1}$ **do**
- 5: Partition and update $\mathcal{G}_i$ using linear constraints of $\mathbf{M}_{\hat{\pi}} \cdot \mathbf{A}(g_{i+1}) \cdot \hat{\pi} \leq 0, \quad \forall \mathbf{M}_{\hat{\pi}} \in \mathcal{M}(\hat{\theta}),$
- 6: **end for**
- 7: **end for**

Fig. 3. An example belief state-space partitioning recursion with $|\mathcal{H}| = 3$.

²In the backward recursion, the number of partitions of the simplex $\Delta_{|\mathcal{H}|}$ can grow exponentially with k depending on the numerical precision of the belief state. Hence, obtaining the optimal EMU strategy sequence, subject to a finite precision, may be computationally tractable for long time-horizon and high dimensional state space problems only with a low belief state precision.

C. Optimal control over successive cycles of finite horizons

Note that the performance of the designed finite-horizon optimal strategies depend on the initial energy state z_1 . Therefore, to achieve optimal performance over successive finite horizons, we formulate an infinite horizon problem with finite-horizon cycles $[\mathcal{K}_1, \mathcal{K}_2, \dots]$. Let $p \geq 1$ denote the index of finite-horizon and $\tilde{r}_{p,k}$, $\tilde{w}_{p,k}$ and $\tilde{c}_{p,k}$ denote the backward cumulative values of the Bayesian risk, the MSDD and the ESS cost corresponding to $k \in \mathcal{K}_p$. Then, extending the finite-horizon problems discussed above to the infinite horizon case, we introduce a discount factor $\epsilon \in [0, 1)$ and recursively solve the finite horizon problems initialized with:

$$\begin{aligned}\tilde{r}_{p,N+1}(s, \hat{\pi}_0) &= \epsilon \cdot \tilde{r}_{p-1,1}(s, \hat{\pi}_0), \\ \tilde{w}_{p,N+1}(s) &= \epsilon \cdot \tilde{w}_{p-1,1}(s), \quad \tilde{c}_{p,N+1}(s) = \epsilon \cdot \tilde{c}_{p-1,1}(s).\end{aligned}$$

Here, for bounded and real-valued vector functions $\mathbf{f}_{\tilde{r}}$, $\mathbf{f}_w$ and $\mathbf{f}_c$, as the discount factor $\epsilon < 1$, the backward cumulative value functions $\tilde{r}_{p,1}$, $\tilde{w}_{p,1}$, and $\tilde{c}_{p,1}$ converges over the finite-horizon iterations p . Based on Banach's fixed point theorem, this successive approximation technique leads to optimal control strategy sequences $\mu_{\tilde{r},1:N}^*$, $\mu_{w,1:N}^*$ and $\mu_{c,1:N}^*$ that achieve minimum expected discounted-cumulative values.

D. Pareto-optimal trade-off of privacy, DSM, and ESS cost

Since the objective functions w_k , c_k , and $\tilde{r}_k$ given in (11), (13), and (15) are linear with respect to the optimization variable $\beta_k \in \Delta_{|\mathcal{D}|}$, the achievable values of their aggregate sum within the finite horizon $\mathcal{K}$ form a convex region and the solutions obtained using the weighted-sum of the objectives lie on the Pareto-optimal boundary curve [37]. Hence, we design the Pareto-optimal trade-off strategy by optimizing the *weighted-sum*, denoted by q_k , which is given as

$$q_k = \omega_c \left[\omega_u \frac{w_k}{\eta_w} + (1 - \omega_u) \frac{\tilde{r}_k}{\eta_{\tilde{r}}} \right] + (1 - \omega_c) \frac{c_k}{\eta_c}, \quad (18)$$

where $\omega_u \in [0, 1]$ denotes the trade-off parameter that weighs the MSDD against the Bayesian risk objective, which are considered as utility to the user; $\omega_c \in [0, 1]$ denotes the trade-off parameter that weighs the utility of the user against the ESS cost; $\eta_w, \eta_{\tilde{r}}, \eta_c$ are the normalization factors of the objectives which are set according to their respective ranges. From (11), (13), and (16), we can represent the weighted-sum q_k as

