On design of optimal smart meter privacy control strategy against adversarial MAP detection

Ramana Avula, and Tobias Oechtering

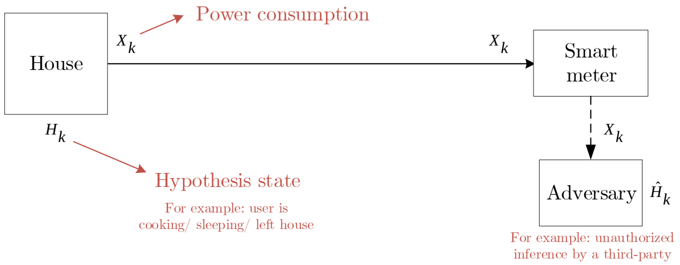
KTH Royal Institute of Technology, Sweden.

45th International Conference on Acoustics, Speech, and Signal Processing (ICASSP)

May 4-8, 2020

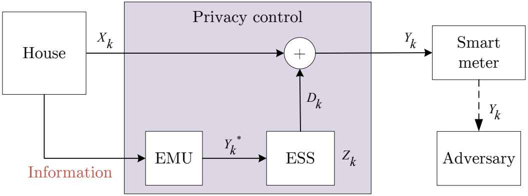
Overview

Smart meter privacy problem



- Patterns in $\{\hat{H}_k\}$ can be used to infer, for example, **religious, economic and social identities** of users.
- In Europe, GDPR regulates collecting, storing, or processing of data with sensitive personal information.

Privacy-by-design



Existing studies design EMU based on:

- **Information theory:** Variance[1], Mutual information[2,3,4] etc,
- **Detection theory:** Bayesian hypothesis testing adversary[5,6,7].

Our previous work[6,7] focused on including real ESS aspects in EMU design.

---

[1] G. Kalogridis, C. Efthymiou, S. Z. Denic, *et al.*, "Privacy for smart meters: Towards...," in *SmartGridComm*, 2010.

[2] D. Varodayan and A. Khisti, "Smart meter privacy using a rechargeable battery...," in *ICASSP*, 2011.

[3] O. Tan, D. Gunduz, and H. V. Poor, "Increasing smart meter privacy...," *IEEE Jour. on Sel. Areas in Comm.*, 2013.

[4] J.-X. Chin, T. T. De Rubira, and G. Hug, "Privacy-protecting energy management...," *IEEE Tran. on Smart Grid*, 2017.

[5] Z. Li, T. J. Oechtering, and M. Skoglund, "Privacy-preserving energy flow...," in *ICASSP*, 2016.

[6] R. R. Avula, T. J. Oechtering, and D. Månsson, "Privacy-preserving smart meter control...," in *ISGT-Europe*, 2018.

[7] R. R. Avula, J.-X. Chin, T. J. Oechtering, *et al.*, "Smart meter privacy control...," in *IEEE Powertech, Milan, Italy, 2019*.

Problem formulation

- **System model:** HMM characterized by $\big(\underbrace{\mathcal{H}, \mathcal{X}}_{\text{alphabets}}, \underbrace{P_{H_k|H_{k-1}}, P_{X_k|H_k}}_{\text{HMM parameters}}\big)$.
- **Privacy model:** Adversarial maximum a posteriori (MAP) detection

$$\begin{aligned}\hat{h}_1^N(y_1^N) &= \underset{h_1^N \in \mathcal{H}^N}{\operatorname{argmax}} P_{H_1^N, Y_1^N}(h_1^N, y_1^N) \\ &= \underset{h_1^N \in \mathcal{H}^N}{\operatorname{argmax}} \sum_{k=1}^{N} \log \Big[P_{H_k, Y_k | H_{k-1}}(h_k, y_k | h_{k-1}) \Big].\end{aligned}$$

- **How to optimally control adversarial MAP detection performance?**
- **Design approach:** Stochastic optimal control of avg. detection cost, known as *Bayesian risk*, in EMU-unaware and -aware adversarial cases.

Optimal control of EMU-unaware MAP detection

- MAP estimate can be obtained using Viterbi (non-causal) algorithm.
- In the controller design, we compute a causal detection strategy ζ_k^* that achieves avg. Viterbi performance using dynamic programming:

Per-step reward: $$r_k(x_k, \hat{h}_{k-1}^k) := \max\Big[\log\Big[P_{H_k, X_k | H_{k-1}}(\hat{h}_k, x_k | \hat{h}_{k-1})\Big], r_{\mathsf{min}}\Big],$$

Aggregate reward: $$V_k(x_k, \hat{h}_{k-1}) := \max_{\hat{h}_k \in \mathcal{H}}\Big[r_k(x_k, \hat{h}_{k-1}^k) + \mathbb{E}\big[V_{k+1}(X_{k+1}, \hat{h}_k)\big]\Big].$$

- The optimal control strategy μ_k^* computed using the dynamic programming[8]:

Per-step cost: $$c_k(w_k, y_k, \zeta_k^*) := f_c(h_k, \zeta_k^*(y_k, \hat{h}_{k-1})),$$

Aggregate cost: $$J_k(w_k) := \min_{y_k \in \mathcal{Y}}\Big[c_k(w_k, y_k, \zeta_k^*) + \mathbb{E}\big[J_{k+1}\left(W_{k+1}\right)\big]\Big].$$

- Discrete state and action spaces $\implies$ **discrete optimization**.

