On Privacy in Smart Metering Systems with Periodically Time-Varying Input Distribution

Yu Liu[a], Ashish Khisti[a], Aditya Mahajan[b]

[a] University of Toronto

[b] McGill University

GlobalSIP Symposium on Privacy and Security

14 Nov, 2017

Smart Meters empower smart grids

Fine grained consumption measurements are needed for:

- Time-of-use pricing
- Demand response
- ...

Smart Meters empower smart grids

Fine grained consumption measurements are needed for:

- Time-of-use pricing
- Demand response
- ...

Comprehensive report: How smart meters invade privacy

August 29, 2014 by *K. T. Weaver*
big data, democracy, Fourth Amendment, privacy, rights, smart meters, spying

by K.T. Weaver, for Take Back Your Power *6 Comments*

Last week, SkyVision Solutions released an updated **report** entitled, “A Perspective on How Smart Meters Invade Individual Privacy.”

Smart Meters empower smart grids

Fine grained consumption measurements are needed for:

- Time-of-use pricing
- Demand response
- ...

Comprehensive

The New York Times

SUBSCRIBE NOW

LOG IN

Doctor, Bully, Futurist, Spy: The 'Smart Meter'

By MATTHEW L. WALD MAY 20, 2010 2:00 PM

Living

Will future energy and health researchers get useful data from "smart meters"?

As utilities around the country install meters that can

Smart Meters empower smart grids

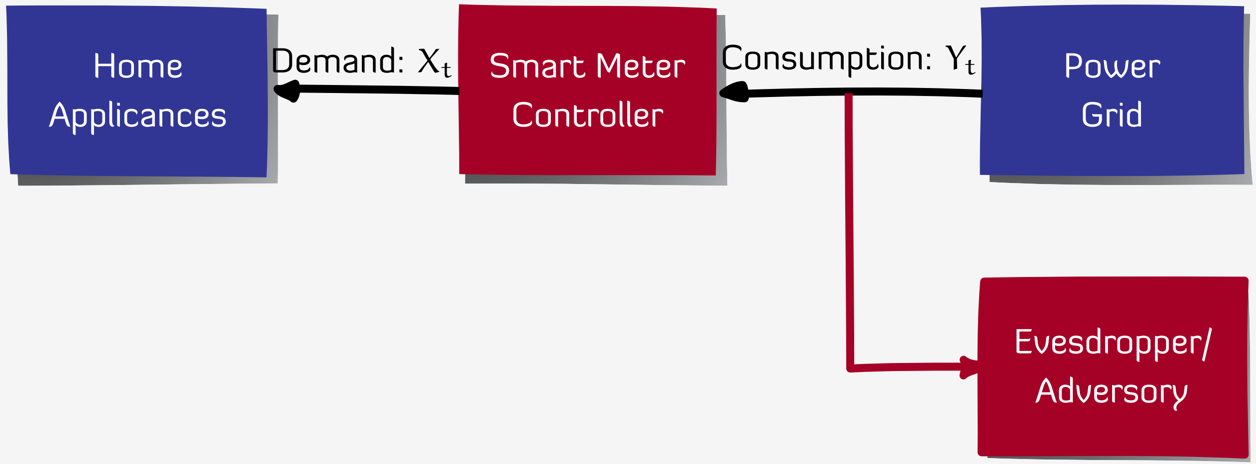
Fine grained consumption measurements are needed for:

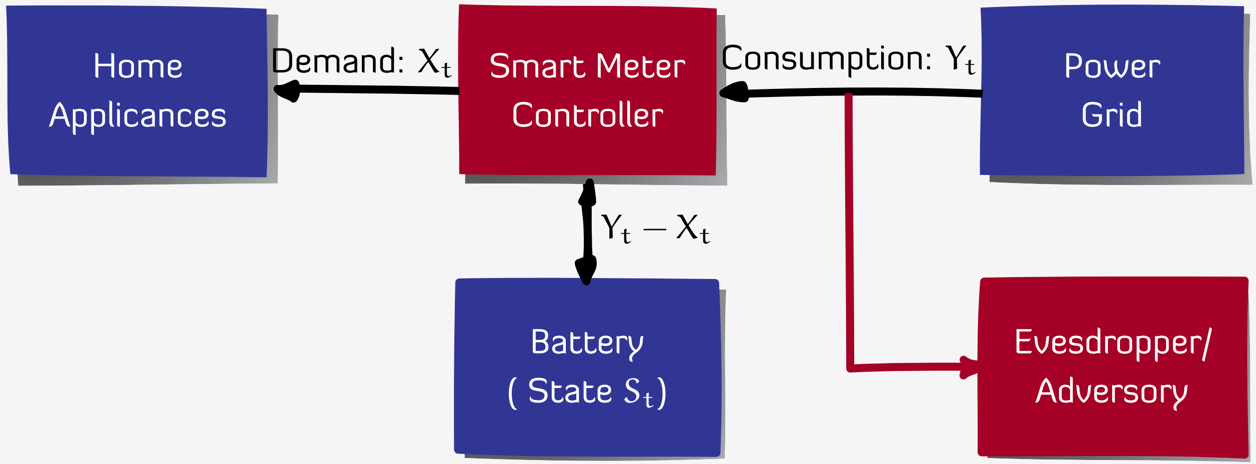
- Time-of-use pricing
- Demand response
- . . .

