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

Postprint

This is the accepted version of a paper presented at *2019 IEEE Milan PowerTech*.

Citation for the original published paper:

Avula, R R., Oechtering, T J., Chin, J-X., Hug, G. (2019)
Smart Meter Privacy Control Strategy Including Energy Storage Degradation
In: *2019 IEEE Milan PowerTech* IEEE
<https://doi.org/10.1109/PTC.2019.8810481>

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-259388>

Smart Meter Privacy Control Strategy Including Energy Storage Degradation

Ramana R. Avula and Tobias J. Oechtering
School of Electrical Engineering and Computer Science
KTH Royal Institute of Technology, Stockholm, Sweden

Jun-Xing Chin and Gabriela Hug
Power Systems Laboratory
ETH Zurich, Switzerland

Abstract—In this paper, we present a degradation-aware privacy control strategy for smart meters by taking into account the capacity fade and energy loss of the battery, which has not been included previously. The energy management strategy is designed by minimizing the weighted sum of both privacy loss and total energy storage losses, where the weightage is set using a trade-off parameter. The privacy loss is measured in terms of Bayesian risk of an unauthorized hypothesis test. By making first-order Markov assumptions, the stochastic parameters of energy loss and capacity fade of the energy storage system are modelled using degradation maps. Using household power consumption data from the ECO dataset, the proposed control strategy is numerically evaluated for different trade-off parameters. Results show that, by including the degradation losses in the design of the privacy-enhancing control strategy, significant improvement in battery life can be achieved, in general, at the expense of some privacy loss.

Index Terms—Smart meter privacy, energy storage system model, partially observable Markov decision process, Bayesian hypothesis testing, energy storage degradation

I. INTRODUCTION

Energy storage systems (ESSs) are key components in sustainable smart grids that act as a buffer for fluctuations in the grid. ESSs are also considered as a promising physical layer solution to the smart meter (SM) privacy problem [1]–[7]. This privacy-by-design approach, also known as *load signature moderation*, uses ESSs to alter the consumers’ energy consumption profile in order to hide the appliances’ usage pattern. In [1], a best-effort privacy algorithm is used to hide the appliance usage information, whereas, in [5], a stochastic control model formulated as a partially observable Markov decision process (PO-MDP) is used. In [4], a differential privacy approach is proposed, where noise is added to the consumers’ energy consumption using a rechargeable battery. In [8], a greedy suboptimal privacy filter is used to trade-off utility and privacy for hidden Markov models. In [6], on the other hand, a model-distribution predictive control strategy is used to minimize the information leakage and energy cost. Further, the joint optimization of privacy and energy cost with a rechargeable battery is addressed in [9]–[11]. However, the effect of the privacy control actions on the degradation of ESSs has not yet been investigated in the literature, nor has there been controllers that consider ESS degradation when reducing the privacy loss. Since different control actions influence the ESS degradation differently, a study on the effect of privacy

Fig. 1. Schematic of the studied smart metering system where the energy management unit (EMU) controls user’s privacy leakage using an energy storage system (ESS).

control actions on ESS degradation is needed to quantitatively evaluate the trade-off between achievable privacy and ESS degradation.

ESS degradation is a non-linear process, which depends highly on storage technology. For battery systems, electrochemical models capture physical processes more accurately, but they are difficult to integrate with optimization problems due to their complexity. In [12], an explicit quadratic cost function is used to incorporate degradation into a model predictive control based approach for the optimal energy storage operation. In [13], and [14], on the other hand, degradation maps are used as deterministic black box models to capture hidden and unknown chemical reactions corresponding to battery degradation. In this paper, we extend this approach by modelling the stochastic parameters of capacity fade and the resistive energy loss using the degradation maps. Similar to [5], we measure privacy in terms of Bayesian risk of unauthorized hypothesis tests, for example, to detect the usage of specific appliances in a house. For the smart metering system shown in Fig. 1, the optimal energy management policy that trade-offs privacy and ESS costs is obtained using the PO-MDP framework.

