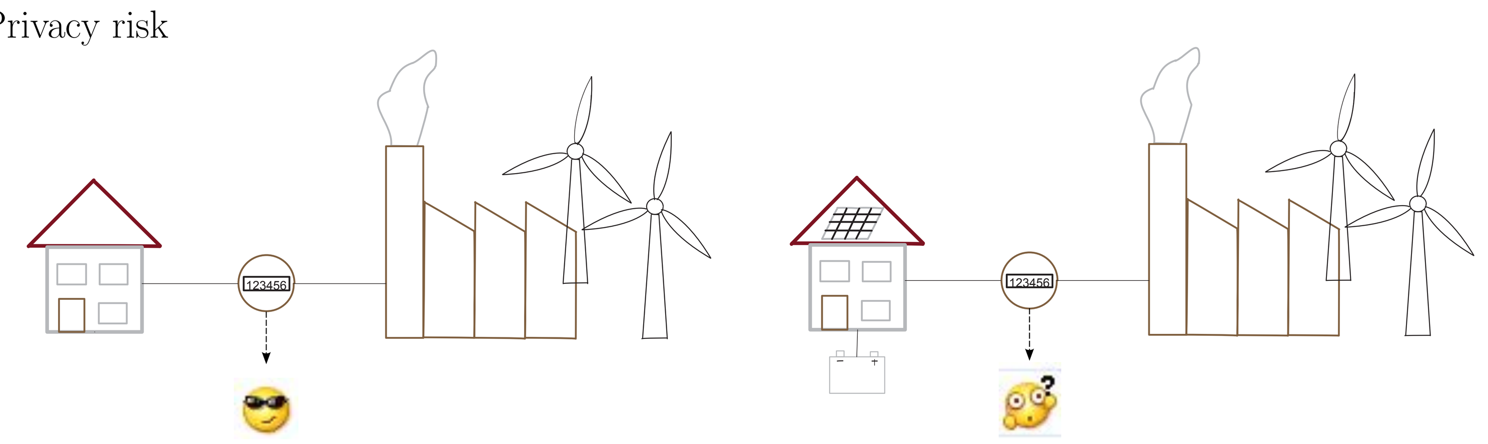
# Study on Smart Meter Privacy

Zuxing Li and Tobias J. Oechtering
School of Electrical Engineering and the ACCESS Linnaeus Centre
KTH Royal Institute of Technology, Stockholm, Sweden
{zuxing,oech@kth.se}

## 1 Motivation

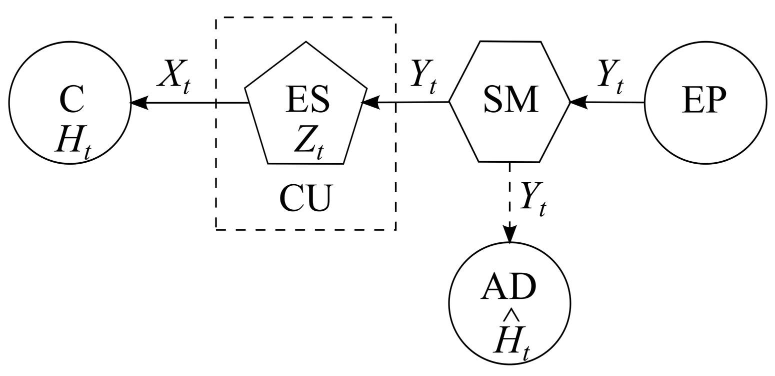
Smart grid
- Monitor the grid more granularly.
- Predicate demand; detect failure; and adapt pricing.
- A more adaptive, reliable, and efficient grid

Smart meter
- Utility
- Privacy risk



State of arts
- Encryption
  - Do not work in the case of having inner threats.
- Distortion
  - Distort the energy supply from energy demand profile.
  - Use alternative energy sources or energy storage devices.
  - Information theoretic objective to maximize adversary uncertainty about the energy demand profile [1, 2, 3, 4, 6, 7]
  - Online algorithm to flatten smart meter readings [5]
  - Belief state MDP formulation [6, 7, 9]
  - Detection theoretic objectives [8, 9]

## 2 Belief State MDP Formulation




Settings
- Control strategy: $p_{Y_t|X_t,Z_t}$ under a constraint $z_t - z_{t+1} + y_t = x_t$
- Markov property:

$$P_{H_{t+1},X_{t+1},Z_{t+1},Y_{t+1}|H^t,X^t,Z^t,Y^t} = p_{Y_{t+1}|X_{t+1},Z_{t+1}} \cdot p_{X_{t+1}|H_{t+1},X_t} \cdot p_{Z_{t+1}|X_t,Z_t} \cdot p_{H_{t+1}|H_t}$$

