Structure of Optimal Privacy-Preserving Policies in Smart-Metered Systems with a Rechargeable Battery

(Invited Paper)

Simon Li
Department of Electrical and
Computer Engineering
University of Toronto
Email: simonli@ece.utoronto.ca

Ashish Khisti
Department of Electrical and
Computer Engineering
University of Toronto
Email: akhisti@ece.utoronto.ca

Aditya Mahajan
Department of Electrical and
Computer Engineering
McGill University
Email: aditya.mahajan@mcgill.ca

***Abstract*—In smart-metered systems, fine-grained time-series power usage data (load profile) is communicated from a user to the utility provider. The correlation of the load profile with a user's private activities leaves open the possibility of inference attacks. Using a rechargeable battery, the user can partially obscure its load profile and provide some protection to the private information using various strategies for charging and discharging the battery (battery management policies). Using mutual information as the privacy metric, we study optimal battery management policies for discrete alphabets. We show that the problem can be formulated as a Markov Decision Process, identify the associated state and action space, and using this framework characterize the optimal policy for the binary alphabet case.**

I. Introduction

Smart electricity meters are becoming a critical part of modern electrical grids. They deliver find-grained household power usage measurements to utility providers. This information allows them to implement reforms to the efficiency of the electrical grid. For instance, the utility provider can use dynamic pricing and planned service delivery to shift power demand off of peak times [1]. However, despite the promise of savings in energy and money, there is potentially a loss of privacy. A utility provider may employ data mining algorithms to infer trends in the usage patterns [2]. Information about a user's private activities is invaluable to advertising agencies for designing targeted advertisements, insurance companies to determine health premiums, or even criminals looking for the best times to commit robbery etc.

One possible solution is to use escrow-based data anonymization [3]; however then the privacy boundary is simply shifted to the escrow service. A complementary solution is to partially obscure the load profile using a rechargeable battery [4]. As rechargeable batteries become more commonplace (for example due to the proliferation of electric vehicles and renewable energy harvester), this approach becomes more practical and economically viable (as it can also be used to take advantage of dynamic pricing [5]). This approach to privacy provides absolute guarantees to how much private information is leaked.

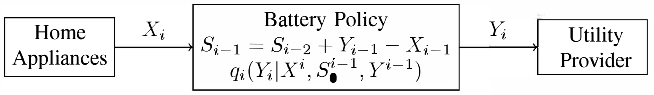
Home Appliances
X_i
Battery Policy
$S_{i-1} = S_{i-2} + Y_{i-1} - X_{i-1}$
$q_i(Y_i|X^i, S_\bullet^{i-1}, Y^{i-1})$
Y_i
Utility Provider

Fig. 1. System Diagram. At each time $i \in \{1, 2, \dots, n\}$, the battery policy defines a with channel with memory from X_i to Y_i.

In this paper, we explore the structure of optimal privacy-preserving battery policies. Through a series of observations, we identify special structure in optimal policies that greatly simplifies the optimization. Then we give an equivalent formulation of the problem as a finite-horizon Markov Decision Problem, and identify the associated state and action space. Finally, we study the binary smart meters model for the case of an i.i.d. load sequence, previously considered in [4], and characterize the optimal policy in this special case.

II. Problem Statement

Consider an electricity consumer with an installed rechargeable battery. At each time $i \in \{1, 2, \dots, n\}$, let $S_{i-1} \in \mathcal{S}$, $X_i \in \mathcal{X}$, and $Y_i \in \mathcal{Y}$ denote the battery state, the power demand, and the energy drawn from the grid respectively. We consider finite alphabets and that $(X_i)_{i=1}^n$ is a first-order Markov process. The battery may be charged and discharged without conversion losses according to

$$S_i = S_{i-1} + Y_i - X_i. \tag{1}$$

Let $W(x, s) = \{y \in \mathcal{Y} : s + y - x \in \mathcal{S}\}$. A battery policy $q(Y^n|X^n, S_0)$ is admissible if and only if it is causal

$$q(Y^n|X^n, S_0) = \bigotimes_{i=1}^{n} q_i(Y_i|X^i, S_0^{i-1}, Y^{i-1}) \tag{2}$$

and consistent with (1) i.e.

$$q_i(W(X_i, S_{i-1})|X^i, S_0^{i-1}, Y^{i-1}) = 1, \text{ for } i \in \{1, 2, \dots, n\}. \tag{3}$$

