Privacy-Preserving Energy Flow Control in Smart Grids

Zuxing Li, Tobias J. Oechtering, and Mikael Skoglund

School of Electrical Engineering and the ACCESS Linnaeus Centre
KTH Royal Institute of Technology, Stockholm, Sweden

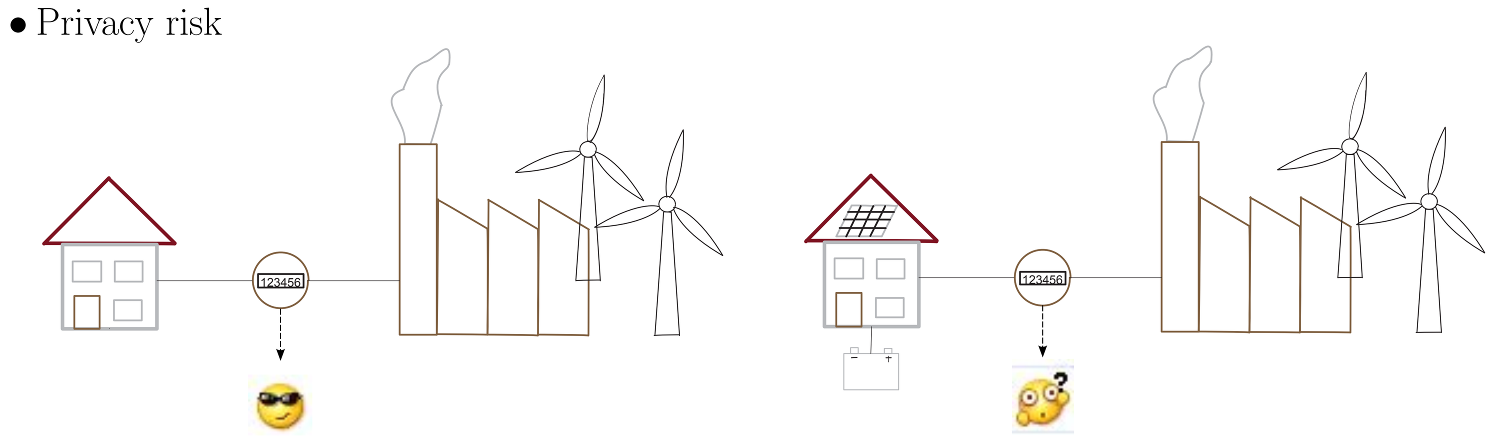
1 Motivation

Smart grid

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

Smart meter

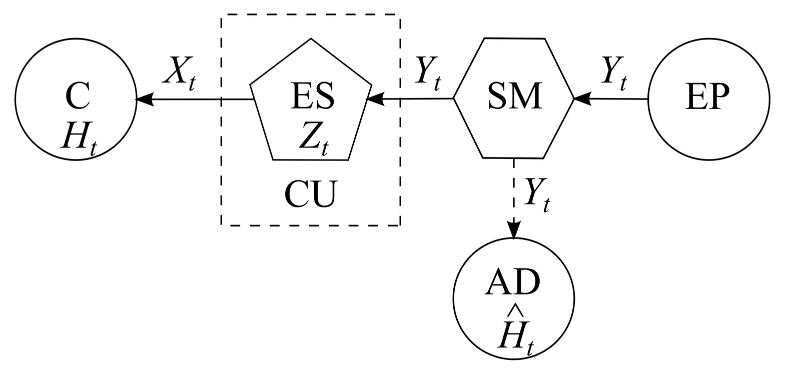
- Utility
- Privacy risk



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]
  - Detection theoretic objective [8]

2 Smart Grid Model



Settings

- H_t, $\hat{H}_t$, X_t, Y_t, and Z_t are defined on finite sets.
- Control strategy: $p_{Y_t|X_t,Z_t}$ under a constraint $z_t - z_{t+1} + y_t = x_t$
- Markov property:

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

3 Bayesian-Detection Operational Privacy Leakage

Assumptions

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

Instantaneous privacy leakage

- **Minimal Bayesian risk** of the adversary to infer on the hypothesis H_t:

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

4 Optimal Energy Flow Control

Optimal privacy-preserving design

$$\left\{p^*_{Y_t|X_t,Z_t}\right\}_{t=0}^{\infty} = \arg\max_{\{p_{Y_t|X_t,Z_t}\}_{t=0}^{\infty}} V$$

- Accumulated discounted minimal Bayesian risk: $V = \sum_{t=0}^{\infty} \beta^t \cdot r_t$ where $0 \le \beta < 1$
- Current control strategy affects the future as

$$p_{H_{t+1},X_{t+1},Z_{t+1}|H_t,X_t,Z_t} = p_{Z_{t+1}|X_t,Z_t} \cdot p_{X_{t+1}|H_{t+1},X_t} \cdot p_{H_{t+1}|H_t}.$$

How to solve it?

