PRIVACY-ENHANCING APPLIANCE FILTERING FOR SMART METERS

Ramana R. Avula, and Tobias J. Oechtering

Department of Intelligent Systems, KTH Royal Institute of Technology, Sweden

ABSTRACT

Non-intrusive load monitoring (NILM) is the process of disaggregating total electricity consumption measured by a smart meter into individual appliances' contributions. In this paper, we present a privacy control strategy that selectively filters appliances' consumption from the smart meter measurements to hinder NILM disaggregation performance. The privacy controller uses charging and discharging operations of an energy storage to achieve desired smart meter measurements. We model the household consumption using both additive and difference factorial hidden Markov models and design a control strategy to minimize privacy leakage measured in terms of Bayesian risk due to maximum a posteriori detection. Due to the high computational complexity of the optimal control strategy, we propose a computationally efficient sub-optimal strategy. We evaluate the proposed approaches using the ECO data set and show their privacy improvements against the Viterbi disaggregation algorithm.

Index Terms— Factorial hidden Markov model, privacy-enhancing control, privacy-by-design, smart meter privacy, Markov decision process

1. INTRODUCTION

Smart meters (SMs) pose privacy risk in smart grids due to the transmission of high-resolution details of user's energy consumption behavior to the utility provider [1]. Several non-intrusive load monitoring (NILM) algorithms [2–8] are known to be quite effective in disaggregating the smart meter readings. Addressing these risks, several privacy-preserving techniques have been proposed in the literature, which are surveyed in [9, 10]. A well studied privacy-by-design approach, known as *load signature moderation*, uses energy storage systems (ESSs) to alter consumers' energy consumption profiles in order to hide their appliances' usage patterns using a heuristic best effort approach in [11], information theoretic approach in [12–15], differential privacy approach in [16] and detection theoretic approach in [17, 18].

In contrast to the existing works, in this paper we present a privacy control strategy targeting a class of NILM algorithms such as Parson's Algorithm [5], Baranski's algorithm [6], Weiss' algorithm [7], and Kolter's algorithm [8] which disaggregate SM data by using steady-state features such as aggregate and difference power measurements [19]. To the best of our knowledge, control strategies against this class of NILM algorithms using both aggregate and difference observations have not yet been studied and the existing works may or may not achieve the least possible privacy leakage against these NILM algorithms.

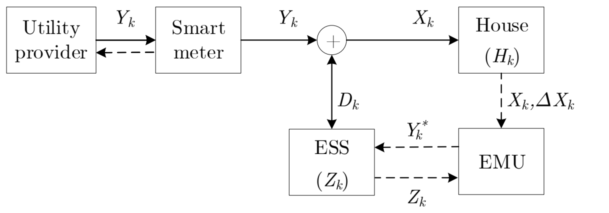


Fig. 1. Schematic of the studied smart metering system where the energy management unit controls privacy leakage by using an energy storage system. Here, the solid lines denote the energy flow and the dotted lines denote the information flow.

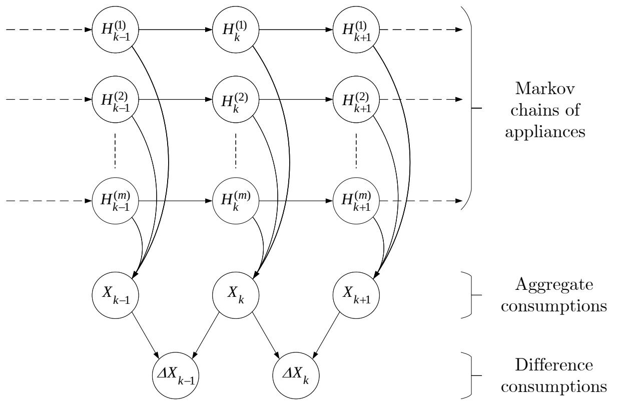


Fig. 2. The additive and difference FHMM of appliances.

The proposed smart metering system uses an ESS for load signature moderation, as shown in Fig. 1. We model the household appliances using the factorial hidden Markov model (FHMM), where each appliance follows a Markov chain and these chains jointly emit aggregate power and the power change observations, as shown in Fig. 2. The energy management unit (EMU) schedules the charging and discharging actions of the ESS to minimize the Bayesian risk due to maximum a posteriori (MAP) detection of privacy-sensitive appliances.

