# COnsumer-centric Privacy in smart Energy gridS (COPES)

PMG: T. Oechtering (KTH, coordinator), H. Sandberg (KTH),
D. Gunduz (ICL), C. Lauradoux (Inria), G. Hug (ETH)

Imperial College London

Inria

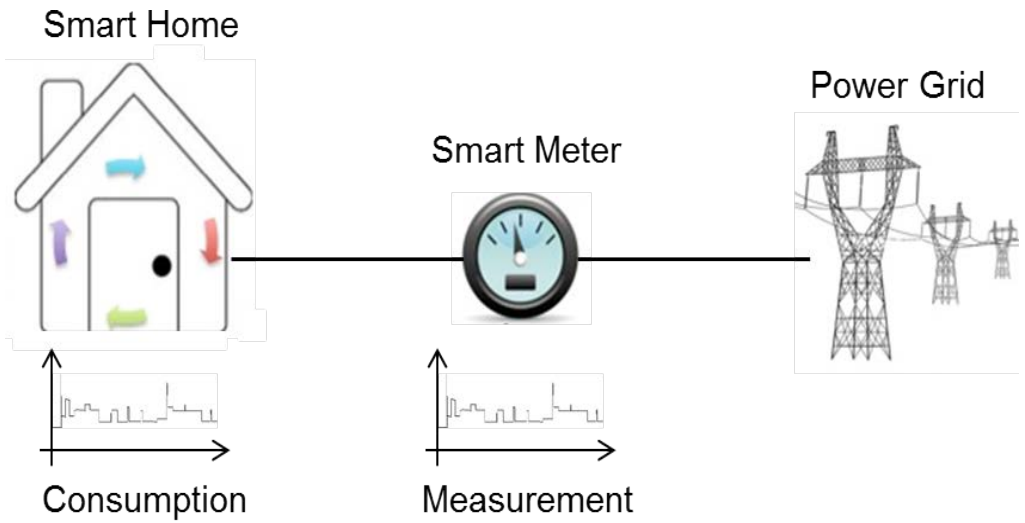
ETH

# Smart Meter Privacy Problem

"**Energy consumption reveals details of personal life**, in the most privacy-sensitive place – the home, and therefore smart metering has to strike a **careful balance** between detailed energy metering and privacy protection."

"Smart metering and privacy in Europe: lessons from the Dutch case"
by C. Cuijpers and B.-J. Koops (2012)
in European Data Protection: Coming of Age

Traditional: Privacy risk!!!



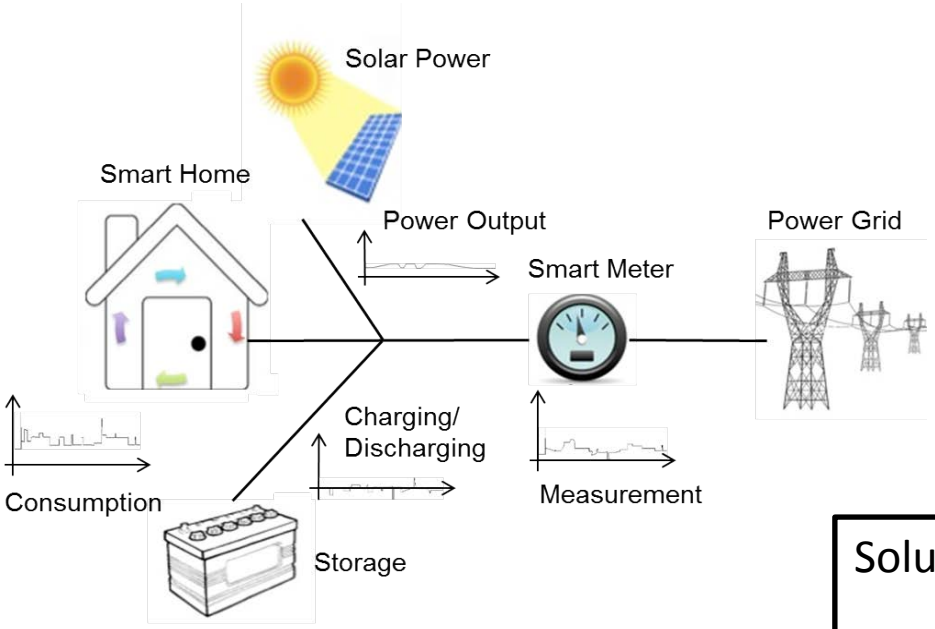
# Privacy can be a show stopper

- Article 8 of the European Convention on Human Rights protects private life of individuals
  - **Stopped the SM role out in the Netherland in 2009**

- Reform of data protection regulation – ***EU General Data Protection Regulation*** *(enforced 24/05/16, applies from 25/05/18)*
  - Guideline: Collection and processing of personal data has to be *reasonable* w.r.t. the purpose
  - Drastic fines for violation

- Consumer concerns in many European countries
  - E.g. Netherland, Germany, England, France
  - Privacy concerns **diminish technology acceptance**

# Innovative Approach of COPES




*Energy is a physical quantity, and the particular consumption pattern is what users deem private.*
=> **Energy flow needs to be kept private**

Solution: Manipulate actual energy prosumption profile!