- Instantaneous privacy leakage:

$$r_t = \sum_{y_t} \left\{ \min_{\hat{h}_t} \sum_{h_t,x_t,z_t} c(\hat{h}_t, h_t) p_{Y_t|X_t,Z_t}(y_t|x_t,z_t) p_{H_t,X_t,Z_t}(h_t,x_t,z_t) \right\}$$

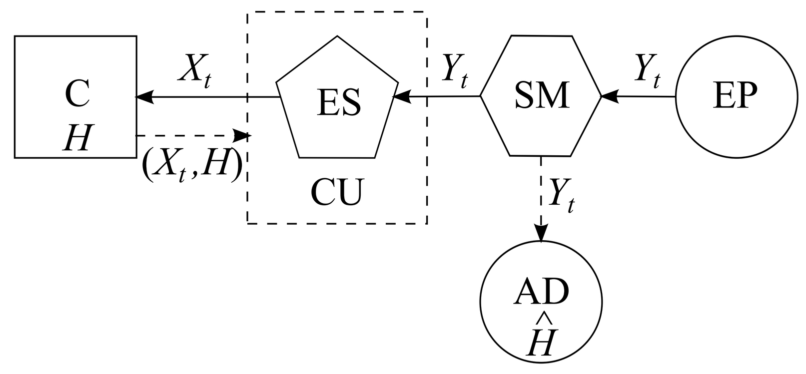
  - Informed and greedy adversary
  - Bayesian detection model of adversary behavior

Belief state MDP elements
- State: $s_t = (h_t, x_t, z_t)$
- Belief state: $b_t = p_{H_t,X_t,Z_t}$
- Action: $a_t = p_{Y_t|X_t,Z_t}$
- Reward: $r_t(b_t, a_t)$
- Policy: $\delta_t : b_t \to a_t$
- Belief state transition: $Pr(b_{t+1}|b_t, a_t)$

On observing (calculating) the belief state $b_t$, $a_t$ is determined based on $\delta_t$. Then, the next belief state $b_{t+1}$ can be calculated (observed) and the reward $r_t$ can be determined.

A privacy-preserving control design in belief state MDP formulation
- Let $\Delta = \{\delta_0, \delta_1, \dots\}$.
- Let $V = \sum_{t=0}^{\infty} \beta^t r_t$ where $0 \le \beta < 1$.
- A privacy-preserving objective: Optimize $\Delta$ to maximize $V$.
- Bellman equation: $V(\Delta^*, b_t) = \max_{a_t}\{r_t(b_t,a_t) + \beta V(\Delta^*, b_{t+1})\}$
  - If the solution exists, there is a stationary optimal policy, i.e., $\delta_t^* = \delta^*$.
  - $\delta^* : b_t \to a_t^*$
  - Established computational methods

## 3 Use an Infinite-Capacity Energy Storage Device




Settings
- Binary hypothesis
- "Ideal" infinite-capacity energy storage device
  - Instantaneous demand $x_t$ is always satisfied.
  - Asymptotic balance: $\lim_{n\to\infty} \sum_{t=1}^{n}(x_t - y_t) = 0,\ \forall h$
  - Law of large numbers leads to average energy supply constraints:

$$\mathrm{E}(Y|H=h_0) = f_0;\ \mathrm{E}(Y|H=h_1) = f_1.$$

- Control strategy: $p_{Y_t|X_t,H}$
- Markov property:

