Privacy-preserving smart meter control strategy including energy storage losses

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

***Abstract*—Privacy-preserving smart meter control strategies proposed in the literature so far make some ideal assumptions such as instantaneous control without delay, lossless energy storage systems etc. In this paper, we present a one-step-ahead predictive control strategy using Bayesian risk to measure and control privacy leakage with an energy storage system. The controller estimates energy state using a three-circuit energy storage model to account for steady-state energy losses. With numerical experiments, the controller is evaluated with real household consumption data using a state-of-the-art adversarial algorithm. Results show that the state estimation of the energy storage system significantly affects the controller's performance. The results also show that the privacy leakage can be effectively reduced using an energy storage system but at the expense of energy loss.**

***Index Terms*—Smart meter privacy, Bayesian hypothesis testing, partially observable Markov decision process (PO-MDP), energy storage losses, dynamic programming**

I. Introduction

A smart grid (SG) is a next-generation energy network with capabilities to improve grid reliability and efficiency of power generation and distribution with smooth integration of renewable energy sources. In this automated network, a smart meter (SM) is a crucial component which measures the energy consumption of the user and transmits the readings to the utility provider at regular intervals of time. This raises privacy concerns [1] since high-resolution readings can allow anyone who has access to this data to infer about consumer's behavior. Since its introduction in [2], non-intrusive load monitoring (NILM) techniques are known to be quite effective in disaggregating the smart meter readings and thereby detecting the states of most of the general types of household appliances [3]. A comparative study was done in [3], which shows that the existing state of the art NILM algorithms are capable of achieving detection accuracy up to 99% for certain appliance types, which is quite concerning in the privacy context.

Addressing this issue, several privacy-preserving techniques have been proposed in the literature, which are surveyed in [4], [5]. Secure communication and cryptographic approaches [6]–[8] may succeed in preventing the unauthorized third party access, but they would fail to protect the consumer privacy from a greedy authorized or compromised utility provider. A promising physical layer privacy approach is load signature moderation (LSM), where an energy storage system (ESS) is used to moderate the consumer's load profile in order to hide appliances' usage information. LSM using rechargeable battery has previously been investigated in [9]–[14] to obtain optimal control strategy under different privacy settings. However, all the works so far make some ideal assumptions such as instantaneous control without delay, lossless ESS etc. These idealized strategies may provide theoretic performance bounds but the feasibility of such strategies in practical situations must be further investigated. In this paper, we present a one-step-ahead predictive control scheme modeled in a PO-MDP framework using an ESS. Similar to [13], we use a privacy metric based on Bayesian risk. The overview of the proposed system is shown in Fig. 1. In this work, we restrict our analysis to the electrochemical battery as an energy storage technology. Nonetheless, the same approach can be followed for other storage technologies by modeling them as their equivalent electrical circuits [15]. For a battery system, we present a model describing its losses in power conversion, losses due to internal resistance and self-dissipation. To the best of our knowledge, this is the first work to consider the non-idealities in ESSs in the context of smart meter privacy.

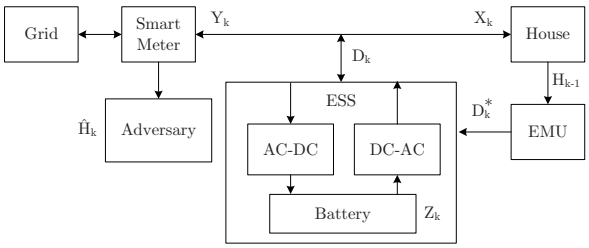


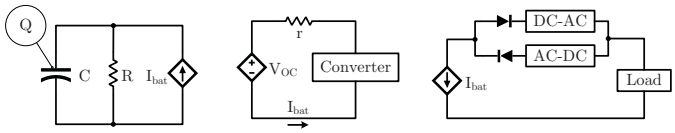
Fig. 1: Schematic of the proposed smart metering system where the energy management unit controls privacy leakage to an adversary by using energy storage system with a model describing its losses and one-step-ahead predictive control.

The rest of the paper is organized as follows. In Section II, we present a model for ESS considering the steady state energy losses. We also present the charge and discharge bounds of ESS and also quantify the energy loss associated with a discrete control action. In Section III, we present an overview of the system along with the control strategy. In Section IV, we evaluate the performance of the controller with real household data using a state-of-the-art NILM algorithm. Lastly, we conclude the paper in Section V.