The rest of the paper is organized as follows. In Section 2, we present the overview of the studied smart metering system. In Section 3 we formulate the design objective and present the optimal control strategy to minimize privacy leakage. In Section 4, we present results from a numerical study and conclude the paper in Section 5. Throughout the paper, we denote random variables by capital letters, their realizations by lower-case letters, and their 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 expectation; $(\cdot)^\intercal$ to denote the transpose; P_A to denote a probability distribution function; $\circledast$ to denote convolution; $\mathbb{1}$ to denote an indicator function for which $\mathbb{1}\{a\}$ is 1 if a is true, and 0 otherwise; $\mathbf{1}_n$ to denote an n dimensional vector with all entries as 1; and Δ_n to denote the $(n-1)$ dimensional simplex.

2. SYSTEM OVERVIEW

The discrete time system in Fig. 1 is controlled for every time slot k within a time horizon $\mathcal{K} = \{1, 2, \dots, n\}$. Each time slot is of a fixed time duration T. Let e and q be the resolution of energy and power measurements respectively. For each $k \in \mathcal{K}$, let $H_k^{(i)}$, defined on a discrete set $\mathcal{H}^{(i)}$, denote the state of i^{th} appliance and let m denote the number of appliances. Further, let $\Delta H_k^{(i)} = H_k^{(i)} - H_{k-1}^{(i)}$, defined on the discrete set $\Delta\mathcal{H}^{(i)} = \{-(|\mathcal{H}^{(i)}| - 1), \dots, (|\mathcal{H}^{(i)}| - 1)\}$, denote the change in the state of of i^{th} appliance. Further, let $\boldsymbol{H}_k = [H_k^{(1)}, \dots, H_k^{(m)}]$ denote the joint state vector which is defined on the discrete vector space $\boldsymbol{\mathcal{H}} := \prod_{i=1}^{m} \mathcal{H}^{(i)}$.

For each $k \in \mathcal{K}$, X_k denotes the aggregated power demand of all appliances in the house and is defined on $\mathcal{X}= \{0, q, 2q, \dots, x_{max}\}$. Let $\Delta X_k = X_{k+1} - X_k$ denote the aggregated power change of the household appliances and is defined on $\Delta\mathcal{X} = \{-x_{max}, \dots, -q, 0, q, \dots, x_{max}\}$. Z_k, defined on $\mathcal{Z}= \{0, e, 2e, \dots, z_{max}\}$, denotes the energy available in the battery at the end of time slot k. The power drawn by the ESS is denoted as D_k and it is defined on a discrete set $\mathcal{D} = \{-d_{min}, \dots, -q, 0, q, \dots, d_{max}\}$, where d_{min} and d_{max} are the maximum discharge and charge powers of the ESS respectively. In the presence of an ESS, the SM records the aggregated power demands of all household appliances and the ESS, which is represented by the random variable $Y_k = X_k + D_k$ which is defined on $\mathcal{Y} = \mathcal{X}$. Let Y_k^*, defined on $\mathcal{Y}$, denote the desired aggregate power demand scheduled by the EMU. Further, we model the dependency between the random variables in the sequences $[\boldsymbol{H}_{1:n}, X_{1:n}, \Delta X_{1:n}]$ using a FHMM with these assumptions:

- The state of each appliance $H_k^{(i)}$ evolves over time, independent of other applainces, according to a first-order Markov chain with transition and initial probabilities $P_{H_k^{(i)}|H_{k-1}^{(i)}}$ and $P_{H_1^{(i)}}$.
- At most one appliance's state transitions at each $k \in \mathcal{K}$.
- Each appliance contributes to the aggregate and difference observations X_k, ΔX_k through hidden emissions $W_k^{(i)}, \Delta W_k^{(i)}$ which follow the emission probabilities $P_{W_k^{(i)}|H_k^{(i)}}$ and $P_{\Delta W_k^{(i)}|\Delta H_k^{(i)}}$.

Consequently, the joint distribution of the variables in the sequence $[\boldsymbol{H}_{1:n}, X_{1:n}, \Delta X_{1:n}]$ considering both additive and difference measurements are given by:

$$P_{\boldsymbol{H}_{1:n},X_{1:n},\Delta X_{1:n}} = P_{\boldsymbol{H}_1} P_{X_1|\boldsymbol{H}_1} \prod_{k=2}^{n} \mathbb{1}\{\Delta X_k = X_k - X_{k-1}\} \times P_{X_k,\boldsymbol{H}_k|X_{k-1},H_{k-1}}, \quad (1)$$

where $P_{\boldsymbol{H}_1}$, $P_{X_1|\boldsymbol{H}_1}$, and $P_{X_k,\boldsymbol{H}_k|X_{k-1},H_{k-1}}$ are obtained using $\{P_{H_k^{(i)}|H_{k-1}^{(i)}}, P_{H_1^{(i)}}, P_{W_k^{(i)}|H_k^{(i)}}, P_{\Delta W_k^{(i)}|\Delta H_k^{(i)}}\}$.