***COPES core objective***

Design of innovative privacy enhancing technologies that

i. allow utility providers to monitor and control the grid, and

ii. assure prosumers' privacy.

# Research Challenges

**Privacy measures** (assessment of privacy risk)

- Identify relevant SM privacy measures
  - Differential privacy, privacy measures based on information theory or statistical inference

**Privacy enhancing methods** (privacy-by-design)

- Innovative energy flow control strategies
- Fundamental performance bounds

**Integration and impact on smart grid** (efficiency, costs)

- Grid service provision and optimization
- Privacy-utility trade-off

**Proof-of-principle tests** (demonstration)

# Partners and Roles

***Privacy measures and privacy-enhancing methods***

- Information theoretic
- Statistical inference
- Computer science

Imperial College London

KTH VETENSKAP OCH KONST

Inria

***Impact on Smart Grid***

- Grid control
- Dynamic Pricing
- Power system operation

ETH

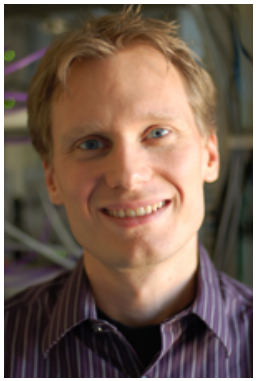
# KTH – Information Science and Engineering Department

- Lead: Tobias Oechtering
  - PMG member, project coordinator, PI
  - Lead WP5 Project Mgmt, Diss., Exploit.
  - Expertise in system design, detection and information theoretic privacy & networked control

- PhD students Zuxing Li and Ramana Reddy
  - MSc student You Yang + BSc students

- Participate in all technical WPs: Defining detection-theoretic system model & privacy measures, design and evaluation of privacy enhancing methods and utility-privacy trade-offs.

# KTH – Automatic Control Dept.



- Henrik Sandberg
  - Lead WP1
- Expertise in networked control and estimation, optimization, and security
- Participates in all technical WPs: Optimal control and estimation under various privacy metrics, and corresponding trade-offs

# Imperial College London

## Electrical and Electronic Eng. Dept.

- Lead: Deniz Gündüz
  - Imperial PI
  - Lead WP2: **Privacy Enhancing Methods and Theory**

- Researchers: Borzoo Rassouli and Giulio Giaconi

- Expertise in information theoretic privacy, signal processing and optimization.

- Participation in all technical WPs: Define system model & privacy measures, design and evaluate privacy enhancing methods and characterize utility-privacy trade-offs.

- **Privatics team:**
  - Lead: Cedric Lauradoux
  - Claude Castelluccia
  - Gabor Guylas

- **Areas of expertise:**
  - **Computer science**
  - Privacy (data anonymization, privacy preserving cryptography, regulations...)
- **Project contributions:**
  - Differential-privacy for smart meters
  - Small-scale demonstrator

# ETH – Power Systems Laboratory

- Gabriela Hug
  - Lead WP4
- Expertise in power systems modeling, operation and optimization
- Participates in all technical WPs: integration into energy management at residential level, interaction with the power grid

# Main scientific results

**International peer reviewed conference papers**

1. J. Chin, T. Tinoco De Rubira, and G. Hug, “Time Aggregation for Privacy-Protecting EMU based on Model-Distribution Predictive Control”, submitted to PowerTech Manchester 2017.
2. Z. Li, T. J. Oechtering, and D. Gunduz, “Smart Meter Privacy Based on Adversarial Hypothesis Testing,” submitted to ISIT 2017.
3. T. Tanaka, M. Skoglund, H. Sandberg, K. H. Johansson, “Directed Information and Privacy Loss in Cloud-based Control”, accepted to American Control Conference 2017.
4. G. Giaconi and D. Gunduz , “Smart meter privacy with renewable energy and a finite capacity battery,“ IEEE Int'l Workshop on Signal Proc. Advances for Wireless Comm. (SPAWC), Edinburgh, UK, Jul. 2016.
5. Z. Li, T. J. Oechtering, and M. Skoglund, ”Privacy-preserving energy flow control in smart grids”, Proc. 41st IEEE ICASSP 2016, Shanghai, China, March 2016.
6. H. Sandberg, G. Dan, R. Thobaben: *"Differentially Private State Estimation in Distribution Networks with Smart Meters"*.,in Proceedings of the 54th IEEE Conference on Decision and Control, Osaka, Japan, December 2015.
7. Z. Li, and T. J. Oechtering, ”Privacy on Hypothesis Testing in Smart Grids,” Proc. IEEE Information Theory Workshop (ITW), Jeju, South Korea, October 2015.