978-1-5386-4505-5/18/$31.00

II. Energy Storage system Model

Since batteries stores the energy as chemical potential in their electrodes, it can only be interfaced with a DC (Direct Current) system. Hence, power converters are needed to integrate the battery with an AC (Alternating Current) system. The battery along with the power converters form the ESS. In this work, we model the ESS using three simple electrical circuits as shown in Fig. 2 to account for the steady state energy losses. Even though several other processes of the ESS such as capacity fade, increase in internal resistance, temperature dependence etc., can also be considered, as a first step, we restrict our focus to the steady state energy losses. In the following, we present our analysis of the three-circuit model in more detail.



(a) Self dissipation loss (b) Internal resistive loss (c) Converter loss

Fig. 2: Three-circuit energy storage system model

A. Losses due to self-dissipation

Self-dissipation occurs even if the ESS is not connected to any load. Similar to [16], we model this phenomenon using an RC circuit as shown in Fig. 2(a). The capacitor C holds the charge content, Q of the battery and dissipates through a parallel resistor R. In this circuit, the power converter and load are together represented as a current source controlled by the current flowing in the second circuit shown in Fig. 2(b). Given the self-discharge rate γ and a constant current $\mathrm{I_{bat}}$ flowing into the battery, the charge content of the battery is updated as

$$\mathrm{Q}_{t+\Delta t} = (1-\gamma)\cdot \mathrm{Q}_t + \beta \cdot \mathrm{I_{bat}} \tag{1}$$

where,

$$\gamma = 1 - \exp\Big(\frac{-\Delta T}{\mathrm{RC}}\Big); \qquad \beta = \frac{-\gamma \Delta T}{\log(1-\gamma)} \tag{2}$$

B. Losses due to internal resistance

Similar to [16], the losses that occur in battery during its charging and discharging operations are modeled using a series resistor r, as shown in Fig. 2(b). The open circuit voltage of the battery, $\mathrm{V_{OC}}$ is represented as a voltage source controlled by the capacitor charge Q in the first circuit shown in Fig. 2(a). For an input power of P from the power converter, the current flowing into the battery is given as

$$\mathrm{I_{bat}} = \frac{\sqrt{\mathrm{V_{OC}^2 + 4rP}} - \mathrm{V_{OC}}}{2\mathrm{r}} \tag{3}$$

C. Losses due to power converters

As shown in Fig. 2(c), we model power converters as elements with a constant efficiency factor within their operating region. For an input power of D from the load, the power at the battery terminals can be written as

$$\begin{aligned}\mathrm{P} &= \mathrm{D}\cdot\big(\eta_c \mathbb{1}\{\mathrm{D}\geq 0\} + \eta_d^{-1}\mathbb{1}\{\mathrm{D}<0\}\big)\\ &= \mathrm{D}\cdot\delta(\mathrm{D})\end{aligned} \tag{4}$$

where η_c, η_d are the efficiency factors of AC-DC and DC-AC converters respectively and $\mathbb{1}\{A\}$ is equal to 1 if A is true, and 0 otherwise. $\delta(\mathrm{D})$ is the common factor for both operations.

D. Three-circuit ESS model

Integrating the three circuits by combining (1), (3) and (4), the controller updates the energy state of the battery evolving over time using the equation given as

$$\mathrm{Z}_{t+\Delta t} = (1-\gamma)\mathrm{Z}_t + \frac{\beta \mathrm{V_{OC}}}{2\mathrm{r}}\left(\sqrt{\mathrm{V_{OC}^2} + 4\mathrm{r}\mathrm{D}_t\delta_t} - \mathrm{V_{OC}}\right) \tag{5}$$

where γ, r are time-invariant parameters, β depends on the time step Δt and δ_t depends on the control variable D_t. By limiting the battery current to $\mathrm{I_{max}}$, from (3), we have the control space limited as

$$\mathrm{D_{max}} = \frac{1}{4\mathrm{r}\eta_d}\left((\mathrm{V_{OC}} + 2\mathrm{r}\mathrm{I_{max}})^2 - \mathrm{V_{OC}^2}\right) \tag{6}$$

$$\mathrm{D_{min}} = \frac{\eta_c}{4\mathrm{r}}\left(\mathrm{V_{OC}^2} - (\mathrm{V_{OC}} - 2\mathrm{r}\mathrm{I_{max}})^2\right) \tag{7}$$

