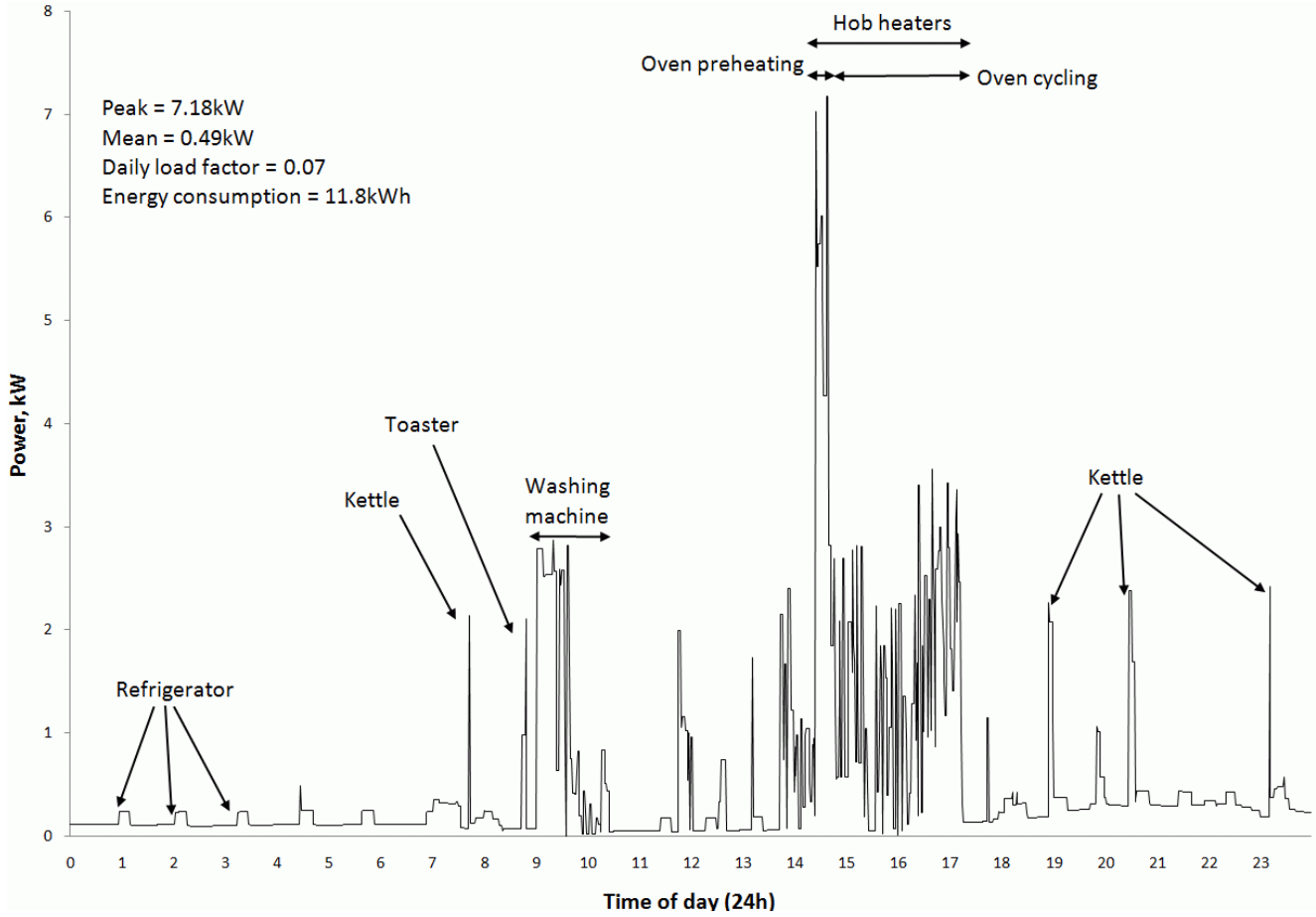
Privacy Preserving Rechargeable Battery Policies for Smart Metering Systems

Simon Li (Toronto), Ashish Khisti (Toronto),
Aditya Mahajan (McGill)

March 3, 2016

Motivation: Privacy Leakage through Power Profile



U. Greveler, P. Glosekotter, B. Justus, and D. Loehr, "Multimedia content identification through smart meter power usage profiles," in Int. Conf. Inform. and Knowledge Eng, 2012.