**International peer reviewed journals**

1. J. Chin, T. Tinoco De Rubira, and G. Hug, “Privacy-Protecting Energy Management Unit through Model-Distribution Predictive Control”, submitted to IEEE Transactions on Smart Grid.
2. F. Farokhi and H. Sandberg, “Fisher Information as a Measure of Privacy: Preserving Privacy of Households with Smart Meters Using Batteries”, accepted to IEEE Transactions on Smart Grid.
3. O. Tan, J. Gomez-Vilardebo and D. Gunduz, “Privacy-cost trade-offs in demand-side management with storage”, to appear, IEEE Transactions on Information Forensics & Security.

# *Hypothesis Testing SM Privacy*

**Test on consumers behavior!**

(operational privacy measure)

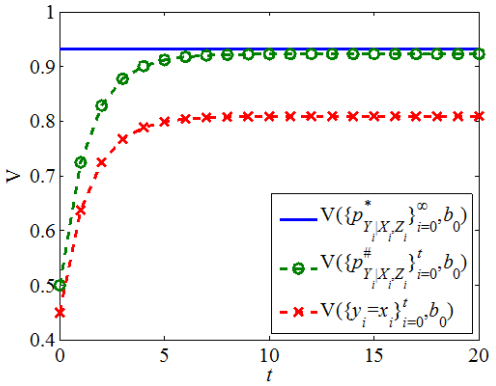
Privacy-preserving schemes with

- renewable energy supply (submitted to ISIT'17)
  - Minimize exponential decay rate of adversarial hypothesis testing probability of error.
  - Privacy-preserving performance bound!

Joint work between KTH and Imperial College London

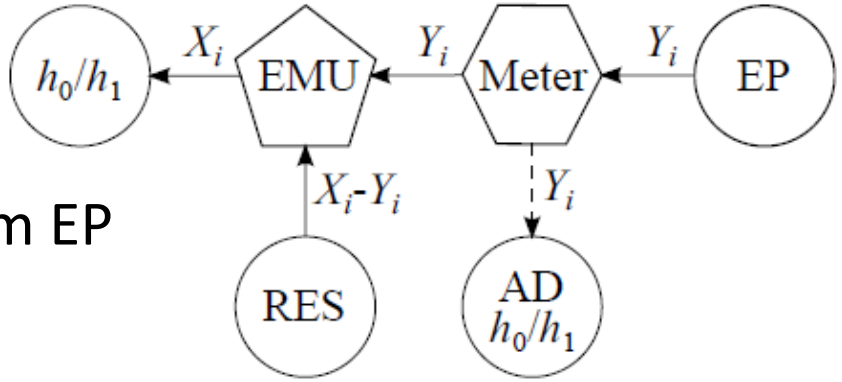
**Fundamental bounds** (highly relevant for privacy risk assessment as required by GDPR)

- finite energy storage capacity (ICASSP'16)
  - Belief state Markov decision process framework
  - Tools for the design of optimal energy flow control policy



# *Smart Meter Privacy Based on Adversarial Hypothesis Testing*

- Binary behavior hypothesis
  - Conditional i.i.d. demands $X_i$
- EMU decides on the supply $Y_i$ from EP
  - RES provides the remaining demand




- ***Adversarial hypothesis testing*** made by the informed AD:
  - Minimize Type II probability of error subject to a Type I probability of error upper bound:

$$\beta(n, \varepsilon, \gamma^n(s)) \triangleq \min_{\mathcal{A}_n \subseteq \mathcal{Y}^n} \{p_{Y^n|h_1}(\mathcal{A}_n) | p_{Y^n|h_0}(\mathcal{A}_n^c) \leq \varepsilon\}$$

- Optimal privacy-preserving performance:

$$\beta_s(n, \varepsilon) \triangleq \max_{\gamma^n(s)} \{\beta(n, \varepsilon, \gamma^n(s))\}$$

