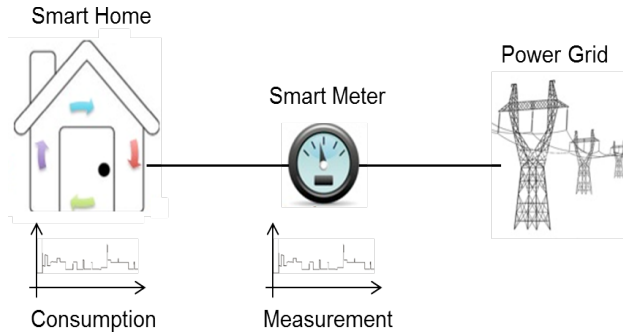


COConsumer-centric Privacy in smart Energy gridS (COPES)

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

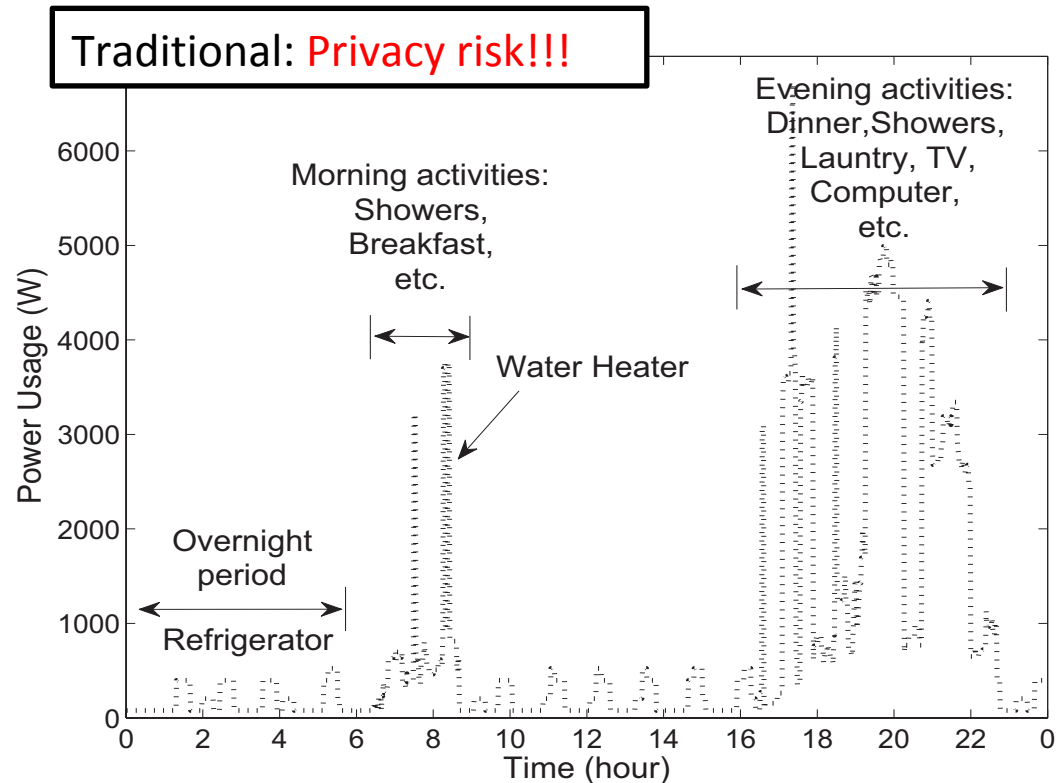


Smart Meter Privacy Problem



“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



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



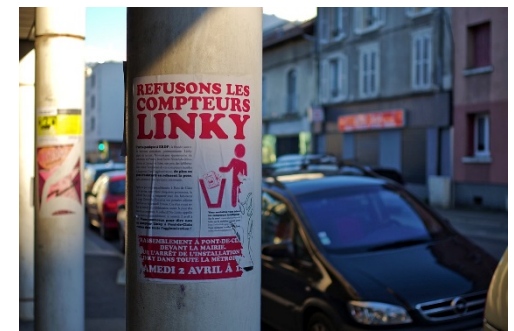
Consumer concerns in many European countries

- E.g. Netherland, Germany, England, France
- Privacy concerns **diminish technology acceptance**

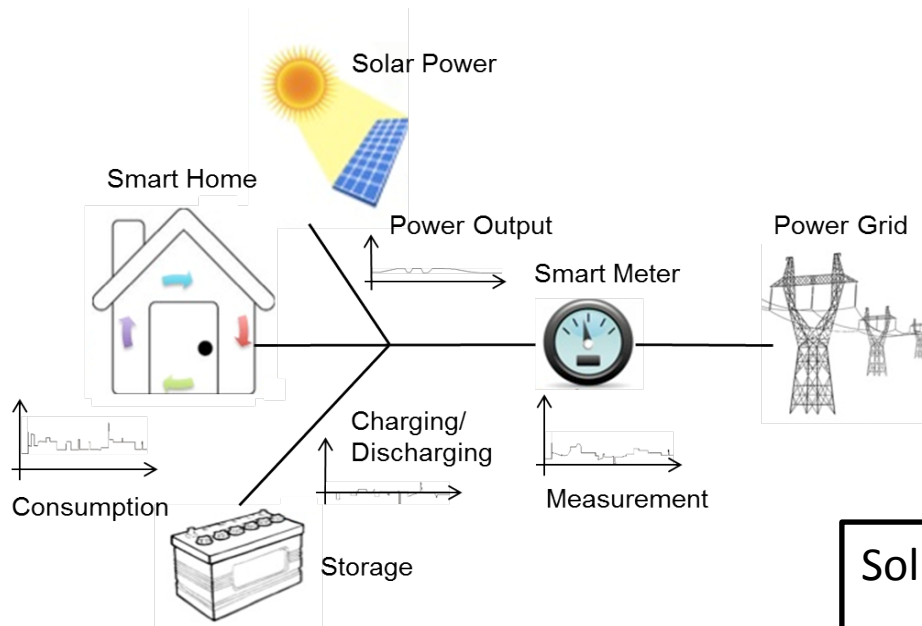


There exists a lot of resistance against SMs

COPES, CHIST-ERA
seminar Paris, Apr 2018



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**

Inria



Imperial College
London

Impact on Smart Grid

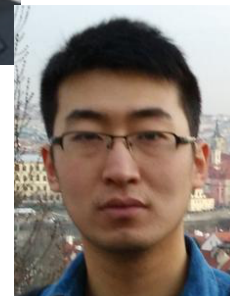
- Grid control
- Dynamic Pricing
- Power system operation