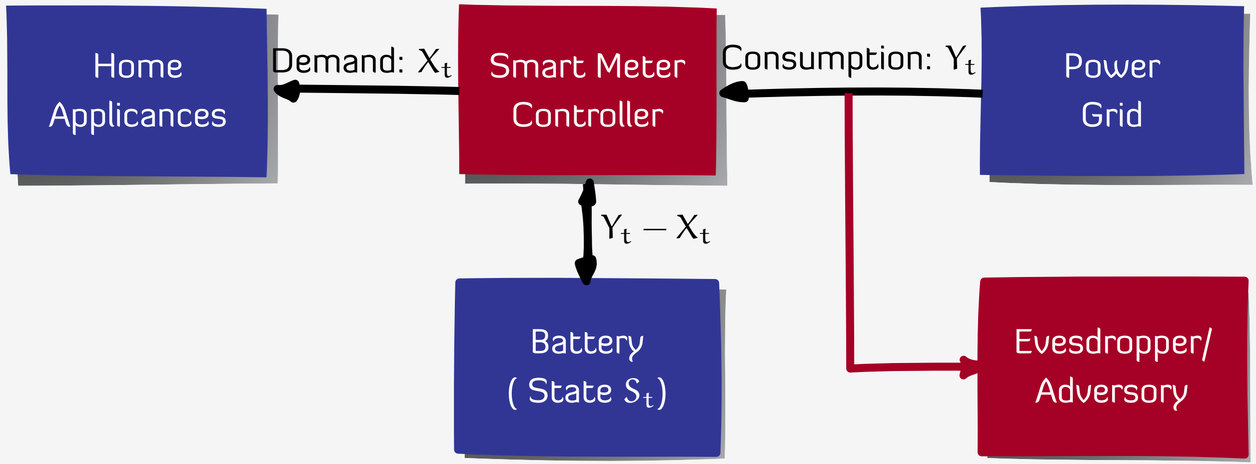
What is the minimum information leakage rate if consumers obfuscate consumption using a rechargeable battery?

What are privacy-optimal battery charging strategies?

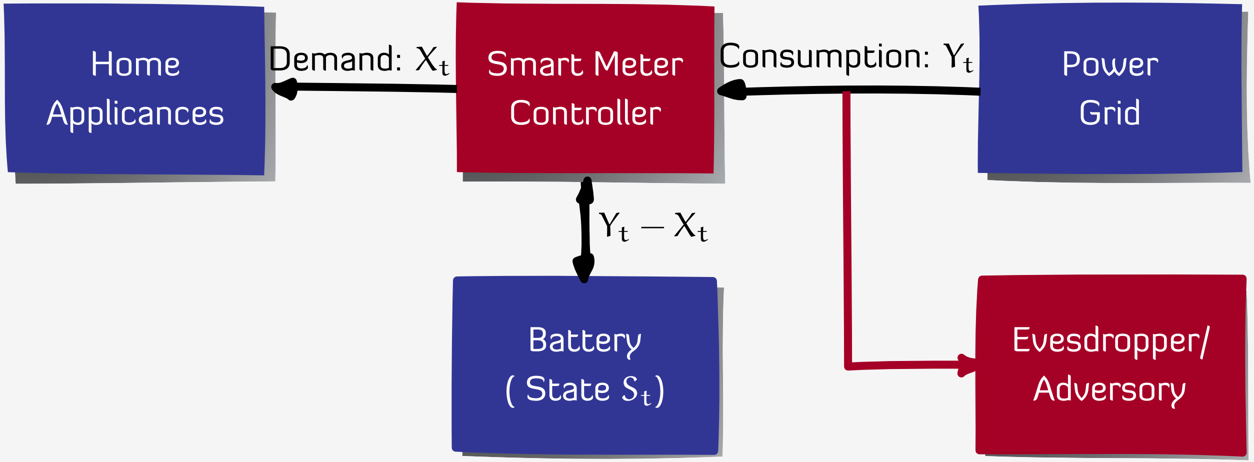

Home Applicances
Demand: X_t
Smart Meter Controller
Consumption: Y_t
Power Grid


Home
Applicances
Demand: X_t
Smart Meter
Controller
Consumption: Y_t
Power
Grid
Evesdropper/
Adversory


Home
Applicances
Demand: X_t
Smart Meter
Controller
Consumption: Y_t
Power
Grid
$Y_t - X_t$
Battery
(State S_t)
Evesdropper/
Adversory