The rest of the paper is organized as follows. In Section II, we present an overview of the smart metering system and the energy storage degradation model. In Section III, we present the degradation-aware privacy control strategy against the hypothesis testing of an adversary unaware of the presence of ESS. In Section IV, we present results from simulation experiments and conclude the paper in Section V.

II. SYSTEM MODEL

We consider a privacy-preserving smart metering system with an energy storage system as shown in Fig. 1. The discrete time system is controlled for every time slot k of fixed time duration T . To simplify the analysis in the control policy design, we consider discrete quantized variables assuming e and q as the resolution of energy and power measurements, respectively. We further use capital letters to denote random variables, their realizations by the corresponding lower-case letters and the range space by calligraphic letters. Also, to denote the probability density function and probability mass function, we use $P_A(a)$, where A is a discrete or continuous random variable and a is its realization.

For each time slot k , X_k denotes the discretized power demand of the house and is defined on $\mathcal{X} = \{0, q, 2q, \dots, x_{max}\}$. Z_k , defined on $\mathcal{Z} = \{z_{min}, z_{min} + e, z_{min} + 2e, \dots, z_{max}\}$, denotes the discretized energy state of the ESS at the start of time slot k . The discretized power drawn by the ESS is denoted by D_k which is defined on $\mathcal{D} = \{-d_{min}, \dots, -q, 0, q, \dots, d_{max}\}$, where d_{min} and d_{max} are the maximum discharge and charge power of the ESS respectively. The smart meter measurements are denoted by Y_k , which are defined on $\mathcal{Y} = \{0, q, \dots, y_{max}\}$, where $y_{max} \leq x_{max} + d_{max}$. H_k defined on $\mathcal{H} = \{1, 2, \dots, n\}$ denotes the hypothesis state of the house and $\hat{H}_k$ denotes the hypothesis guess of the adversary. For instance, an adversary who wants to learn about the cooking habits of a consumer will try to detect the usage of the stove, which is a standard binary hypothesis testing problem.

A. Privacy loss measure

Similar to [5] and [7], we use an operational privacy metric corresponding to an unauthorized adversarial hypothesis test. Let $C_{h,\hat{h}}$ be the normalized cost of the energy management unit (EMU) when the adversary guesses the hypothesis as $\hat{h}$ while h is true. Then, the average normalized cost of detection or the *Bayesian (privacy) risk*, denoted by $\mathcal{R}_k$, is given as

$$\mathcal{R}_k = \sum_{h,\hat{h}} C_{h,\hat{h}} \cdot P_{H_k, \hat{H}_k}(h, \hat{h}). \quad (1)$$

Here, we define the costs in the privacy context, so that a higher Bayesian risk corresponds to a higher privacy loss. Accordingly, the worst-case adversary uses a strategy that maximizes the Bayesian risk and the control strategy of the EMU aims to minimize it.

B. Energy storage degradation model

In this work, we model the energy storage degradation in terms of capacity loss due to side reactions, and energy loss due to variations in internal resistance. A comprehensive review of capacity fade mechanisms in Lithium-ion batteries is given in [15], according to which the processes that irreversibly lead to capacity loss can be characterized by chemical side reactions. We, therefore, use the *side reaction flux* (denoted by J_k) estimate from electrochemical models to measure the capacity loss associated with each discrete control

action. However, we consider the capacity loss, denoted by B_k , as a random variable which depends on (D_k, Z_k) with a first-order Markov assumption, given as

$$B_k \Big|_{(D_k=d, Z_k=z)} = F J_k \Big|_{(D_k=d, Z_k=z)}, \quad (2)$$

where F is the Faraday's constant. The energy loss, denoted by L_k , and the battery energy state Z_{k+1} , assuming a constant internal resistance are given by the three-circuit energy storage system model from [7] as

$$\begin{aligned} L_k &= Z_k + D_k T - Z_{k+1}, \\ Z_{k+1} &= (1 - \gamma) Z_k + \frac{\beta V}{2r} \left(\sqrt{V^2 + 4r D_k \delta_k} - V \right), \end{aligned} \quad (3)$$

where γ, β are self-dissipation parameters, V is the battery open-circuit voltage, δ_k is the converter efficiency, and r is the steady state internal resistance of the energy storage. In this work, we consider the *variation in internal resistance* (Δr) due to the control actions as the difference between the internal resistance of the battery when the energy storage is being used and when it is not being used. Assuming that Δr depends on (D_k, Z_k) following a first-order Markov chain, we can write

$$\Delta r_k \Big|_{(D_k=d, Z_k=z)} = \left(r_k \Big|_{(D_k=d, Z_k=z)} - r_k \Big|_{(D_k=0, Z_k=z)} \right). \quad (4)$$