ETH



KTH – Information Science and Engineering Department

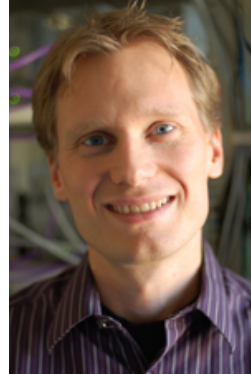
- Lead: Tobias Oechtering
 - PMG member, project coordinator, PI
 - Lead WP5 Project Mgmt, Diss., Exploit.
 - Expertise in system design, detection and information theoretic privacy & networked control
- PhD students Zuxing Li graduated Sept 2017
- New PhD students:
 - Ramana Reddy (since Jan 2017) and
 - Yang You (since Oct 2017)
- 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



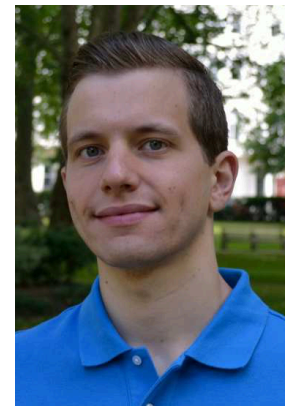
- Expertise in networked control and estimation, optimization, and security
- Participates in all technical WPs: Optimal control and estimation under various privacy metrics, and corresponding trade-offs

Imperial College London

Electrical and Electronic Eng. Dept.



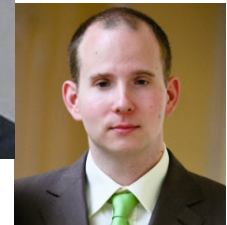
- Lead: Deniz Gündüz
 - Imperial PI
 - Lead WP2: **Privacy Enhancing Methods and Theory**
- Researchers: Borzoo Rassouli and Giulio Giaconi
- Expertise in information theoretic privacy, signal processing and optimization.
- Participation in all technical WPs: Define system model & privacy measures, design 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

- Gabriela Hug
– Lead WP4
- PhD student Chin Jun Xing
- 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. 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.
2. Z. Li, and T. J. Oechtering, "Privacy on Hypothesis Testing in Smart Grids," Proc. IEEE Information Theory Workshop (ITW), Jeju, South Korea, October 2015.
3. 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.
4. 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.
5. Z. Li, T. J. Oechtering, and D. Gunduz, "Smart Meter Privacy Based on Adversarial Hypothesis Testing," ISIT 2017.
6. T. Tanaka, M. Skoglund, H. Sandberg, K. H. Johansson, "Directed Information and Privacy Loss in Cloud-based Control", American Control Conference 2017.
7. J. Chin, G. Giaconi, T. Tinoco De Rubira, D. Gunduz and G. Hug, "Considering Time Correlation in the Estimation of Privacy Loss for Consumers with Smart Meters", accepted to Power Systems Computation Conference (PSCC), Dublin, Ireland, June 2018.
8. G. Giaconi, D. Gunduz, and H. V. Poor, Optimal demand-side management for joint privacy-cost optimization with energy storage, IEEE Int'l Conference on Smart Grid Communications, Dresden, Germany, Oct. 2017.
9. F. Farokhi and H. Sandberg, Optimal privacy-preserving policy using constrained additive noise to minimize the Fisher information. IEEE 56th Annual Conference on Decision and Control (CDC), 2017
10. B. Rassouli and D. Gunduz, Optimal Utility-Privacy Trade-off with Total Variation Distance as a Privacy Measure, accepted at IEEE ISIT 2018.
11. Y. You, Z. Li, and T.J. Oechtering, "Optimal Privacy-enhancing and Cost-efficient Energy Management Strategies for Smart Grid Consumers," submitted to IEEE SSP 2018.
12. R. Reddy, T. J. Oechtering, and D. Månsson, "Optimal Privacy-preserving Control Strategies for Smart Meters Including Energy Storage Losses," submitted to IEEE PES ISGT Europe 2018.

Main scientific results

International peer reviewed journals

1. J. Chin, T. Tinoco De Rubira, and G. Hug, “Privacy-Protecting Energy Management Unit through Model-Distribution Predictive Control”, *IEEE Transactions on Smart Grid*, vol. 8, no. 6, Nov. 2017.
2. F. Farokhi and H. Sandberg, “Fisher Information as a Measure of Privacy: Preserving Privacy of Households with Smart Meters Using Batteries”, *IEEE Transactions on Smart Grid*, 2017
3. O. Tan, J. Gomez-Vilardebo and D. Gunduz, “Privacy-cost trade-offs in demand-side management with storage”, *IEEE Transactions on Information Forensics & Security*, vol. 12, no. 6, pp. 1458-1469, Jun. 2017.
4. G. Giaconi, D. Gunduz and H. V. Poor, “Privacy-aware smart metering: Progress and challenges,” revised, *IEEE Signal Processing Magazine*.
5. G. Giaconi, D. Gunduz, and H. V. Poor, “Smart meter privacy with renewable energy and storage device,” to appear, *IEEE Transactions on Information Forensics & Security*, vol. 13, no. 1, pp. 129 - 142, Jan. 2018.
6. Z. Li, T. J. Oechtering and D. Gunduz, “Smart Meter Privacy: Adversarial Hypothesis Testing Models,” submitted to *IEEE Transactions on Information Forensics & Security*.

Tutorial & Student Theses

Tutorial

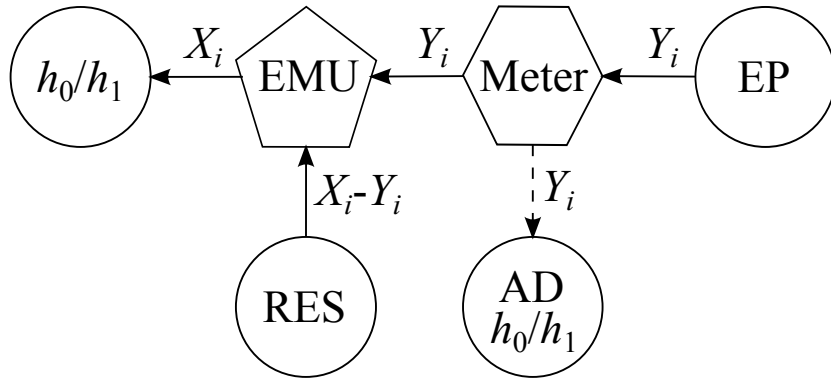
- D. Gunduz and T. J. Oechtering, “Privacy in Smart Metering Systems,” was accepted at ICASSP 2018 but has been canceled, Calgary, Canada.