[8] **Controller state:** $w_k = \{x_k, z_k, h_k, \hat{h}_{k-1}\}$

Optimal EMU-aware MAP detection

- The adversarial belief state $\hat{\pi}_k$ on the state $s_k = f_s(h_k, z_{k+1})$ is

$$\hat{\pi}_k = \frac{\mathbf{M}_k\Big(y_k, \hat{h}_{k-1}, \mu_k\Big)\hat{\pi}_{k-1}}{\mathbf{1}_{|\mathcal{H}|}^{\mathsf{T}}\mathbf{M}_k\Big(y_k, \hat{h}_{k-1}, \mu_k\Big)\hat{\pi}_{k-1}}; \quad [\hat{\pi}_k]_s = P_{S_k|Y_1^k}(s|y_1^k),$$

  where $\mathbf{M}_k$ is belief transformation matrix function given by the HMM.
- The optimal detection strategy $\bar{\zeta}_k^*$ computed using dynamic programming[9]:

$$\textbf{Per-step reward:} \quad \tilde{r}_k(\gamma_k, \hat{h}_k, \mu_k) := \max\left[\log\left[\frac{\mathbf{a}^{\mathsf{T}}\Big(y_k, \hat{h}_{k-1}^k, \mu_k\Big)\,\hat{\pi}_{k-1}}{\mathbf{b}^{\mathsf{T}}\Big(\hat{h}_{k-1}, \mu_k\Big)\,\hat{\pi}_{k-1}}\right], r_{\min}\right],$$

$$\textbf{Aggregate reward:} \quad \tilde{V}_k(\gamma_k, \mu_k) := \max_{\hat{h}_k \in \mathcal{H}}\Big[\tilde{r}_k(\gamma_k, \hat{h}_k, \mu_k) + \mathbb{E}\big[\tilde{V}_{k+1}(\Gamma_{k+1}, \mu_{k+1})\big]\Big],$$

  where $\mathbf{a}, \mathbf{b}$ are vector functions given by the HMM.

[9] **Control strategy** $\mu_k : \mathcal{W} \to \mathcal{Y}$; **Adversarial state:** $\gamma_k := [y_k, \hat{h}_{k-1}, \hat{\pi}_{k-1}]$

Optimal control of EMU-aware MAP detection

- Similarly, the optimal control strategy $\bar{\mu}_k^*$ computed using the dynamic programming[10]:

$$\textbf{Per-step cost:} \quad \tilde{c}_k(\lambda_k, \mu_k, \bar{\zeta}_k^*) := f_c(h_k, \bar{\zeta}_k^*(\gamma_k, \mu_k)),$$

$$\textbf{Aggregate cost:} \quad \tilde{J}_k(\lambda_k) := \min_{\mu_k \in \mathcal{U}} \Big[\tilde{c}_k(\lambda_k, \mu_k, \bar{\zeta}_k^*) + \mathbb{E}\left[\tilde{J}_{k+1}(\Lambda_{k+1}) \right] \Big].$$

- **Challenges:**
  1. γ_k and λ_k contain $\hat{\pi}_{k-1} \implies$ **continuous optimization**.
  2. The aggregate adversarial reward $\tilde{V}_k$ is piecewise concave w.r.t. $\hat{\pi}_{k-1}$.

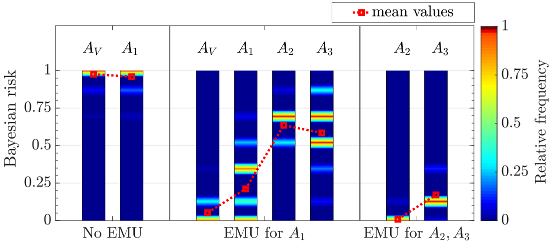
[10] **Controller state:** $\lambda_k = \{x_k, z_k, h_k, \hat{h}_{k-1}, \hat{\pi}_{k-1}\}$

Sub-optimal control: Adaptive-grid approximation algorithm

1. Find $\mathcal{Q}$, the partitions of the simplex $\Delta_{|\mathcal{S}|}$ using the hyperplanes $\{\pi \in \Delta_{|\mathcal{S}|} : (\mathbf{a}_i - \mathbf{a}_j)^\intercal \pi = 0\}$ for all possible vectors $\mathbf{a}_i, \mathbf{a}_j$ which gives per-step reward decision regions.
2. Recursively partition the simplex $\Delta_{|\mathcal{S}|}$ using $\mathcal{Q}$ and propagate them using all possible belief transformation matrices $\mathbf{M}_k$.
3. Approximate each resulting partition with a finite number of points and solve the dynamic programming equation at these finite points.

Numerical study

- Simulation study: binary states; $|\mathcal{K}| = 6$; risk = detection prob.; 2000 MC simulations, $P_{X_k|H_k} = \begin{bmatrix} 0.95 & 0.05 \\ 0.05 & 0.95 \end{bmatrix}$, $P_{H_k|H_{k-1}} = \begin{bmatrix} 0.01 & 0.9 \\ 0.99 & 0.1 \end{bmatrix}$.



  - EMU: Energy management unit
  - A_V : Standard Viterbi algorithm
  - A_1 : EMU-unaware causal adversary
  - A_2 : EMU-aware causal adversary (regular grid approx.)
  - A_3 : EMU-aware causal adversary (proposed suboptimal approx.)

Conclusion

- We have presented the design of an optimal control against an adversarial MAP detection.
- The optimal control strategy against EMU-unaware adversary can be computed efficiently by solving discrete optimization problems.
- Whereas, the optimal control against EMU-aware adversary becomes non-convex due to piece-wise concave structure of Bellman's equation. We presented a sub-optimal control strategy exploiting Bayesian evolution of belief state.
- Numerical study shows that the sub-optimal algorithm achieves close to the optimal performance.

Thank you!