Due to the highly coupled noise in the thermal and chemical processes, it is difficult to identify a parametric model for the probability density functions of B and L analytically. In this work, we restrict our focus by parametrizing their moments as time-independent maps given by

$$\mathbb{E} \left[B_k^n \mid D_k = d, Z_k = z \right] = \alpha_n(d, z), \quad (5)$$

$$\mathbb{E} \left[L_k^n \mid D_k = d, Z_k = z \right] = \xi_n(d, z). \quad (6)$$

Maps of α_n and ξ_n , called *degradation maps*, can be estimated using J_k and Δr_k samples from high-fidelity electrochemical models such as DUALFOIL [16], [17] or LI-ONSIMBA (Li-ION SIMulation BAttery) [18]. The generated maps can be easily integrated in the optimization problems.

III. ENERGY MANAGEMENT STRATEGY

The objective of the EMU is to reduce the ESS losses while protecting consumer privacy against adversarial hypothesis testing. To design the control strategy, we model the system by making the following assumptions:

- 1) The state H_k evolves as a first-order Markov chain with time-invariant transition probabilities $P_{H_k|H_{k-1}}$.
- 2) The state H_k generates observation X_k with time-invariant emission probabilities $P_{X_k|H_k}$.
- 3) The adversary is unaware of the battery's presence.
- 4) The adversary knows the Markov chain probabilities and makes a guess on H_k in real time using only the information $\mathcal{I}_k = \{P_{H_0}, P_{X_k|H_k}, P_{H_k|H_{k-1}}, y_1, \dots, y_k\}$.

It is optimal for the adversary to use complete $\mathcal{I}_k$, also known as the *statistic*, to make a guess on H_k in real time. As per [19], in PO-MDP framework, a *sufficient statistic* of $\mathcal{I}_k$ is the posterior distribution of H_k , defined as a *belief state* ($\hat{\pi}_k$). Since the adversary is unaware of the battery's presence, the adversarial belief state is computed assuming $x_k = y_k$. Using Bayes' rule, we can express the belief state as

$$\hat{\pi}_k(h) = P_{H_k|X_k, \hat{\pi}_{k-1}}(h | y_k) = \frac{P_{X_k, H_k|\hat{\pi}_{k-1}}(y_k, h)}{\sum_h P_{X_k, H_k|\hat{\pi}_{k-1}}(y_k, h)}, \quad (7)$$

where

$$P_{X_k, H_k|\hat{\pi}_{k-1}}(y_k, h) = \sum_{h' \in \mathcal{H}} P_{X_k|H_k}(y_k | h') \times P_{H_k|H_{k-1}}(h | h') P_{H_{k-1}|\hat{\pi}_{k-1}}(h'). \quad (8)$$

Since the domain of $\hat{\pi}$ is continuous with infinitely many possible states, in our design, we discretize the probability measure in order to limit the domain to a finite set. In this discretized space, for a given adversarial strategy (denoted by $\hat{\zeta}_k$), and $\hat{\pi}_{k-1}$, the privacy risk in (1) seen by the adversary can be expressed as:

$$\begin{aligned} \hat{\mathcal{R}}_k(\hat{\pi}_{k-1}) &= \sum_{x, h, \hat{h}} C_{h, \hat{h}} \underbrace{P_{\hat{H}_k|X_k, \hat{\pi}_{k-1}}(\hat{h} | x)}_{\hat{\zeta}_k} P_{X_k, H_k|\hat{\pi}_{k-1}}(x, h) \\ &= \mathbf{M}_k^T \hat{\zeta}_k. \end{aligned} \quad (9)$$

where $\mathbf{M}_k$ is a matrix which is derived from $\hat{\pi}_{k-1}$ and $\hat{\zeta}_k$ is the decision strategy vector. For a finite-time horizon of length N , the optimal strategy of the adversary is to maximize the aggregate privacy risk given by

$$\hat{\mathcal{V}}_N := \max_{[\hat{\zeta}_1, \dots, \hat{\zeta}_N]} \left(\sum_{k=1}^N \hat{\mathcal{R}}_k \right), \quad (10)$$