Student project theses

1. Z. Li, “Privacy-by-Design for Cyber-Physical Systems,” PhD thesis, Sept. 2017. Available online: <http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-214410>
2. G. Giaconi, Information-Theoretic Privacy in Smart Meters, PhD thesis, submitted, Feb. 2018.
3. Y. Yang, “Privacy-enhancing and Cost-efficient Energy Management for an End-User Smart Grid in the Presence of an Energy Storage,” KTH Master thesis report, Sept. 2017. Available online: <http://urn.kb.se/resolve?urn=urn:nbn:se:kth:diva-214410>
4. N. Chrysogelos, “Energy Disaggregation via Current Smart Metering Infrastructure - Study and Implementation Based on Present Constraints”, ETH semester project, May 2016. Available online: <http://www.psl.ee.ethz.ch/Publications/SAMA.html>
5. M. Ansart, “Considering the effect of uncertainty in privacy-protecting MDPC”, ETH semester project, Jan. 2018. Available online: <http://www.psl.ee.ethz.ch/Publications/SAMA.html>
6. A. Sarbach, “Comparing the performance of smart meter privacy protection schemes”, ETH semester project, to appear.
7. S. Jaichuen, “Data Mining / Machine Learning Techniques For Smart Grids,” Imperial College London, MSc thesis, Sep. 2017.
8. A. Asif,, “Load monitoring techniques for smart meters and privacy protection,” Imperial College London, MSc thesis, Jun. 2017.

Fundamental bounds on Hypothesis Testing SM Privacy

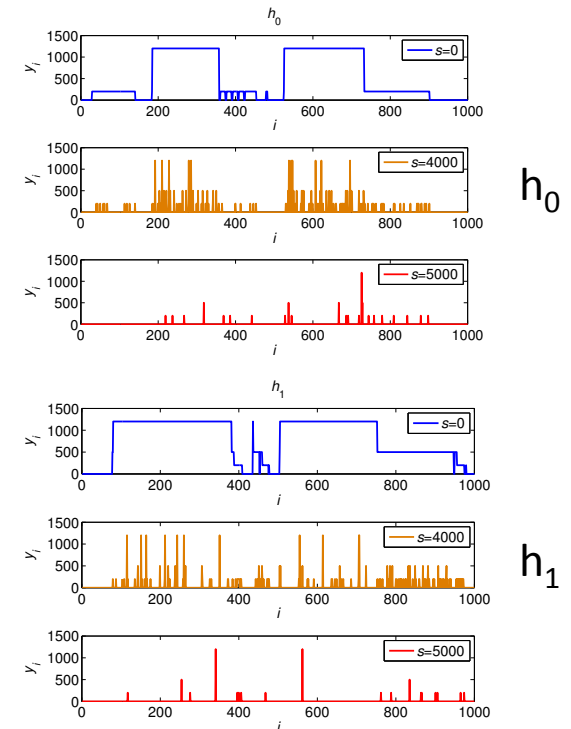
Fundamental bounds
(highly relevant
for privacy risk
assessment as
required by GDPR)



Test on consumers behavior!
(operational privacy measure)

Privacy-preserving schemes with renewable energy supply (bounds and optimal designs)

- Minimize exponential decay rate of adversarial *Neyman Pearson* hypothesis testing probability of error (published at IEEE ISIT'17)
- Extension to adversarial *Bayesian* hypothesis testing (submitted to IEEE T-IFS)
- Recent research considers *privacy-utility trade-off* (presented Apr 10, 2018 at ETIS, Univ. Cergy-Pontoise)



Energy Loss-aware Privacy Control based on Adversarial Hypothesis Testing

- System setting:**

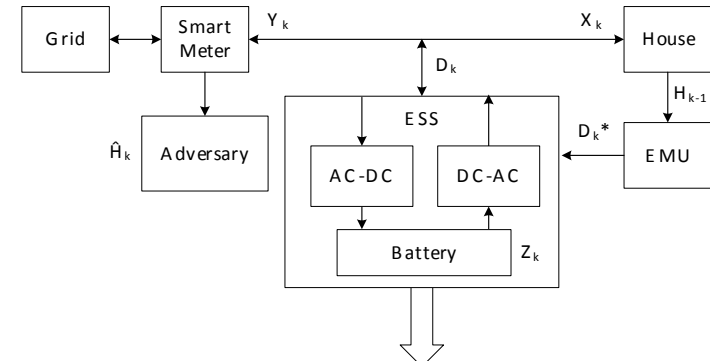
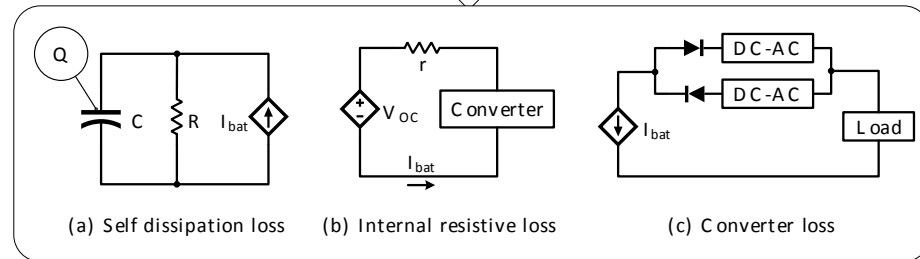
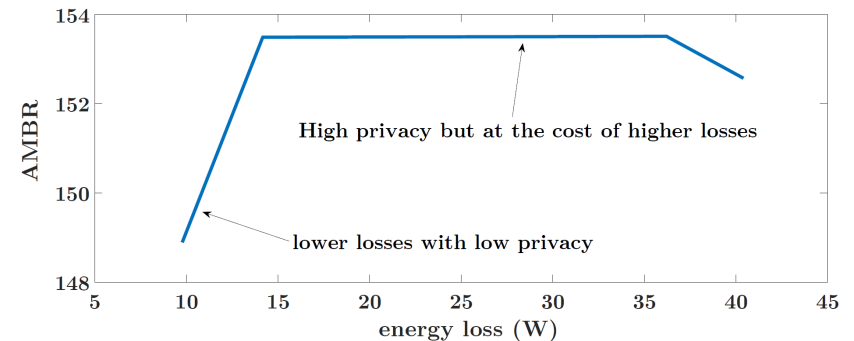
- Markovian hypothesis
- finite-capacity energy storage
- three-circuit model to account for energy storage losses

- PO-MDP Design objective:**

- estimate the state of energy storage while accounting for energy losses due to control actions
- maximize the Accumulated Minimum Bayesian Risk (AMBR).