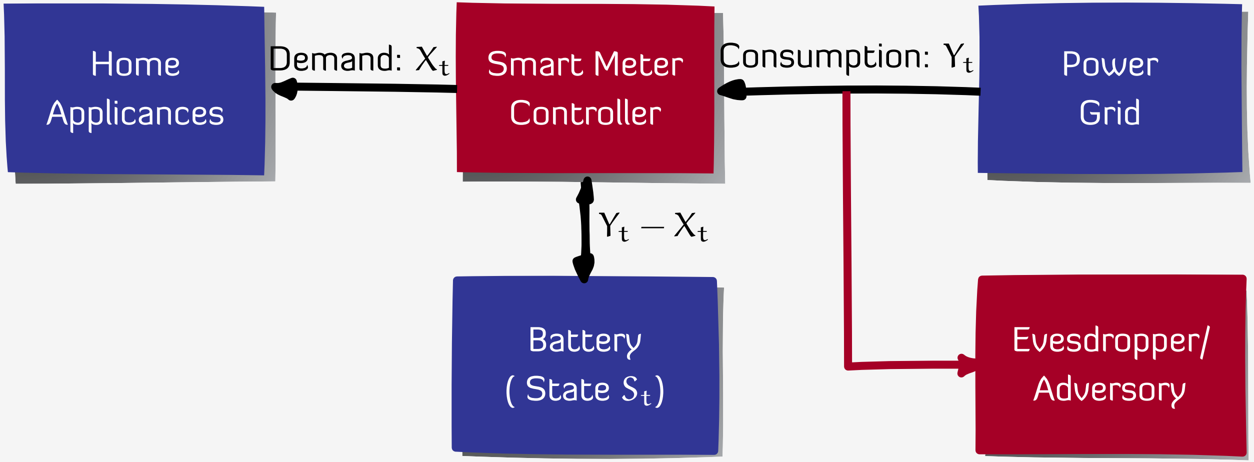


Energy conservation $\quad S_{t+1} = S_t + Y_t - X_t, \quad S_t \in \mathcal{S}$ (Size of battery)



Energy conservation $S_{t+1} = S_t + Y_t - X_t, \quad S_t \in \mathcal{S}$ (Size of battery)

Randomized charging strategy $q_t(y_t \mid x^t, s^t, y^{t-1})$: Choose consumption given history ...



Energy conservation $S_{t+1} = S_t + Y_t - X_t, \quad S_t \in \mathcal{S}$ (Size of battery)

Randomized charging strategy $q_t(y_t \mid x^t, s^t, y^{t-1})$: Choose consumption given history . . .

Objective Choose battery charging strategy $\mathbf{q} = \{q_t\}_{t \geqslant 1}$ to

$$\min \lim_{T \to \infty} \frac{1}{T} I^{\mathbf{q}}(X^T; Y^T) \quad \text{(mutual information rate)}$$

Why is the problem non-trivial?

$\mathcal{X} = \mathcal{Y} = \mathcal{S} = \{0, 1\}$, $P_X = [0.5, \ \ 0.5]$ (Binary model)

Consv: $S_t + Y_t - X_t \in \mathcal{S}$

Why is the problem non-trivial?

$\mathcal{X} = \mathcal{Y} = \mathcal{S} = \{0, 1\}$, $P_X = [0.5, \ \ 0.5]$ (Binary model) Consv: $S_t + Y_t - X_t \in \mathcal{S}$

Empty state $S_t = 0$

- $X_t = 0 \implies Y_t \in \{0, 1\}$
- $X_t = 1 \implies Y_t = 1$

Full state $S_t = 1$

- $X_t = 0 \implies Y_t = 0$
- $X_t = 1 \implies Y_t \in \{0, 1\}$

Why is the problem non-trivial?

$\mathcal{X} = \mathcal{Y} = \mathcal{S} = \{0, 1\}$, $P_X = [0.5, \; 0.5]$ (Binary model)

Consv: $S_t + Y_t - X_t \in \mathcal{S}$

Empty state $S_t = 0$

- $X_t = 0 \implies Y_t \in \{0, 1\}$
- $X_t = 1 \implies Y_t = 1$

Full state $S_t = 1$

- $X_t = 0 \implies Y_t = 0$
- $X_t = 1 \implies Y_t \in \{0, 1\}$

Consider performance of memoryless policies

Why is the problem non-trivial?

$\mathcal{X} = \mathcal{Y} = \mathcal{S} = \{0, 1\}$, $P_X = [0.5, \ \ 0.5]$ (Binary model) Consv: $S_t + Y_t - X_t \in \mathcal{S}$

Empty state $S_t = 0$

- $X_t = 0 \implies Y_t \in \{0, 1\}$
- $X_t = 1 \implies Y_t = 1$

Full state $S_t = 1$

- $X_t = 0 \implies Y_t = 0$
- $X_t = 1 \implies Y_t \in \{0, 1\}$

Consider performance of memoryless policies

Deterministic Memoryless Policy

- $P(Y|X = 0, S = 0) = [1 \ \ 0]$; $P(Y|X = 1, S = 1) = [0 \ \ 1]$: Leakage $= 1$ ($\because Y_t = X_t$).
- $P(Y|X = 0, S = 0) = [0 \ \ 1]$; $P(Y|X = 1, S = 1) = [1 \ \ 0]$: Leakage ≈ 1 ($\because Y_t = 1 - S_t$).

Why is the problem non-trivial?

$\mathcal{X} = \mathcal{Y} = \mathcal{S} = \{0, 1\}$, $P_X = [0.5, \; 0.5]$ (Binary model)

Consv: $S_t + Y_t - X_t \in \mathcal{S}$

Empty state $S_t = 0$

- $X_t = 0 \implies Y_t \in \{0, 1\}$
- $X_t = 1 \implies Y_t = 1$

Full state $S_t = 1$

- $X_t = 0 \implies Y_t = 0$
- $X_t = 1 \implies Y_t \in \{0, 1\}$

Consider performance of memoryless policies

Deterministic Memoryless Policy

- $P(Y|X=0, S=0) = [1 \;\; 0]$; $P(Y|X=1, S=1) = [0 \;\; 1]$: Leakage $= 1$ ($\because Y_t = X_t$).
- $P(Y|X=0, S=0) = [0 \;\; 1]$; $P(Y|X=1, S=1) = [1 \;\; 0]$: Leakage ≈ 1 ($\because Y_t = 1 - S_t$).

Randomized Memoryless Policy

- $P(Y|X=0, S=0) = [0.5 \;\; 0.5]$; $P(Y|X=1, S=1) = [0.5 \;\; 0.5]$: Leakage $= 0.5$.
- Is this the **best** memoryless policy?
- Is this the **optimal** policy?
- How do we evaluate the performance of an arbitrary policy? Need $\mathbb{P}(X^T, Y^T)$?