Problem Setup

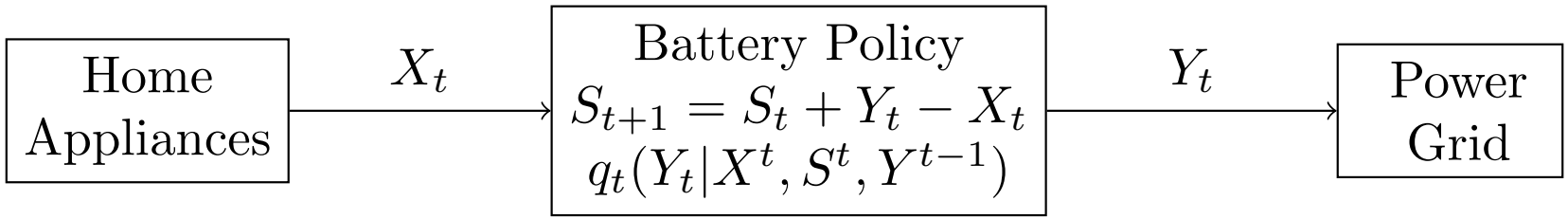


Figure 1: System Diagram.

- User Load: $X_t \in \mathcal{X}$
- Output Load: $Y_t \in \mathcal{Y}$
- Battery State: $S_t \in \mathcal{S}$
- $\mathcal{X}$, $\mathcal{Y}$ and $\mathcal{S}$: discrete
- $X_t \sim P_X(\cdot)$ (i.i.d.)
- Battery Update: $S_{t+1} = S_t + Y_t - X_t$
- Policy: $q_t\left(Y_t|X_1^t, S_1^t, Y_1^{t-1}\right)$
- Leakage Rate $L_T = \frac{1}{T} I(X_1^T; Y_1^T)$
- Asymptotic Leakage: L_∞

Example: Binary System

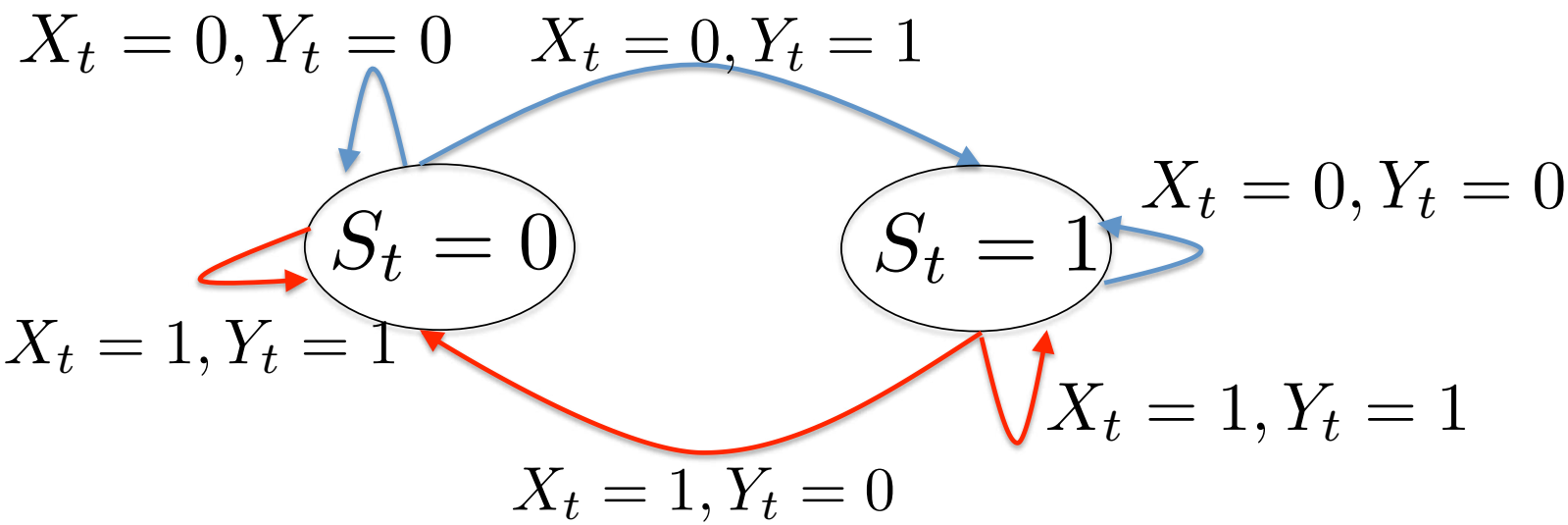
$\mathcal{X}, \mathcal{Y}, \mathcal{S} = \{0, 1\}$, $p_X(0) = p_X(1) = 1/2$.