- Control strategy:**

$$\mu^* = \underset{\mu}{argmax} \sum_{k=1}^N \min \left\{ \sum_{h, \hat{h}} C(h, \hat{h}) \cdot P(h, \hat{h}) \right\}$$



Optimal Privacy-enhancing and Cost-efficient Energy Management Strategies in Smart Grids

- **System setting:**
 - Binary energy consuming hypothesis
 - Random energy demand and price (first-order Markov chain)
 - Finite-capacity energy storage

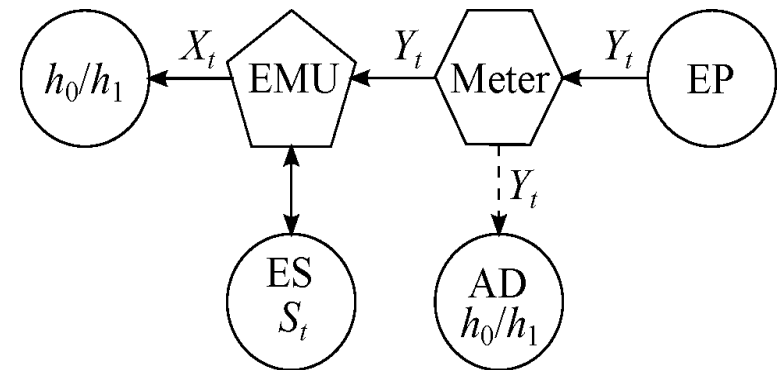
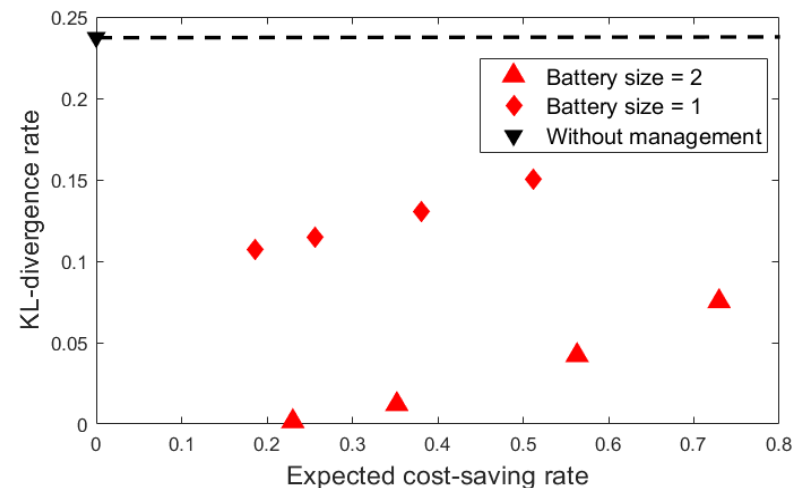
- **Objectives:** Minimize weighted sum of
 - Privacy leakage rate:

$$\frac{1}{T} D(P_{Y^T, P^T}^f |_{h_0} \| P_{Y^T, P^T}^f |_{h_1})$$

- Expected cost-saving rate:

$$\frac{1}{T} \sum_{t=1}^T \{ \mathbb{E}[(X_t - Y_t) P_t | h_0] P(h_0) + \mathbb{E}[(X_t - Y_t) P_t | h_1] P(h_1) \}$$

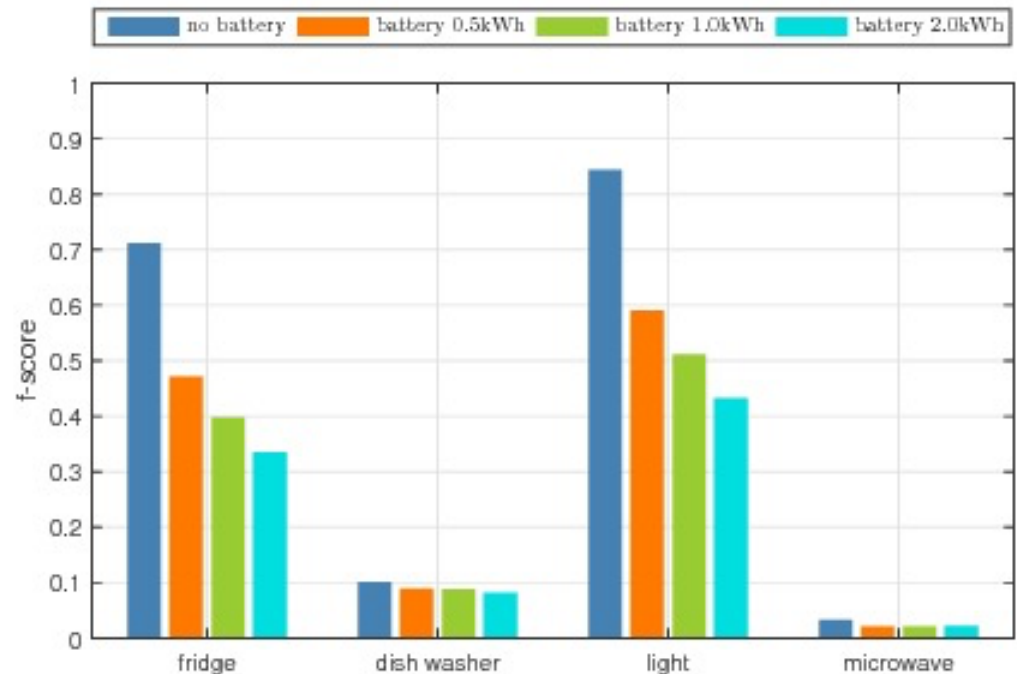
- **Strategy design:**
 - Belief-state MDP formulation
 - Bellman dynamic programming



Reference: Y. You, Z. Li and T. J. Oechtering, "Optimal Privacy-enhancing and Cost-efficient Energy Management Strategies for Smart Meter Consumers", Accepted to IEEE SSP 2018.