We denote the set of all admissible battery management policies by $\mathcal{Q}_A$. A policy $q \in \mathcal{Q}_A$ induces a joint distribution

$$P^q(Y^n, X^n, S_0) = q(Y^n|X^n, S_0)P(X^n)P(S_0).$$

978-1-4799-1931-4/15/$31.00 ©2015 IEEE

We define the leakage rate as

$$L(q) := \frac{1}{n} I^q(S_0, X^n; Y^n) \text{ for } q \in \mathcal{Q}_A \tag{4}$$

where the mutual information is evaluated according to the induced joint distribution. We are interested in the following optimization problem:

Problem A In the model described above, find an optimal battery policy q^* that minimizes the leakage rate

$$L(q^*) = \min_{q \in \mathcal{Q}_A} L(q).$$

III. The MDP Formulation

We identify simplifications to Problem A by observing that the optimal policies have certain special structure. These simplifications reduce the size of the optimization and ultimately lead to the MDP formulation. (The proof for some results are in the appendix.)

A. Optimal Structure and Simplifications

Using the properties of mutual information we can state the following lemmas. Define $Z_i := (X_i, S_{i-1})$.

Lemma 1. *Problem A is a convex optimization problem: Let $\lambda \in [0,1]$, $\{q_1, q_2\} \subset \mathcal{Q}_A$, and $q_\lambda = \lambda q_1 + (1-\lambda) q_2$, then $q_\lambda \in \mathcal{Q}_A$ and*

$$L(q_\lambda) \leq \lambda L(q_1) + (1-\lambda) L(q_2).$$

We now identify a subset of $\mathcal{Q}_A$ that is optimal, let

$$\mathcal{Q}_B := \left\{ q \in \mathcal{Q}_A : q_i(Y_i | Z^i, Y^{i-1}) = q_i(Y_i | Z_i, Y^{i-1}), \forall i \right\}.$$

Now we define a new cost

$$L_B(q) := \sum_{i=1}^{n} I^q(Z_i; Y_i | Y^{i-1}), \; q \in \mathcal{Q}_B. \tag{5}$$

Lemma 2. *In Problem A, the optimization over $\mathcal{Q}_A$ can be replaced by $\mathcal{Q}_B$ without loss of optimality such that*

$$\min_{q \in \mathcal{Q}_A} L(q) = \min_{q \in \mathcal{Q}_B} L(q).$$

Furthermore,

$$L(q) = L_B(q), \; q \in \mathcal{Q}_B.$$

Lemma 1 implies that Problem A can have a simpler objective function and domain.

Problem B Find a battery policy $q^* \in \mathcal{Q}_B$ such that

$$L_B(q^*) = \min_{q \in \mathcal{Q}_B} L_B(q).$$

In the next section, using the simplified Problem B, we will introduce an equivalent formulation using MDP. To do so, we identify suitable state and action spaces, policies, and cost function. We follow the convention in [6].

B. Sufficient Statistics

Let $\mathcal{P}_{Y|Z}$ be the set of all stochastic kernels $\mathcal{Z}$ to $\mathcal{Y}$. Let the action space be $\mathcal{P}_W = \{u \in \mathcal{P}_{Y|Z} : u(W(Z)|Z) = 1\}$. Let the state space be $\mathcal{H}^{i-1} = \mathcal{Y}^{i-1} \times \mathcal{U}^{i-1}$. A policy is a sequence $f = (f_i)_{i=1}^n$ such that $f_i : \mathcal{H}^{i-1} \to \mathcal{P}_W$. The cost at each stage is $I^f(Z_i; Y_i | h^{i-1})$.

The MDP proceeds as follows at stage i, f_i observes state h^{i-1} and selects u_i, a cost $I^f(Z_i; Y_i | h^{i-1})$ is incurred, a y_i is produced, then the transition $h^i = (h^{i-1}) \cup (y_i, u_i)$ occurs.

A policy f induces a joint distribution on the variables as follows. Let $P^f(y_i | z^i, y^{i-1}, u^i) := u_i(y_i | z_i)$ and $P^f(u_i | z^{i-1}, y^{i-1}, u^{i-1}) := \delta_{\{f_i(h^{i-1})\}}(u_i)$, then

$$\begin{aligned} P^f(y^n, z^n, u^n) &= \bigotimes_{i=1}^{n} P^f(y_i, z_i, u_i | y^{i-1}, z^{i-1}, u^{i-1}) \\ &= \bigotimes_{i=1}^{n} u_i(y_i | z_i) P(z_i | z_{i-1}, y_{i-1}) \delta_{\{f_i(h^{i-1})\}}(u_i) \end{aligned} \tag{6}$$

where $P(z_i | y_{i-1}, z_{i-1}) = \mathbb{1}(s_{i-1} = s_{i-2} + y_{i-1} - x_{i-1}) P(x_i | x_{i-1})$ is given in the system definition.

