TECHNISCHE UNIVERSITÄT DRESDEN

Smart Meter Privacy: A Theoretical Framework

Pedro Barbosa

May, 2013

Lalitha Sankar, S. Raj Rajagopalan, Soheil Mohajer and H. Vicent Poor

Smart Meter Privacy: A Theoretical Framework

IEEE Transactions on Smart Grid, 2012

Outline

- Introduction
- Model
- Utility-privacy tradeoff region
- Conclusion and future work

Introduction

- Current approaches lack a formal model of privacy and thus cannot answer some questions such as:
  - how much privacy is lost in such methods?
  - how much sensitive information can and should be left in the data so that it is still useful?

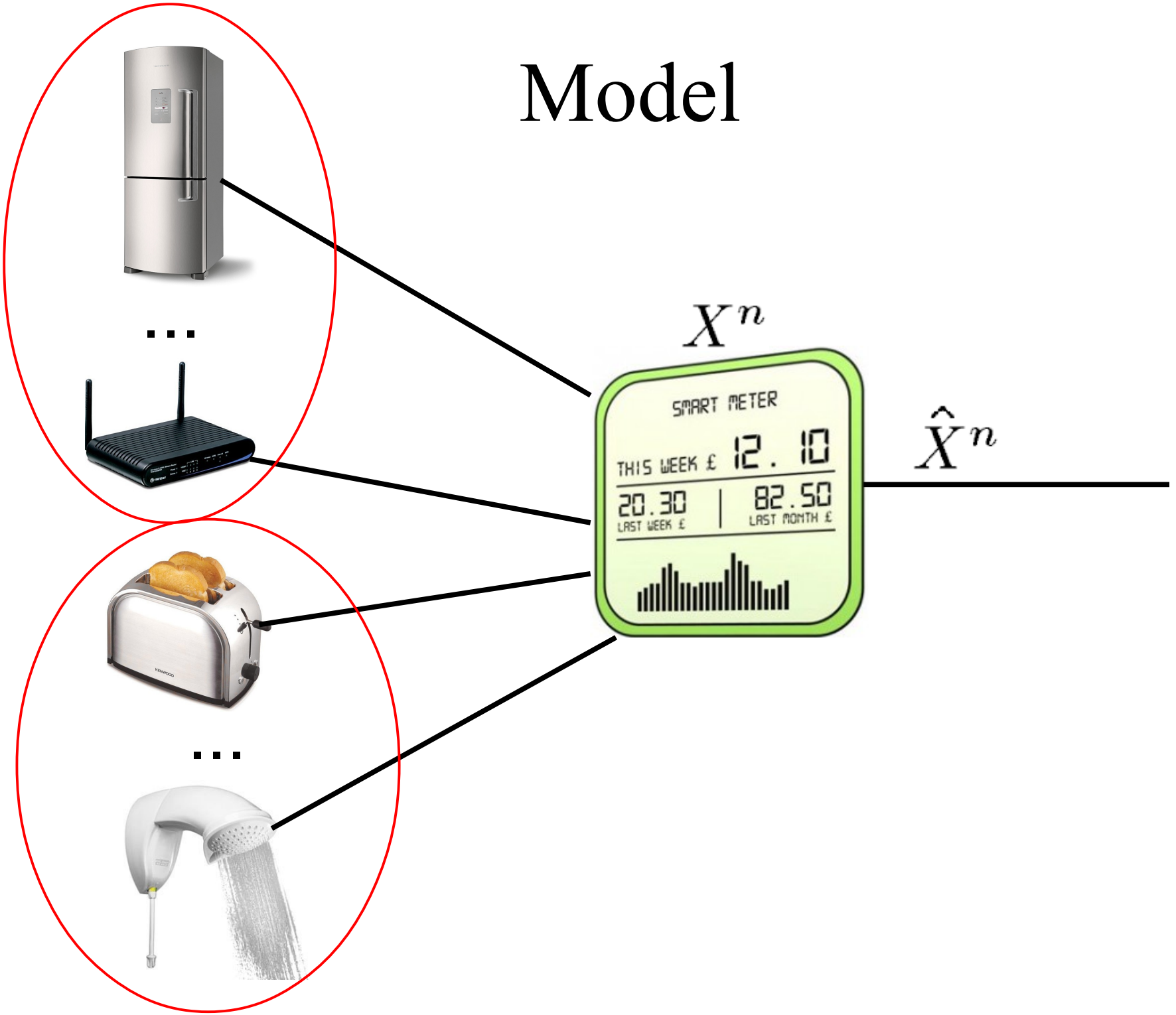
- In other words, current approaches to privacy only provide privacy assurances, but cannot provide any guarantees.

Introduction

- The paper presents a formal model
  - Hidden Markov model
  - Stationary Gaussian model

- Appliances are classified as:
  - Continuously (less revealing of personal details)
  - Intermittently (more revealing)