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



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

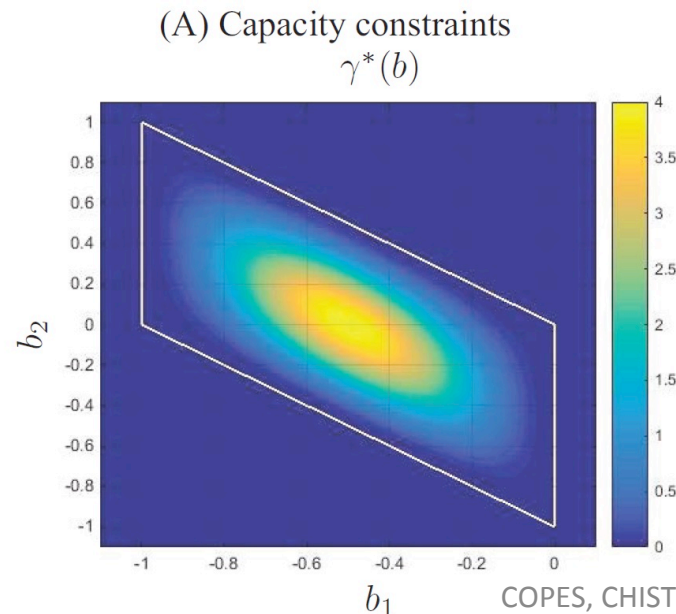
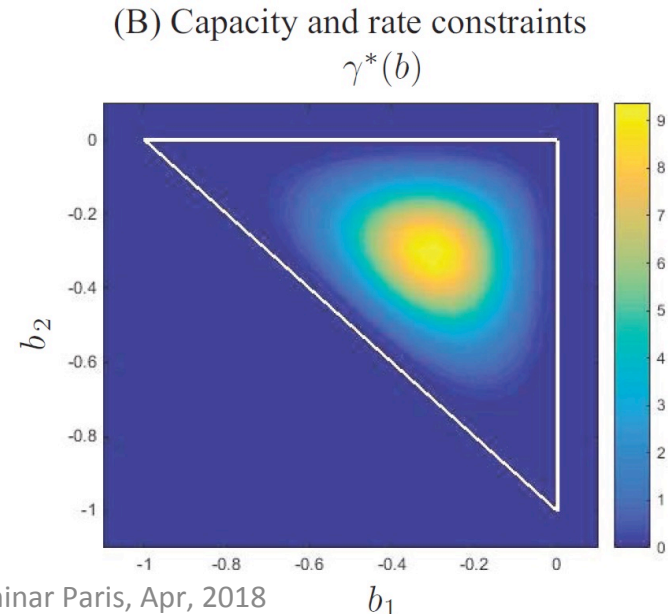
FN = False negatives

FP = False positives

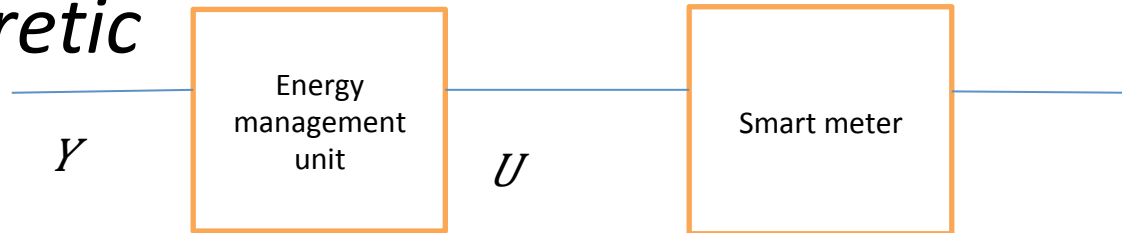
TP = True positives

More Realistic Battery Models: Rate and Dynamical Constraints

- **Problem:**
 - Choose battery charging rates $b=(b_1, b_2, \dots)$ [b_k =charging at time k]
 - make point estimation of true energy consumption $s=(s_1, s_2, \dots)$ as hard as possible
 - given access to SM data sequence $x=(x_1, x_2, \dots)$.
- **Solution:** Compute sequence b to make Fisher information $I(s)$ as small as possible, subject to dynamical and rate constraints on battery
- **Example:** (A) shows optimal pdf of b subject to dynamical (capacity) constraints. In (B), there are also charging rate constraints.



Information-theoretic privacy



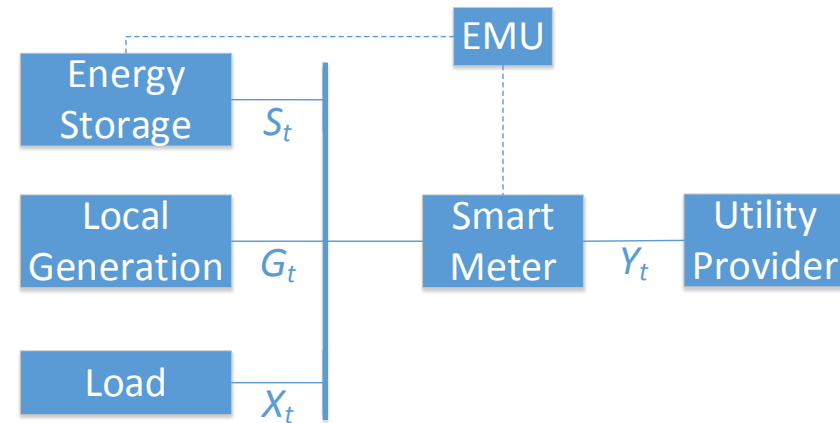
- **System setting:** X-Y-U form a Markov chain
 - X is the private latent variable, e.g. number of people living in a house
 - Y is the observed data, e.g. the energy consumption
 - U is the released data, e.g. noisy version of Y that is revealed to the utility provider
- **Perfect privacy:** Minimum distortion between Y and U, while U is independent of X (accepted at IEEE ISIT'18)
 - Standard linear program for distortion meas. as mutual inf, MMSE,...
- **Total variation as privacy measure** (to be submitted to IEEE ITW'18)

$$T(X; U) = \max_u \|p_{X|U}(\cdot | u) - p_X(\cdot)\|_{TV} = \frac{1}{2} \max_u \|\mathbf{p}_{X|u} - \mathbf{p}_X\|_1$$