Due to the finite energy capacity of the battery Z_{max}, from (5) we have the following constraints on D_t:

$$\mathrm{D}_{t,max} = \frac{\mathrm{V_{OC}^2}}{4\mathrm{r}\eta_d}\left(\left(\frac{2\mathrm{r}\big[\mathrm{Z}_{max} - (1-\gamma)\mathrm{Z}_t\big]}{\beta \mathrm{V_{OC}^2}} + 1\right)^2 - 1\right) \tag{8}$$

$$\mathrm{D}_{t,min} = \frac{\eta_c \mathrm{V_{OC}^2}}{4\mathrm{r}}\left(\left(\left[\frac{-(1-\gamma)2\mathrm{r}\mathrm{Z}_t}{\beta \mathrm{V_{OC}^2}} + 1\right]^+\right)^2 - 1\right) \tag{9}$$

where $[x]^+$ is equal to x if $x \geq 0$, and 0 otherwise. In comparision to (5), the energy state of an ideal lossless battery evolves over time as

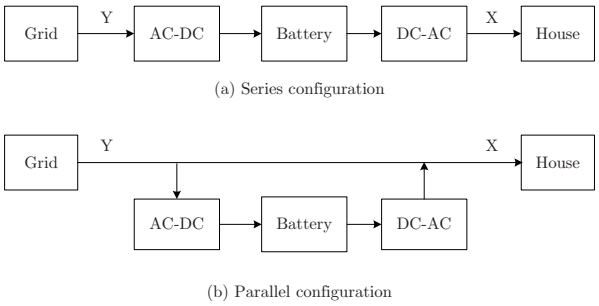
$$\mathrm{Z}_{t+\Delta t,ideal} = \mathrm{Z}_t + \mathrm{D}_t \cdot \Delta t \tag{10}$$

Using (5) and (10), the energy loss associated with a discrete control action can be given as

$$\mathcal{E}_{loss}(\mathrm{Z}_t, \mathrm{D}_t) = \mathrm{Z}_t + \mathrm{D}_t\cdot\Delta t - \mathrm{Z}_{t+\Delta t} \tag{11}$$

III. System overview and Control strategy

The proposed smart metering system uses an ESS for load signature moderation. The ESS can be placed either in series or in parallel configurations, in between the SM and house as shown in Fig. 3. Both these configurations have been used in the literature for SM privacy. Under ideal assumptions, the two configurations are equivalent. However, considering the energy losses, we have the following proposition.



(a) Series configuration

(b) Parallel configuration

Fig. 3: Placement of ESS between smart meter and house.

Proposition 1. *The average energy loss in the parallel configuration is strictly less than that of series configuration.*

Proof. Let X be the average energy demand by the house and Y be the average energy request from the grid. Assuming that the energy from the battery is not discharged back into the grid, only $(\mathrm{Y}-\mathrm{X})$ flows through the ESS components in parallel configuration, however, the total energy Y from the grid flows through the ESS components in series configuration, leading to higher energy losses. □

In order to reduce the energy losses, we consider a system with ESS in the parallel configuration as shown in Fig. 1. The discrete time system is controlled for every time slot k within a finite time horizon $\{1, 2, \ldots, N\}$. Each time slot k is of a fixed time duration T. Let e and q be the resolution of energy and power measurements respectively. In the following analysis, we use the capital letters to denote random variables, their realizations by the lower-case letters and the range space by calligraphic letters.