3. ENERGY MANAGEMENT UNIT STRATEGY

In this work, we design an EMU strategy using the Markov decision process (MDP) framework by minimizing the Bayesian risk due to MAP detection. We first present an optimal strategy using both aggregate and difference observations $X_k, \Delta X_k$ jointly. We then present a low complexity sub-optimal strategy that uses a fusion rule to combine the information in both additive and difference FHMMs. Here we assume that an adversary employs existing NILM algorithms tuned for disaggregation of appliances' consumption using unmodified household consumption data. That is, the adversary is assumed to be unaware of the existence of privacy-preserving EMU and the MAP detection is performed under the assumption that $Y_{1:n} = X_{1:n}$.

3.1. Optimal strategy

The MAP state sequence estimate given both the aggregate and difference observation sequences $[y_{1:n}, \Delta y_{1:n}]$ is obtained by solving the optimization problem:

$$\hat{\boldsymbol{h}}_{1:n}(y_{1:n}, \Delta y_{1:n}) = \operatorname*{argmax}_{\boldsymbol{h}_{1:n} \in \mathcal{H}^n} \Big\{ \log\big[P_{X_1|\boldsymbol{H}_1}(y_1|\boldsymbol{h}_1) P_{\boldsymbol{H}_1}(\boldsymbol{h}_1)\big] + \sum\nolimits_{k=2}^{n} \log\big[P_{X_k,\boldsymbol{H}_k|X_{k-1},\boldsymbol{H}_{k-1}}(y_k, \boldsymbol{h}_k | y_{k-1}, \boldsymbol{h}_{k-1})\big] \Big\}. \quad (2)$$

The MAP state sequence estimate $\hat{h}_{1:n}$ obtained from (2) uses non-causal data i.e., the detection is performed block-wise after a sequence of SM readings is received. However, as the EMU operates causally, similar to [20], we first compute a causal detection strategy that achieves the expected performance of non-causal MAP detection given the causal data $[y_{1:k}, \Delta y_{1:k}]$. At each $k \in \mathcal{K}$, we model the state estimate of the causal detection strategy using a discrete random variable $\hat{H}_k^{(i)} \in \mathcal{H}^{(i)}$ for the i^{th} appliance. Let $\hat{\boldsymbol{H}}_k$ denote the joint state estimate vector corresponding to all appliances at time instant k. Let $\hat{\pi}_k \in \Delta_{|\mathcal{H}|}$ denote the posterior distribution of $\boldsymbol{H}_k$ given causal data $[y_{1:k}, \Delta y_{1:k}]$ which is the information state [21] of the modeled adversary. We refer to $\hat{\pi}_k$ as *controlled belief state*, which is given by

$$\begin{aligned}\big[\hat{\pi}_k(y_{1:k}, \Delta y_{1:k})\big]_{\boldsymbol{h}_k} &= P_{\boldsymbol{H}_k|X_{1:k},\Delta X_{1:k}}\big(\boldsymbol{h}_k|y_{1:k}, \Delta y_{1:k}\big)\\ &= \frac{P_{X_k,\boldsymbol{H}_k|X_{1:k-1},\Delta X_{1:k-1}}(y_k, \boldsymbol{h}_k|y_{1:k-1}, \Delta y_{1:k-1})}{P_{X_k|X_{1:k-1},\Delta X_{1:k-1}}(y_k|y_{1:k-1}, \Delta y_{1:k-1})},\end{aligned} \tag{3}$$

where

$$\begin{aligned}P_{X_k,\boldsymbol{H}_k|X_{1:k-1},\Delta X_{1:k-1}}(y_k, \boldsymbol{h}_k|y_{1:k-1}, \Delta y_{1:k-1}) = \\ \textstyle\sum_{\tilde{\boldsymbol{h}}\in\boldsymbol{\mathcal{H}}} P_{X_k,\boldsymbol{H}_k|X_{k-1},\boldsymbol{H}_{k-1}}(y_k, \boldsymbol{h}_k|y_{k-1}, \tilde{\boldsymbol{h}})\times \\ \big[\hat{\pi}_{k-1}(y_{1:k}, \Delta y_{1:k})\big]_{\tilde{\boldsymbol{h}}}.\end{aligned} \tag{4}$$