The dimensionality of the optimization in (10) increases with N . To reduce complexity, as in [5], we consider the stationary value of discounted aggregate privacy risk given by

$$\tilde{\mathcal{V}} := \sum_{k=1}^{\infty} \theta^k \hat{\mathcal{R}}_k, \quad (11)$$

where $\theta \in [0, 1)$ is the discount factor which controls the memory in the aggregate privacy risk. The optimal stationary decision strategy ($\hat{\zeta}^*$) can be obtained by formulating a recursive backward dynamic programming problem given by

$$\tilde{\mathcal{V}}_k(\hat{\pi}_{k-1}) = \max_{\hat{\zeta}_k} \left(\hat{\mathcal{R}}_k + \theta \mathbb{E} [\tilde{\mathcal{V}}_{k+1}(\hat{\pi}_k)] \right), \quad (12)$$

where

$$\mathbb{E} [\tilde{\mathcal{V}}_{k+1}(\hat{\pi}_k)] = \sum_{x, h} \tilde{\mathcal{V}}_{k+1}(\hat{\pi}_k) P_{X_k, H_k|\hat{\pi}_{k-1}}(x, h). \quad (13)$$

From (9), we can see that $\hat{\mathcal{R}}_k$ varies linearly with $\hat{\zeta}_k$ and $\mathbb{E}[\tilde{\mathcal{V}}_{k+1}]$ is independent of $\hat{\zeta}_k$, as seen from (13). Hence, $\hat{\zeta}^*$ can be obtained using standard linear programming solvers.

In this work, we restrict our design to the class of memoryless and hypothesis-unaware control policies of the form $P_{Y_k|X_k, Z_k}$, which simplifies the privacy risk seen by EMU as

$$\begin{aligned} \mathcal{R}_k(\hat{\pi}_{k-1}, z_k) &= \sum_{y, x, h, \hat{h}} \overbrace{P_{\hat{H}_k|Y_k, \hat{\pi}_{k-1}}(\hat{h} | y)}^{\hat{\zeta}^*} \overbrace{P_{Y_k|X_k, Z_k}(y | x, z_k)}^{\mu_k} \times \\ &\quad C_{h, \hat{h}} P_{X_k, H_k|\hat{\pi}_{k-1}}(x, h) \\ &= \mathbf{Q}_k^T \mu_k, \end{aligned} \quad (14)$$

where $\mathbf{Q}_k$ is a matrix which is derived from $(\hat{\pi}_{k-1}, z_k, \hat{\zeta}^*)$ and μ_k is the control strategy vector. Taking ρ as the price of ESS capacity in €/Ah, λ_k as the price of energy in €/Wh, the mean ESS cost due to capacity fade and energy losses can be expressed as:

$$\begin{aligned} \mathcal{C}_k(\hat{\pi}_{k-1}, z_k) &= \rho \mathbb{E} [B_k] + \lambda_k \mathbb{E} [L_k] \\ &= \sum_{y, x, h} P_{Y_k|X_k, Z_k}(y | x, z_k) P_{X_k, H_k|\hat{\pi}_{k-1}}(x, h) \times \\ &\quad [\rho \alpha_1(y - x, z_k) + \lambda_k \xi_1(y - x, z_k)] \\ &= \mathbf{S}_k^T \mu_k, \end{aligned} \quad (15)$$

where α_1 and ξ_1 are the degradation maps corresponding to the first moments of the capacity fade and energy loss respectively and $\mathbf{S}_k$ is a matrix which is derived from $(\hat{\pi}_{k-1}, z_k, \alpha_1, \xi_1)$. Considering the ESS degradation and energy losses due to the privacy-preserving control actions, we can trade off some privacy in order to reduce ESS cost. To formulate a joint weighted optimization problem, we assign the price σ (in €) to the Bayesian risk. Similar to (11), we consider the stationary value of the weighted privacy and ESS cost as