  - Optimizer denotes **optimal energy flow control strategy**

# *Fundamental Bound on the Asymptotic Privacy-Preserving Performance*

- **Kullback-Leibler divergence** rate:

$$\theta(s) \triangleq \inf_{k,\gamma^k(s)} \left\{ \frac{1}{k} \mathrm{D}(p_{Y^k|h_0} || p_{Y^k|h_1}) \right\}$$

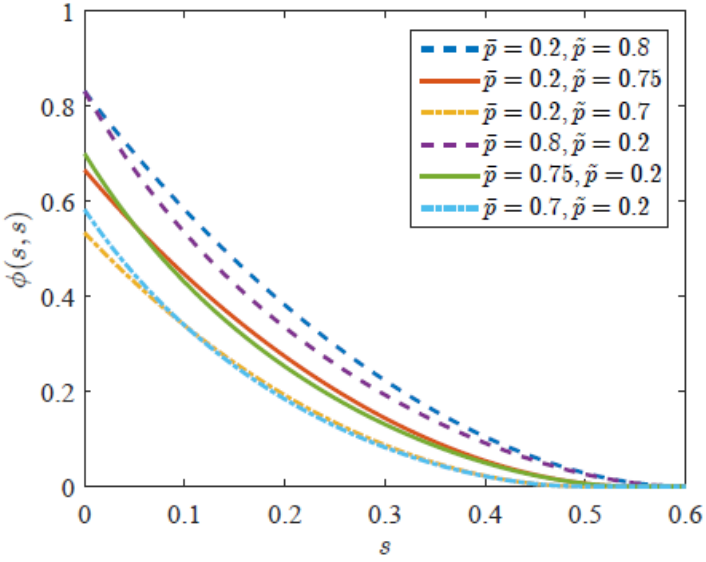
- Asymptotic exponential decay rate of the maximum minimal Type II probability of error can be bounded as:

$$\limsup_{n\to\infty} \frac{1}{n} \log \frac{1}{\beta_s(n,\varepsilon)} \leq \theta(s), \ \forall \varepsilon \in (0,1)$$

$$\lim_{\varepsilon\to 1} \lim_{n\to\infty} \frac{1}{n} \log \frac{1}{\beta_s(n,\varepsilon)} = \theta(s)$$

# *Memoryless Hypothesis-Aware Policy v.s. Hypothesis-Unaware Policy with Memory*

- **Memoryless** hypothesis-**aware** policy
  - An i.i.d. policy
    - Constructive proof - characterizes optimal control strategy
  - Define a privacy-preserving guarantee.

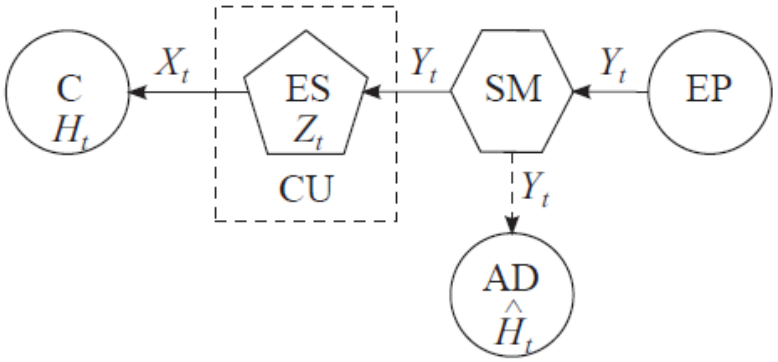



- Hypothesis-**unaware** policy **with memory**
  - Hypothesis can be learned by EMU with an arbitrarily small probability of error.
    - Constructive proof

=> Memoryless hypothesis-aware policy cannot outperform hypothesis-unaware policy with memory!

# *Privacy-Preserving Energy Flow Control in the Presence of an Energy Storage*

- Evolving hypothesis $H_t$
- System **with memory**:
  - Markov settings
  - Finite-capacity battery




- **Design objective** of the control strategy:
  - Maximize the accumulated discounted minimal Bayesian risk (ICASSP'16);
  - Minimize the Kullback-Leibler divergence including utility/energy costs (ongoing master thesis project).
- Approach: Formulate problem as **belief state Markov decision process** (enables to use existing framework for the design)