Therefore, the belief state evolution is given by

$$\hat{\pi}_k = \frac{\mathbf{M}_\pi(y_{k-1:k}, k)\cdot\hat{\pi}_{k-1}}{\mathbf{1}_{|\mathcal{H}|}^{\mathsf{T}}\cdot\mathbf{M}_\pi(y_{k-1:k}, k)\cdot\hat{\pi}_{k-1}}, \tag{5}$$

where $\mathbf{M}_\pi$ is a deterministic function of $|\mathcal{H}| \times |\mathcal{H}|$ dimensional matrices with its elements given by (4). For any $x_{k-1:k}$, the random variable $\Delta X_k|X_{k-1:k} = x_{k-1:k}$ is deterministic and is redundant in the computation of $\hat{\pi}_k$. Let the causal detection strategy of the EMU-unaware adversary be denoted by $\zeta_k : \mathcal{Y}^2 \times \Delta_{|\boldsymbol{\mathcal{H}}|} \to \boldsymbol{\mathcal{H}}$, which specifies the state estimate $\hat{\boldsymbol{h}}_k \in \boldsymbol{\mathcal{H}}$ given the MDP state $(y_{k-1:k}, \hat{\pi}_{k-1})$. Let $\mathcal{G}$ denote the set of all valid causal detection strategy functions ζ_k. Based on the objective function in (2), we define a per-step MDP reward function for $k \geq 2$ given by

$$\begin{aligned}r_k(y_{k-1:k}, \hat{\pi}_{k-1}, \hat{\boldsymbol{h}}_k) = \textstyle\sum_{\tilde{\boldsymbol{h}}\in\boldsymbol{\mathcal{H}}} \max\Big\{r_{\min},\\ \log\big[P_{X_k,\boldsymbol{H}_k|X_{k-1},\boldsymbol{H}_{k-1}}(y_k, \hat{\boldsymbol{h}}_k|y_{k-1}, \tilde{\boldsymbol{h}})\big]\Big\}\hat{\pi}_{k-1}(\tilde{\boldsymbol{h}}),\end{aligned} \tag{6}$$

where $r_{\min} < 0$ is an arbitrarily small constant so that the MDP reward is lower bounded. Let ζ_k^* denote the optimal causal MAP detection strategy for each $k \in \mathcal{K}$. Using the Bellman's dynamic programming [21], a sequence of optimal strategies $\zeta_{1:n}^*$ that achieves the maximum expected cumulative reward over the horizon $\mathcal{K}$ can be obtained by solving:

$$\begin{aligned}v_k(y_{k-1:k}, \hat{\pi}_{k-1}) = \max_{\hat{\boldsymbol{h}}_k\in\boldsymbol{\mathcal{H}}}\Big\{r_k(y_{k-1:k}, \hat{\pi}_{k-1}, \hat{\boldsymbol{h}}_k) +\\ \mathbb{E}\big[v_{k+1}(X_{k:k+1}, \hat{\Pi}_k)\big|X_{k-1:k} = y_{k-1:k}\big]\Big\},\end{aligned} \tag{7}$$

where v_k is the expected reward over $[k, \ldots, n]$ due to optimal causal MAP detection strategies $\zeta_{k:n}^*$ and the recursion is initialized by a terminal reward function v_{n+1}. Note that the second term in the objective function of (7) does not depend on the optimization variable $\hat{\boldsymbol{h}}_k$ since $\hat{\pi}_{k-1}$ evolves to $\hat{\pi}_k$, independent of $\hat{\boldsymbol{h}}_k$, using only $y_{k-1:k}$ as given in (5). Therefore, the optimal causal MAP detection strategy at each $k \in \mathcal{K}$ is obtained by simplifying (7) as

$$\zeta_k^*(y_{k-1:k}, \hat{\pi}_{k-1}) = \underset{\hat{\boldsymbol{h}}_k\in\boldsymbol{\mathcal{H}}}{\operatorname{argmax}}\Big\{r_k(y_{k-1:k}, \hat{\pi}_{k-1}, \hat{\boldsymbol{h}}_k)\Big\}. \tag{8}$$