Consequently, the objective function for the n-stage problem is defined as

$$L_C(f) := \sum_{i=1}^{n} I^f(Z_i; Y_i | H^{i-1}) \tag{7}$$

and is evaluated according to the induced joint distribution.

Problem C Find a policy f^* that minimizes (7)

$$L_C(f^*) = \min_f L_C(f).$$

Lemma 3. *Problems B and C are equivalent.*

Proof. Since the policies f in Problem C are deterministic, $I^f(Z_i; Y_i | Y^{i-1}) = I^f(Z_i; Y_i | H^{i-1})$, and it is clear that for every f there exists a $q \in \mathcal{Q}_B$ such that $L_B(q) = L_C(f)$, and vice-versa. □

Note the resemblance of the problem to a POMDP with hidden state Z_i, observation Y_i and action U_i. The discrepancy is that the objective cannot be expressed as a function $c : \mathcal{Z} \times \mathcal{P}_W \to \mathbb{R}$ but rather, it is a function $c : \mathcal{P}_Z \times \mathcal{P}_W \to \mathbb{R}$. However, we can show that we can formulate the problem directly as an MDP instead.

Let us define a statistic π_i, the receiver's estimate of the state and power demand Z_i given all past observations and actions h^i. We define $\pi_1[\emptyset](z_i) := P(z_1)$ and for each i,

$$\begin{aligned} &\pi_i[h^{i-1}](z_i) := \phi(\pi_{i-1}[h^{i-2}], u_{i-1}, y_{i-1}) \\ &= \frac{\sum_{z_{i-1}} P(z_i | y_{i-1}, z_{i-1}) u_{i-1}(y_{i-1} | z_{i-1}) \pi_{i-1}[h^{i-2}](z_{i-1})}{\sum_{z_{i-1}} u_{i-1}(y_{i-1} | z_{i-1}) \pi_{i-1}[h^{i-2}](z_{i-1})}. \end{aligned} \tag{8}$$

Lemma 4. *Given a policy f and π_i as defined in (8)*

$$\pi_i[h^{i-1}](Z_i) = P^f(Z_i | h^{i-1})$$

holds true for almost all (h^{i-1}) for each i. Note that given h^{i-1}, the posterior is independent of the policy f.

Lemma 5. *$(\pi_i)_{i=1}^n$ is a u-controlled Markov process*

$$\begin{aligned} P^f(\pi_{i+1}|u^i,\pi^i) &= P(\pi_{i+1}|u_i,\pi_i) \\ &= \sum_{y_i} \mathbb{1}\left(\pi_{i+1} = \phi(\pi_i,u_i,y_i)\right) \sum_{z_i} u_i(y_i|z_i)\pi_i(z_i) \end{aligned} \tag{9}$$

Note that the transitions are independent of the policy f.

Now we define a new cost function $c : \mathcal{P}_Z \times \mathcal{P}_W \to \mathbb{R}$ as

$$c(\pi_i,u_i) := \sum_{y_i,z_i} u_i(y_i|z_i)\pi_i(z_i) \log \frac{u_i(y_i|z_i)}{\sum_{z_i'} u_i(y_i|z_i')\pi_i(z_i')}. \tag{10}$$

Lemma 6. *$(\pi_i)_{i=1}^n$ is a sufficient statistic for $(h^{i-1})_{i=1}^n$. In particular, the per-stage cost can be expressed as*

$$I^f(Z_i;Y_i|h^{i-1}) = c(\pi_i[h^{i-1}],u_i)$$

and is independent of the policy f given the action.

The Markovian nature $(\pi_i)_{i=1}^n$ and the fact that it is a sufficient statistic implies Problem C can be recast as an MDP. We present this formulation in the next section.

Remark: The sufficient statistic in problems with IID sources can be simplified to be the posterior of the battery state only. We show an example of that in Section IV.