For each time slot k, X_k denotes the aggregate power drawn by all the appliances in the house and is defined on $\mathcal{X}=\{0, q, 2q, \ldots, x_{max}\}$. Z_k defined on $\mathcal{Z}=\{0, e, 2e, \ldots, z_{max}\}$ denotes the energy available in the battery. The power drawn by the ESS is denoted as D_k and it is the control variable which is defined on $\mathcal{D} = \{-d_{min}, \ldots, -q, 0, q, \ldots, d_{max}\}$, where d_{min} and d_{max} are the maximum discharge and charge power of the ESS respectively, given in (6) and (7). D_k^* defined on $\mathcal{D}$ denotes the desired battery power consumption scheduled by the energy management unit (EMU). In the presence of an ESS, the SM records the aggregate power demands of consumer and ESS. In this work, we allow the energy from the battery to be discharged to the grid resulting in negative values of SM measurements. It is represented by the random variable $Y_k = X_k + D_k$ which is defined on $\mathcal{Y} = \{-d_{min}, \ldots, -q, 0, q, \ldots, x_{max} + d_{max}\}$. H_k defined on $\mathcal{H}$ denotes the n-ary joint hypothesis of all the appliances in the house and $\hat{H}_k$ defined on $\mathcal{H}$ denotes the hypothesis detected by the adversary having access to the consumer's statistical and real-time data as well as the control strategy employed by the EMU.

A. Bayesian risk

Similar to [13], we use detection-theoretic approach by formulating the smart meter privacy problem into an adversarial Bayesian hypothesis testing where an adversary having access to the consumer's statistical and real-time data tries to make a guess on the hypothesis state using a decision strategy. In the Bayesian formulation, each of the hypothesis test outcomes is assigned a cost and the decision strategy that minimizes the average decision-making cost will be employed by the adversary [17]. The average cost or *Bayesian risk* function, $\mathcal{R}$, is given as

$$\mathcal{R}_k = \sum_{i,j \in \mathcal{H}^2} C_{i,j} \cdot P(\hat{H}_k = i \mid H_k = j) \cdot P(H_k = j) \quad (12)$$

where $C_{i,j}$ is the cost of deciding $\hat{H}_k = i$ when $H_k = j$ is true. By setting the cost of a correct decision to zero and the cost of an error to unity, the risk function gives the average error probability of an adversarial detection strategy.

In this work, the *accumulated minimum Bayesian risk* (AMBR) is chosen as a privacy metric, which is given as

$$\text{AMBR} = \sum_{k=1}^{N} \mathcal{R}_k^* \quad (13)$$

where $\mathcal{R}_k^* = \min\{\mathcal{R}_k\}$. The AMBR is a good choice for measuring privacy due to its operational meaning. It explicitly characterizes the best possible detection performance achievable by any adversary.

B. Control strategy

Ideally, the controller uses all the information available until time k (denoted as $\mathcal{I}_k$) to choose an action d_{k+1}. However, as described in [18], since $\mathcal{I}_k$ is increasing in dimension with k, its sufficient statistic given by the posterior distribution of the Markov chain H_k conditioned on $\mathcal{I}_k$ (denoted as π_k) is used instead of $\mathcal{I}_k$ to choose the action d_{k+1}. For a given initial battery state z_0, this posterior distribution forms a *information state* or *belief state* at time k, given as

$$\begin{aligned} \pi_k(i) &= P(H_k = i \mid \mathcal{I}_k) \\ &= P(H_k = i \mid \pi_{k-1}, x_k) \end{aligned} \quad (14)$$

where $\mathcal{I}_k = \{z_0, \pi_0, x_1, y_1, \pi_1, \ldots, \pi_{k-1}, x_k\}$. The control system is modeled as a PO-MDP controlled sensor, as shown in Fig. 4, by making the following assumptions:

- The hypothesis of the house H_k evolves over time following a first-order Markov chain with a time-invariant transition probability $P_{H_k|H_{k-1}}$.
- The controller observes the Markov chain H_k only through a noisy measurement X_k made with a time-invariant observation probability $P_{X_k|H_k}$.
- The control signal D_k^* is generated by the controller using time-dependent control strategy $P_{Y_k|X_{k-1},Z_{k-1},\Pi_{k-1}}$.

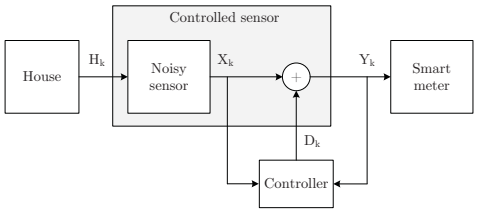


Fig. 4: EMU modelled as a PO-MDP controlled sensor.