Next, we formulate another MDP problem to obtain the EMU control strategy. Let $\boldsymbol{\mathcal{A}} := \mathcal{X} \times \mathcal{Z} \times \mathcal{Y}$ denote a vector space and $\boldsymbol{A}_k := [X_k, Z_{k-1}, Y_{k-1}]$ denote a vector defined on $\boldsymbol{\mathcal{A}}$. Let $\pi_k \in \Delta_{|\mathcal{H}|}$ denote the posterior distribution of $\boldsymbol{H}_k$ given causal data $(x_{1:k}, \Delta x_{1:k})$ which is the information state [21] of the EMU. We refer to π_k as *exact belief state*, which follows the linear-fractional transformation in (5) using $x_{k-1:k}$ instead of $y_{k-1:k}$. Let $\mu_k : \boldsymbol{\mathcal{A}} \times \Delta_{|\mathcal{H}|}^2 \to \mathcal{Y}$ denote the EMU strategy, which specifies the desired control action $y_k^* \in \mathcal{Y}$ given the MDP state $(\boldsymbol{a}_k, \pi_k, \hat{\pi}_{k-1})$. Let $\mathcal{U}$ denote the set of all valid control strategies μ_k. To compute optimal control strategy μ_k^*, we define the per-step MDP cost function for the EMU based on the Bayesian risk, which is the average cost due to the adversarial MAP detection attack on privacy sensitive appliances, given by

$$c_k(\boldsymbol{a}_k, \pi_k, \hat{\pi}_{k-1}, y_k) = \sum_{\boldsymbol{h}_k} \bar{c}\left(\boldsymbol{h}_k, \zeta_k^*(y_{k-1:k}, \hat{\pi}_{k-1})\right)\pi_k(\boldsymbol{h}_k),$$

where $\bar{c}(\boldsymbol{h}, \hat{\boldsymbol{h}})$ denotes the cost incurred when an adversary detects $\hat{\boldsymbol{h}} \in \boldsymbol{\mathcal{H}}$ while the true joint state is $\boldsymbol{h} \in \boldsymbol{\mathcal{H}}$. Here, we assume that the cost for a correct detection of privacy sensitive appliance state is higher compared to that of the wrong state detection, such that the EMU aims to minimize the cumulative Bayesian risk. Similar to (7), a sequence of optimal EMU strategies $\mu_{1:n}^*$ that achieve the minimum cumulative Bayesian risk over $\mathcal{K}$ can be obtained by solving:

$$\begin{aligned}s_k(\boldsymbol{a}_k, \pi_k, \hat{\pi}_{k-1}) = \min_{y_k\in\mathcal{Y}_k(\boldsymbol{a}_k)}\Big\{c_k(\boldsymbol{a}_k, \pi_k, \hat{\pi}_{k-1}, y_k) +\\ \mathbb{E}\big[s_{k+1}(\boldsymbol{A}_{k+1}, \Pi_{k+1}, \hat{\Pi}_k)\big|\boldsymbol{A}_k = \boldsymbol{a}_k\big]\Big\},\end{aligned} \tag{9}$$

where $\mathcal{Y}_k(\boldsymbol{a}_k)$ is the set of valid control actions given by the ESS model; s_k is the expected cost over $[k, \ldots, n]$ due to optimal strategies $\mu_{k:n}^*$; and the recursion is initialized by a terminal cost function s_{n+1}. Note that (9) needs to be solved over continuous spaces of the belief states π_k and $\hat{\pi}_{k-1}$. In the following, we have a proposition on computing an optimal strategy with respect to the continuous variable π_k.

Proposition 1. *Consider the optimal strategy $\bar{\mu}_k^* : \boldsymbol{\mathcal{A}} \times \mathcal{H} \times \Delta_{|\mathcal{H}|} \to \mathcal{Y}$ obtained, when the joint-state $\mathbf{h}_k$ is observable by the EMU, using Bellman's equation similar to (9). For any given $\pi_k \in \Delta_{|\mathcal{H}|}$, a randomized strategy $\tilde{\mu}_k^*$ that achieves the minimum expected cumulative Bayesian risk equivalent to the optimal strategies $\mu_{1:n}^*$ given by (9) is given by*

$$\big[\tilde{\mu}_k^*(\boldsymbol{a}_k,\pi_k,\hat{\pi}_{k-1})\big]_y = \sum_{\boldsymbol{h}_k\in\boldsymbol{\mathcal{H}}} \mathbb{1}\big\{y = \bar{\mu}_k^*(\boldsymbol{a}_k,\boldsymbol{h}_k,\hat{\pi}_{k-1})\big\}\pi_k(\boldsymbol{h}_k).$$

The proposition follows from the fact that the exact belief state π_k evolves to π_{k+1} using only $x_{k-1:k}$ and independent of the optimization variable y_k. Furthermore, since the controlled belief state $\hat{\pi}_{k-1}$ evolves using the linear-fractional transformation in (5) and the objective function in (8) is linear with respect to $\hat{\pi}_{k-1}$, the optimal strategy $\tilde{\mu}_k^*$ can be obtained using the simplex partitioning approach in [22].