Literature overview

Evaluate privacy of specific battery management policies

- [Kalogridis et al., 2010] Monte-Carlo evaluation of best-effort policy
- [Varodayan Khisti, 2011] Computing performance of battery conditioned stochastic charging policies using BCJR algorithm.
- [Tan Gündüz Poor, 2012] Generalized results of [Varodayan Khisti] to include models with energy harvesting.
- [Giulio Gündüz Poor, 2015] Bounds on performance of best-effort and hide-and-store policies for infinite battery size.

Literature overview

Evaluate privacy of specific battery management policies

- [Kalogridis et al., 2010] Monte-Carlo evaluation of best-effort policy
- [Varodayan Khisti, 2011] Computing performance of battery conditioned stochastic charging policies using BCJR algorithm.
- [Tan Gündüz Poor, 2012] Generalized results of [Varodayan Khisti] to include models with energy harvesting.
- [Giulio Gündüz Poor, 2015] Bounds on performance of best-effort and hide-and-store policies for infinite battery size.

Dynamic programming decomposition to identify optimal policies

- [Yao Venkitasubramanian, 2013] Dynamic program, computable inner and upper bounds.
- Li Kshiti Mahajan, 2016 Dynamic program, closed form optimal strategy for i.i.d. case.

[LKM] Main results: Markovian demand

Structure of optimal strategies

- Define belief state $\pi_t(x, s) = \mathbb{P}(X_t = x, S_t = s | Y^{t-1})$
- Charging strategies of the form $q_t(y_t | x_t, s_t, \pi_t)$ are optimal.

[LKM] Main results: Markovian demand

Structure of optimal strategies

- Define belief state $\pi_t(x, s) = \mathbb{P}(X_t = x, S_t = s | Y^{t-1})$
- Charging strategies of the form $q_t(y_t | x_t, s_t, \pi_t)$ are optimal.

Dynamic programming decomposition

Let $\mathcal{A}$ denote the class of conditional distributions on $\mathcal{Y}$ given $(\mathcal{X}, \mathcal{S})$.

Suppose there exists a $J \in \mathbb{R}$ and $v \colon \mathcal{P}_{X,S} \to \mathbb{R}$ that satisfies the following:

$$J^* + v(\pi) = \inf_{a \in \mathcal{A}} \Big\{ I(a; \pi) + \sum_{x,s,y} \pi(x, s) a(y | x, s) v(\varphi(\pi, y, a)) \Big\}$$

Then,

- J^* is the minimum leakage rate
- Let $f^*(\pi)$ denote the arg min of the RHS and $a^* = f^*(\pi)$.
  Then, J^* is achieved by the charging policy
  $$q^*(y | x_t, s_t, \pi_t) = a^*(y | x_t, s_t) \quad \text{(note } a^* \text{ depends on } \pi_t\text{)}$$

[LKM] Main results- Markovian demand

- Inspired by the approach used for capacity of Markov channels with feedback (Goldsmith Varaiya 1996, Tatikonda Mitter 2009, Permuter et al 2008)
- The DP is similar to the DP for POMDPs but the per-step cost is concave rather than linear.
- $v(\pi)$ is concave. So, computational approaches for POMDPs work.

Suppose there exists a $J \in \mathbb{R}$ and $v \colon \mathcal{P}_{X,S} \to \mathbb{R}$ that satisfies the following:

$$J^* + v(\pi) = \inf_{a \in \mathcal{A}} \Big\{ I(a;\pi) + \sum_{x,s,y} \pi(x,s) a(y|x,s) v(\varphi(\pi, y, a)) \Big\}$$

Then,

- J^* is the minimum leakage rate
- Let $f^*(\pi)$ denote the arg min of the RHS and $a^* = f^*(\pi)$.
  Then, J^* is achieved by the charging policy

$$q^*(y|x_t, s_t, \pi_t) = a^*(y|x_t, s_t) \quad \text{(note } a^* \text{ depends on } \pi_t\text{)}$$

[LKM] Main results: i.i.d. demand

Solution of the dynamic program

$$J^* \coloneqq \min_{\theta \in \mathcal{P}_S} I(S - X; X)$$

where $X \sim P_X$ and $S \sim \theta$. Let θ^* denote the arg min of the RHS.

Then, J^* is the minimum leakage rate

[LKM] Main results: i.i.d. demand

Solution of the dynamic program

$$J^* \coloneqq \min_{\theta \in \mathcal{P}_S} I(S - X; X)$$

where $X \sim P_X$ and $S \sim \theta$. Let θ^* denote the arg min of the RHS.

Then, J^* is the minimum leakage rate

Optimal strategies

Define $b^*(y|x,s) = \begin{cases} \dfrac{P_X(y)\theta^*(y + x - s)}{\text{Normalize}} & \text{if } y \in \mathcal{X} \text{ and } y \text{ is feasible} \\ 0, & \text{otherwise} \end{cases}.$

Then, J^* is achieved by time-invariant action

$$q^*_t(y|x_t, s_t, \pi_t) = b^*(y|x_t, s_t) \quad \text{(note } b^* \text{ does not depend on } \pi_t\text{)}$$

[LKM] Salient features of the solution

$I(S - X; X)$ is concave in $\mathcal{P}_{\mathcal{S}}$

J^* and θ^* may be computed using Blahut-Arimoto algorithm.