$$p_{X_{t+1},Y_{t+1}|X^t,Y^t,H} = p_{Y_{t+1}|X_{t+1},H} \cdot p_{X_{t+1}|H}$$

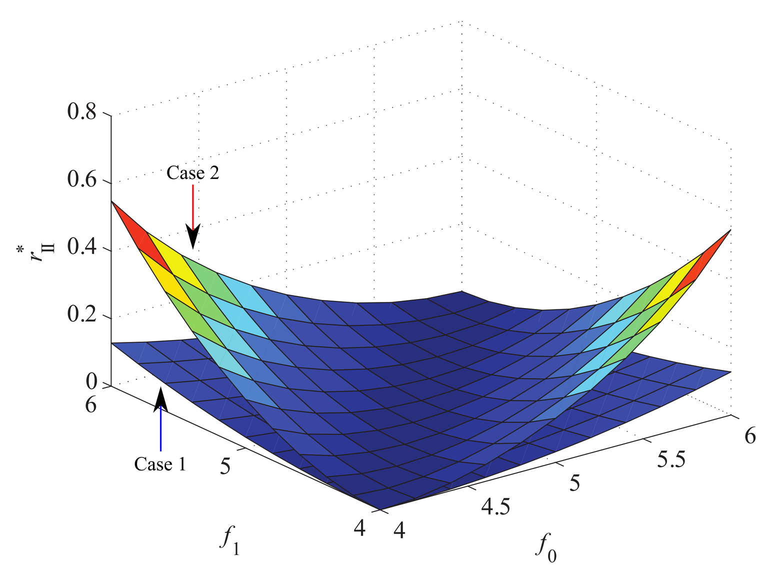
- Assumptions on the adversary
  - Informed and greedy adversary
  - Neyman-Pearson hypothesis testing model of adversary behavior:

$$p^{\min}_{\hat{H}|H}(h_0|h_1) = \min p_{\hat{H}|H}(h_0|h_1),\ \text{s.t. } p_{\hat{H}|H}(h_1|h_0) \le \phi$$

Asymptotic measure of privacy leakage risk
- Chernoff-Stein Lemma: The Kullback-Leibler divergence $\mathrm{D}(p_{Y|H=h_0}||p_{Y|H=h_1})$ is the asymptotic exponential decay rate of $p^{\min}_{\hat{H}|H}(h_0|h_1)$.
- Privacy leakage metric: $r^*_{\mathrm{II}} = \mathrm{D}(p_{Y|H=h_0}||p_{Y|H=h_1})$
  - Reducing $r^*_{\mathrm{II}}$ means that the adversary needs more observations to achieve a certain value of $p^{\min}_{\hat{H}|H}(h_0|h_1)$ from an asymptotic perspective.

Optimal privacy-preserving control design
- Optimize $p_{Y_t|X_t,H}$ to minimize $r^*_{\mathrm{II}}$ and to satisfy average energy supply constraints.
- Results about $p^*_{Y_t|X_t,H}$:
  - Energy control depends on $H$ only such that $p^*_{Y_t|X_t,H}$ is a constant given $(y_t, h)$.
  - $|\mathcal{Y}^*| \le 2$.
  - If $|\mathcal{Y}^*| = 2$, $\mathcal{Y}^* = \{y_{\min}, y_{\max}\}$.

Numerical illustration




- Assumptions:
  - $f_0, f_1 \in [4, 6]$
  - Case 1: $y_{\min} = 1$, $y_{\max} = 9$
  - Case 2: $y_{\min} = 3$, $y_{\max} = 7$
- Two ways to suppress the privacy risk:
  - Increase the difference $y_{\max} - y_{\min}$.
  - Decrease the difference $|f_0 - f_1|$.

## References

[1] D. Varodayan and A. Khisti,"Smart meter privacy using a rechargeable battery: Minimizing the rate of information leakage," in *Proc. of ICASSP 2011*, 2011, pp. 1932-1935.

[2] L. Sankar, S. R. Rajagopalan, S. Mohajer, and H. V. Poor, "Smart meter privacy: A theoretical framework," *IEEE Transactions on Smart Grid*, vol. 4, no. 2, pp 837-846, 2013.

[3] D. Gündüz and J. Gomez-Vilardebo, "Smart meter privacy in the presence of an alternative energy source," in *Proc. of ICC 2013*, 2013, pp. 2027-2031.

[4] O. Tan, D. Gündüz, and H. V. Poor, "Increasing smart meter privacy through energy harvesting and storage devices," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1331-1341, 2013.

[5] L. Yang, X. Chen, J. Zhang, and H. V. Poor, "Optimal privacy-preserving energy management for smart meters," in *Proc. of INFOCOM 2014*, 2014, pp. 513-521.

[6] J. Yao and P. Venkitasubramaniam, "On the privacy-cost tradeoff of an in-home power storage mechanism," in *Proc. of Allerton 2013*, 2013, pp. 115-122.

[7] S. Li, A. Khisti, and A. Mahajan, "Structure of optimal privacy-preserving policies in smart-metered systems with a rechargeable battery," in *Proc. of SPAWC 2015*, 2015, pp. 375-379.

[8] Z. Li and T. J. Oechtering, "Privacy on hypothesis testing in smart grids," accepted at ITW 2015 Fall.

[9] Z. Li, T. J. Oechtering, and M. Skoglund, "Privacy-preserving energy flow control in smart grids," submitted at ICASSP 2016.