3.2. Sub-optimal strategy

In the computation of the optimal strategy $\tilde{\mu}_k^*$ the partitions of simplex $\Delta_{|\boldsymbol{\mathcal{H}}|}$ can grow exponentially with k and quickly becomes intractable even for small state-space $\boldsymbol{\mathcal{H}}$ when the time horizon is large. Hence, we present a sub-optimal control strategy designed considering a sub-optimal detection strategy $\zeta_k^{\#} : \mathcal{Y}^2 \times \boldsymbol{\mathcal{H}} \to \boldsymbol{\mathcal{H}}$ without using the information state $\hat{\pi}_{k-1}$ in (7). Instead, the sub-optimal detection strategy $\zeta_k^{\#}$ uses $(y_{k-1:k}, \hat{\boldsymbol{h}}_{k-1})$ as MDP state, and a hyper-parameter $\theta(\hat{\boldsymbol{h}}_k) := P_{\boldsymbol{H}_k|\hat{\boldsymbol{H}}_k=\hat{\boldsymbol{h}}_k}$ that describes the a priori detection accuracy of $\zeta_k^{\#}$. Similar to (7), $\zeta_k^{\#}$ can by obtained using the Bellman's equation:

$$v_k^{\#}(y_{k-1:k}, \hat{\boldsymbol{h}}_{k-1}) = \max_{\hat{\boldsymbol{h}}_k \in \boldsymbol{\mathcal{H}}} \Big\{ r_k(y_{k-1:k}, \theta(\hat{\boldsymbol{h}}_{k-1}), \hat{\boldsymbol{h}}_k) + \mathbb{E}\big[v_{k+1}^{\#}(X_{k:k+1}, \hat{\boldsymbol{h}}_k) \big| X_{k-1:k} = y_{k-1:k}\big]\Big\}. \quad (10)$$

Further, we approximate the distribution $P_{X_k, X_{k-1}|\boldsymbol{H}_{k-1:k}}$ using additive and difference emissions separately, given by

1. Additive FHMM: $P_{X_k|\boldsymbol{H}_k} = \circledast_{i=1}^{m} P_{W_k^{(i)}|H_k^{(i)}}$,
2. Difference FHMM: $P_{\Delta X_k|\Delta \boldsymbol{H}_k} = \circledast_{i=1}^{m} P_{\Delta W_k^{(i)}|\Delta H_k^{(i)}}$.

Next, we compute exact belief states $\pi_k^{(i)}$ and randomized strategies $\tilde{\mu}_k^{(i)}$ given in Prop. 1 corresponding to both FHMMs, where $i = 1$ denotes additive FHMM and $i = 2$ denotes difference FHMM. Lastly, we combine both FHMMs using the following fusion rule:

$$\eta^{(i)}(x_{k-1:k}, \pi_{k-1}) = \mathbf{1}_{|\mathcal{H}|}^{\mathsf{T}} \cdot \mathbf{M}_{\pi}^{(i)}(x_{k-1:k}, k) \cdot \pi_{k-1}, \quad (11)$$

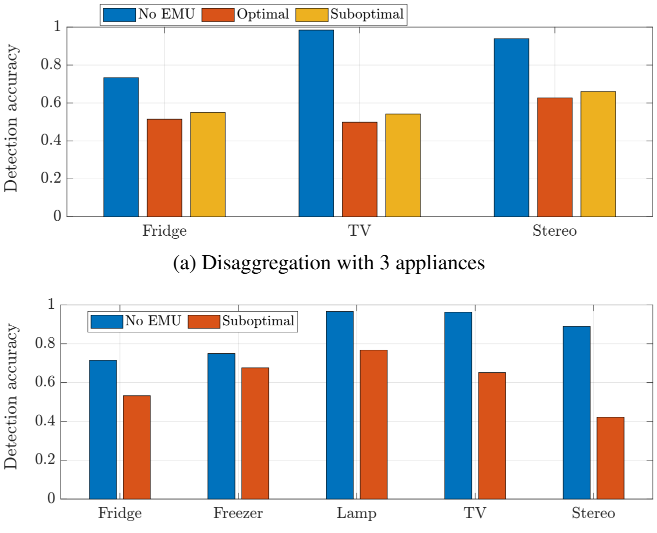
$$\tilde{\mu}_k = \frac{\sum_i \eta^{(i)}(x_{k-1:k}, \pi_{k-1}) \cdot \tilde{\mu}_k^{(i)}}{\sum_i \eta^{(i)}(x_{k-1:k}, \pi_{k-1})}, \quad (12)$$