$$\tilde{\mathcal{J}} := \sum_{k=1}^{\infty} \theta^k [(1 - \omega) \sigma \mathcal{R}_k + \omega \mathcal{C}_k], \quad (16)$$

where $\omega \in [0, 1]$ is the trade-off parameter. Similar to (12), the optimal stationary control strategy (μ^*) can be obtained by reformulating (16) into a recursive backward dynamic programming problem given by

$$\tilde{\mathcal{J}}_k(\hat{\pi}_{k-1}, z_k) = \min_{\mu_k} \left((1 - \omega) \sigma \mathcal{R}_k + \omega \mathcal{C}_k + \theta \mathbb{E} [\tilde{\mathcal{J}}_{k+1}(\hat{\pi}_k, z_{k+1})] \right), \quad (17)$$

$$\begin{aligned} \mathbb{E} [\tilde{\mathcal{J}}_{k+1}(\hat{\pi}_k, z_{k+1})] &= \sum_{y, x, h} \tilde{\mathcal{J}}_{k+1}(\hat{\pi}_k, z_{k+1}) \times \\ &\quad P_{Y_k|X_k, Z_k}(y | x, z_k) P_{X_k, H_k|\hat{\pi}_{k-1}}(x, h) \\ &= \bar{\mathbf{J}}_{k+1}^T \mu_k. \end{aligned} \quad (18)$$

where $\bar{\mathbf{J}}_{k+1}$ is a vector which depends on $(\hat{\pi}_{k-1}, z_k, \tilde{\mathcal{J}}_{k+1})$. From (14), (15) and (18), we can see that $\mathcal{R}_k$, $\mathcal{C}_k$ and $\mathbb{E}[\tilde{\mathcal{J}}_{k+1}]$ vary linearly with μ_k . Hence, the optimal stationary control strategy μ^* can be obtained using standard linear programming solvers.

IV. NUMERICAL STUDY

In this work, numerical simulations were performed using MATLAB R2018a and the Gurobi [20] optimization solver. To evaluate the control strategy, we use SM readings and occupancy data corresponding to household 2 in the ECO reference dataset [21] with 15-minute resolution. The data used was collected over a period of 80 days during summer 2012, out of which 35 days were used for training and the remaining 45 days for validation. The missing SM measurement data (observed less than 1%) in the selected days are set to 0. As the adversary is unaware of the battery's presence, we compute the adversarial strategy and belief states considering $Y_k = X_k$. We simulate a scenario where the adversary is interested in detecting the presence or absence of the user, i.e., the hypothesis state $H_k = 1$ when the user is absent and $H_k = 2$ when the user is present in the house. In this setup, a 48V-60Ah lithium-ion battery system with the parameters listed in Tables I & II is selected. The household energy cost corresponding to Sweden is taken from [22]. Assuming that the end of battery life is when 20% of its rated capacity is lost, the degradation cost is calculated by taking the lithium-ion battery cost to be 130 €/kWh [23].

A. Degradation maps

To generate the degradation maps, we use the LIONSIMBA [18] toolbox in MATLAB as a substitute to a real battery. The toolbox is based on a pseudo-two-dimensional (P2D) finite volume model that captures the side reactions and thermal behaviour using non-linear partial differential equations. In our simulations, we used default toolbox parameters, unless otherwise stated in Table I. By initializing with a fully charged battery, it is subjected to uniformly distributed random charge and discharge actions. The internal resistance of the battery for zero current is computed by using short duration current pulses. The simulation is performed to obtain 100 measurement samples of capacity loss and energy loss corresponding to each discrete action-state pair, computed using (2) and (3). The regime outside the SoC interval [0.1, 0.9] is not considered in our simulations. It was observed that the side reaction current is computed only during battery charging in the LIONSIMBA toolbox. As in [14], we consider equal capacity degradation for charge and discharge battery currents of