Optimal policy is stationary and memoryless

$q_t^*(y|x^t, s^t) = b^*(y|x_t, s_t)$ (note b^* does not depend on π_t)

If $S_t \sim \theta^*$, then $S_{t+1} \sim \theta^*$ and $S_{t+1} \perp Y^t$.

Support of consumptions

Even if $\mathcal{Y} \supset \mathcal{X}$, under the optimal policy the support of P_Y is $\mathcal{X}$.

This paper: Periodic Input Distribution

Periodic input $X_{\text{odd}} \sim Q_1(\cdot)$ and $X_{\text{even}} \sim Q_2(\cdot)$.

We assume that the input cycles between two distributions (each of length one). Results easily generalize to a larger cycle or staying at each distribution for a different amount of time.

Conceptual diff. Same as before. The leakage rate is a multi-letter mutual information expression that depends on $\mathbb{P}(X^T, Y^T)$.

This paper: Periodic Input Distribution

Periodic input $X_{\text{odd}} \sim Q_1(\cdot)$ and $X_{\text{even}} \sim Q_2(\cdot)$.

We assume that the input cycles between two distributions (each of length one). Results easily generalize to a larger cycle or staying at each distribution for a different amount of time.

Conceptual diff. Same as before. The leakage rate is a multi-letter mutual information expression that depends on $\mathbb{P}(X^T, Y^T)$.

Solution idea We can use the qualitative properties of the i.i.d. solution to get achievable upper bounds. Compare them with non-achievable lower bounds.

Achievable scheme and lower bound

Achievable scheme

Arbitrarily restrict attention to periodic policies:

- For odd time: $q_1(y_t|x_t, s_t)$
- For even time: $q_2(y_t|x_t, s_t)$

Pick q_1 and q_2 to ensure invariance condition: $S_{t+1} \perp Y^t$.

This induces $\mathbb{P}(S_t) = P_{S_1}$ for odd times and P_{S_2} for even times.

$$L^* \leqslant L_\infty(\mathbf{q}) = \frac{1}{2} I(S_1, X_1; X_1) + \frac{1}{2} I(S_2, X_2; X_2).$$

Achievable scheme and lower bound

Achievable scheme

Arbitrarily restrict attention to periodic policies:

- For odd time: $q_1(y_t|x_t, s_t)$
- For even time: $q_2(y_t|x_t, s_t)$

Pick q_1 and q_2 to ensure invariance condition: $S_{t+1} \perp Y^t$.
This induces $\mathbb{P}(S_t) = P_{S_1}$ for odd times and P_{S_2} for even times.

$$L^* \leqslant L_\infty(\mathbf{q}) = \frac{1}{2} I(S_1, X_1; X_1) + \frac{1}{2} I(S_2, X_2; X_2).$$

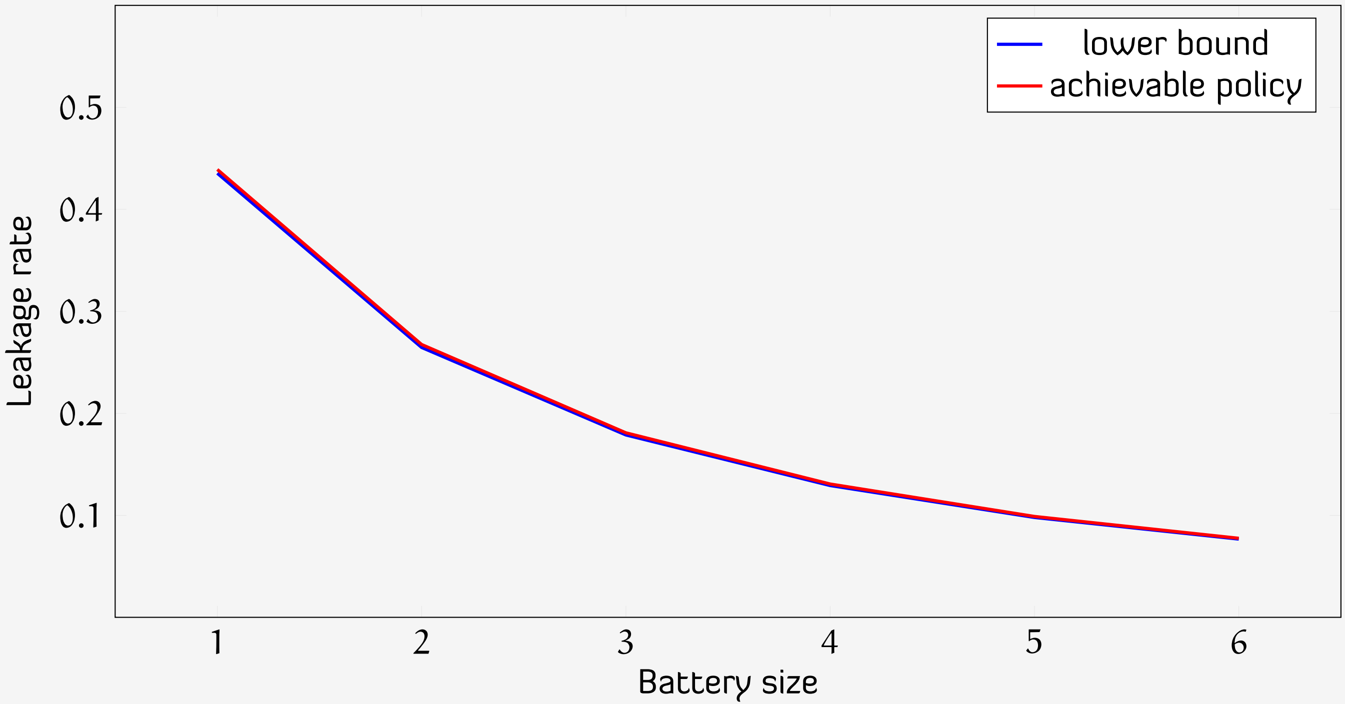
Lower bound

$$L^* \geqslant \frac{1}{2} \min_{P_{S_1}} I(S_1 - X_1; X_1) + \frac{1}{2} \min_{P_{S_2}} I(S_2 - X_2; X_2)$$