$$\pi_k = \frac{\sum_i \eta^{(i)}(x_{k-1:k}, \pi_{k-1}) \cdot \pi_k^{(i)}}{\sum_i \eta^{(i)}(x_{k-1:k}, \pi_{k-1})}, \quad (13)$$

where $\eta^{(i)}$ represents the likelihood of the observations x_k and Δx_k corresponding to each of the FHMMs.

4. NUMERICAL STUDY

We evaluate the proposed approaches with a numerical study using energy consumption data from the ECO dataset [23]. We first consider 3 appliances with binary states: fridge, TV, and stereo of house 2 with 10 minute and 75W resolution and use a 48V-30Ah Li-battery to implement the EMU. We model the battery using a three-circuit model [18] with cell internal resistance of 46mΩ. In the controller design, we assume that TV and stereo are privacy sensitive and use the cost function as $\bar{c}(\boldsymbol{h}, \hat{\boldsymbol{h}}) = \sum_{i \in \mathcal{I}} \mathbb{1}\{h^{(i)} = \hat{h}^{(i)}\}$, where $\mathcal{I}$ is the set of privacy-sensitive appliances. For simplicity, we designed an optimal stationary strategy considering infinite horizon with a discount factor of 0.6 and a precision of 0.25 for controlled belief state $\hat{\pi}_k$. Further, we designed sub-optimal strategy using a deterministic hyper-parameter $\theta(\hat{\boldsymbol{h}}_k) = \hat{\boldsymbol{h}}_k$. Fig. 3(a) shows the detection accuracy of the Viterbi algorithm, where we observe 41% and 38% reductions in detection accuracy of TV and stereo, using optimal and sub-optimal strategies. Further, Fig. 3(b) shows the Viterbi performance when considering 5 appliances with binary states: fridge, freezer, lamp, TV, and stereo. In this case, due to high dimensional state space, the optimal strategy is computationally intensive to solve. In this case, we observe a 42% reduction in detection accuracy of TV and stereo using proposed sub-optimal strategy[1].



(a) Disaggregation with 3 appliances

(b) Disaggregation with 5 appliances

Fig. 3. Detection accuracy of Viterbi algorithm with EMU considering TV and Stereo as privacy-sensitive appliances.

5. CONCLUSION

In this paper, we have presented a privacy control strategy that selectively filters appliances' consumption from the smart meter measurements. We have specifically designed a control strategy to counter existing NILM algorithms which use steady-state power and power change measurements for disaggregation. Using the MDP framework, we have presented an exact optimal strategy to minimize the Bayesian risk due to MAP detection, which is computationally intractable even for small state-space problems when the time horizon is large. A sub-optimal strategy with a simplified adversarial model and using a fusion rule based on additive and difference FHMMs is presented. In a numerical study using real household data, the proposed strategy is shown to perform reasonably well compared to the optimal strategy.

[1] The MATLAB code for these simulations can be downloaded from `https://github.com/r2avula/FHMM-Privacy-Controller`.

6. REFERENCES

[1] Patrick McDaniel and Stephen McLaughlin, "Security and privacy challenges in the smart grid," *IEEE Security & Privacy*, vol. 7, no. 3, pp. 75–77, 2009.

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

[3] Alan Marchiori, Douglas Hakkarinen, Qi Han, and Lieko Earle, "Circuit-level load monitoring for household energy management," *IEEE Pervasive Computing*, vol. 10, no. 1, pp. 40–48, 2011.

[4] Leslie K. Norford and Steven B. Leeb, "Non-intrusive electrical load monitoring in commercial buildings based on steady-state and transient load-detection algorithms," *Energy Build.*, vol. 24, no. 1, pp. 51–64, 1996.

[5] Oliver Parson, Siddhartha Ghosh, Mark Weal, and Alex Rogers, "Non-intrusive load monitoring using prior models of general appliance types," *Proc. 26th AAAI Conf. Artif. Intell.*, p. 356–362, 2012.