TABLE I
LIONSIMBA SETUP

Parameter	Value
Cell area (m ²)	2
Cell capacity (Ah)	60
Max. cur. density (A/m ²)	30
Conductivity of side reaction product (S/m)	1e-2 ^a
Mol. weight of side reaction product (kg/mol)	7.3e-4 ^a
Density of side reaction product (kg/m ³)	2.1e-3 ^a
Side reaction exchange cur. density (A/m ²)	3.2e-7 ^b

^a taken from [24]

^b tuned for a linear extrapolated life of 2500 cycles (80% DoD)

TABLE II
EMU SETUP

Parameter	Value
Time slot (s)	900
Power resolution (W)	300
Energy resolution (Wh)	50
Avg. int. resistance (mΩ)	13.1
Li-ion cells in series	12
Battery nom. voltage (V)	48
Power converter eff. (%)	95
Self dissipation (%/month)	3
Energy cost (€/kWh)	0.2
Degradation cost (€/kWh)	650
Max. ESS power (W)	2700

(a) Mean energy loss (b) Mean capacity loss
Fig. 2. Degradation maps corresponding to 15 minute intervals

equal magnitude. Since the designed control strategy requires only the mean energy and capacity losses, the first moments are computed with the measurements and the resulting mean degradation maps are shown in Fig. 2. The same approach can be extended to include more stochastic features in the design. In general, the mean energy loss increases with the magnitude of ESS output power and mean capacity loss increases with operating SoC.

B. Evaluation of privacy-cost trade-off

To evaluate the privacy-cost trade-off, we assume that the three-circuit model [7] along with the generated degradation maps constitute a real ESS, thereby neglecting the error due to the ESS model approximations. We select the Bayesian cost $C_{h,\hat{h}}$ defined in (1) as $C_{11} = C_{22} = 1$ and $C_{12} = C_{21} = 0$ such that the Bayesian privacy risk corresponds to the average adversarial detection probability. To simplify the simulations, we divide a day into 3 time-homogeneous intervals (12AM - 8AM), (8AM - 4PM), and (4PM - 12AM) denoted as Δ_1 , Δ_2 , and Δ_3 respectively. Within each interval, the Markov chain probabilities $P_{H_k|H_{k-1}}$, $P_{X_k|H_k}$ are assumed to be time-invariant. The corresponding time-dependent Markov parameters are computed using the training data and the stationary control strategies are computed with different discount factors $\theta \in [0.1, 0.9]$, prices of privacy leakage $\sigma \in [0.05\text{€}, 0.45\text{€}]$ and trade-off parameters $\omega \in [0, 1]$.

Starting with a fully charged battery on day 0, the designed control strategies are evaluated for 45 consecutive days using the validation data. Fig. 3 shows the average power demand of the user and normalized frequency of true presence, i.e., ($H_k = 2$) observed in the validation data. It can be seen that the user was always present during night time and was absent almost 50% of the time at mid-day. Also, high power consumption is observed during Δ_2 and Δ_3 . An adversary, having access to the same training data, is simulated with the same Markov assumptions as the EMU. Fig. 4 shows the average ESS output power, evolution of its SoC, mean energy loss and mean capacity loss when evaluated with control strategies corresponding to $\theta = 0.5$, $\sigma = 0.05\text{€}$, and different ω . It can be seen that, when $\omega = 1$, the EMU does not use the battery at all, thereby minimizing the ESS related costs, but revealing the user's true power consumption to the adversary. As ω decreases, the privacy cost is prioritized over the ESS related cost and the resulting control strategy uses

Fig. 3. Average power demand of house and average frequency of true presence ($H_k = 2$) observed in the validation data.

Fig. 4. Average values output power, SoC, energy loss, and capacity loss of the energy storage system.

the ESS more in order to manipulate the energy profile. When $\omega = 0$, the EMU ignores the ESS related cost in order to minimize the Bayesian risk. The plots of average energy loss and capacity loss in Fig. 4 show the correlation between the trade-off parameter and ESS degradation.

