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

Simon Li, Ashish Khisti, Aditya Mahajan

University of Toronto, McGill University

Introduction

- Smart electricity meters deliver household power usage data to utility providers. However, despite the benefits these systems offer, there is potentially a loss of privacy.
- Time horizon: $i \in \{1, 2, \ldots, n\}$
  Battery state: $S_i \in \mathcal{S}$
  Aggregate load: $X_i \in \mathcal{X}$
  Power drawn from the grid: $Y_i \in \mathcal{Y}$
  (Y_i is reported to the utility provider)

Binary Smart Meters Model

Let $\mathcal{X} = \mathcal{Y} = \mathcal{S} = \{0, 1\}$, $(X_i)_{i=1}^n$ IID Bern(1/2) and $P(S_0) = 1/2$. We consider energy-efficient policies that satisfying $S_{i-1} + Y_i - X_i \in \mathcal{S}$.

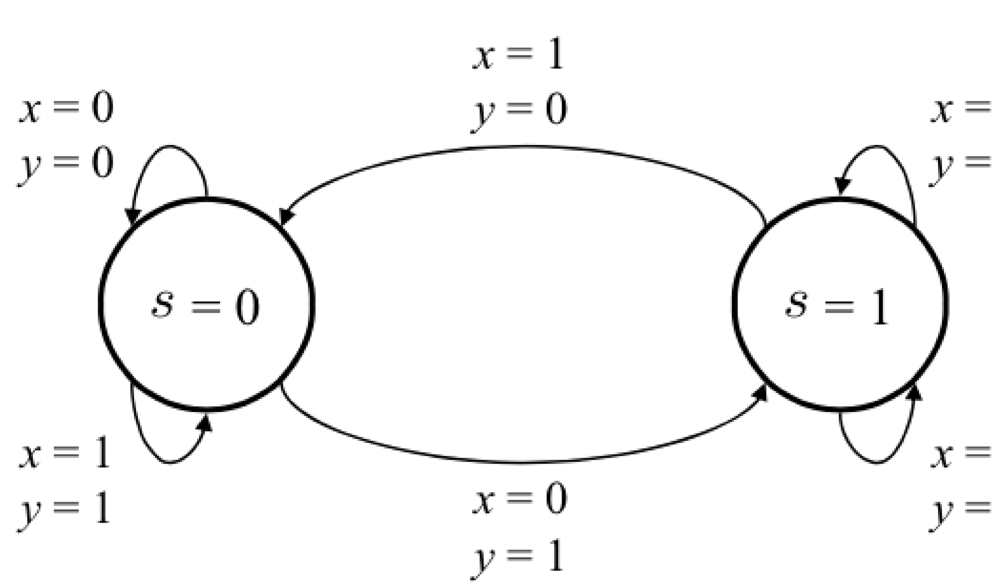

Figure 1: Finite-state-machine representation for binary model.

Consider the following policies and the sample paths they yield starting at battery state 0.

- P1: $q_{i,(1)}(y_i|x^i, s^{i-1}, y^{i-1}) = \delta(y_i = x_i),\ \forall i$
- P2: $q_{i,(2)}(y_i|x^i, s^{i-1}, y^{i-1}) = \delta(y_i = \overline{s_{i-1}}),\ \forall i$
- P3: $q_{i,(3)}(y_i|x^i, s^{i-1}, y^{i-1}) = 1/2$ if $x_i \neq s_{i-1},\ \forall i$

i	0	1	2	3	4	5	6	7	8	9
X_i		1	0	1	0	0	0	0	0	1
P1: S_i	0	0	0	0	0	0	0	0	0	0
P1: Y_i		1	0	1	0	0	0	0	0	1
P2: S_i	0	0	1	0	1	1	1	1	1	0
P2: Y_i		1	1	0	1	0	0	0	0	0
P3: S_i	0	0	0	0	0	0	1	1	1	0
P3: Y_i		1	0	1	0	0	1	0	0	0

Equivalent Problem Formulations

The battery policy effectively creates a noisy channel from the user to the utility provider. Let $(X_i)_{i=1}^n$ be a first-order Markov source, $Z_i = (X_i, S_{i-1})$, and $W(x, s) = \{y \in \mathcal{Y} : s + y - x \in \mathcal{S}\}$.

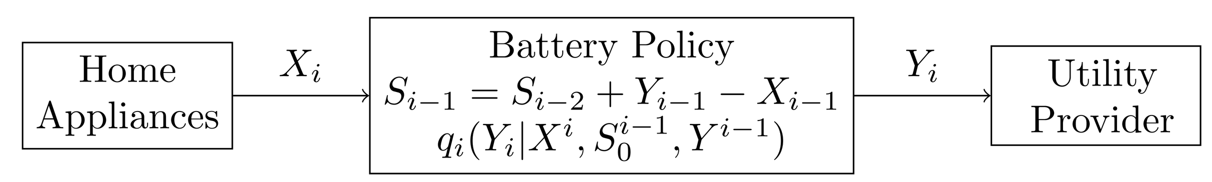

Figure 2: System Diagram. At each time $i \in \{1, 2, \ldots, n\}$, the battery policy defines a with channel with memory.

We define our problem using mutual information as the measure of information leakage.