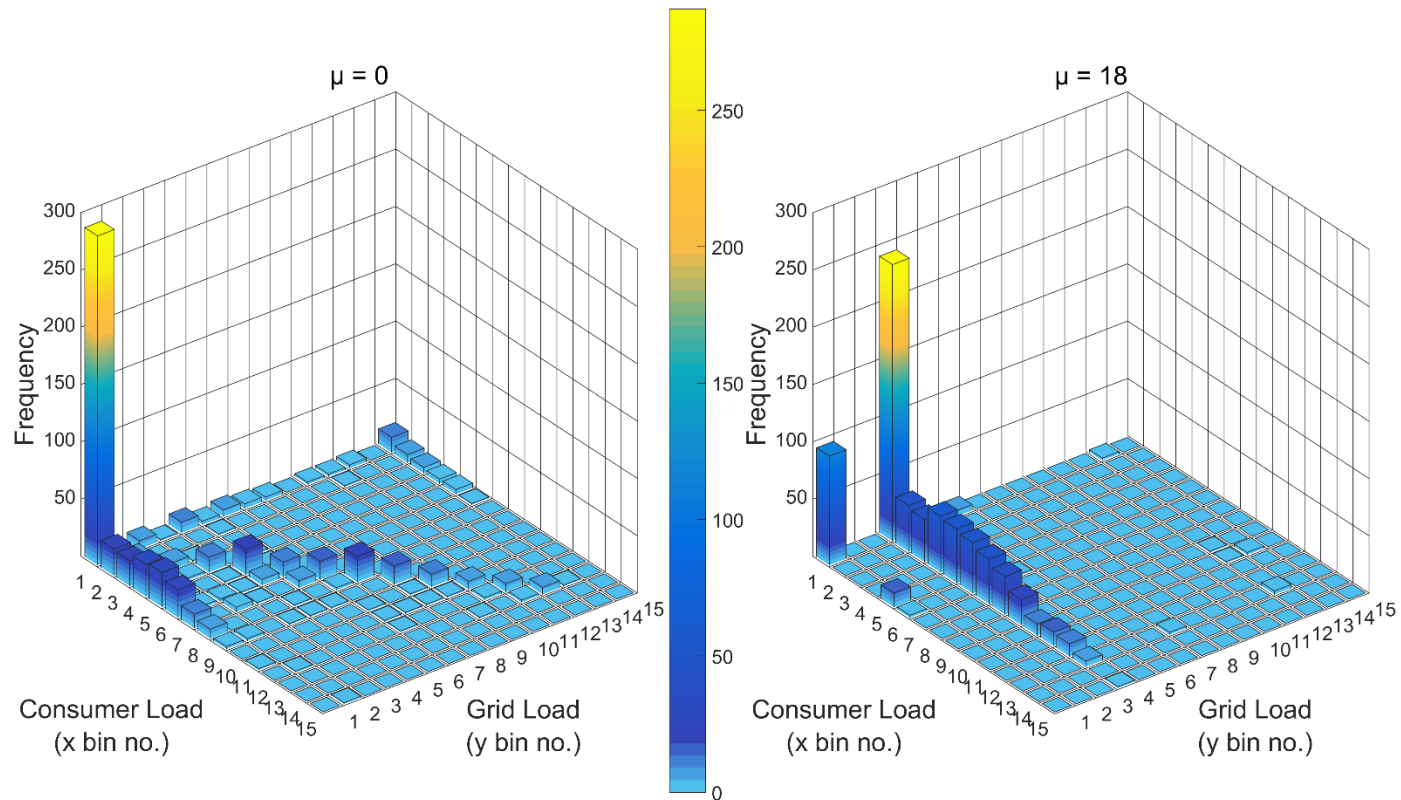
- Whole utility-privacy trade-off region obtained by a linear program
- Upper bound for some other well-known privacy measures, like maximal leakage, mutual information

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

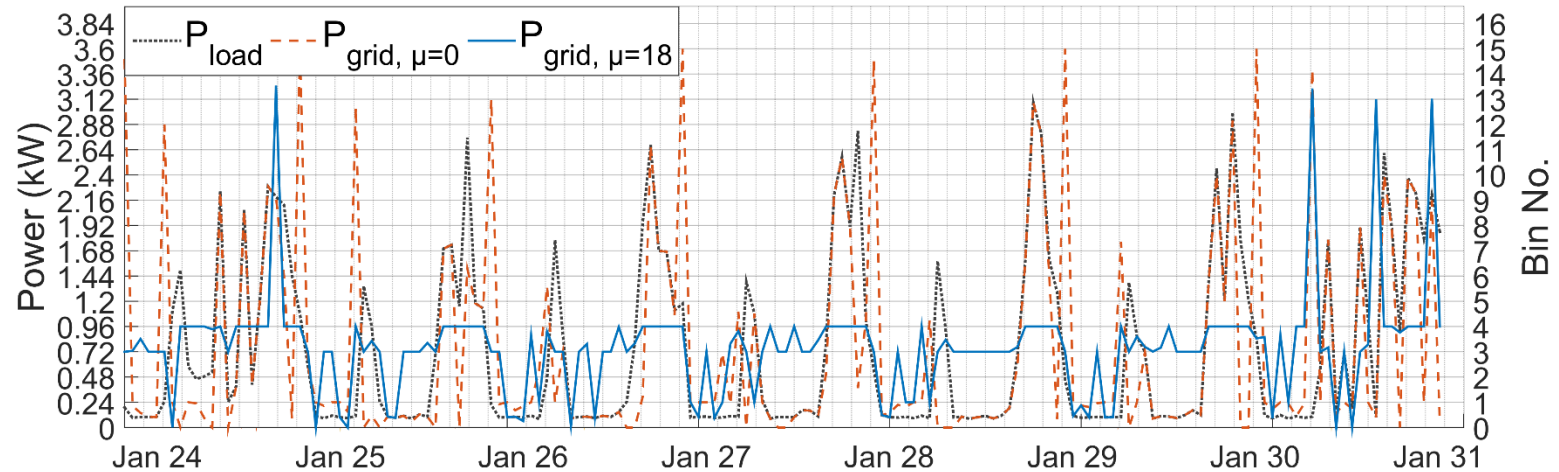
- An approach based on **Model Predictive Control (MPC)**
- **Privacy loss:** mutual information between *Consumer Load* and *Grid-Visible Load*
- Statistics of both loads are estimated **online** through counting past and predicted observations
 - Binary variables are used to capture effects of controller actions on estimated probabilities and hence on privacy