Given the initial energy state, z_0, the controller estimates the state of ESS at any time k using the equation

$$z_k = f(z_{k-1}, d_k) \tag{15}$$

where $d_k = y_k - x_k$ and f is a deterministic function of ESS model given by (5). As described in [17], the minimum Bayesian risk function based on our assumptions is given as

$$\mathcal{R}_k^*(\pi_{k-1}, z_{k-1}, \mu_k) = \sum_{y\in\mathcal{Y}} \min_{\hat{h}\in\mathcal{H}} \Big\{ \sum_{g,h,x\in\mathcal{H}^2\times\mathcal{X}} C(\hat{h}, h)\cdot P_{Y_k|X_{k-1},Z_{k-1}}(y \mid x, z)\cdot P_{X_{k-1}|H_{k-1}}(x \mid g)\cdot P_{H_k|H_{k-1}}(h \mid g)\cdot P_{H_{k-1}}(g) \Big\}$$

For the finite time horizon, the optimal control strategy is the solution to the nonlinear optimization problem with objective function given as

$$\mu^* = \underset{\{\mu_1,\cdots,\mu_N\}}{\operatorname{argmax}} \sum_{k=1}^{N} \mathcal{R}_k^*(\pi_{k-1}, z_{k-1}, \mu_k) \tag{16}$$

subject to the constraints given as

$$P_{Y_k|Z_{k-1}}(y_k \mid z_{k-1}) = 0 \text{ if } \begin{cases} y_k < d_{k,min} \\ \quad \text{or} \\ y_k > d_{k,max} + x_{max} \end{cases}$$

The *belief state space* (denoted as Π) is a $|\mathcal{H}| - 1$ dimensional unit simplex. Solving this optimization problem requires discretization of Π in order to get a finite set. The optimization variable in (16) is of dimension $N \times |\mathcal{Y}| \times |\mathcal{X}|$ and solving it in its original form is computationally complex as the dimensionality of the the problem increases with N. This can be formulated into a recursive dynamic programming problem as given in the following proposition, the proof of which follows from [18].

Proposition 2. *For the finite horizon PO-MDP with model given in Section III, the optimal control strategy $\mu^* = \{\mu_1^*, \mu_2^*, \ldots, \mu_N^*\}$ is the solution to the following backward recursion: Initialize $\mathcal{V}_N(\pi, z)$ and then for $k = N-1, \ldots, 1$ iterate*

$$L_k(\pi_{k-1}, z_{k-1}, \mu_k) = \mathcal{R}_k^*(\pi_{k-1}, z_{k-1}, \mu) + \sum_{x_k, y_k \in \mathcal{X}\times\mathcal{Y}} \mathcal{V}_{k+1}(\pi_k, z_k)\cdot P(x_k, y_k)$$

$$\mathcal{V}_k(\pi_{k-1}, z_{k-1}) = \max_{\mu_k} \Big\{ L_k(\pi_{k-1}, z_{k-1}, \mu_k) \Big\}$$

$$\delta_k^*(\pi_{k-1}, z_{k-1}) = \underset{\mu_k}{\operatorname{argmax}} \Big\{ L_k(\pi_{k-1}, z_{k-1}, \mu_k) \Big\} \qquad \square$$

With the designed optimal strategy μ^*, a real-time PO-MDP controller is implemented as shown in the following algorithm.

Algorithm 1 Realtime PO-MDP controller

Initialisation: π_0, z_0
for $k = 1$ to N **do**
  Pre-process :
    Choose action $y_k^* = \mu_k^*(\pi_{k-1}, z_{k-1})$
  ESS control :
    if $(y_k^* < x_k + d_{k,min})$ **then**
      Limit $y_k = x_k + d_{k,min}$
    else if $(y_k^* > x_k + d_{k,max})$ **then**
      Limit $y_k = x_k + d_{k,max}$
    else
      Allow $y_k = y_k^*$
    end if
  Post-process :
    Update the belief state $\pi_k = T(\pi_{k-1}, x_k)$
    Update the ESS state $z_k = f(z_{k-1}, y_k - x_k)$
end for

IV. Numerical Experiments

The simulation experiments to validate our control scheme are implemented in MATLAB using real household consumption data from ECO reference dataset [19]. The control strategy is obtained by solving the optimization problem using the nonlinear programming solver based on interior point algorithm [20]. We simulate a scenario where the controller is tasked to protect the events of a water kettle every day between 8 AM and 9 AM. The controller chooses an action every minute by observing the real-time appliance consumption data. For this objective, a 12V 100Ah lithium-ion battery is selected, which can sufficiently satisfy the power requirements of the kettle. To simplify the problem, we assume a fixed V_{OC} equal to the nominal battery voltage. The parameters used in the simulation are listed in Table I. The Markov chain probabilities of the PO-MDP control model are estimated from 30 days of labeled training data and listed in the Table II.