Same as assuming that the input distribution was Q_1 for first $T/2$ time steps and Q_2 as last $T/2$ time steps.

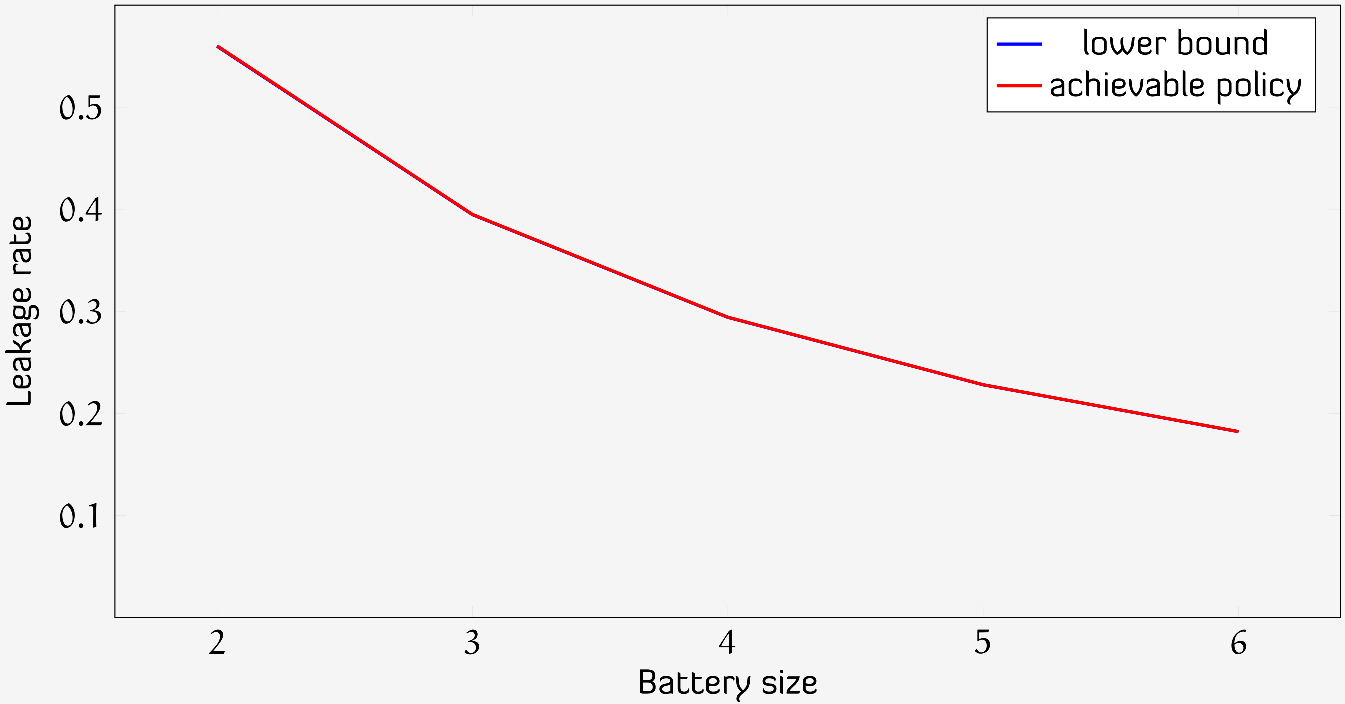
Numerical Results

Binary Model $\mathcal{X} = \mathcal{Y} = \{0, 1\}$. $Q_1 = [0.7\ 0.3]$, $Q_2 = [0.3\ 0.7]$.