For the same $\theta = 0.5$ and $\sigma = 0.05\text{€}$, Fig. 5 shows the average SM readings, normalized frequency of guessed presence ($\hat{H}_k = 2$) by the simulated adversary, average Bayesian risk computed using (14) and the average Bayesian risk measured using (1) for the observed pairs of $(H_k, \hat{H}_k)$. During the transitions from Δ_l and Δ_m , we assume that the adversarial belief state is reset to the initial belief state of Δ_m . Consequently, we observe abrupt changes in the hypothesis guess of the simulated adversary at these transitions. From the plots of computed and measured Bayesian risk, we can see that the trained hidden Markov model accurately matches the validation data during Δ_1 , since the user is almost always present and consumes low energy. This makes it easy for the adversary to guess the hypothesis correctly, resulting in a very high privacy risk during Δ_1 . As a consequence, when $\omega = 0$, we can observe that the EMU schedules the ESS charging during Δ_1 , but the achievable Bayesian risk is limited by the ESS capacity. Whereas, during Δ_2 and Δ_3 , the EMU discharges the battery during periods of high power demand.

Fig. 5. Average values of smart meter readings, frequency of guessed presence by adversary ($\hat{H}_k = 2$), computed Bayesian risk, and measured Bayesian risk.

Fig. 6. Aggregate Bayesian risk normalized with time, aggregate ESS cost, and linearly extrapolated battery life vs. ω .

On the other hand, the mismatch between the trained model and the validation data is high during Δ_2 , resulting in a high mismatch between the computed and measured Bayesian risks. Also, when $\omega = 1$, this mismatch results in the adversary not being able to guess the true hypothesis correctly.

For the 45 days tested, the aggregate Bayesian risk normalized with time, aggregate ESS cost, achievable battery life for the same $\theta = 0.5$ and $\sigma = 0.05\text{€}$ are shown in Fig. 6. The illustrated battery life is extrapolated linearly based only on the operational capacity loss observed within 45 days. In addition, ESS capacity and internal resistance degrade with calendar ageing, which is not considered in this work. From the plots of normalized aggregate Bayesian risk and aggregate ESS cost, we can see that the control strategy with $\omega = 0.7$ performs better than $\omega = 0$, with almost same aggregate privacy risk, but with an improved battery life of 430%. This

Fig. 7. Normalized aggregate Bayesian risk vs. aggregate ESS cost and linearly extrapolated battery life.

loss of optimality can be attributed to the design choices and model inaccuracies, which can also be seen in Fig. 7. Each point in the figure represents the normalized aggregate Bayesian risk, the aggregate ESS cost, and the battery life corresponding to different θ , σ , and ω . From the plots, we can see that the points corresponding to $\theta = 0.5$ and $\sigma = 0.05$ €, in general, do not lie on the Pareto-optimal trade-off curve i.e., the boundary of points at which both objectives cannot be improved simultaneously. However, the results show that by considering the ESS cost when minimizing privacy risk, significant improvements in battery life can be achieved, in general, at the expense of some privacy loss.

V. CONCLUSION

In this paper, we used degradation maps to model the stochastic parameters of energy loss and capacity fade of the lithium-ion battery system due to discrete charge and discharge operations. The generated maps are used to trade-off privacy risk and ESS losses by solving a weighted optimization problem. We designed a degradation-aware EMU against the Bayesian hypothesis testing of an adversary unaware of the presence of ESS. With a numerical study, we evaluated the trade-off between privacy risk and ESS cost due to privacy control actions. The results show that, by considering the degradation due to privacy control actions in the design, significant improvements in battery life can be achieved, in general, at the expense of some privacy loss. Further studying the battery-aware adversarial case and including more energy storage processes such as rate capacity effect to model the energy storage dynamics will be of interest for future work.