- Empty State: $S_t = 0$
  - $X_t = 1 \Rightarrow Y_t = 1$
  - $X_t = 0 \Rightarrow Y_t \in \{0, 1\}$
- Full State: $S_t = 1$
  - $X_t = 0 \Rightarrow Y_t = 0$
  - $X_t = 1 \Rightarrow Y_t \in \{0, 1\}$

Example: Binary System

$\mathcal{X}, \mathcal{Y}, \mathcal{S} = \{0, 1\}$, $p_X(0) = p_X(1) = 1/2$.

- Empty State: $S_t = 0$
  - $X_t = 1 \Rightarrow Y_t = 1$
  - $X_t = 0 \Rightarrow Y_t \in \{0, 1\}$
- Full State: $S_t = 1$
  - $X_t = 0 \Rightarrow Y_t = 0$
  - $X_t = 1 \Rightarrow Y_t \in \{0, 1\}$



Binary System

Example Policies

Policy 1: $Y_t = X_t$

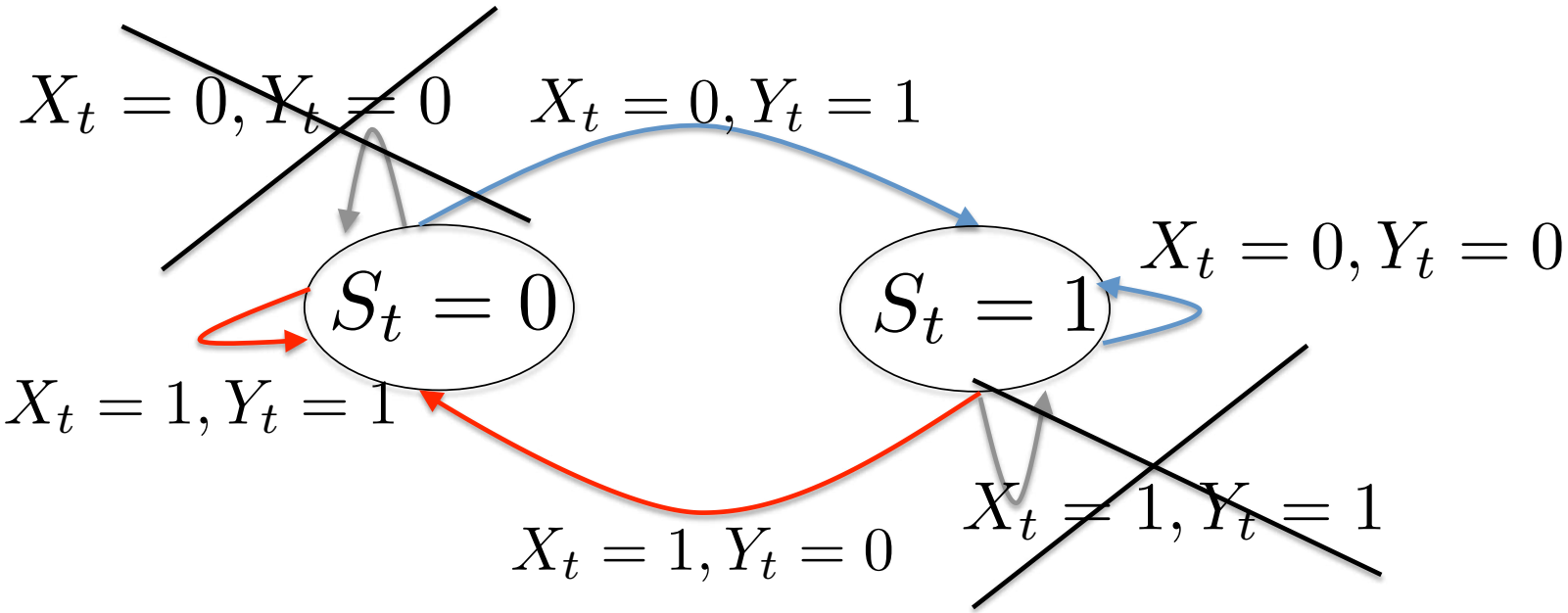
t	1	2	3	4	5	6	7
X_t	0	1	1	0	1	0	1
S_t	0	0	0	0	0	0	0
Y_t	0	1	1	0	1	0	1