C. The MDP Formulation and Algorithms

Problem D

State space:	$\pi_i \in \mathcal{P}_Z$
Action space:	$u_i \in \mathcal{P}_W$
Policy:	$f_i : \mathcal{P}_Z \to \mathcal{P}_W$
Transition law:	$P(\pi_i|\pi_{i-1},u_{i-1})$
Per-stage cost:	$c(\pi_i,u_i)$

The transition and cost functions are defined in (9) and (10).

Theorem 7. *Problem A can be reformulated as a Markov Decision Process defined in Problem D.*

1) Define the cost-to-go functions $J_{n+1}(\pi_{n+1}) = 0$ and

$$J_i(\pi_{i-1}) = \min_{u_i \in \mathcal{P}_W} \left\{ c(\pi_i,u_i) + \sum_{z_i,y_i} u_i(y_i|z_i)\pi_i(z_i)J_{i+1}(\phi(\pi_i,u_i,y_i)) \right\} \tag{11}$$

for $i \in \{1,2,\dots,n\}$, where ϕ is defined in (8).

2) The minimum leakage rate is obtained from J_1.

$$L(q^*) = \frac{1}{n} J_1(\pi_1) \text{ for } \pi_1 = P(X_1)P(S_0)$$

Proof. The proof for 1) is the dynamic programming recursion (see [8]) and 2) follows from Lemmas 4-6. □

The main difficulty with evaluating the cost-to-go functions in Theorem 7 is due to the uncountability of the state and action spaces. To evaluate the dynamic program recursion numerically, it is necessary to employ some discretization procedure. For instance, by discretizing the action space, Sondik's α-vector algorithm for POMDPs can be used [9]. Otherwise, by discretizing both the state and action spaces, the classical value iteration algorithm can be used.

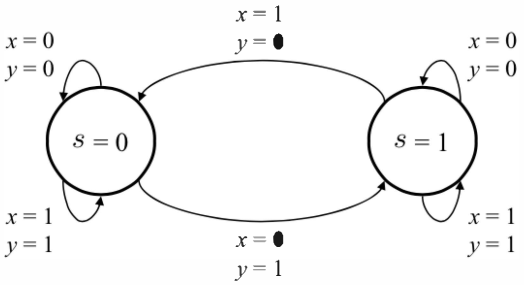

Fig. 2. Finite-state-machine representation for binary smart meters model.

IV. The Binary Smart Meters Model

We define the binary smart meters model as follows. Let $\mathcal{X} \in \{0,1\}$, $\mathcal{Y} \in \{0,1\}$, $\mathcal{S} \in \{0,1\}$ and $(X_i)_{i=1}^n$ be an IID equiprobable Bernoulli process and $P(S_0) = 1/2$.

Theorem 8. *For the binary model, the minimum leakage rate is $1/2$ the optimal action at each stage is*

$$u_i^*(Y_i|Z_i) = 1/2, \text{ if } X_i = S_{i-1}.$$

The convexity of Problem A will reveal some structure in the set of optimal policies for Problem D. Given an admissible policy q, we define the "flipped" policy

$$\begin{aligned} \bar{q}(Y^n = y^n|X^n = x^n, S_0 = s_0) \\ := q(Y^n = \overline{y^n}|X^n = \overline{x^n}, S_0 = \overline{s_0}) \end{aligned} \tag{12}$$

where $\overline{y^n}$ denotes the element-wise NOT operation. The following results pertain only to the binary model.

Lemma 9. *The "flipped" policy $\bar{q}$ is admissible.*

Proof. It is clear that causality (2) is satisfied, then for (3) it is sufficient to show that $\bar{q} = 0$ for any sequence (y^n, x^n, s_0) inconsistent with the FSM in Figure 2. Observe that if (y^i, x^i, s_0) is inconsistent, then by inspection, $(\overline{y^i}, \overline{x^i}, \overline{s_0})$ is inconsistent, so $\bar{q}(y^i, x^i, s_0) = q(\overline{y^i}, \overline{x^i}, \overline{s_0}) = 0$. □

Lemma 10. *1) A policy q yields the same leakage as $\bar{q}$*

$$L(q) = L(\bar{q}), \text{ for } q \in \mathcal{Q}_A$$

2) Without loss of optimality, we may optimize over symmetric policies

$$\mathcal{Q}_{A,sym} = \{q \in \mathcal{Q}_A : q = \bar{q}\}.$$

Now consider J_1 in the DP (11). Lemma 10 implies that we may optimize over $\mathcal{P}_{W,sym} = \{u \in \mathcal{P}_W : u = \bar{u}\}$ without loss of optimality.