[6] M. Baranski and J. Voss, "Genetic algorithm for pattern detection in nialm systems," in *IEEE Int. Conf. Syst. Man Cybern.*, 2004, vol. 4, pp. 3462–3468 vol.4.

[7] Markus Weiss, Adrian Helfenstein, Friedemann Mattern, and Thorsten Staake, "Leveraging smart meter data to recognize home appliances," in *IEEE Int. Conf. Pervasive Comput. Commun.*, 2012, pp. 190–197.

[8] J. Zico Kolter and Tommi Jaakkola, "Approximate inference in additive factorial hmms with application to energy disaggregation," in *Proc. 15th Int. Conf. Artif. Intell. Stat.* 2012, vol. 22, pp. 1472–1482, PMLR.

[9] Giulio Giaconi, Deniz Gunduz, and H. Vincent Poor, "Privacy-aware smart metering: Progress and challenges," *IEEE Signal Processing Magazine*, vol. 35, no. 6, pp. 59–78, 2018.

[10] Muhammad Rizwan Asghar, György Dán, Daniele Miorandi, and Imrich Chlamtac, "Smart meter data privacy: A survey," *IEEE Communications Surveys & Tutorials*, vol. 19, no. 4, pp. 2820–2835, 2017.

[11] Georgios Kalogridis, Costas Efthymiou, Stojan Z. Denic, Tim A. Lewis, and Rafael Cepeda, "Privacy for smart meters: Towards undetectable appliance load signatures," in *1st IEEE Int. Conf. Smart Grid Communications*, 2010, pp. 232–237.

[12] David Varodayan and Ashish Khisti, "Smart meter privacy using a rechargeable battery: Minimizing the rate of information leakage," in *IEEE Int. Conf. Acoust., Speech, Signal Process.*, 2011, pp. 1932–1935.

[13] Onur Tan, Deniz Gunduz, and H. Vincent Poor, "Increasing smart meter privacy through energy harvesting and storage devices," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1331–1341, 2013.

[14] Jun-Xing Chin, Tomas Tinoco De Rubira, and Gabriela Hug, "Privacy-protecting energy management unit through model-distribution predictive control," *IEEE Trans. Smart Grid*, vol. 8, no. 6, pp. 3084–3093, 2017.

[15] Lei Yang, Xu Chen, Junshan Zhang, and H. Vincent Poor, "Optimal privacy-preserving energy management for smart meters," in *IEEE Conf. Computer Communications*, 2014, pp. 513–521.

[16] Michael Backes and Sebastian Meiser, "Differentially private smart metering with battery recharging," in *Proc. 8th Int. Workshop Data Privacy Management*. 2013, pp. 194–212, Springer.

[17] Zuxing Li, Tobias J. Oechtering, and Mikael Skoglund, "Privacy-preserving energy flow control in smart grids," in *IEEE Int. Conf. Acoust., Speech, Signal Process.*, 2016, pp. 2194–2198.

[18] Ramana R. Avula, Tobias J. Oechtering, and Daniel Månsson, "Privacy-preserving smart meter control strategy including energy storage losses," in *IEEE PES Innov. Smart Grid Technol. Conf. Eur.*, 2018, pp. 1–6.

[19] Ahmed Zoha, Alexander Gluhak, Muhammad Ali Imran, and Sutharshan Rajasegarar, "Non-intrusive load monitoring approaches for disaggregated energy sensing: A survey," *Sensors*, vol. 12, no. 12, pp. 16838–16866, 2012.

[20] Ramana R. Avula and Tobias J. Oechtering, "On design of optimal smart meter privacy control strategy against adversarial map detection," in *IEEE Int. Conf. Acoust., Speech, Signal Process.*, 2020, pp. 5845–5849.

[21] Vikram Krishnamurthy, *Partially Observed Markov Decision Processes: From Filtering to Controlled Sensing*, Cambridge University Press, 2016.

[22] Ramana R. Avula, Jun-Xing Chin, Tobias J. Oechtering, Gabriela Hug, and Daniel Månsson, "Design framework for privacy-aware demand-side management with realistic energy storage model," *IEEE Trans. Smart Grid*, vol. 12, no. 4, pp. 3503–3513, 2021.

[23] Christian Beckel, Wilhelm Kleiminger, Romano Cicchetti, Thorsten Staake, and Silvia Santini, "The eco data set and the performance of non-intrusive load monitoring algorithms," in *Proc. 1st ACM Conf. Embed. Syst. Energy-Efficient Build.*, 2014, p. 80–89.