$$L_T = \frac{1}{T} I(X^T; Y^T) = 1$$

Binary System

Example Policies

Policy 2: $Y_t = \bar{S}_t$



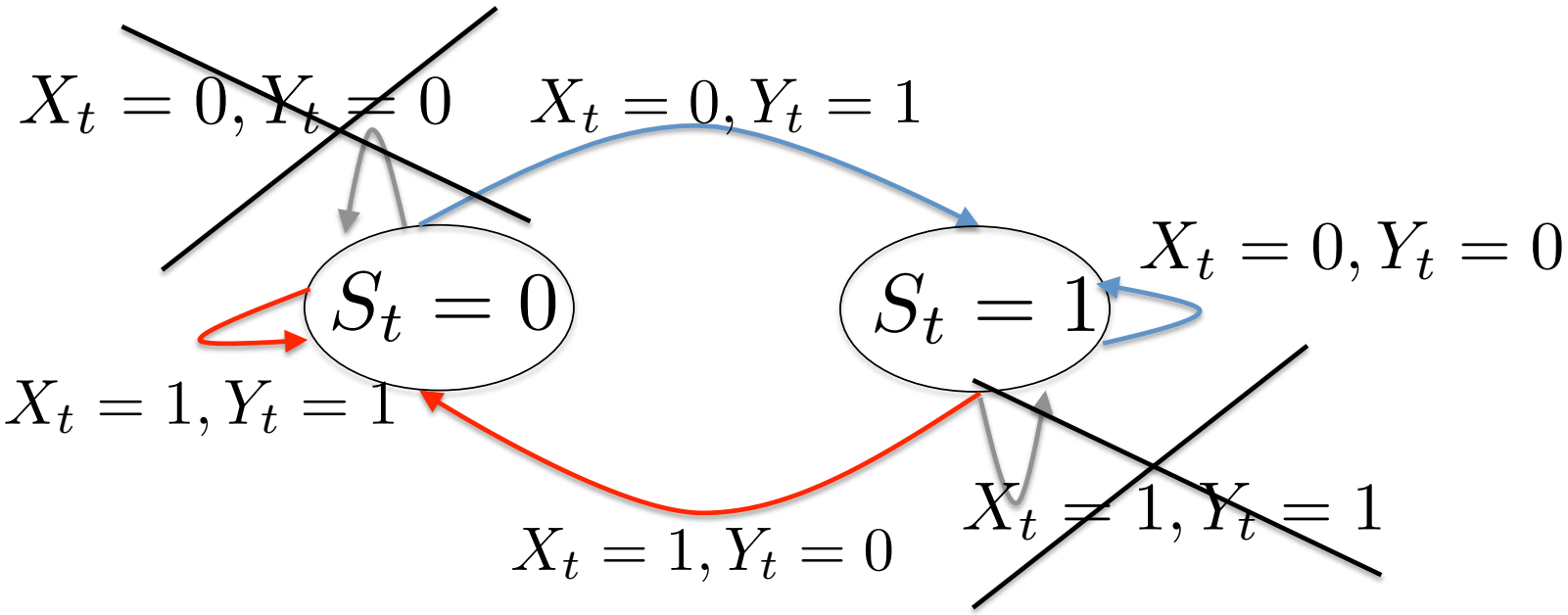
t	1	2	3	4	5	6	7
X_t	0	1	1	0	1	0	1
S_t	0	1	0	0	1	0	1
Y_t	1	0	1	1	0	1	0

- $L_T = \frac{1}{T} I(X^T; Y^T)$?