# *Fisher-information-based Privacy*

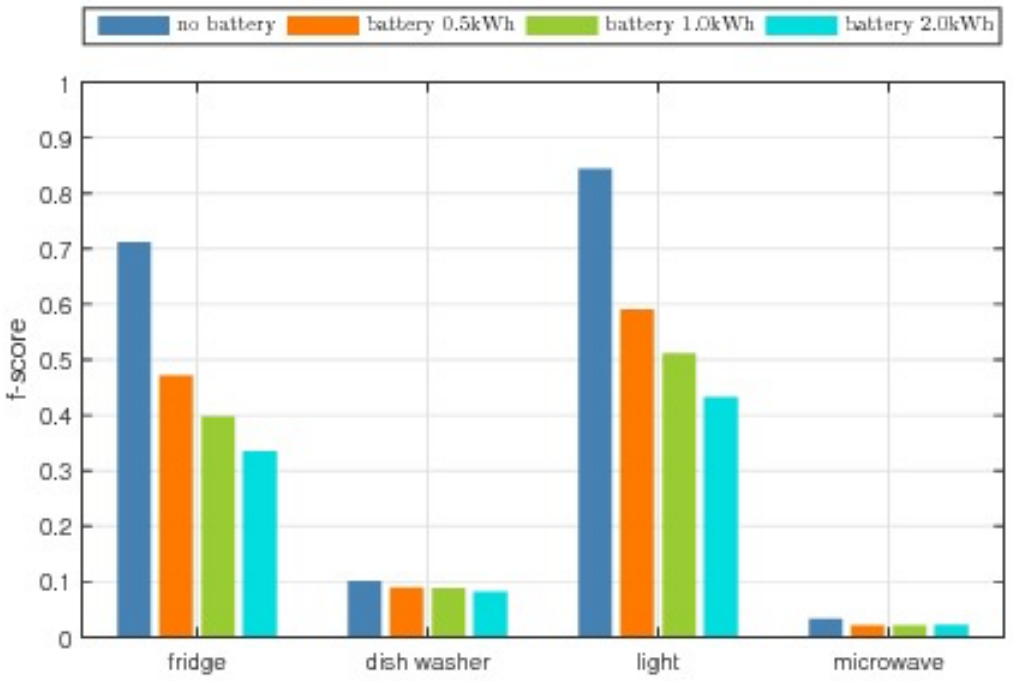
- Run battery so as to make **estimation of privacy-sensitive information** as hard as possible given SM data

- *Cramér-Rao bound* provides a lower operational bound for adversary:

$$\mathbb{E}\{\|s - \hat{s}(x)\|_2^2\} \geq \mathrm{Tr}(\mathcal{I}(s)^{-1})$$

- We develop efficient schemes to run battery to **make Fisher information as small as possible**.

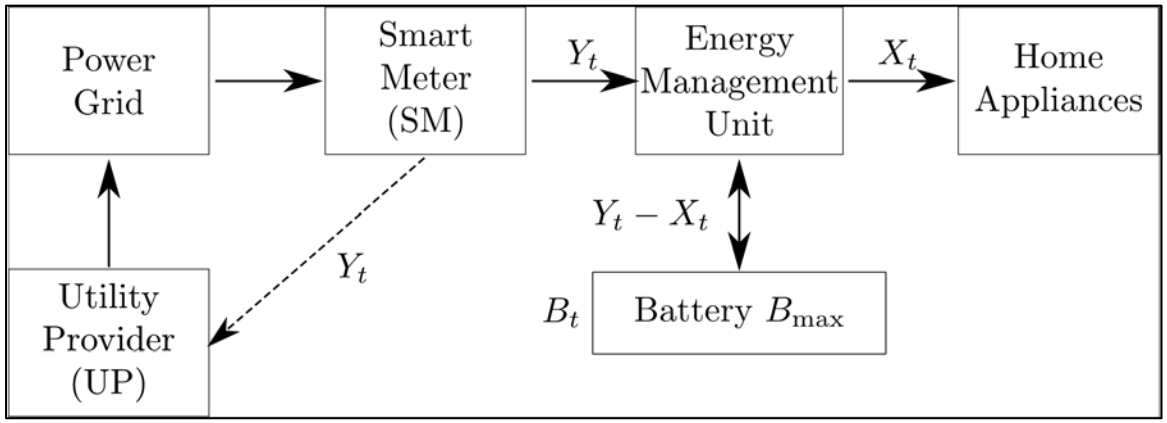
- Result illustrated on REDD-data and off-the-shelf disaggregation algorithm for varying battery size