$$q_k(i_k, \beta_k) = \beta_k^\top \cdot \mathbf{f}_q(s_k, \hat{\pi}_{k-1}), \quad (19)$$

where $\mathbf{f}_q : \mathcal{S} \times \Delta_{|\mathcal{H}|} \rightarrow \mathbb{R}_+^{|\mathcal{D}|}$ is a deterministic vector function, which can be obtained from the weighted-sum of the vector functions $\mathbf{f}_w$, $\mathbf{f}_{\tilde{r}}$, and $\mathbf{f}_c$, similar to (18). As the weighted-sum objective in (19) is similar to the Bayesian risk function in (16), the Pareto-optimal strategy sequence $\mu_{1:N}^*$ corresponding to some fixed (ω_u, ω_c) can be obtained using backward recursion similar to (17) and following the belief state-space partition approach given in Algorithm 1.

IV. NUMERICAL STUDY

A. Simulation Setup

To evaluate the design approach, we performed numerical simulations in MATLAB and COMSOL. We consider a utility-driven DSM scenario where the user receives a target demand signal from the grid which is constant throughout the day. The target signal is generated by the grid operator using the historical demands of the user averaged during the day. For simplicity, we consider a privacy scenario where the information about the presence or absence of the users in a house is to be protected in the SM measurements, i.e., the hypothesis state is defined as $H_k = 1$ when the users are absent and $H_k = 2$ when the users are present in the house. Other more complex hypothesis states may be considered given sufficient computational resources and data, but it is left for future work. We assign the Bayesian reward in hypothesis testing as $\bar{c}(i, i) = 1$ and $\bar{c}(i, j) = 0$ for $i, j \in \{1, 2\}, j \neq i$ so that the Bayesian risk corresponds to the average adversarial detection probability.

In the simulations, we have used data from the ECO dataset [38] corresponding to 5 houses measured during the summer of 2012. We consider a scenario where the adversary attempts to infer occupancy information of house 2 from which the adversary has no historical data, but has access to data from similar houses. We perform the simulations until the end of life of the ESS by repeating the available 83 days of household 2 data in cycles. In the simulations, we have set $x_{\max} = 2\text{kW}$ based on maximum power observed in the dataset, $d_{r,c} = d_{r,d} = 2.4\text{kW}$ corresponding to 1C ampere rating of 48V-50Ah battery, $y_{\max} = x_{\max} + d_{r,c} = 4.4\text{kW}$, $\tilde{z}_{\text{ref}} = \tilde{z}_r/5$ assuming that the battery reaches end of life after 20% of its initial capacity, $T = 1\text{h}$, $\mathcal{K} = \{1, \dots, 24\}$, $\sigma_l = 0.95$, $\gamma_l = 1$ assuming that self-dissipation within 1h time-slot is negligible, $\epsilon = 0.5$ as discount factor for infinite-horizon, $\lambda_l = 0.2\text{€/kWh}$ corresponding to the household energy cost in Sweden [39], $\rho = 650\text{€/kWh}$ using the lithium-ion battery cost from [40], the power resolution as 100W, and the belief state resolution as 0.01. For simplicity, the adversary is assumed to use a homogeneous HMM θ , whereas, the EMU strategies are designed using a non-homogeneous HMM θ . Throughout the simulations, we assume that the real-time energy state z_l (obtained either by direct measurements of three-circuit model parameters or estimated using high fidelity models) is available to the EMU.

B. Emulation of ESS using high fidelity models

In this study, we consider a 48V-50Ah lithium-ion battery as an ESS. To generate the data samples, we emulate a cylindrical 18650 Graphite/LiFePO₄ battery cell with a capacity of 1800mAh in COMSOL using high-fidelity electrochemical models developed in [28] and [29]³. Also, we

³The models in [28] and [29] capture the isothermal battery aging mechanism only at the negative electrode during the constant CC-CV charging operations. The suitability of these models for measuring the degradation during intermittent charging and discharging operations needs to be verified experimentally. The MATLAB and COMSOL programs to generate the data can be downloaded from <https://github.com/ravula93/Li-Ion-Degradation-Model>.