Binary System

Example Policies

Policy 2: $Y_t = \bar{S}_t$



t	1	2	3	4	5	6	7
X_t	0	1	1	0	1	0	1
S_t	0	1	0	0	1	0	1
Y_t	1	0	1	1	0	1	0

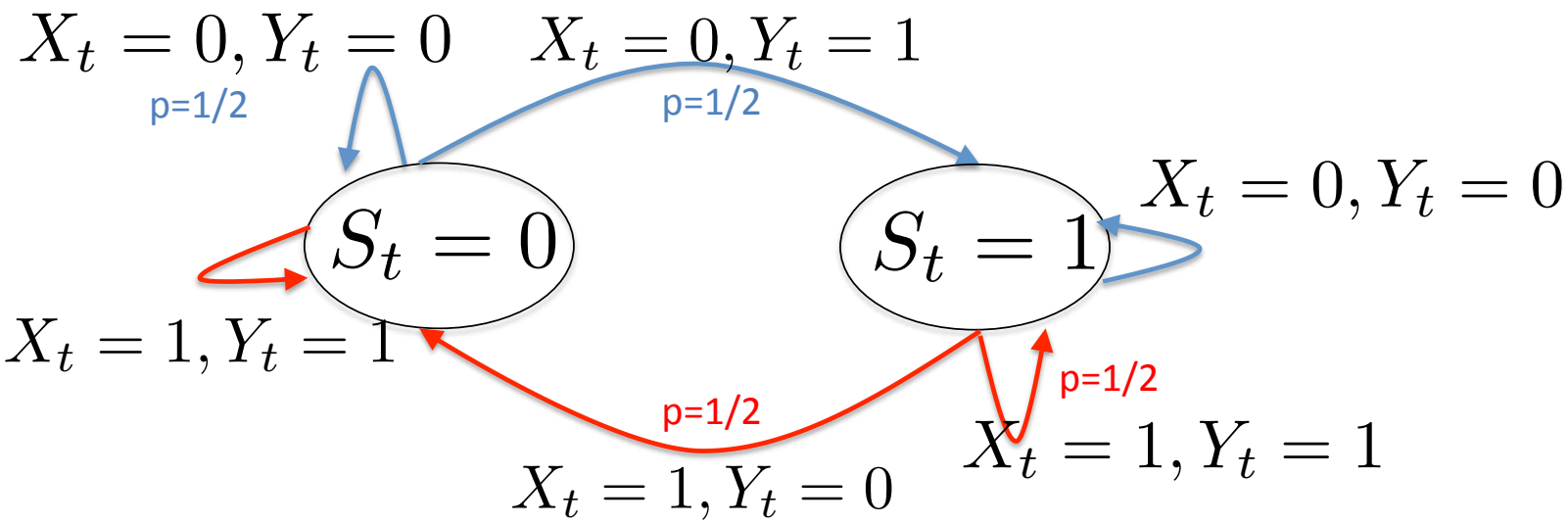
- $L_T = \frac{1}{T} I(X^T; Y^T)$?
- $Y_1^T \Rightarrow S_1^T$ is known
- $(Y_1^T, S_1^T) \Rightarrow X_1^{T-1}$
- $\frac{1}{T} I(X^T; Y^T) \approx 1$

Binary System

Example Policies

Policy 3: Randomized Policy

- $q(Y_t = 0|S_t = 0, X_t = 0) = q(Y_t = 1|S_t = 0, X_t = 0) = 1/2$
- $q(Y_t = 0|S_t = 1, X_t = 1) = q(Y_t = 1|S_t = 1, X_t = 1) = 1/2$



- Equiprobable Binary Input
- Leakage Rate: $L_\infty = 0.5$
- Optimality?

Prior Work

- Kalogridis et al (2010): Rechargeable Battery for Privacy. Metrics such as clustering and regression.
- Varodayan and Khisti (2011): Mutual Information as a Privacy Metric, Binary Smart Meters Model, Randomized Policies, Numerical Simulation Technique
- Giaconi, Gunduz, and Poor (2015): Energy Harvesting/ Alternative Sources and Smart Meter Privacy
- Yao and Venkitasubramaniam (2013): Markov Decision Process
- Li-Khisti-Mahajan (2015, 2016): MDP, Identified optimal policy as a solution to a fixed point equation.

This Work: Information Theoretic Proof of Optimality

Problem Setup

Admissible charging policies: $\mathbf{q} = (q_1, q_2, \cdots) \in \mathcal{Q}_A$ where

$$q_t(y_t \mid x^t, s^t, y^{t-1})$$

Battery constraints:

$$\sum_{y \in \mathcal{Y}_\circ(s_t, x_t)} q_t(y \mid x^t, s^t, y^{t-1}) = 1$$

where: $\mathcal{Y}_\circ(s_t, x_t) = \{y \in \mathcal{Y} : s_t - x_t + y \in \mathcal{S}\}$.

Problem Setup

Admissible charging policies: $\mathbf{q} = (q_1, q_2, \cdots) \in \mathcal{Q}_A$ where

$$q_t(y_t \mid x^t, s^t, y^{t-1})$$

Battery constraints:

$$\sum_{y \in \mathcal{Y}_\circ(s_t, x_t)} q_t(y \mid x^t, s^t, y^{t-1}) = 1$$

where: $\mathcal{Y}_\circ(s_t, x_t) = \{y \in \mathcal{Y} : s_t - x_t + y \in \mathcal{S}\}$.
Joint probability distribution:

$$\begin{aligned}
&\mathbb{P}^{\mathbf{q}}(S^T = s^T, X^T = x^T, Y^T = y^T) \\
&\quad = P_{S_1}(s_1) P_{X_1}(x_1) q_1(y_1 \mid x_1, s_1) \prod_{t=2}^{T} \Big[\mathbb{1}_{s_t}\{s_{t-1} - x_{t-1} + y_{t-1}\} \\
&\qquad\qquad \times P_X(x_t) q_t(y_t \mid x^t, s^t, y^{t-1}) \Big].
\end{aligned}$$