Lemma 11. *For $u_1 \in \mathcal{P}_{W,sym}$, the following are true*
1) $\pi_1 = \phi(\pi_1,u_1,y_1)$, $\forall y_1$
2) $\min_{u_1 \in \mathcal{P}_{W,sym}} c(\pi_1,u_1) = 1/2$
3) $u_1^*(y_1|z_1) = 1/2$, if $x_1 = s_0$

Using Lemma 11, consider the following equalities:

$$\begin{aligned} J_1(\pi_1) &= \min_{u_1 \in \mathcal{P}_W} \left\{ c(\pi_1, u_1) + \sum_{\pi_2} P(\pi_2|\pi_1, u_1) J_2(\pi_2) \right\} \\ &= \min_{u_1 \in \mathcal{P}_{W,sym}} c(\pi_1, u_1) + J_2(\pi_1) \\ &= \frac{n}{2}. \end{aligned}$$

Using forward induction, we apply this argument to $J_2, J_3, \ldots$ Then by Theorem 6, we have $L(q^*) = \frac{1}{n} J_1(\pi_1) = 1/2$ where $q^*(Y^n|X^n, S_0) = \bigotimes_{i=1}^n u_1^*(Y_i|Z_i)$.

V. Conclusion

In this paper, we consider the method of using a rechargeable battery to enhance privacy in smart metered systems. We cast the problem into an information theoretic framework and used it to find optimal battery management policies for minimizing information leakage. We simplify the optimization by finding the associated sufficient statistics for the policies and then reformulated the problem as a Markov decision process. We then studied the binary smart meters model and characterized the optimal policy that minimizes information leakage. For more complex versions of the problem (i.e. for sources with memory), the MDP formulation provided here allows one to use dynamic programming techniques such as value-iteration to solve for optimal policies and leakage rates.

In future work, we will extend the analysis to the infinite horizon case and consider complex models with more general alphabets and sources and characterize the effect of increasing battery size where we expect to see a connection with [10].

VI. Appendix

Proof of Lemma 1. If q_λ satisfies (2) and (3), then $q_\lambda \in \mathcal{Q}_A$. We first show causality (2). For each i,

$$\begin{aligned} q_{\lambda,i}(y_i|x^n, y^{i-1}, s_0) &= \frac{\sum_{y_{i+1}^n} q_\lambda(y_1^n|x_1^n, s_0)}{\sum_{y_i^n} q_\lambda(y_1^n|x_1^n, s_0)} \\ &= \frac{\sum_{y_{i+1}^n} \lambda q_1(y_1^n|x_1^n, s_0) + (1-\lambda) q_2(y_1^n|x_1^n, s_0)}{\sum_{y_i^n} \lambda q_1(y_1^n|x_1^n, s_0) + (1-\lambda) q_2(y_1^n|x_1^n, s_0)} \\ &\overset{(a)}{=} \frac{\lambda q_1(y_1^i|x_1^i, s_0) + (1-\lambda) q_2(y_1^i|x_1^i, s_0)}{\lambda q_1(y_1^{i-1}|x_1^{i-1}, s_0) + (1-\lambda) q_2(y_1^{i-1}|x_1^{i-1}, s_0)}. \end{aligned}$$

We have causality since (a) is independent of the future x_{i+1}^n. Now we show (3) is satisfied. For each i,

$$\begin{aligned} & q_{\lambda,i}(W(z_i)|z^i, y^{i-1}) q_\lambda(y^{i-1}|x^{i-1}, s_0) \\ &= q_\lambda(Y_i \in W(z_i), y^{i-1}|x^i, s_0) \\ &= \lambda q_{2,i}(W(z_i)|z^i, y^{i-1}) q_1(y^{i-1}|x^{i-1}, s_0) \\ &\qquad + (1-\lambda) q_{2,i}(W(z_i)|z^i, y^{i-1}) q_2(y^{i-1}|x^{i-1}, s_0) \\ &= \lambda q_1(y^{i-1}|x^{i-1}, s_0) + (1-\lambda) q_2(y^{i-1}|x^{i-1}, s_0) \\ &= q_\lambda(y^{i-1}|x^{i-1}, s_0) \implies q_{\lambda,i}(W(z_i)|z^i, y^{i-1}) = 1. \end{aligned}$$