$$\text{f-score} := \frac{1}{1 + (\mathrm{FN} + \mathrm{FP})/(2\mathrm{TP})}$$

FN = False negatives
FP = False positives
TP = True positives

# *Privacy-cost trade-offs in demand-side management with storage (T-IFS to appear)*

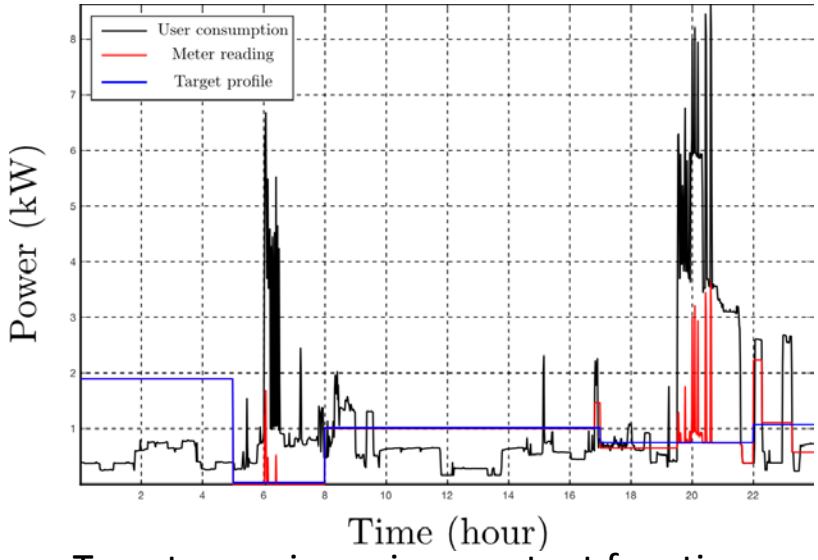



$X_t$: user energy demand
$Y_t$: smart meter readings
$Y_t$-$X_t$: energy to/from energy storage
$B_t$: battery state-of-charge
$B_{max}$: battery capacity

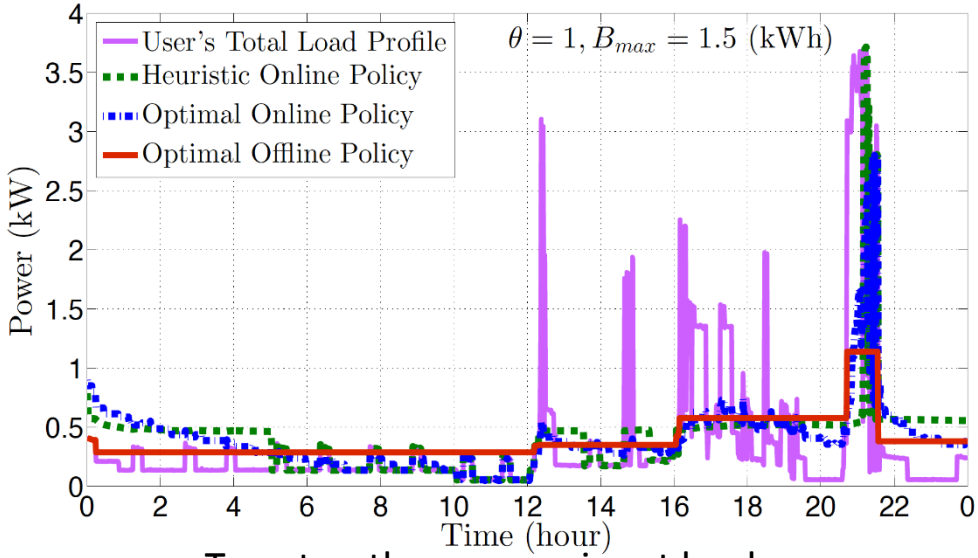
- **Time-of-use pricing:** $C=\Sigma_t Y_t \times C_t$ where $C_t$ is energy cost at time t
  - Also considered scenario where energy can be sold to the grid
- **Privacy metric:** Variance of output load from a target profile W: $P=1/T \Sigma_t (Y_t-W_t)^2$
  - Target can be a constant value, or might imitate a different consumption profile
- **Joint privacy-cost optimization:** $\min \alpha P + (1-\alpha) C$
  - $\alpha$ trades off privacy and cost
  - Offline and online problems studied

# *Privacy-cost trade-offs in demand-side management with storage – cont'd*

- **Offline problem**: Energy demand known over finite time frame. Formulated as a convex optimization problem. Optimal solution has a water-filling interpretation.
  - Water levels depend on price and $\alpha$ parameter.
  - Time-varying target: water levels change over time.
- **Online optimization:** Dynamic programming.
  - Low-complexity heuristic policy.
  - It is shown through simulation that variance is a good proxy for a more complex information theoretic privacy measure.




Target as a piecewise constant function.