Finite horizon Leakage rate: $\frac{1}{T} I^{\mathbf{q}}(S_1, X^T; Y^T)$

Main Result

Problem

Find $\mathbf{q} \in \mathcal{Q}_A$ *to minimize the infinite horizon leakage rate*

$$L_\infty(\mathbf{q}) := \lim_{T\to\infty} \frac{1}{T} I^{\mathbf{q}}(S_1, X^T; Y^T).$$

Main Result

Problem

Find $\mathbf{q} \in \mathcal{Q}_A$ *to minimize the infinite horizon leakage rate*

$$L_\infty(\mathbf{q}) := \lim_{T\to\infty} \frac{1}{T} I^{\mathbf{q}}(S_1, X^T; Y^T).$$

Theorem

The minimum leakage rate is given by:

$$L_\infty^\star = \min_{\mathbb{P}_S(\cdot)} I(S - X; X) \tag{1}$$

where $X \sim \mathbb{P}_X(\cdot)$ *is independent of* S.
The optimal policy is a time invariant, memoryless policy:

$$q^\star(y|x,s) = \frac{\mathbb{P}_X(y)\mathbb{P}_S^\star(y+s-x)}{\mathbb{P}_{S-X}^\star(s-x)}$$

where $\mathbb{P}_S^\star(\cdot)$ *achieves the minimum above.*

Remarks

Properties of Optimal Policy:

$$q^\star(y|x,s) = \frac{\mathbb{P}_X(y)\mathbb{P}^\star_S(y+s-x)}{\mathbb{P}^\star_{S-X}(s-x)}$$

- Stationary and Memoryless: $q_t(y_t|x^t,s^t) = q(y_t|x_t,s_t)$
- Invariance: $S_1 \sim \mathbb{P}^\star_S(\cdot)$ then $S_t \sim \mathbb{P}^\star_S(\cdot)$ and $S_t \perp Y^{t-1}$
- $\mathbb{P}_Y(\cdot)$ must have the same support as $\mathbb{P}_X(\cdot)$. Thus it suffices to use $\mathcal{Y} = \mathcal{X}$.

Remarks

Properties of Optimal Policy:

$$q^\star(y|x,s) = \frac{\mathbb{P}_X(y)\mathbb{P}^\star_S(y+s-x)}{\mathbb{P}^\star_{S-X}(s-x)}$$

- Stationary and Memoryless: $q_t(y_t|x^t,s^t) = q(y_t|x_t,s_t)$
- Invariance: $S_1 \sim \mathbb{P}^\star_S(\cdot)$ then $S_t \sim \mathbb{P}^\star_S(\cdot)$ and $S_t \perp Y^{t-1}$
- $\mathbb{P}_Y(\cdot)$ must have the same support as $\mathbb{P}_X(\cdot)$. Thus it suffices to use $\mathcal{Y} = \mathcal{X}$.

Example:

- Binary System $\mathcal{X} = \mathcal{Y} = \mathcal{S} = \{0,1\}$
- Equiprobable Input: $\mathbb{P}_X(X=0) = \mathbb{P}_X(X=1) = 1/2$
- $\mathbb{P}^\star_{S_1}(S_1=0) = \mathbb{P}^\star_{S_1}(S_1=1) = 1/2$
- $q^\star(Y_1=0|X_1=S_1) = q^\star(Y_1=1|X_1=S_1) = 1/2$

Stationary Posterior Policies

Definition (Invariance property)

Given an initial battery state distribution $\mathbb{P}_{S_1}$, a stationary memoryless policy $\mathbf{q}$ satisfies the invariance property if

$$\mathbb{P}^{\mathbf{q}}(S_2 = s_2 | Y_1 = y_1) = \mathbb{P}_{S_1}(S_1 = s_2), \ \forall s_2 \in \mathcal{S}, y_1 \in \hat{\mathcal{Y}}$$

where $\hat{\mathcal{Y}} := \{y : P_{Y_1}(y_1) > 0\}$. We call such a policy as a **Stationary Posterior Policy**.

Stationary Posterior Policies

Definition (Invariance property)

Given an initial battery state distribution $\mathbb{P}_{S_1}$, a stationary memoryless policy $\mathbf{q}$ satisfies the invariance property if

$$\mathbb{P}^{\mathbf{q}}(S_2 = s_2 | Y_1 = y_1) = \mathbb{P}_{S_1}(S_1 = s_2), \ \forall s_2 \in \mathcal{S}, y_1 \in \hat{\mathcal{Y}}$$

where $\hat{\mathcal{Y}} := \{y : P_{Y_1}(y_1) > 0\}$. We call such a policy as a **Stationary Posterior Policy**.