Statistics of Consumer and Grid-Visible Loads

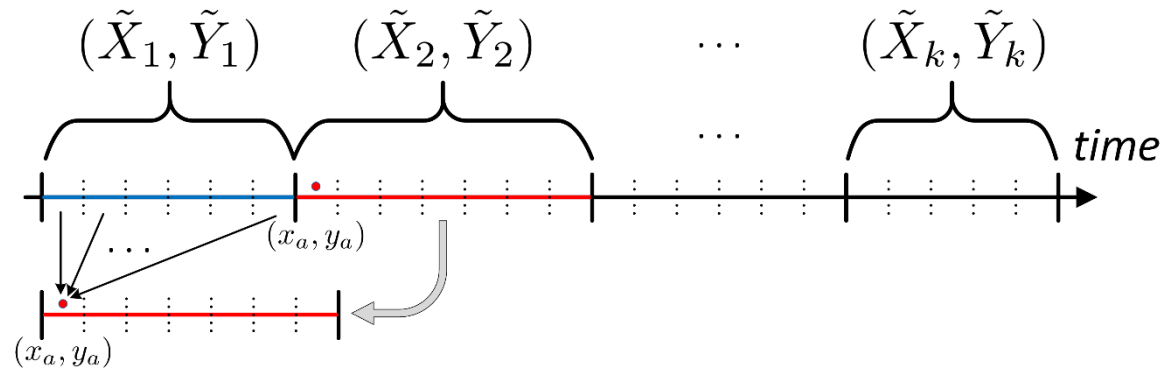


Resultant Grid-Visible Load



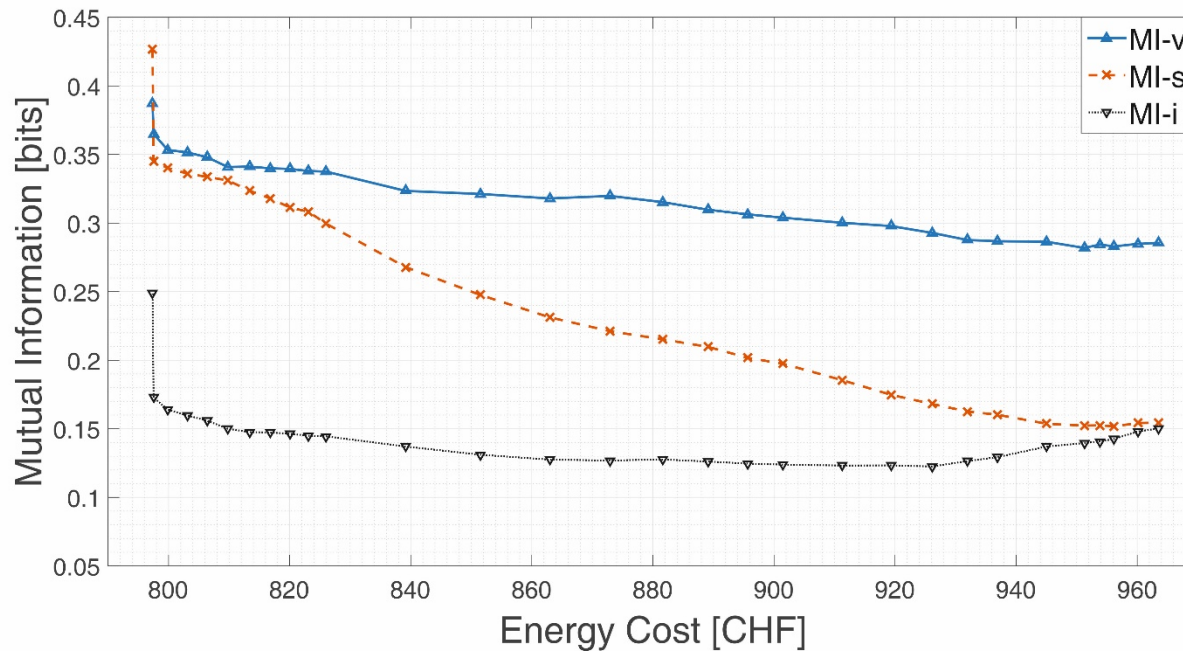
- At sufficiently high prices of privacy loss, μ , the resultant grid-visible load no longer resembles the consumer load.
- This is also reflected in the correlation between the statistics.
- Adjusting μ balances between energy cost and privacy loss.

Estimating Mutual Information Considering Time Correlation



- Ignoring time-correlation in consumer loads lead to under-estimation of mutual information (MI)
- First-order Markov processes adequately capture inter-temporal components of consumer load statistics
- Previous works assume stationarity to overcome data scarcity
- Feature-dependent Markov process allows for non-stationarity despite limitations on data availability

Accuracy of MI Estimate is Improved when Modelled as Feature-Dependent Markov Chains



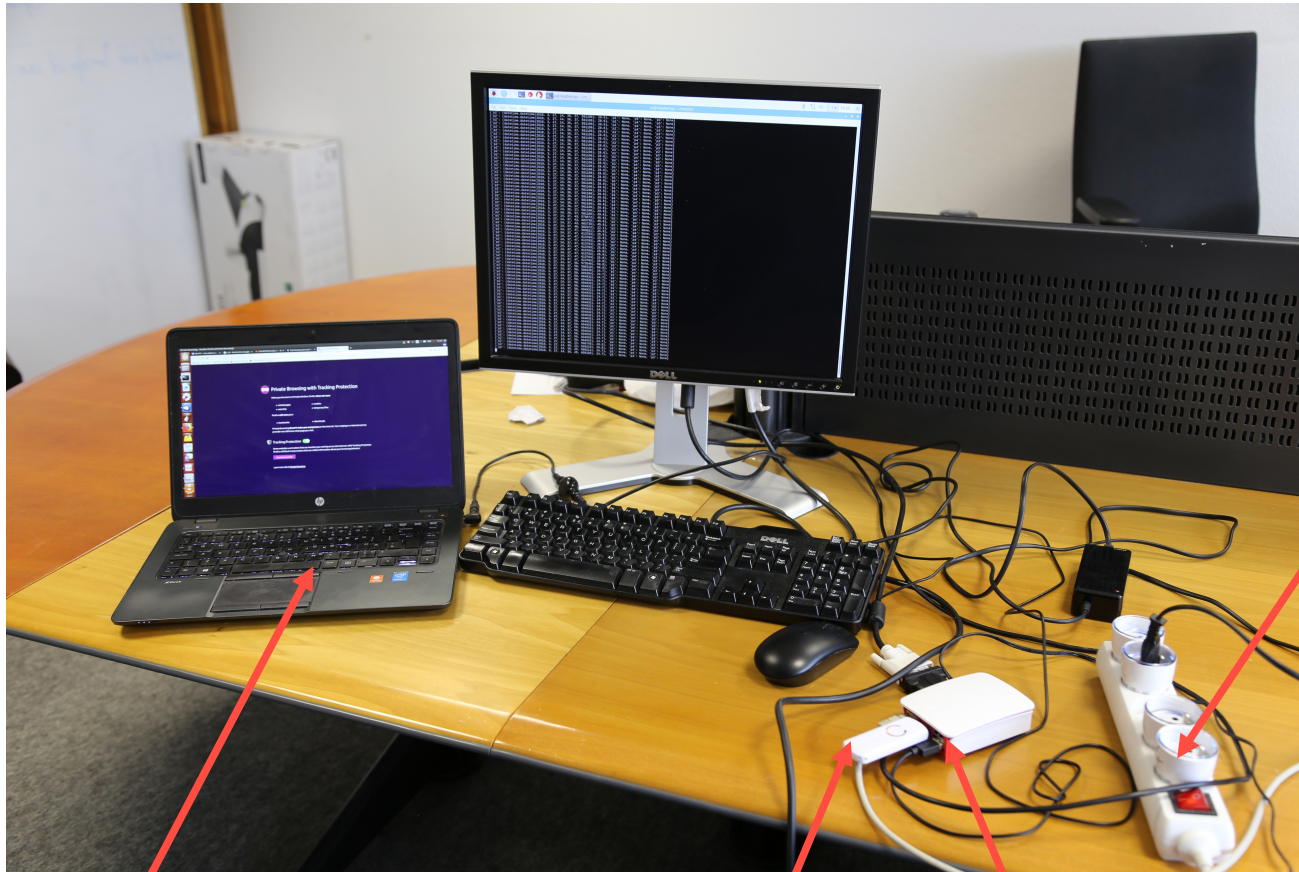
- Stationarity assumption may lead to underestimation of MI (MI-s curve)
- MI estimate based on feature-dependent Markov process better captures privacy-loss of consumer loads (MI-v curve)