Fig. 4. Observed ESS characteristics using uniformly distributed (Z_l, D_l) .

consider calendar aging by taking a minimum state-dependent capacity loss at each discrete ESS state-action pair by linearly interpolating experimental data from [41]. In the simulations, we have limited the voltage range to $[2.5V, 4.2V]$ and the state-of-charge (SOC) range to $[0.1, 0.9]$ to avoid numerically infeasible solutions in the emulated models. Further, we have divided the age range $[0, 1]$ into 3 intervals, and starting with a new cell, we applied uniformly distributed random battery currents within each age interval. For each discrete state-action pair (z_l, d_l) , we measure 50 data sample $(\tilde{b}_l, \psi_l)$ and estimate $(\tilde{z}_{l+1}, \tilde{e}_l)$ using (2) and (4). Further, to avoid error accumulation in $\tilde{z}_{l+1}$ estimates, we reset the estimate to the actual energy state when the ESS reaches the SOC limits.

The resulting mean capacity loss, mean resistive energy loss and relative variance of discrete SOC estimates are shown in Fig. 4. We can see that, on average, the capacity loss decreases with aging, which can be attributed to the decrease in the net amount of cyclable lithium ions with aging. However, the resistive energy loss increases with aging which is due to the increase in the solid-electrolyte-interface (SEI) layer [28]. Further, the low variance observed in the SOC transitions can be explained by the isothermal setting in the emulated cell. In practice, the variations in cell temperature affect its internal resistance [42] and consequently the SOC transitions. In the control strategy design, starting with the data generated using uniformly distributed control actions (Z_l, D_l) , we iteratively compute empirical estimate of $P_{Z_{l+1}, \tilde{B}_l, \tilde{E}_l | Z_l, D_l}$ and its corresponding optimal strategies using data samples observed during real-time implementation.

C. Evaluation of the proposed ESS model & optimal strategies

We first design the optimal DSM and privacy risk control strategies $\mu_{w,1:N}^*$ and $\mu_{r,1:N}^*$ using the proposed ESS model and evaluate them on the emulated ESS in COMSOL. Fig. 5

Fig. 5. Optimal risk control strategy designed using the proposed ESS model.

Fig. 6. Optimal DSM strategy designed using the proposed ESS model.

and Fig. 6 show the performance of the designed EMU after 3 iterations of $P_{Z_{l+1} | Z_l, D_l}$ and the EMU strategies. We can see that the privacy control actions result in peak demands at time instances differing from that of actual peak demands and tend to increase variations in the SM readings. On the other hand, the DSM control actions result in low variations in the SM readings since the EMU tries to follow a daily-constant DSM target signal. Here, deviations from the target signal are observed mainly when the SOC reaches its limits.

Next, we design and evaluate the optimal strategies designed using the three-circuit model with time-invariant parameters: $r_l = 20m\Omega$ (the empirical average internal resistance); $\gamma_l = 1$; and $v_l = 48V$. To assess how well the two different models capture the ESS energy state transition characteristics, we use the root-mean-square error (RMSE) in discrete SOC estimates at each time-step. Note that the computed SOC estimates are not used in real-time control as the real-time energy state z_l is available to the EMU. They are used only to assess the mismatch between the energy state transition characteristics of the actual ESS and that of the model used in the EMU strategy design. Further, we use root-mean-square demand deviation (RMSDD) from the DSM reference signal $\bar{Y}_l$ as a metric to assess the DSM performance. In Table II, we list the average values of the RMSE in SOC estimates, Bayesian risk, and the RMSDD in different test cases. Here, we can see that the EMU strategies designed using the proposed ESS model achieve lower RMSE in SOC estimates and better privacy / DSM control performance compared to when designed using a deterministic time-invariant three-circuit model. This shows that the optimal strategies when designed using a less accurate ESS model perform sub-optimally.