For the convexity of mutual information, see [11]. □

Proof of Lemma 2. Consider this chain of inequalities:

$$\begin{aligned} I(S_0, X^n; Y^n) &\overset{(a)}{=} \sum_{i=1}^n I(S_0, X^i; Y_i|Y^{i-1}) \\ &\overset{(b)}{=} \sum_{i=1}^n I(Z^i; Y_i|Y^{i-1}) \\ &\overset{(c)}{\geq} \sum_{i=1}^n I(Z_i; Y_i|Y^{i-1}). \end{aligned}$$

For (a), use the chain rule of mutual information and the fact that $(Z^{i-2}, Y^{i-1}) \rightarrow X_{i-1} \rightarrow X_i$. For (b), note that the battery process is a deterministic function of the past variables (see (1)). For (c), q achieves the lower bound iff $q \in \mathcal{Q}_B$.

We will show that given any $q_A \in \mathcal{Q}_A$, $\exists q_B \in \mathcal{Q}_B$ such that $\sum_{i=1}^n I^{q_B}(Z_i; Y_i|Y^{i-1}) = \sum_{i=1}^n I^{q_A}(Z_i; Y_i|Y^{i-1})$. A sufficient condition is if $P^{q_A}(Y^n) = P^{q_B}(Y^n)$ and $P^{q_A}(Z_i|Y^{i-1}) = P^{q_B}(Z_i|Y^{i-1})$ for each i. We can obtain this q_B by marginalizing

$$\begin{aligned} & q_{B,i}(y_i|z_i, y^{i-1}) = q_{A,i}(y_i|z_i, y^{i-1}) \\ &= \frac{\sum\limits_{z^{i-1}} \bigotimes\limits_{j=1}^{i} q_{A,i}(y_j|z^j, y^{j-1}) P(z_j|y_{j-1}, z_{i-1})}{\sum\limits_{y_i, z^{i-1}} \bigotimes\limits_{j=1}^{i} q_{A,i}(y_j|z^j, y^{j-1}) P(z_j|y_{j-1}, z_{j-1})}. \end{aligned}$$

Using induction, let $i = 1$, then $P^{q_A}(z_1) = P^{q_B}(z_1)$, then

$$\begin{aligned} & P^{q_A}(z_i|y^{i-1}) = \frac{\sum_{z_{i-1}} P(z_i, z_{i-1}, y^{i-1})}{P(y^{i-1})} \\ &= \frac{\sum\limits_{z_{i-1}} P(z_i|y_{i-1}, z_{i-1}) q_{A,i}(y_{i-1}|z_{i-1}, y^{i-2}) P^{q_A}(z_{i-1}|y^{i-2})}{\sum\limits_{z_{i-1}} q_{A,i}(y_{i-1}|z_{i-1}, y^{i-2}) P^{q_A}(z_{i-1}|y^{i-2})} \\ &= \frac{\sum\limits_{z_{i-1}} P(z_i|y_{i-1}, z_{i-1}) q_{B,i}(y_{i-1}|z_{i-1}, y^{i-2}) P^{q_B}(z_{i-1}|y^{i-2})}{\sum\limits_{z_{i-1}} q_{B,i}(y_{i-1}|z_{i-1}, y^{i-2}) P^{q_B}(z_{i-1}|y^{i-2})} \\ &= P^{q_B}(z_i|y^{i-1}), \text{ for } i \in \{2, \ldots, n\}. \end{aligned}$$

Again using induction, let $i = 1$, then $P^{q_A}(y_1) = \sum_{z_1} P^{q_A}(y_1|z_1) P^{q_A}(z_1) = \sum_{z_1} P^{q_B}(y_1|z_1) P^{q_B}(z_1) = P^{q_B}(y_1)$, then

$$\begin{aligned} P^{q_A}(y^i) &= \sum_{z_i} q_{A,i}(y_i|z_i, y^{i-1}) P^{q_A}(z_i|y^{i-1}) P_1(y^{i-1}) \\ &= \sum_{z_i} q_{B,i}(y_i|z_i, y^{i-1}) P^{q_B}(z_i|y^{i-1}) P^{q_B}(y^{i-1}) \\ &= P^{q_B}(y^i). \end{aligned}$$