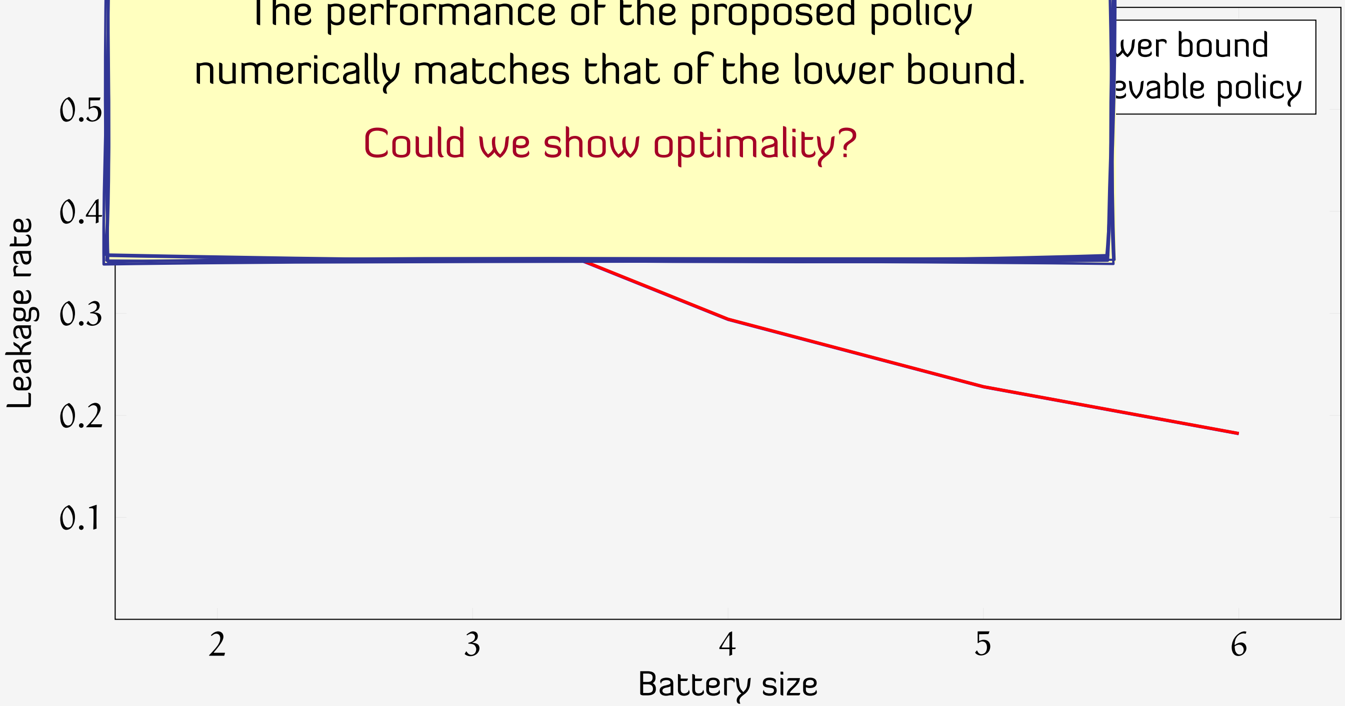
Numerical Results

Ternary Model $\mathcal{X} = \mathcal{Y} = \{0, 1, 2\}$. $Q_1 = [0.33\ 0.33\ 0.33]$, $Q_2 = [0.25\ 0.5\ 0.25]$.



Numerical Results

Ternary Mo

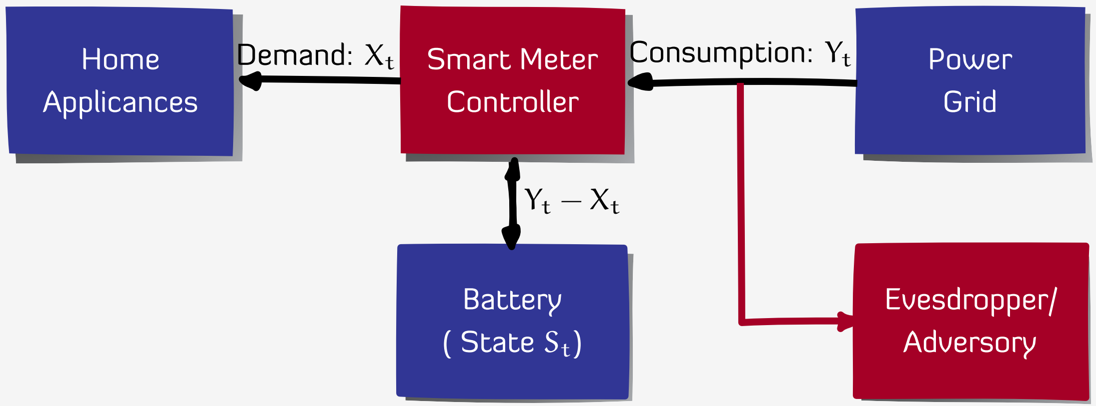


The performance of the proposed policy numerically matches that of the lower bound.

Could we show optimality?

Summary

Summary



Energy conservation $S_{t+1} = S_t + Y_t - X_t, \quad S_t \in \mathcal{S}$ (Size of battery)

Randomized charging strategy $q_t(y_t \,|\, x^t, s^t, y^{t-1})$: Choose consumption given history ...

Objective Choose battery charging strategy $\mathbf{q} = \{q_t\}_{t \geq 1}$ to

$$\min \lim_{T \to \infty} \frac{1}{T} I^{\mathbf{q}}(X^T; Y^T) \quad \text{(mutual information rate)}$$

Smart-meter privacy–(Liu, Khisti, and Mahajan)

[LKM] Main results: Markovian demand

Structure of optimal strategies

- Define belief state $\pi_t(x, s) = \mathbb{P}(X_t = x, S_t = s | Y^{t-1})$
- Charging strategies of the form $q_t(y_t | x_t, s_t, \pi_t)$ are optimal.

Dynamic programming decomposition

Let $\mathcal{A}$ denote the class of conditional distributions on $\mathcal{Y}$ given $(\mathcal{X}, \mathcal{S})$.