Lemma

For a stationary posterior policy:

$$L_\infty(\mathbf{q}) = I^{\mathbf{q}}(S_1, X_1; Y_1),$$

where $(S_1, X_1, Y_1) \sim \mathbb{P}_{S_1}(s_1)\mathbb{P}_X(x_1)q(y_1|x_1, s_1)$.

Stationary Posterior Policies

Lemma

An initial battery distribution $\mathbb{P}_{S_1}$ *and a stationary memoryless policy* $\mathbf{q} = (q, q, \dots)$ *satisfies the invariance property iff for each* $(s_2, y_1) \in \mathcal{S} \times \mathcal{X}$*, we have*

$$\mathbb{P}_{S_1}(s_2)\mathbb{P}_X(y_1) = \sum_{(\tilde{x}_1, \tilde{s}_1) \in \mathcal{D}(s_2 - y_1)} q(y_1 | \tilde{x}_1, \tilde{s}_1)\mathbb{P}_X(\tilde{x}_1)\mathbb{P}_{S_1}(\tilde{s}_1).$$

where

$$\mathcal{D}(w) := \{(x, s) \in \mathcal{X} \times \mathcal{S} : s - x = w\}.$$

Optimal Stationary Posterior Policy

Lemma (Optimal stationary posterior policy)

Given a fixed $\mathbb{P}_{S_1}$ the optimal policy satisfying the invariance property is

$$q^*(y|x,s) = \frac{\mathbb{P}_X(y)\mathbb{P}_{S_1}(y+s-x)}{\mathbb{P}_{S_1-X_1}(s-x)}$$

achieving a leakage rate of

$$L_\infty(\mathbf{q}^*) = I(S_1 - X_1; X_1)$$

where $(S_1, X_1) \sim \mathbb{P}_{S_1}(s_1)Q(x_1)$.

Converse

$$I(S_1, X^T; Y^T) = \sum_{t=1}^{T} I(S_1, X^T; Y_t | Y^{t-1})$$

$$= \sum_{t=1}^{T} I(S_1, X^t; Y_t | Y^{t-1}) \qquad \text{(Causality)}$$

$$= \sum_{t=1}^{T} I(S^t, X^t; Y_t | Y^{t-1}) \qquad (S_{t+1} = S_t - X_t + Y_t)$$

$$\geq \sum_{t=1}^{T} I(S_t, X_t; Y_t | Y^{t-1}) \qquad (I(\ ;\ ) \geq 0)$$

$$\geq \sum_{t=1}^{T} I(S_t - X_t; Y_t | Y^{t-1}) \qquad \text{(Data Processing Inequality)}$$

Converse

Lemma

If X_t is i.i.d. and $S_{t+1} = S_t - X_t + Y_t$ then:

$$I(S_t - X_t; Y_t | Y^{t-1}) = H(S_t - X_t | Y^{t-1}) - H(S_{t+1} - X_{t+1} | Y^t, X_{t+1})$$

$$\begin{aligned}
I(S_t - X_t; Y_t | Y^{t-1}) &= H(S_t - X_t; Y_t | Y^{t-1}) - H(S_t - X_t | Y^t) \\
&= H(S_t - X_t | Y^{t-1}) - H(S_t - X_t + Y_t | Y^t) \\
&= H(S_t - X_t | Y^{t-1}) - H(S_{t+1} | Y^t) \\
&= H(S_t - X_t | Y^{t-1}) - H(S_{t+1} | Y^t, X_{t+1}) \\
&= H(S_t - X_t | Y^{t-1}) - H(S_{t+1} - X_{t+1} | Y^t, X_{t+1})
\end{aligned}$$