Thus we have $P^{q_A}(y^n) = P^{q_B}(y^n)$. □

Proof of Lemma 4. By induction, $P^f(z_1) = \pi_1[\emptyset](z_i)$ for

$i = 1$, and then

$$\begin{aligned}
&P^f(h^i)\pi_{i+1}[h^i](z_{i+1})\\
&\overset{\text{(a)}}{=} \left(\sum_{z_i} u_i(y_i|z_i)\pi_i[h^{i-1}](z_i)\delta_{\{f(h^{i-1})\}}(u_i)P^f(h^{i-1})\right)\\
&\qquad\times\left(\frac{\sum_{z_i} P(z_{i+1}|y_i,z_i)u_i(y_i|z_i)\pi_i[h^{i-1}](z_i)}{\sum_{z_i} u_i(y_i|z_i)\pi_i[h^{i-1}](z_i)}\right)\\
&= \sum_{z_i} P(z_{i+1}|y_i,z_i)u_i(y_i|z_i)\pi_i[h^{i-1}](z_i)\\
&\qquad\times \delta_{\{f(h^{i-1})\}}(u_i)P^f(h^{i-1})\\
&\overset{\text{(b)}}{=} \sum_{z_i} P(z_{i+1}|y_i,z_i)P^f(z_i,h^i)\\
&= P^f(z_{i+1},h^i), \text{for } i \in \{1,2,\dots,n\}
\end{aligned}$$

where (a) is due to (6) and (8), while (b) is due to (6). □

Proof of Lemma 5. Consider this chain of equalities:

$$\begin{aligned}
&P^f(\pi_{i+1}|u^i,\pi^i) = \sum_{y_i} P^f(\pi_{i+1}|y_i,u^i,\pi^i)P^f(y_i|u^i,\pi^i)\\
&= \sum_{y_i} \mathbb{1}\left(\pi_{i+1} = \phi(\pi_i,u_i,y_i)\right)\sum_{z_i} u_i(y_i|z_i)\pi_i(z_i)\\
&= P(\pi_{i+1}|u_i,\pi_i)
\end{aligned}$$

where ϕ is defined in (8). □

Proof of Lemma 6. Consider the per stage cost:

$$\begin{aligned}
&I^f(Z_i;Y_i|h^{i-1})\\
&= \mathbb{E}^f\left[\log\frac{P^f(Y_i|Z_i,h^{i-1})}{\sum_{z_i} P^f(Y_i|z_i,h^{i-1})P^f(z_i|h^{i-1})}\middle| h^{i-1}\right]\\
&= \mathbb{E}^f\left[\log\frac{u_i(Y_i|Z_i)}{\sum_{z_i} u_i(Y_i|z_i)\pi_i[h^{i-1}](z_i)}\middle| h^{i-1}\right]\\
&= c(\pi_i[h^{i-1}],u_i)
\end{aligned}$$

where c is defined in (10). □

Proof of Lemma 10. For Part 1), let $q_\lambda = \lambda q + (1-\lambda)\bar{q}$ for $\lambda \in [0,1]$. Given $P(X^n,S_0) = P(X^n)P(S_0) = 2^{-(n+1)}$,

$$\begin{aligned}
&2^{n+1}L(q) = 2^{n+1}I^q(S_0,X^n;Y^n)\\
&= 2^{n+1}\sum_{y^n,x^n,s_0}\log\left(\frac{q(y^n|x^n,s_0)}{\sum_{x'^n,s'_0} q(y^n|x'^n,s'_0)P(x'^n,s'_0)}\right)\\
&\qquad\qquad\times q(y^n|x^n,s_0)P(x^n,s_0)\\
&= \sum_{y^n,x^n,s_0}\log\left(\frac{q(y^n|x^n,s_0)2^{n+1}}{\sum_{x'^n,s'_0} q(y^n|x'^n,s'_0)}\right)q(y^n|x^n,s_0)\\
&\overset{\text{(a)}}{=} \sum_{y^n,x^n,s_0}\log\left(\frac{q(\bar{y}^n|\bar{x}^n,\bar{s}_0)2^{n+1}}{\sum_{x'^n,s'_0} q(\bar{y}^n|\bar{x}'^n,\bar{s}'_0)}\right)q(\bar{y}^n|\bar{x}^n,\bar{s}_0)\\
&\overset{\text{(b)}}{=} \sum_{y^n,x^n,s_0}\log\left(\frac{\bar{q}(y^n|x^n,s_0)2^{n+1}}{\sum_{x'^n,s'_0} \bar{q}(y^n|x'^n,s'_0)}\right)\bar{q}(y^n|x^n,s_0)\\
&= 2^{n+1}I^{\bar{q}}(S_0,X^n;Y^n) = 2^{n+1}L(\bar{q})
\end{aligned}$$

where (a) is because we are summing over (y^n,x^n,s_0) and (b) is by (12). For Part 2), by Lemma 1, q_λ may improve the leakage unless q was already symmetric (i.e. $q = \bar{q}$). □