Suppose there exists a $J \in \mathbb{R}$ and $v \colon \mathcal{P}_{X,S} \to \mathbb{R}$ that satisfies the following:

$$J^* + v(\pi) = \inf_{a \in \mathcal{A}} \left\{ I(a; \pi) + \sum_{x,s,y} \pi(x, s) a(y | x, s) v(\varphi(\pi, y, a)) \right\}$$

Then,

- J^* is the minimum leakage rate
- Let $f^*(\pi)$ denote the arg min of the RHS and $a^* = f^*(\pi)$.
  Then, J^* is achieved by the charging policy
  $q^*(y | x_t, s_t, \pi_t) = a^*(y | x_t, s_t)$ (note a^* depends on π_t)

Smart-meter privacy–(Liu, Khisti, and Mahajan) 12

[LKM] Main results: i.i.d. demand

Solution of the dynamic program

$$J^* \coloneqq \min_{\theta \in \mathcal{P}_S} I(S - X; X)$$

where $X \sim P_X$ and $S \sim \theta$. Let θ^* denote the arg min of the RHS.

Then, J^* is the minimum leakage rate

Optimal strategies

Define $b^*(y|x,s) = \begin{cases} \dfrac{P_X(y)\theta^*(y+x-s)}{\text{Normalize}} & \text{if } y \in \mathcal{X} \text{ and } y \text{ is feasible} \\ 0, & \text{otherwise} \end{cases}$.

Then, J^* is achieved by time-invariant action

$$q_t^*(y|x_t, s_t, \pi_t) = b^*(y|x_t, s_t) \quad \text{(note } b^* \text{ does not depend on } \pi_t\text{)}$$

Summary

This paper: Periodic Input Distribution

Periodic input $X_{\text{odd}} \sim Q_1(\cdot)$ and $X_{\text{even}} \sim Q_2(\cdot)$.

We assume that the input cycles between two distributions (each of length one). Results easily generalize to a larger cycle or staying at each distribution for a different amount of time.

Conceptual diff. Same as before. The leakage rate is a multi-letter mutual information expression that depends on $\mathbb{P}(X^T, Y^T)$.

Solution idea We can use the qualitative properties of the i.i.d. solution to get achievable upper bounds. Compare them with non-achievable lower bounds.

Summary

Achievable scheme and lower bound

Achievable scheme

Arbitrarily restrict attention to periodic policies:

- For odd time: $q_1(y_t|x_t, s_t)$
- For even time: $q_2(y_t|x_t, s_t)$

Pick q_1 and q_2 to ensure invariance condition: $S_{t+1} \perp Y^t$.
This induces $\mathbb{P}(S_t) = P_{S_1}$ for odd times and P_{S_2} for even times.

$$L^* \leqslant L_\infty(\mathbf{q}) = \frac{1}{2}I(S_1, X_1; X_1) + \frac{1}{2}I(S_2, X_2; X_2).$$

Lower bound

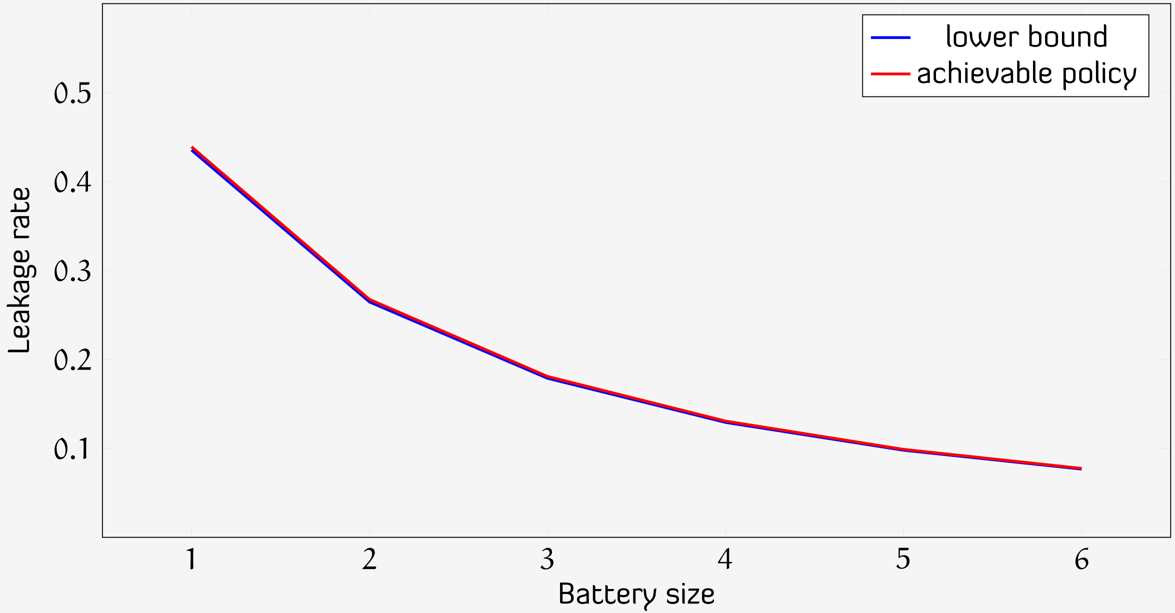
$$L^* \geqslant \frac{1}{2}\min_{P_{S_1}} I(S_1 - X_1; X_1) + \frac{1}{2}\min_{P_{S_2}} I(S_2 - X_2; X_2)$$

Same as assuming that the input distribution was Q_1 for first $T/2$ time steps and Q_2 as last $T/2$ time steps.

Summary

Numerical Results

Binary Model $\mathcal{X} = \mathcal{Y} = \{0, 1\}$. $Q_1 = [0.7\ 0.3]$, $Q_2 = [0.3\ 0.7]$.



Summary

Numerical Results

Binary Model $\mathcal{X} = \mathcal{Y} = \{0, 1\}$. $Q_1 = [0.7\ 0.3]$, $Q_2 = [0.3\ 0.7]$.