Evaluation of Existing Monitoring Systems (WP4)

- Smartplugs are cheap smartmeters with (often) poor security (WIFI).
- Study of  **smappee**
 - Analysis of the information flow.
 - Risks → minimization problem.
- Creation of annotated traces using Amiqua4Home Equipment



Small scale demonstrator (WP4)



Smartplugs

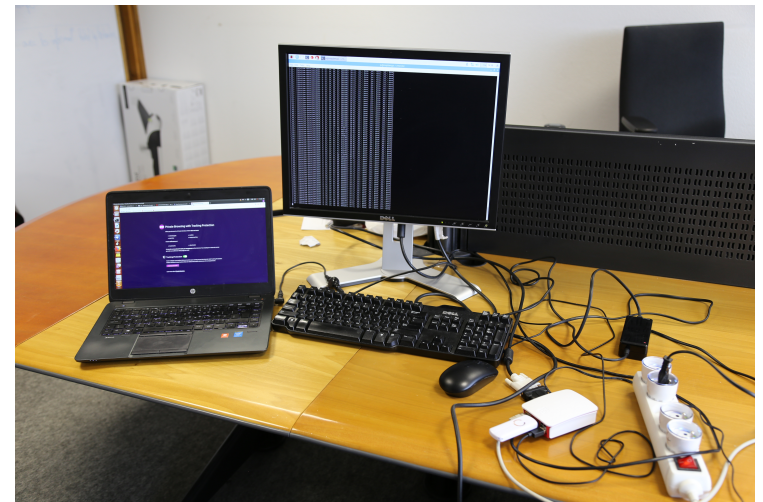
Laptop (MQTT)

Z-Wave dongle

Raspberry PI

Small scale demonstrator (WP4)

- **Goals:** *demonstrate how batteries can help privacy in smartgrids.*
- **How?** *We want to hide laptops activity:*
 - *a smartplug monitors the power consumption,*
 - *smartplugs can be turn on/off to switch to battery mode,*
 - *everything is connected through a Raspberry Pi.*
- **Scheduler:** *implements privacy policies.*
- Many new research possibilities:
 - *synchronization,*
 - *communication between all the laptops,*
 - *usage modulation.*



Dissemination 04/16-04/17

- COPES been communicated through multiple channels to several stakeholders
 - to Swiss Energy agency, Swedish Energy agency, Swedish Data Protection authority, and Swedish Energy Market Inspectorate
 - on an ERA-Net Smart Grid+ event in April 2016
 - on an EPSRC New Opportunities in Signal Processing event
 - Project was highlighted on the ETH Energy Science Centre's Weekly Spotlight on Energy Research in Feb 2017
 - to the Grenoble Smart Grid Campus which include include ERDF (électricité réseau distribution France)
 - UK power network operator, ABB, Kamstrup, Schneider, ...
 - at Imperial's Doctoral Student Elevator Pitch Competition
 - at Energy TechElevator event at Imperial Business School in March '17
 - at an event of KTH's Graduate School on Digitalization of Swedish EE industry
 - on the own project webpage <http://copes.gforge.inria.fr> and on ResearchGate

Main message: COPES develops the basis for a **technological solution to the SM privacy problem** to assure smart grid potentials!

Dissemination 04/17-04/18

- COPES been communicated through multiple channels
 - To politicians at **World Economic Forum '18** in Davos by G. Hug (ETH IdeasLab, presentation is available on YouTube)
 - **MOOC** (Feb-Mar '18) on privacy by C. Lauradoux (13000 people registered)
 - INRIALITY interview of C. Lauradoux on privacy issues of LINKY
 - Invited presentation and panel member of D. Gunduz at Workshop on Next Steps Toward Securing Smart Grids at IEEE Conf. on Smart Grid Com 2017.
 - at KTH Campus 100 year celebration to the general public
 - to industry: Vattenfall, Northvolt
 - at a stakeholder event of KTH Living Lab (established exchange w. start-up Zyax)
 - at internal seminars of KTH Dept. Electric Power & Energy Systems and Dept. of Philosophy & History
 - on the own project webpage, Twitter, and on ResearchGate

Main message: COPES develops the basis for a **technological solution to the SM privacy problem** to assure smart grid potentials!

Education, Mobility, and Advisory

- **Educational purposes:** COPES serves/d as a platform for several degree projects on graduate and undergraduate level
 - **PhD student research projects** at KTH (one finished), ETH & Imperial
 - Master/Semester thesis projects at KTH (1), Imperial (2), ETH (3)
 - Bachelor thesis projects: KTH (4 students), Imperial (1)
 - **MOOC** on privacy by INRIA (11000 persons registered)
- **Mobility**
 - R. R. Avula (PhD student, KTH) visited ETH Zurich for two months in winter 2017, results of continued research discussion should be soon published
 - J. Chin (PhD student, ETH) visited Imperial College London for a week in Aug 2017, collaboration led to the joint work submitted to PSCC 2018
 - Z. Li (PhD student, KTH) visited Imperial College London for two months in summer 2016, collaboration has led to one submitted high quality joint conference paper ISIT 2017.
- **Expert advisor**
 - Inria advises *Grenoble city* on smart meter privacy
 - T. Oechtering became advising expert in Smart Grid+ ERA-Net knowledge community Expera

Follow-up research projects

COPES (mostly) assumes idealized components

- **Granted follow-up projects** to study

- Impact of real energy storages with non-ideal parameters

EE Graduate school Digitalization of Swedish EE industry

- Storage systems suitable for SM privacy



- Intelligent heating system with batteries

Industry project with



- Experimental follow-up project at ETH

- Testing algorithms on equipment
- Funding sought from SFOE (governmental dep)

- Experiments in **KTH Live-In Lab**

- Proof-of-concept experiments with inhabited apartments (test of algorithms, create reference data set for research)
- Planned start: Autumn 2018 (legal & ethical approval pending)
- Northvolt will support project with a battery and are interested in deeper collaboration

northvolt

- + additional discussions within COPES on additional funding opportunities