Converse

$$I(S_1, X^T; Y^T) \geq \sum_{t=1}^{T} I(S_t - X_t; Y_t | Y^{t-1})$$

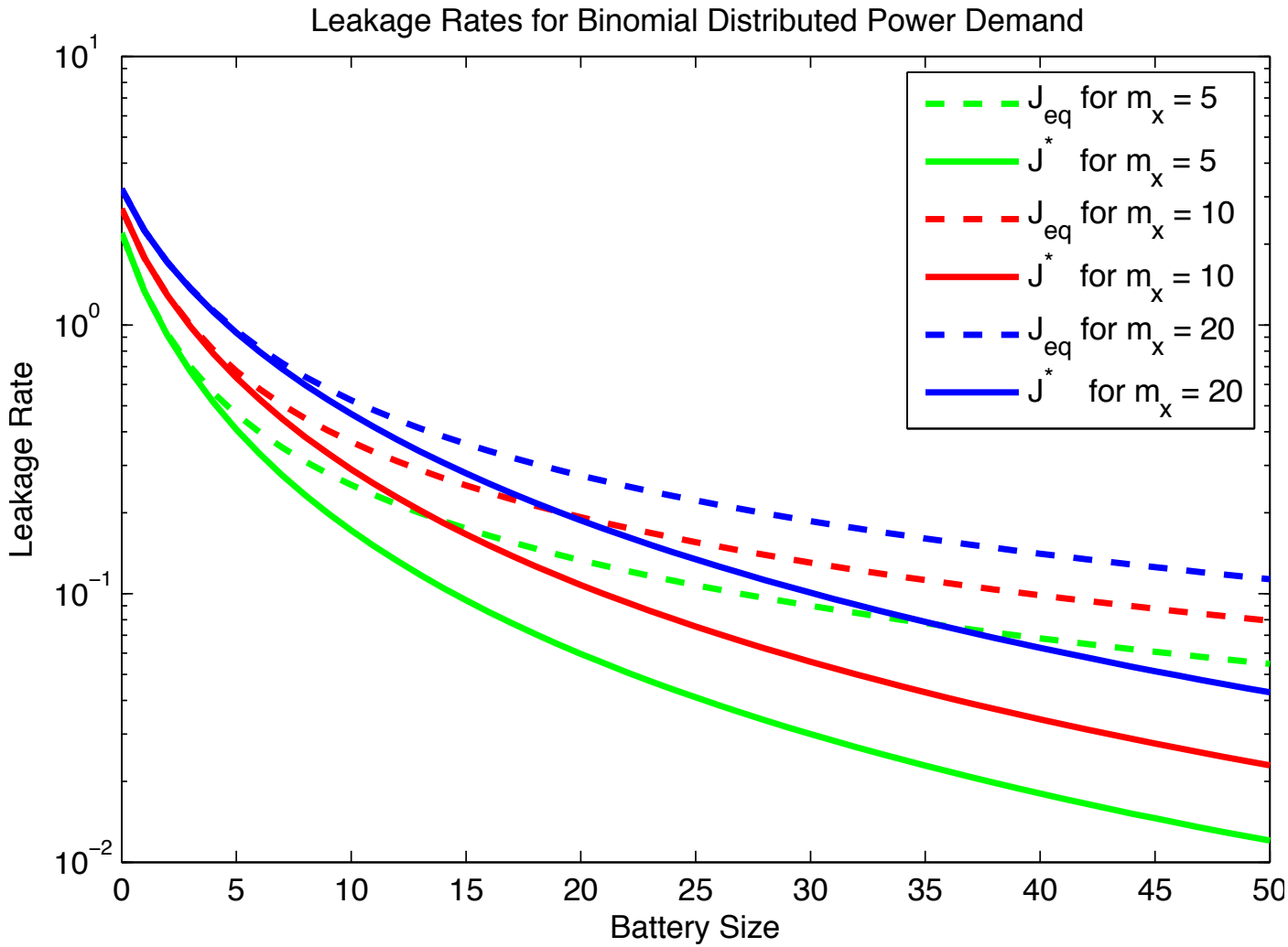
$$\geq H(S_1 - X_1) + \sum_{t=2}^{T} I(S_t - X_t; X_t | Y^{t-1}) - H(S_T - X_T | Y^T)$$

$$L_\infty^* = \min_{\mathbf{q} \in \mathcal{Q}_A} \lim_{T \to \infty} \frac{1}{T} I^{\mathbf{q}}(S_1, X^T; Y^T)$$

$$\geq \min_{\mathbf{q} \in \mathcal{Q}_A} \lim_{T \to \infty} \frac{1}{T} \left[\sum_{t=2}^{T} I^{\mathbf{q}}(S_t - X_t; X_t | Y^{t-1}) \right]$$

$$\geq \min_{\theta \in \mathcal{P}_S} I(S - X; X)$$

Numerical Example: Binomial distributed power demand



Conclusions

- Information Theoretic Privacy in Smart Metering Systems with a Rechargeable Battery
- Single-Letter Expression for Optimal Leakage Rate for i.i.d. Sources
- Optimal Policy is Stationary, Memoryless, and satisfies an Invariance Property
- Suffices to restrict $\mathcal{Y} = \mathcal{X}$ without loss of loss of optimality.

Future work and open problems:

- Markov power demand
- Other extensions (e.g. Multiuser Systems, Energy Harvesting etc.)