Proof of Lemma 11. Note that for $u \in \mathcal{P}_{W,sym}$, u is completely characterized by a number $a \in [0,1]$ since by (3) $u_1(y=1|z=(1,0)) = u_1(y=0|z=(0,1)) = 1$ and let $u_1(y=1|z=(0,0)) = u_1(y=0|z=(1,1)) = a$ and then $u_1(y=0|z=(0,0)) = u_1(y=1|z=(1,1)) = 1-a$.

Part 1): By Lemma 5, $\pi_2(s_1) = P^u(s_1|y_1)$, so it is sufficient to show $S_1 \perp Y_1$. Note that (1) and the definition of the joint distribution

$$P(s_1,y_1) = \frac{1}{4}\sum_{z_1}\mathbb{1}\{s_1 = s_0 - x_1 + y_1\}u_1(y_1|z_1)$$

Let's consider each case. For $s_1 = y_1$,

$$P(s_1,y_1) = \frac{1}{4}(u_1(y_1|z_1=(0,0)) + u_1(y_1|z_1=(1,1)) = 1/4$$

And for $s_1 \neq y_1$,

$$P(s_1,y_1) = \frac{1}{4}u_1(y_1|z_1=(y_1,s_1)) = 1/4.$$

Parts 2) and 3): Note that $\sum_z u(y|z) = 2$. Then

$$\begin{aligned}
c(\pi_i,u_i) &= \frac{1}{4}\sum_{y_i,z_i} u_i(y_i|z_i)\log\frac{4u_i(y_i|z_i)}{\sum_{z'_i} u_i(y_i|z'_i)}\\
&= 1 + \frac{1}{4}\sum_{y_i,z_i} u_i(y_i|z_i)\log u_i(y_i|z_i)\\
&= 1 - 0.5H_b(a)
\end{aligned}$$

where H_b is the binary entropy function. Let $a = 0.5$ to achieve the minimum. □

References

[1] A. Ipakchi and F. Albuyeh, "Grid of the future", in *IEEE Power Energy Mag., vol. 7, no. 2, pp. 52-62*, Mar.-Apr. 2009.

[2] A. Predunzi, "A neuron nets based procedure for identifying domestic appliances pattern-of-use from energy recordings at meter panel", in *Proc. IEEE Power Eng. Society Winter Meeting, New York*, Jan. 2002.

[3] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data", in *Proc. IEEE Smart Grid Commun. Conf., Gaithersburg*, Oct. 2010.

[4] D. Varodayan and A. Khisti, "Smart meter privacy using a rechargeable battery: Minimizing the rate of information leakage", in *Proc. IEEE Int. Conf. Acoust. Speech Sig. Proc. Prague, Czech Republic*, May 2011.

[5] P. Harsha, and M. Dahleh, "Optimal Management and Sizing of Energy Storage Under Dynamic Pricing for the Efficient Integration of Renewable Energy", in *IEEE Transactions on Power Systems, vol.PP, no.99, pp.1,18.*

[6] S. Tatikonda and S. Mitter, "The capacity of channels with feedback", *IEEE Trans. on Inform. Theory, vol. 55, no. 1, pp. 323-349*, January 2009.

[7] O. Tan, D. Gunduz and H. V. Poor, "Smart meter privacy in the presence of energy harvesting and storage devices", in *Proc. IEEE Int'l Conf. Smart Grid Comm., Tainan City, Taiwan*, Nov 2012.

[8] D. Bertsekas, "Dynamic Programming and Optimal Control" *Athena Scientific, Belmont, Massachusetts.* Volumes 1 and 2.

[9] R. D. Smallwood and E. J. Sondik, "The Optimal Control of Partially Observable Markov Processes over a Finite Horizon", in *Operations Research, Vol. 21, pp. 1071- 1088. doi:10.1287/opre.21.5.1071*, 1973.

[10] D. Gunduz and J.Gomez-Vilardebo, "Smart meter privacy in the presence of an alternative energy source", in *2013 IEEE International Conference on Communications (ICC)*, June 2013.

[11] T . M. Cover and J. A. Thomas, "Elements of Information Theory", New York, Wiley, 1991.