A. Visualization of control actions

With this setup, the control actions for different initial states of the battery are simulated and are shown in Fig. 5. Due to the measurement quantization, switching events are noticed as peaks in the smart meter measurements as shown in Fig. 6. These residual peaks are informative to an adversary operating with high precision measurements. However, the cardinality of the state space increases with measurement precision, which increases the dimensionality of the optimization problem by $\mathcal{O}(n^2)$. Fig. 7 shows the evolution of the state of charge (SOC) of the battery due to control actions. It is interesting to notice that without any design objective on the battery state, the control scheme is steering the battery towards the full charge state. This result in the degradation of controller's performance which is discussed in the following.

TABLE I: Simulation parameters

Parameter	Symbol	Value
Max. appliance power demand	$x_{\max}$ (W)	1700
Time slot duration	T (s)	60
Time horizon length	N	60
Power measurement resolution	q (W)	500
Energy measurement resolution	e (Wh)	5
Battery nominal voltage	V_{nom} (V)	12
Battery capacity	Q_{max} (Ah)	100
Max. allowed battery charging current	I_{max} (A)	80
Max. allowed battery discharging current	I_{min} (A)	80
Battery internal resistance	r (Ω)	0.006
Battery self-discharge rate	γ (%/month)	3
Power converter efficiency	η_c, η_d (%)	95
Cardinality of $\mathcal{X}$	$\lvert\mathcal{X}\rvert$	4
Cardinality of $\mathcal{Y}$	$\lvert\mathcal{Y}\rvert$	8
Cardinality of $\mathcal{Z}$	$\lvert\mathcal{Z}\rvert$	241
Cardinality of $\mathcal{H}$	$\lvert\mathcal{H}\rvert$	2
Cardinality of Π	$\lvert\Pi\rvert$	11
Max. allowed battery input power	D_{max}	+2q
Min. allowed battery input power	D_{min}	-2q
ESS model parameter	β	0.017

TABLE II: PO-MDP control parameters

Parameter	Value
$C_{i,j}$	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
π_0	$\begin{bmatrix} 0.95 & 0.05 \end{bmatrix}^T$
$P(H_k\|H_{k-1})$	$\begin{bmatrix} 0.98 & 0.34 \\ 0.02 & 0.65 \end{bmatrix}$
$P(X_k\|H_k)$	$\begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 0.17 & 0.14 & 0.17 \end{bmatrix}^T$

B. Evaluation of controller's performance

To evaluate the performance of the controller, we simulate an adversary using NILM algorithm. In particular, we simulated Weiss' algorithm [21] which extracts switching events from the aggregate smart meter data and assigns each event to the appliance with the best match in a signature database. This algorithm is implemented using NILM toolbox developed by [19]. We use 30 days of labeled training data to create the signature database. Weiss algorithm utilizes three-dimensional consumption data (i.e., real, reactive, and distortion powers) in order to match an event signature. We tested its detection performance by injecting the controlled battery current in-phase to the supply voltage resulting in corrupted real power measurements. The accuracy of the adversarial detection is measured using F-score, which is given as

$$\text{F-score} = \frac{1}{1 + (\text{FN} + \text{FP})/(2\text{TP})} \tag{17}$$

where FN, FP and TP denote false negative, false postive and true positive respectively. The F-score lies between 0 and 1, where F-score = 0 indicates no detection and F-score = 1 indicates complete detection.