- View it as a **belief state Markov decision process**.
  - State: $s_t = (h_t, x_t, z_t) \in \mathcal{S}$
  - Belief state: $b_t = p_{H_t,X_t,Z_t} \in \mathcal{B}$
  - Action: $a_t = p_{Y_t|X_t,Z_t} \in \mathcal{A}$
  - Reward: $r_t(b_t, a_t)$
  - Policy: $\delta_t : \mathcal{B} \to \mathcal{A}$
  - Belief state update: $b_{t+1}(s_{t+1}) = \sum_{s_t \in \mathcal{S}} Pr(s_{t+1}|s_t) \cdot b_t(s_t)$

  Define $\Delta = \{\delta_0, \delta_1, \dots\}$. Then,

$$\Delta^* = \arg\max_{\Delta} V(\Delta, b_0), \text{ for all } b_0 \in \mathcal{B}.$$

- **Bellman's principle of optimality**

  For all $t \in \{0, 1, \dots\}$ and all $b \in \mathcal{B}$,

$$V(\Delta^*, b) = \max_{a \in \mathcal{A}} r_t(b, a) + \beta \cdot V(\Delta^*, b'(b, a)),$$
$$\delta^*_t(b) = \arg\max_{a \in \mathcal{A}} r_t(b, a) + \beta \cdot V(\Delta^*, b'(b, a)).$$

- Optimal privacy-preserving energy control strategies
  - Established algorithms to solve Δ^* and $V(\Delta^*, b_0)$
  - With b_0 and Δ^*, solve $\left\{p^*_{Y_t|X_t,Z_t}\right\}_{t=0}^{\infty}$ and $\{b_t\}_{t=1}^{\infty}$ successively.

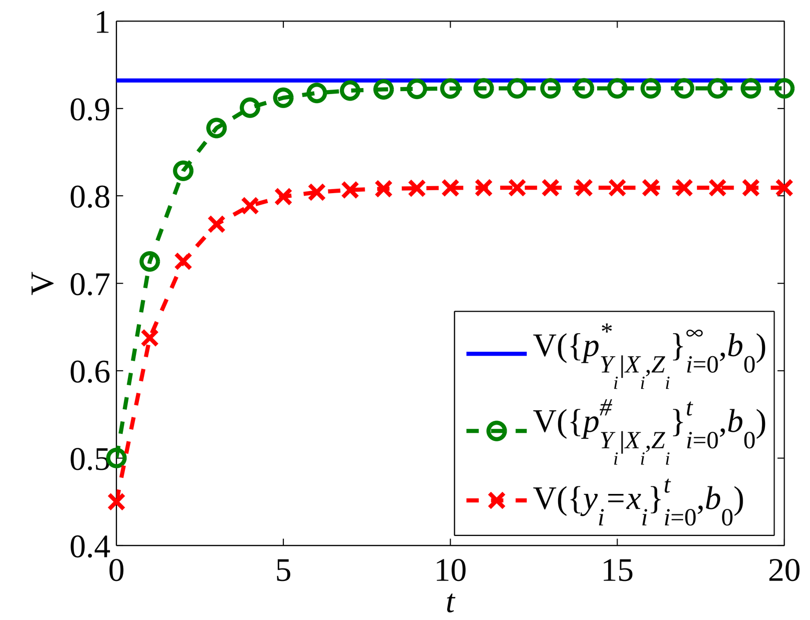
5 Instantaneous Energy Flow Control

Instantaneous privacy-preserving energy control strategy

$$p^{\#}_{Y_t|X_t,Z_t} = \arg\max_{p_{Y_t|X_t,Z_t} \in \mathcal{A}} r_t\left(b_t\left(b_0, \left\{p^{\#}_{Y_i|X_i,Z_i}\right\}_{i=0}^{t-1}\right), p_{Y_t|X_t,Z_t}\right)$$

- Ignore the impact of the current control strategy on the future.
- With b_0, solve $\left\{p^{\#}_{Y_t|X_t,Z_t}\right\}_{t=0}^{\infty}$ and $\{b_t\}_{t=1}^{\infty}$ successively.
- The optimization of instantaneous privacy-preserving energy control strategy $p^{\#}_{Y_t|X_t,Z_t}$ can be equivalently reformulated as a set of linear programmings.

6 Numerical Result



Settings

- Binary hypothesis H_t, e.g., "in" or "out"
- $x_t \in \{0, u\}$, $z_t \in \{0, u, 2u\}$, and $y_t \in \{0, u, 2u, 3u\}$
- $c(\hat{h}_t, h_t) = 0$ if $\hat{h}_t = h_t$; otherwise, $c(\hat{h}_t, h_t) = 1$. Then, r_t is the minimal probability of error of the adversary to infer on H_t.
- $\beta = 0.5$

An upper bound:

$$V\left(\left\{p^*_{Y_i|X_i,Z_i}\right\}_{i=0}^{\infty}, b_0\right) \le 1$$

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," in *Proc. of ITW 2015 Fall*, 2015, pp. 337-341.