TABLE II
COMPARISON OF EMU STRATEGIES IN DIFFERENT TEST CASES

EMU strategy	ESS model	Avg. RMSE in SOC (%)	Avg. Bayes risk	Avg. RMSDD (W)
Optimal privacy	proposed	2.74	0.186	400
	three-circuit	5.33	0.213	424
Optimal DSM	proposed	2.07	0.741	135
	three-circuit	5.07	0.740	137
No control	—	—	0.740	213

D. Evaluation of the trade-off between the EMU objectives

Here, we evaluate the trade-off between the optimal privacy, DSM, and ESS cost objectives. To reduce the complexity of the simulations, we emulate the ESS using the proposed ESS model instead of using the high-fidelity models. That is, we assume that the proposed ESS model learned using sufficient data samples represents the stochastic characteristics of the high-fidelity model accurately. Fig. 7 shows the average values of RMSDD, Bayesian risk, ESS lifetime, and its operational cost obtained by varying the trade-off parameters (ω_u, ω_c) over 50 Monte-Carlo simulations. Here we observe that the Bayesian risk and the RMSDD behave as opposing objectives and there exists a clear trade-off between the two. As there is no mismatch between the simulated ESS and the model used in the EMU strategy design, we observe that close to zero Bayesian risk is achievable when using $(\omega_u, \omega_c) = (0, 1)$, significantly lower than the value observed when evaluated using the high fidelity models. This shows the need for using more accurate ESS models in the privacy-preserving control strategy designs to meet strict privacy requirements.

As shown in Fig. 7, by using $(\omega_u, \omega_c) = (0, 0.2)$, we observe that the Bayesian risk remained close to zero while the ESS life increased significantly by 137%, which in turn reduces the ESS cost. This shows that by considering the ESS cost in the design, privacy risk can be reduced while significantly improving the ESS life. On the other hand, when using $(\omega_u, \omega_c) = (1, 0.4)$, the RMSDD increased by 7% while the ESS life increased only by 8% compared to the

case when using the optimal DSM control strategy. That is, the improvement in the ESS life observed by trading off some RMSDD is not as significant as compared to the improvement in the ESS life observed by trading off some Bayesian risk. This shows that DSM by tracking a reference signal incurs significant ESS cost and the trade-off between these two objectives must be designed by considering the DSM monetary incentives. In general, the EMU strategy designed with a higher ω_c resulted in a shorter lifetime and consequently higher ESS cost. Due to calendar aging, a non-zero ESS cost is observed when it is not used at all, which achieves the minimum ESS cost. The results show that the ESS operational cost can be controlled while providing desired privacy and demand shaping performance.

V. CONCLUSION

In this paper, we have presented a framework for privacy-aware DSM that includes important ESS aspects such as energy and capacity losses. We proposed a stochastic ESS model based on a three-circuit model for general storage technologies, which can be used in optimization problems to capture these ESS aspects. To achieve privacy, we model an adversary employing sequential Bayesian hypothesis testing and characterize the adversarial optimal detection performance using a deterministic set of polyhedral decision regions. Using the Markov decision process framework, we designed optimal control strategies with respect to privacy, DSM, and ESS cost objectives. Further, we present a novel recursive approach to compute the exact optimal privacy control strategy that minimizes the detection performance of the modeled adversary.

We note that the designed control strategy is optimal corresponding to an adversary employing Bayesian hypothesis testing using HMM $\hat{\theta}$, which provides us a generic adversarial model. In particular, if the adversary uses a different inference technique, uses different HMM model parameters, or tries to infer on a different hypothesis, there will be a model-mismatch in the system. In such a case, the exact adversarial detection performance and user privacy leakage cannot be predicted a priori. Nonetheless, using the optimal strategy presented in this paper we could provide privacy guarantees with respect to specific adversaries such as a common-case adversary who uses publicly available datasets or a worst-case adversary who knows the exact HMM θ .

Using numerical simulations, we have evaluated the proposed ESS model and the optimal control strategies using real household data and an emulated lithium-ion battery. From the results, we conclude that the proposed ESS model can be used to represent the ESS with improved accuracy. We have identified the trade-off between privacy and DSM objectives and conclude that optimal privacy or optimal DSM can be achieved only at the expense of ESS degradation. However, using the presented design approach, we have shown that the ESS degradation can be controlled while providing the desired level of privacy and demand shaping performance.

Investigating the impact on the privacy-controller performance when the adversary knows the implemented EMU strategy and designing an optimal control strategy for such an adversarial model are interesting topics for future research.

Fig. 7. Pareto-optimal trade-off between DSM, privacy, and ESS cost.