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

where $\mathcal{Q}_A$ is the set of feasible battery policies

$$\mathcal{Q}_A := \Big\{ q \in \mathcal{P}(\mathcal{Y}^n | \mathcal{X}^n, \mathcal{S}) : q(Y^n|X^n, S_0) = \bigotimes_{i=1}^n q_i(Y_i|X^i, S_0^{i-1}, Y^{i-1}), \quad q_i(W(X_i, S_{i-1})|X^i, S_0^{i-1}, Y^{i-1}) = 1,\ \forall i \Big\}.$$

Problem A Find a policy $q^* \in \mathcal{Q}_A$ such that

$$L(q^*) = \min_{q \in \mathcal{Q}_A} I^q(S_0, X^n; Y^n).$$

1. Problem A is a convex optimization problem.
2. Without loss of optimality, in Problem A, the optimization over $\mathcal{Q}_A$ can be replaced by

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

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

$$L(q^*) = \min_{q \in \mathcal{Q}_B} \sum_{i=1}^n I^q(Z_i; Y_i | Y^{i-1}).$$

Next, we recast the problem into a control framework.

Problem C

State space:	$\mathcal{H}^{i-1} = \mathcal{Y}^{i-1} \times \mathcal{U}^{i-1}$
Action space:	$\mathcal{P}_W = \{u \in \mathcal{P}(\mathcal{Y}|\mathcal{Z}) : u(W(Z)|Z) = 1\}$
Policy:	$f_i : \mathcal{H}^{i-1} \to \mathcal{P}_W$
Transition law:	$h^i = (h^{i-1}) \cup (y_i, u_i)$
Per-stage cost:	$I^f(Z_i; Y_i | h^{i-1})$

MDP Formulation and Algorithms

Let us define a statistic π_i which is computed recursively. Let $\pi_1[\emptyset](z_i) := P(z_1)$, and for $i > 1$

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

Let us define a cost function $c : \mathcal{P}(Z) \times \mathcal{P}_W \to \mathbb{R}$

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

The following statements are true for almost all (h^{i-1}) for each i:

1. π_i is the receiver's estimate of $Z_i | h^{i-1}$. Given h^{i-1} and a policy f as defined in Problem C,
$$\pi_i[h^{i-1}](Z_i) = P^f(Z_i | h^{i-1})$$
Note that given h^{i-1}, the posterior is independent of the policy f.
2. $(\pi_i)_{i=1}^n$ 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 u_i and the belief state π_i.
3. $(\pi_i)_{i=1}^n$ is a u-controlled Markov process
$$P^f(\pi_{i+1} | u^i, \pi^i) = P(\pi_{i+1} | u_i, \pi_i) = \sum_{y_i} \mathbb{1}(\pi_{i+1} = \phi(\pi_i, u_i, y_i)) \sum_{z_i} u_i(y_i|z_i) \pi_i(z_i)$$
Note that the transitions are independent of the policy f.

Problem D

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

Dynamic Programming Algorithm

$$J_{n+1}(\pi_{n+1}) = 0$$
$$J_i(\pi_i) = \min_{u_i \in \mathcal{P}_W} \left\{ c(\pi_i, u_i) + E_{\pi_i}^{u_i} [J_{i+1}(\phi)] \right\},\ i \leq n$$

Binary Model Solution

Let us consider a class of symmetric policies:

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

1. If $q \in \mathcal{Q}_A$ then $\bar{q} \in \mathcal{Q}_A$. Since if (y^n, x^n, s^{n-1}) is a valid sample path through the FSM, $(\overline{y}^n, \overline{x}^n, \overline{s}^{n-1})$ is also valid.
2. A policy q yields the same leakage as $\bar{q}$, i.e.
$$L(q) = L(\bar{q}), \text{ for } q \in \mathcal{Q}_A.$$
3. By the convexity of Problem A, we may optimize over symmetric policies without loss of optimality.
$$\mathcal{Q}_{A,sym} = \{q \in \mathcal{Q}_A : q = \bar{q}\}$$
4. For Problem D, at time 1, in belief state $\pi_1(s_1) = 1/2$, the action space can be reduced to
$$\mathcal{P}_{W,sym} = \{u \in \mathcal{P}_W : u = \bar{u}\}.$$
Moreover, the following statements are true:
   - Fixed Transitions: $\pi_1 = \phi(\pi_1, u_1, y_1),\ \forall y_1, u_1 \in \mathcal{P}_{W,sym}$
   - Optimal Single-Stage Cost: $\min_{u_1 \in \mathcal{P}_{W,sym}} c(\pi_1, u_1) = 1/2$
   - Optimal Single-Stage Action: $u_1^*(y_1|z_1) = 1/2,$ if $x_1 = s_0$
5. Using forward induction, we apply the following argument to $J_2, J_3, \ldots, J_n$.
$$J_1(\pi_1) = \min_{u_1 \in \mathcal{P}_W} \left\{ c(\pi_1, u_1) + \sum_{\pi_2} P(\pi_2 | \pi_1, u_1) J_2(\pi_2) \right\} = \min_{u_1 \in \mathcal{P}_{W,sym}} c(\pi_1, u_1) + J_2(\pi_1) = \frac{n}{2}.$$

In conclusion, for the binary model, the minimum leakage rate is $\frac{1}{n} L(q^*) = 1/2,\ \forall n$ and is achievable using Policy 3 (i.e. $q^* = q_{(3)}$).

Contact Information

- simonli@ece.utoronto.ca
- akhisti@ece.utoronto.ca
- aditya.mahajan@mcgill.ca