REFERENCES

- [1] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda, "Privacy for smart meters: Towards undetectable appliance load signatures," in *Proc. 1st IEEE Int. Conf. on Smart Grid Commun. (Smart-GridComm)*, Gaithersburg, MD, USA, 2010, pp. 232–237.
- [2] 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.
- [3] O. Tan, D. Gunduz, and H. V. Poor, "Increasing smart meter privacy through energy harvesting and storage devices," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1331–1341, 2013.
- [4] M. Backes and S. Meiser, "Differentially private smart metering with battery recharging," in *Data Privacy Management and Autonomous Spontaneous Security*. Springer, 2014, pp. 194–212.
- [5] 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.
- [6] 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.
- [7] R. R. Avula, T. J. Oechtering, and D. Månsson, "Privacy-preserving smart meter control strategy including energy storage losses," unpublished, presented at the IEEE Innov. Smart Grid Tech. Conf. Europe (ISGT-Europe), Sarajevo, Bosnia and Herzegovina, 2018. [Online]. Available: <https://arxiv.org/abs/1803.07864>
- [8] R. Mochaourab and T. J. Oechtering, "Private filtering for hidden markov models," *IEEE Signal Process. Letters*, vol. 25, no. 6, pp. 888–892, 2018.
- [9] O. Tan, J. Gómez-Vilardebó, 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.
- [10] 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, 2015.
- [11] J. Yao and P. Venkatasubramanian, "On the privacy-cost tradeoff of an in-home power storage mechanism," in *Annual Allerton Conference on Communication, Control, and Computing*. IEEE, 2013, pp. 115–122.
- [12] M. Koller, T. Borsche, A. Ulbig, and G. Andersson, "Defining a degradation cost function for optimal control of a battery energy storage system," in *Proc. IEEE PowerTech*, Grenoble, France, 2013, pp. 1–6.
- [13] S. J. Moura, J. L. Stein, and H. K. Fathy, "Battery-health conscious power management in plug-in hybrid electric vehicles via electrochemical modeling and stochastic control," *IEEE Transactions on Control Systems Technology*, vol. 21, no. 3, pp. 679–694, 2013.
- [14] P. Fortenbacher and G. Andersson, "Battery degradation maps for power system optimization and as a benchmark reference," in *Proc. IEEE PowerTech*, Manchester, UK, 2017, pp. 1–6.
- [15] J. Vetter, P. Novák, M. R. Wagner, C. Veit, K.-C. Möller, J. Besenhard, M. Winter, M. Wohlfahrt-Mehrens, C. Vogler, and A. Hammouche, "Ageing mechanisms in lithium-ion batteries," *Journal of power sources*, vol. 147, no. 1-2, pp. 269–281, 2005.
- [16] M. Doyle, T. F. Fuller, and J. Newman, "Modeling of galvanostatic charge and discharge of the lithium/polymer/insertion cell," *Journal of the Electrochemical Society*, vol. 140, no. 6, pp. 1526–1533, 1993.
- [17] C. M. Doyle, "Design and simulation of lithium rechargeable batteries," Ph.D. dissertation, University of California at Berkeley, 1995.
- [18] M. Torchio, L. Magni, R. B. Gopaluni, R. D. Braatz, and D. M. Raimondo, "Lionsimba: A matlab framework based on a finite volume model suitable for li-ion battery design, simulation, and control," *Journal of The Electrochemical Society*, vol. 163, no. 7, pp. A1192–A1205, 2016.
- [19] V. Krishnamurthy, *Partially Observed Markov Decision Processes*. Cambridge University Press, 2016.
- [20] L. Gurobi Optimization, "Gurobi optimizer reference manual," 2018. [Online]. Available: <http://www.gurobi.com>
- [21] 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 *Proc. 1st ACM Int. Conf. on Embedded Sys. for Energy-Eff. Buildings (BuildSys)*, Memphis, TN, USA, 2014, pp. 80–89.
- [22] Eurostat and U. européenne. Commission européenne, *Energy, transport and environment indicators*. Office for Official Publications of the European Communities, 2017.
- [23] G. Berckmans, M. Messagie, J. Smekens, N. Omar, L. Vanhaverbeke, and J. Van Mierlo, "Cost projection of state of the art lithium-ion batteries for electric vehicles up to 2030," *Energies*, vol. 10, no. 9, p. 1314, 2017.
- [24] S. Santhanagopalan, Q. Guo, P. Ramadass, and R. E. White, "Review of models for predicting the cycling performance of lithium ion batteries," *Journal of Power Sources*, vol. 156, no. 2, pp. 620–628, 2006.