REFERENCES

- [1] E. Union, "Directive 2009/72/ec of the european parliament and of the council of 13 july 2009 concerning common rules for the internal market in electricity and repealing directive 2003/54/ec," *Of. J. Eu. Un. L*, 2009.
- [2] C. Cuijpers and B.-J. Koops, "Smart metering and privacy in europe: lessons from the dutch case," in *European data protection: coming of age*. Springer, 2013, pp. 269–293.
- [3] A. Zoha, A. Gluhak, M. A. Imran, and S. Rajasegarar, "Non-intrusive load monitoring approaches for disaggregated energy sensing: A survey," *Sensors*, vol. 12, no. 12, pp. 16 838–16 866, 2012.
- [4] G. Giacon, D. Gunduz, and H. V. Poor, "Privacy-aware smart metering: Progress and challenges," *IEEE Sig. Proc. Mag.*, vol. 35, 2018.
- [5] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda, "Privacy for smart meters: Towards undetectable appliance load signatures," in *IEEE SmartGridComm*, Gaithersburg, MD, USA, 2010.
- [6] J. Yao and P. Venkatasubramanian, "On the privacy-cost tradeoff of an in-home power storage mechanism," in *Allerton Conf.* IEEE, 2013.
- [7] F. Rigoll, C. Hirsch, S. Kochannek, H. Schmeck, and I. Mauser, "A privacy-aware architecture for energy management systems in smart grids," in *IEEE 11th Intl. Conf. on Ubi. Intel. and Comp.* IEEE, 2014.
- [8] M. Backes and S. Meiser, "Differentially private smart metering with battery recharging," in *Da. Pri. Ma. & Au. Spon. Sec.* Springer, 2014.
- [9] L. Yang, X. Chen, J. Zhang, and H. V. Poor, "Cost-effective and privacy-preserving energy management for smart meters," *IEEE Transactions on Smart Grid*, vol. 6, no. 1, pp. 486–495, 2014.
- [10] D. Varodayan and A. Khisti, "Smart meter privacy using a rechargeable battery: Minimizing the rate of information leakage," in *Proc. IEEE Int. Conf. on Acoust., Speech and Signal Process. (ICASSP)*, Prague, Czech Republic, 2011, pp. 1932–1935.
- [11] L. Sankar, S. R. Rajagopalan, S. Mohajer, and H. V. Poor, "Smart meter privacy: A theoretical framework," *IEEE Tran. on Sm. Gr.*, 2012.
- [12] J. Gomez-Vilardebo and D. Gündüz, "Smart meter privacy for multiple users in the presence of an alternative energy source," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 1, pp. 132–141, 2014.
- [13] G. Giacon, D. Gündüz, and H. V. Poor, "Smart meter privacy with renewable energy and an energy storage device," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 1, pp. 129–142, 2017.
- [14] O. Tan, J. Gómez-Vilardebo, and D. Gündüz, "Privacy-cost trade-offs in demand-side management with storage," *IEEE Transactions on Information Forensics and Security*, vol. 12, no. 6, pp. 1458–1469, 2017.
- [15] J.-X. Chin, T. T. De Rubira, and G. Hug, "Privacy-protecting energy management unit through model-distribution predictive control," *IEEE Transactions on Smart Grid*, vol. 8, no. 6, pp. 3084–3093, 2017.
- [16] Y. Hong, W. M. Liu, and L. Wang, "Privacy preserving smart meter streaming against information leakage of appliance status," *IEEE Tran. on infor. forensics and security*, vol. 12, no. 9, pp. 2227–2241, 2017.
- [17] E. Erdemir, P. L. Dragotti, and D. Gündüz, "Privacy-cost trade-off in a smart meter system with a renewable energy source and a rechargeable battery," in *IEEE Int. Conf. on Ac., Sp. and Sig. Proc. (ICASSP)*, 2019.
- [18] Y. You, Z. Li, and T. J. Oechtering, "Optimal privacy-enhancing and cost-efficient energy management strategies for smart grid consumers," in *IEEE Statistical Signal Processing Workshop (SSP)*, 2018.
- [19] M. B. Hossain, I. Natgunanathan, Y. Xiang, L.-X. Yang, and G. Huang, "Enhanced smart meter privacy protection using rechargeable batteries," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 7079–7092, 2019.
- [20] J. Yao and P. Venkatasubramanian, "Privacy aware stochastic games for distributed end-user energy storage sharing," *IEEE Trans. on Sig. and Inf. Proc. over Net.*, vol. 4, no. 1, pp. 82–95, 2018.