The Weiss's algorithm is simulated under different test conditions using 30 days of validation data and the obtained average F-scores, energy losses and the AMBR are listed in Table III. It can be seen from the results that the AMBR and the F-score are correlated. The test case without a battery resulted in the highest F-score. While using a battery, the controller is able to reduce the F-score significantly. However, it can be observed that the ability of the controller to preserve privacy depends on the initial state of the battery. For this simulation setup, the controller performed better when initialized with a battery of 25%-50% SOC compared to full charge. This indicates that if the battery state is steered towards 25%-50% SOC by the end of the control time horizon, it would result in better performance for the next control horizon. However, this improved performance is achieved at the cost of increased energy loss.

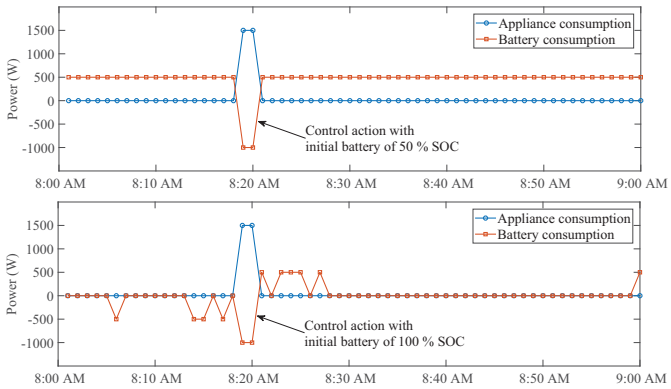


Fig. 5: Control actions of battery.

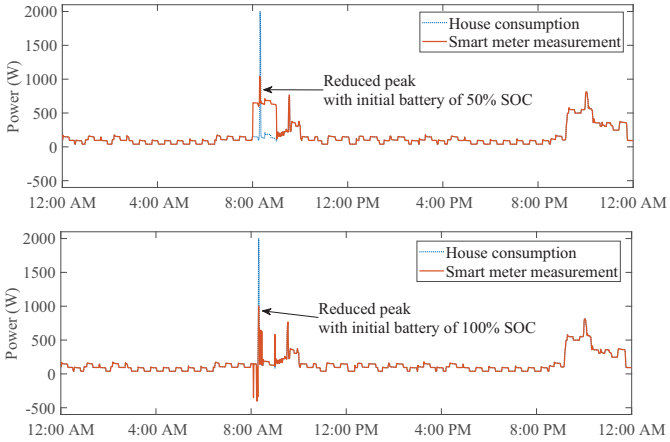


Fig. 6: Smart meter readings vs household consumption.

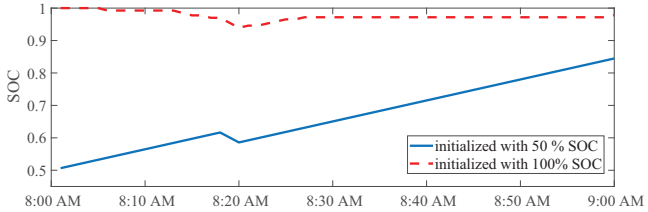


Fig. 7: Evolution of SOC of battery due to control actions.

TABLE III: Evaluation of controller against NILM algorithm with different initial battery states

Initial battery SOC (%)	F-score	Energy loss (Wh)	AMBR
0	0.1333	40.421	152.57
25	0.0357	36.217	153.51
50	0.0357	36.230	153.51
75	0.2667	26.770	153.50
90	0.4833	14.174	153.49
100	0.6333	9.779	148.89
Without battery	0.7931	0	0

C. ESS model comparision

For the simulated battery, Fig. 8 shows the difference between the % change in the state of charge of the battery estimated by three-circuit model and an ideal lossless model for different input powers. The model difference is particularly significant at high power levels. Due to very low γ for electrochemical batteries, the difference in state estimation is negligible when comparing three-circuit models with and without considering self-dissipation. However, for energy storage systems with high self-dissipation rate such as flywheels, the self-dissipation phenomenon cannot be neglected.

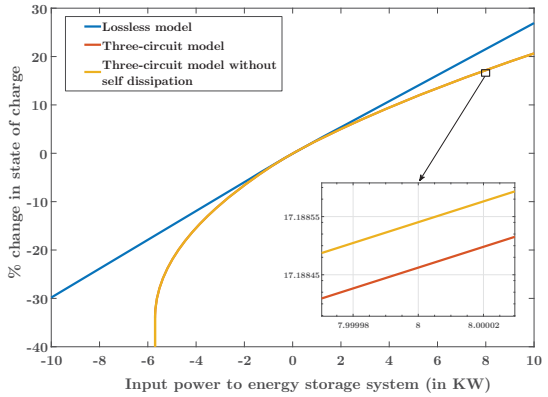


Fig. 8: Comparision of ESS models at 50% SOC.