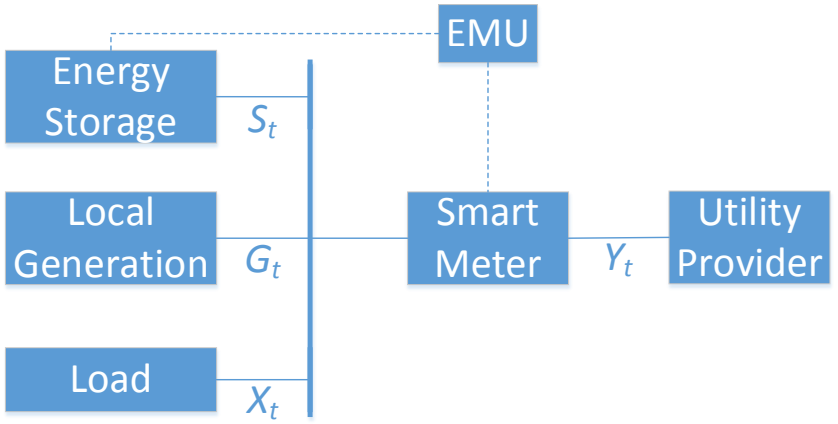



Target as the average input load.

# *Privacy-Protecting Energy Management Unit through Model-Distribution Predictive Control*

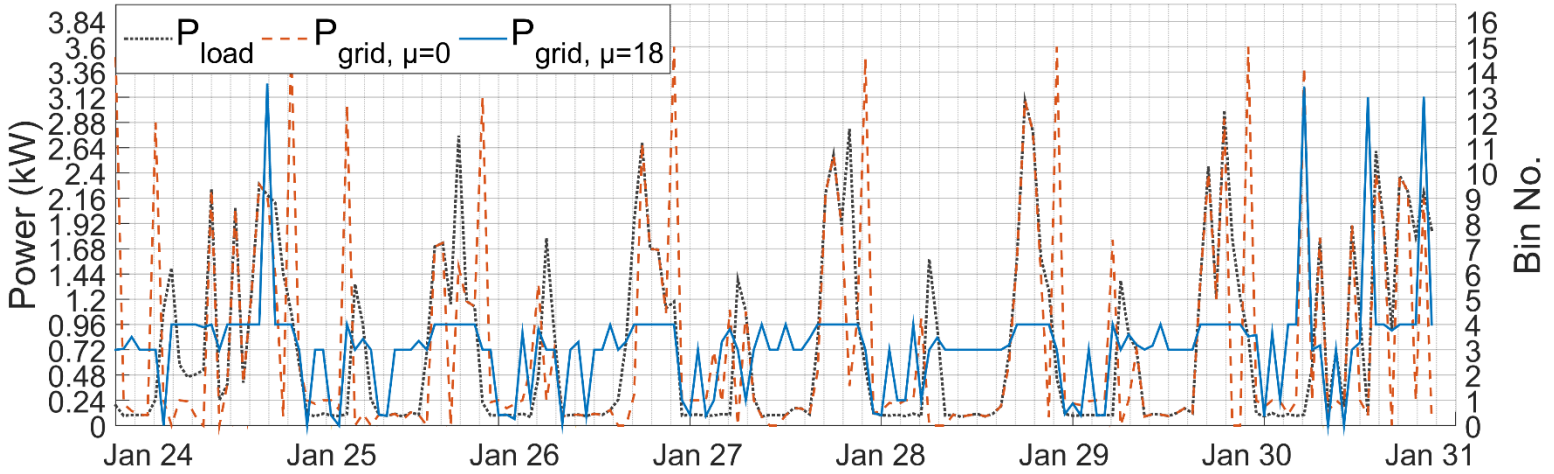
- An approach based on **Model Predictive Control** (MPC)