- [21] Z. Li, T. J. Oechtering, and M. Skoglund, "Privacy-preserving energy flow control in smart grids," in *Proc. IEEE Int. Conf. on Acoust. Speech Signal Process. (ICASSP)*, Shanghai, PR China, 2016, pp. 2194–2198.
- [22] R. R. Avula, T. J. Oechtering, and D. Månsson, "Privacy-preserving smart meter control strategy including energy storage losses," in *IEEE Innov. Sm. Grid Tech. Conf. Eur. (ISGT-Europe)*, Sarajevo, B&H, 2018.
- [23] R. R. Avula, J.-X. Chin, T. J. Oechtering, and G. Hug, "Smart meter privacy control strategy including energy storage degradation," in *IEEE Powertech, Milan, Italy*, 2019.
- [24] R. R. Avula and T. J. Oechtering, "Optimal privacy-by-design strategy for user demand shaping in smart grids," in *IEEE Innovative Smart Grid Technologies Conference (ISGT)*, Washington D.C., USA, 2020.
- [25] J.-X. Chin, K. Baker, and G. Hug, "Consumer privacy protection using flexible thermal loads: Theoretical limits and practical considerations," *Applied Energy*, vol. 281, p. 116075, 2021.
- [26] P. K. Varshney, *Distributed detection and data fusion*. Springer Science & Business Media, 2012.
- [27] A. Barré, B. Deguilhem, S. Grolleau, M. Gérard, F. Suard, and D. Riu, "A review on lithium-ion battery ageing mechanisms and estimations for automotive applications," *Jr. of Power Sources*, 2013.
- [28] P. Ramadass, B. Haran, P. M. Gomadam, R. White, and B. N. Popov, "Development of first principles capacity fade model for li-ion cells," *Jr. of The Elec.chem. Soc.*, vol. 151, no. 2, pp. A196–A203, 2004.
- [29] H. Ekström and G. Lindbergh, "A model for predicting capacity fade due to sei formation in a commercial graphite/lifepo4 cell," *Journal of The Electrochemical Society*, vol. 162, no. 6, pp. A1003–A1007, 2015.
- [30] M. Chen and G. A. Rincon-Mora, "Accurate electrical battery model capable of predicting runtime and iv performance," *IEEE transactions on energy conversion*, vol. 21, no. 2, pp. 504–511, 2006.
- [31] R. C. Kroeze and P. T. Krein, "Electrical battery model for use in dynamic electric vehicle simulations," in *Power El. Spec. Conf.*, 2008.
- [32] T. Kim and W. Qiao, "A hybrid battery model capable of capturing dynamic circuit characteristics and nonlinear capacity effects," *IEEE Transactions on Energy Conversion*, vol. 26, no. 4, pp. 1172–1180, 2011.
- [33] C.-T. Pham and D. Månsson, "On the physical system modelling of energy storages as equivalent circuits with parameter description for variable load demand (part i)," *Jr. of En. Stor.*, vol. 13, pp. 73–84, 2017.
- [34] —, "Experimental validation of a general energy storage modelling approach (part iii)," *Jr. of En. Storage*, 2018.
- [35] P. Fortenbacher, "On the integration of distributed battery storage in low voltage grids," Ph.D. dissertation, ETH Zurich, 2017.
- [36] V. Krishnamurthy, *Partially Observed Markov Decision Processes*. Cambridge University Press, 2016.
- [37] K. Miettinen, *Nonlinear multiobjective optimization*. Springer Science & Business Media, 2012, vol. 12.
- [38] C. Beckel, W. Kleiminger, R. Cicchetti, T. Staake, and S. Santini, "The eco data set and the performance of non-intrusive load monitoring algorithms," in *BuildSys*, Memphis, TN, USA, 2014, pp. 80–89.
- [39] E. Commission, *Energy, transport and environment indicators*. Publications Office of the European Union, 2019.
- [40] G. Berckmans, M. Messagie, J. Smekens, N. Omar, and et.al, "Cost projection of state of the art lithium-ion batteries for electric vehicles up to 2030," *Energies*, vol. 10, no. 9, p. 1314, 2017.
- [41] M. Naumann, M. Schimpe, P. Keil, H. C. Hesse, and A. Jossen, "Analysis and modeling of calendar aging of a commercial lifepo4/graphite cell," *Journal of Energy Storage*, vol. 17, pp. 153–169, 2018.
- [42] C. Forgez, D. V. Do, G. Friedrich, M. Morcrette, and C. Delacourt, "Thermal modeling of a cylindrical lifepo4/graphite lithium-ion battery," *Journal of Power Sources*, vol. 195, no. 9, pp. 2961–2968, 2010.