V. Conclusion

In this paper, we presented a privacy-preserving control scheme based on Bayesian risk and a three-circuit model to estimate the energy loss associated with a control action. The controller is modeled as a PO-MDP controlled sensor to maximize the Bayesian risk function of an adversarial hypothesis testing and the resulting nonlinear optimization objective is solved in a backward recursion. Extensive numerical experiments were carried out to evaluate the performance of the controller thoroughly. Especially, we tested the controller's performance against a state-of-the-art NILM algorithm using real energy consumption data. We investigated the effect of the initial state of the energy storage system on the controller's performance. An important conclusion from this work is that the privacy leakage can be reduced by using an energy storage system but at the expense of energy loss. Without an accurate model, the error in state estimation propagates and if not corrected, leads to suboptimal privacy control.

Future work will focus on the trade-off between the privacy and energy loss, time dependency of the model parameters as well as control strategy and including more energy storage technologies.

References

[1] P. McDaniel and S. McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security & Privacy*, vol. 7, no. 3, 2009.

[2] G. W. Hart, "Nonintrusive appliance load monitoring," *Proceedings of the IEEE*, vol. 80, no. 12, pp. 1870–1891, 1992.

[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] M. R. Asghar, G. Dán, D. Miorandi, and I. Chlamtac, "Smart meter data privacy: A survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2820–2835, 2017.

[5] G. Giaconi, D. Gunduz, and H. V. Poor, "Privacy-aware smart metering: Progress and challenges," *arXiv preprint arXiv:1802.01166*, 2018.

[6] M. LeMay, G. Gross, C. A. Gunter, and S. Garg, "Unified architecture for large-scale attested metering," in *System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on*. IEEE, 2007, pp. 115–115.

[7] M. Jawurek, M. Johns, and K. Rieck, "Smart metering de-pseudonymization," in *Proceedings of the 27th Annual Computer Security Applications Conference*. ACM, 2011, pp. 227–236.

[8] A. Rial and G. Danezis, "Privacy-preserving smart metering," in *Proceedings of the 10th annual ACM workshop on Privacy in the electronic society*. ACM, 2011, pp. 49–60.

[9] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda, "Privacy for smart meters: Towards undetectable appliance load signatures," in *Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on*. IEEE, 2010, pp. 232–237.

[10] D. Varodayan and A. Khisti, "Smart meter privacy using a rechargeable battery: Minimizing the rate of information leakage," in *Acoustics, Speech and Signal Processing (ICASSP), 2011 IEEE International Conference on*. IEEE, 2011, pp. 1932–1935.

[11] 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.

[12] 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.

[13] Z. Li, T. J. Oechtering, and M. Skoglund, "Privacy-preserving energy flow control in smart grids," in *Acoustics, Speech and Signal Processing (ICASSP), 2016 IEEE International Conference on*. IEEE, 2016, pp. 2194–2198.

[14] 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*, 2017.

[15] 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)," *Journal of Energy Storage*, vol. 13, pp. 73–84, 2017.

[16] 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.

[17] P. K. Varshney, *Distributed detection and data fusion*. Springer Science & Business Media, 2012.

[18] V. Krishnamurthy, *Partially Observed Markov Decision Processes*. Cambridge University Press, 2016.

[19] 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 *Proceedings of the 1st ACM International Conference on Embedded Systems for Energy-Efficient Buildings (BuildSys 2014). Memphis, TN, USA*. ACM, Nov. 2014, pp. 80–89.

[20] R. H. Byrd, J. C. Gilbert, and J. Nocedal, "A trust region method based on interior point techniques for nonlinear programming," *Mathematical Programming*, vol. 89, no. 1, pp. 149–185, 2000.

[21] M. Weiss, A. Helfenstein, F. Mattern, and T. Staake, "Leveraging smart meter data to recognize home appliances," in *Pervasive Computing and Communications (PerCom), 2012 IEEE International Conference on*. IEEE, 2012, pp. 190–197.