Model


X^n
SMART METER
THIS WEEK £ 12.10
20.30
LAST WEEK £
82.50
LAST MONTH £
$\hat{X}^n$

Model

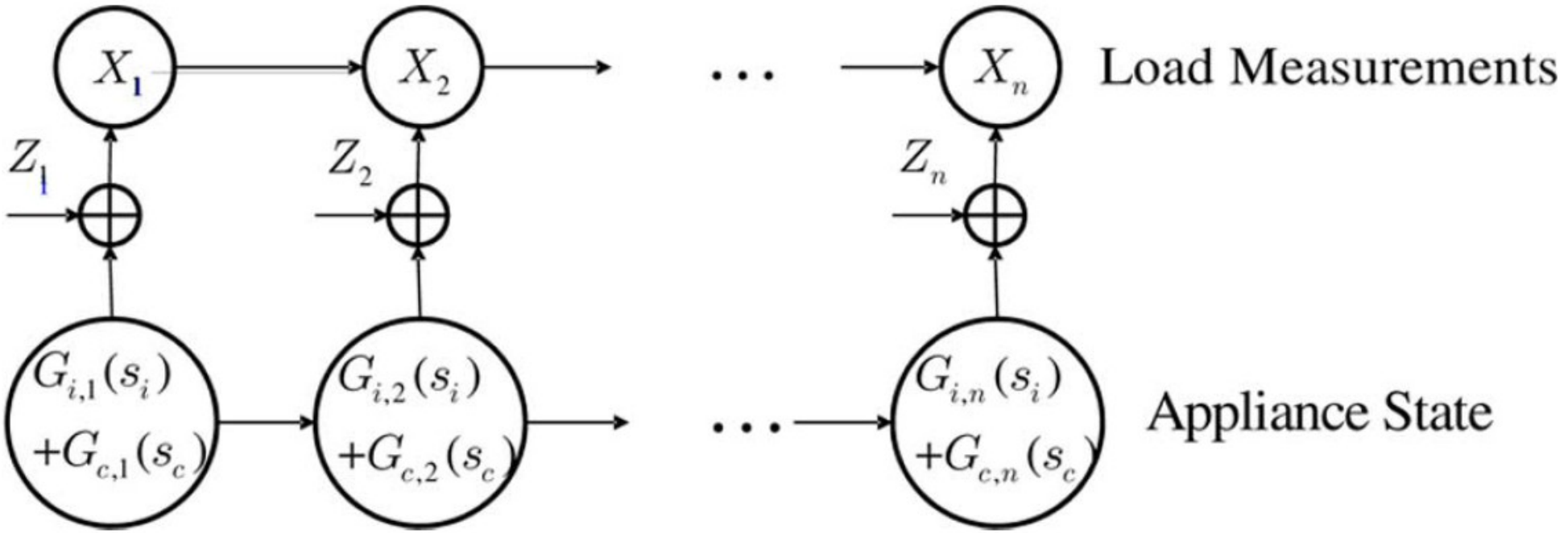


Fig. 2. Meter measurements obtained as a noisy sum of two Gaussian processes, corresponding to the intermittent and continous appliances, respectively over a time window of length n.

$$X^n(S) = G_c^n(S_c) + G_i^n(S_i) + Z^n$$

Utility and Privacy Metrics

- Utility metric is an average “distance” distortion function between the original and the perturbed data
  - e.g., mean-square error

- Privacy metric measures the difficulty of inferring private information leaked by the appliance state via the meter measurements
  - e.g., mutual information

Privacy-Preserving Mapping

- Formally, an (n, M, D, L) code involves an encoder and a decoder described below:
  - Encoding: $F_E : \mathcal{X}^n(\mathcal{S}) \to \mathcal{M} = \{1, 2, \ldots, 2^{nR}\}$
  - Decoding: $F_D : \mathcal{M} \to \hat{\mathcal{X}}^n.$
  - Desired utility: $D = \frac{1}{n} \sum_{k=1}^{n} \mathbb{E}[(X_k - \hat{X}_k)^2]$
  - Information leakage: $L = \frac{1}{n} I(Y^n; \hat{X}^n)$

Utility-Privacy Tradeoff Region

- The smart meter utility-privacy tradeoff region T: is the set of all pairs (D, L) such that, for every $\epsilon > 0$ and all sufficiently large n, there exists a coding scheme with parameters (n, M, D + ϵ, L + ϵ)

- for a desired D we seek to minimize the average number of bits-per-entry of the correlated sequence Y^n (that we wish to hide) that are leaked from the revealed sequence $\hat{X}^n$

Utility-Privacy Tradeoff Region

- The minimal leakage λ(D) achievable for a desired distortion D for a source with memory subject to distortion and leakage constraints is given by

$$\lambda(D) = \lim_{n\to\infty} \inf_{p(x^n,y^n)p(\hat{x}^n|x^n)} \frac{1}{n} I(Y^n;\hat{X}^n).$$

Privacy Preserving Spectral Waterfilling

- Specially, we seek to hide the intermittently used appliances:

$$L = \frac{1}{n} I(G_i^n; \hat{X}^n)$$

- Filtering out all frequencies that have power below a certain threshold (determined directly by λ)

Privacy Preserving Spectral Waterfilling

$$\Delta(f) = \begin{cases} 0; & F_i(f) < F_c(f) + \sigma^2; \text{ (or)} \\ & \lambda < F_c(f) + \sigma^2 < F_i(f) \\ D_1(f); & F_c(f) + \sigma^2 < \lambda < F_i(f) \\ D_2(f); & \lambda > F_i(f) > F_c(f) + \sigma^2 \end{cases}$$

where

$$D_1(f) = (\lambda - F_c(f) - \sigma^2)^+$$
$$D_2(f) = (F_i(f) - F_c(f) - \sigma^2)^+.$$

Conclusion

- The theoretical framework allows us to quantify the utility-privacy tradeoff in smart meter data.
- The privacy guarantee comes from the bound on information leakage while the utility guarantee come from the upper bound on the MSE
- The distortion model can be viewed as a filter on the load signal that suppresses those appliance (intermittent) signatures that reveal the most private information

Future Works

- Apply the model on measured data to validate whether the filter eliminates or decreases the signatures of intermittent devices to the desired degree.

- Another interesting avenue to explore would be to apply and demonstrate the power of these concepts in a practical context

TECHNISCHE UNIVERSITÄT DRESDEN

Smart Meter Privacy: A Theoretical Framework

Pedro Barbosa

May, 2013