Ramana R. Avula (S'18) received his B.Tech. and M.Tech. degrees in Electrical Engineering from the Indian Institute of Technology, Madras, India in 2015. From 2015 to 2017, he was a Senior Engineer at the Robert Bosch Engineering and Business Solutions, India. Since 2017, he is pursuing his Ph.D. degree at the Division of Information Science and Engineering, KTH Royal Institute of Technology, Sweden. His current research interests include statistical signal processing and inference with an emphasis on privacy in smart metering systems.

Jun-Xing Chin (S'15, M'20) received the B.Eng. degree in electronic engineering and the B.BA degree in general business management from the Hong Kong University of Science and Technology in 2010, the M.Sc. degree from the University of Nottingham in 2011, and the Ph.D. degree from ETH Zurich in 2020. From 2011 to 2015, he was an electrical engineer at the engineering consultancy firm Ove Arup and Partners H.K. Ltd. in Hong Kong. Currently, he is a Postdoctoral Researcher with the Future Resilient Systems programme at the Singapore-ETH Centre, where he is currently working on using microgrids to enhance the resilience of power systems with high degrees of distributed energy resources.

Tobias J. Oechtering (S'01-M'08-SM'12) received his Dipl-Ing degree in Electrical Engineering and Information Technology in 2002 from RWTH Aachen University, Germany, his Dr-Ing degree in Electrical Engineering in 2007 from the Technische Universität Berlin, Germany. In 2008 he joined KTH Royal Institute of Technology, Stockholm, Sweden and has been a Professor since 2018. In 2009, he received the "Förderpreis 2009" from the Vodafone Foundation. Dr. Oechtering is currently Senior Editor of IEEE Transactions on Information Forensics and Security

since May 2020 and served previously as Associate Editor for the same journal since June 2016, and IEEE Communications Letters during 2012-2015. He has served on numerous technical program committees for IEEE sponsored conferences, and he was general co-chair for IEEE ITW 2019. His research interests include communication and information theory, physical layer privacy and security including in particular smart meter privacy, statistical signal processing, and communication for networked control.

Gabriela Hug (S'05-M'08-SM'14) was born in Baden, Switzerland. She received the M.Sc. degree in electrical engineering in 2004 and the Ph.D. degree in 2008, both from the Swiss Federal Institute of Technology, Zurich, Switzerland. After the Ph.D. degree, she worked with the Special Studies Group of Hydro One, Toronto, ON, Canada, and from 2009 to 2015, she was an Assistant Professor with Carnegie Mellon University, Pittsburgh, PA, USA. She is currently a Professor with the Power Systems Laboratory, ETH Zurich, Zurich, Switzerland. Her

research is dedicated to control and optimization of electric power systems.

Daniel Månsson received the M.Sc. and Ph.D. degrees in Engineering Physics from Uppsala University, Uppsala, Sweden, in 2003 and 2008, respectively. In 2016 he received his Docent degree in Electrical Engineering. He is an Associate Professor at the KTH Royal Institute of Technology, Stockholm, Sweden working with Smart Electricity Grids and Power System Components. His research is currently mainly focused on different aspects of energy storage systems, their implementation and ability to deliver services to prosumers and the grid.

Dr. Månsson is a member of the Swedish National Committee for Radio Science, section E (Electromagnetic environment and interference). He is a reviewer of the IEEE Transactions on Electromagnetic Compatibility, the PIER [Progress in Electromagnetic Research journals (regular, B, C, and M)] and occasionally also for other journals.