- Privacy loss: mutual information between *Consumer Load and Grid-Visible Load*



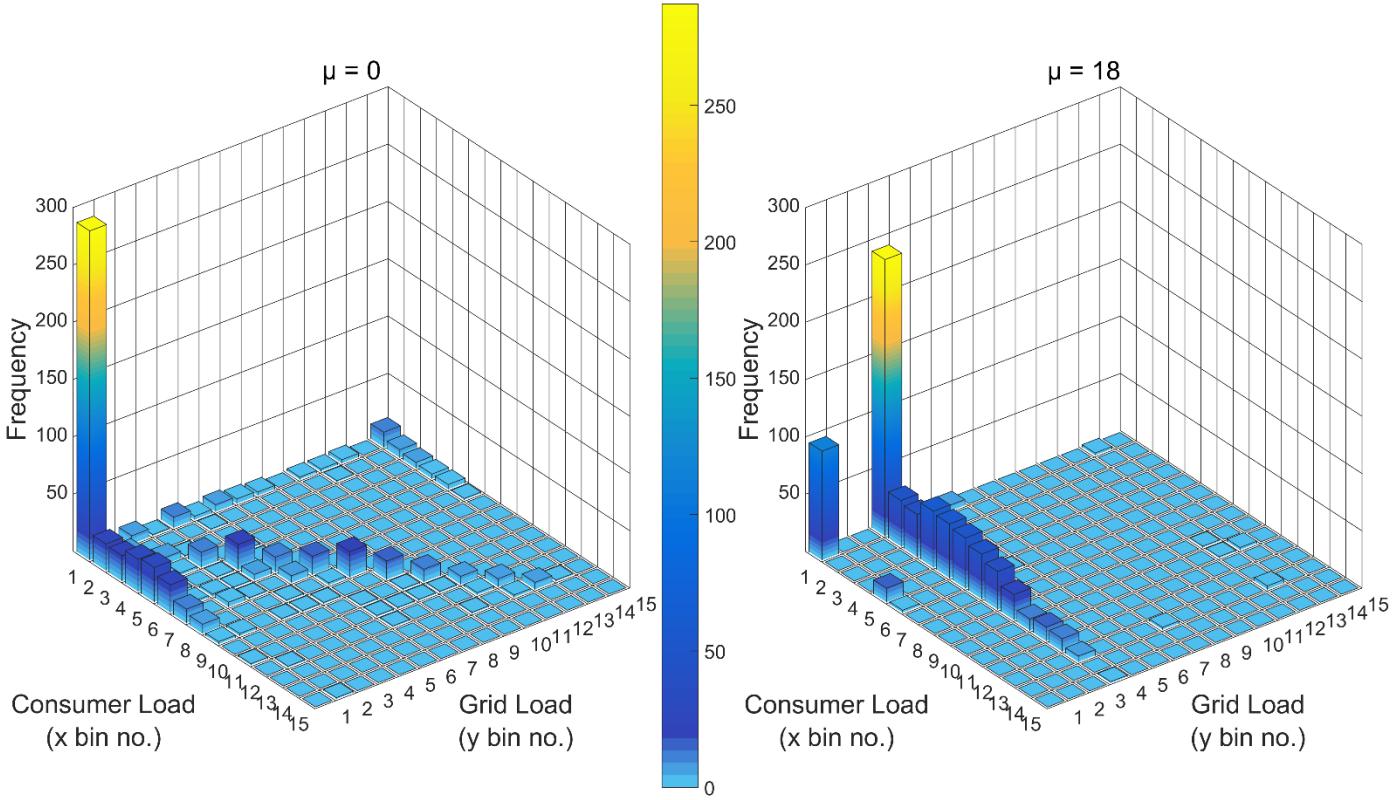

- Statistics of both loads are estimated **online** through counting past and predicted observations
  - Binary variables are used to capture effects of controller actions on estimated probabilities and hence on privacy

# *Resultant Grid-Visible Load*




- At sufficiently high prices of privacy loss, μ, the resultant grid-visible load no longer resembles the consumer load.
- This is also reflected in the correlation between the statistics.
- Adjusting μ balances between energy cost and privacy loss.

# *Statistics of Consumer and Grid-Visible Loads*



# *Evaluation of Smartplugs and experiments (WP4)*

- Smartplugs are cheap smartmeters with (often) poor security (WIFI).
- They can be used to monitor or control several appliances
- Evaluation of their precision and capacity to observe how appliances are being used.

- Experiments with several appliances, laptops to evaluate the possibilities to validate approaches using batteries.

# Valorization

- **Educational purposes**: COPES serves/d as a platform for several degree projects on graduate and undergraduate level
- **Mobility**
  - Z. Li (PhD student, KTH) visited Imperial College London for two month in summer 2016, collaboration has led to one submitted high quality joint conference paper ISIT 2017.
  - More visits are planned (e.g. it planned that KTH PhD student R. R. Avula will visit ETH at the end of 2017)
- **Expert advisor**
  - Inria advises *Grenoble city* on smart meter privacy
  - T. Oechtering became advising expert in Smart Grid+ ERA-Net knowledge community Expera
- **Dissemination**
  - The project has been communicated through multiple channels to several stakeholders (agencies, events, industry) with good response
- **Follow-up research projects**
  - Three follow-up projects have been granted to enhance the technology readiness level.
  - A project with additional proof-of-concept experiments is planned.