

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)

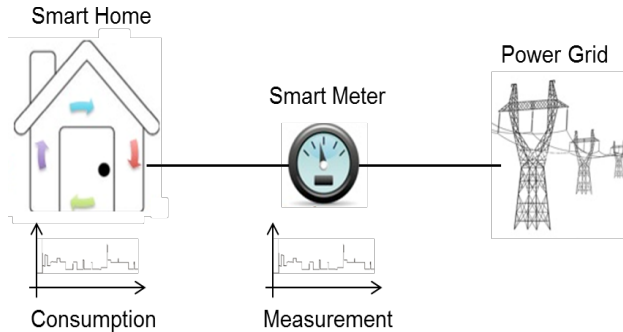


Imperial College
London

Inria

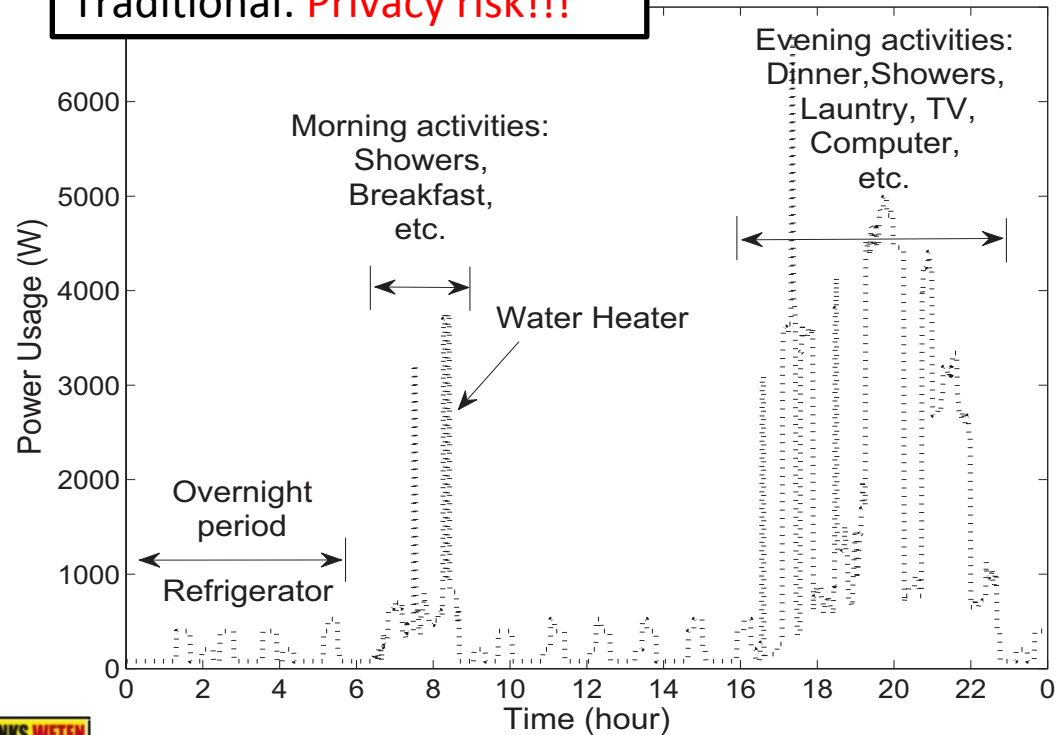
ETH

Smart Meter Privacy Problem

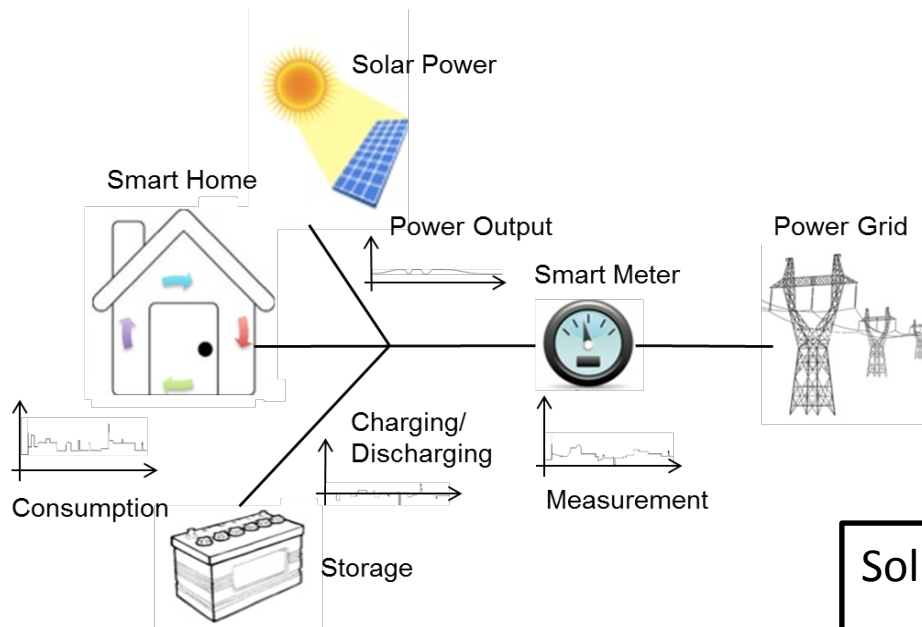


- **GDPR** enforces protection of personal data
- **Privacy can be show stopper**
- Consumer concerns in many countries

Traditional: **Privacy risk!!!**



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



Div. Information Science and Engineering & Div. Decision and Control Systems

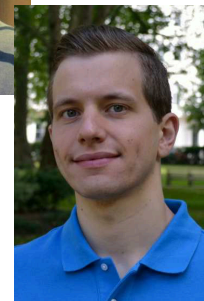
- Prof. Tobias Oechtering
 - Project coordinator, lead WP 5
- Prof. Henrik Sandberg
 - Co-PI, lead WP 1
- Dr. Zuxing Li (graduated 09/2017)
 - Now post-doc Centrale Supelec, Paris
- PhD student Ramana Reddy (since 01/2017)
- PhD student Yang You (since Oct 2017)
- Expertise in system design, detection and information theoretic privacy, networked control and estimation, optimization, and security
 - Main focus: Optimal design of privacy-preserving energy flow control algorithms & trade-offs



Information Processing and Communications Lab

- Dr. Deniz Gündüz
 - Imperial PI
 - Lead WP2
- Dr. Borzoo Rassouli
 - (now with University of Essex as a Lecturer)
- Dr. Giulio Giaconi
 - (now with British Telecom as a Research Scientist)

Imperial team has expertise in information theory and has mainly focused on developing new privacy measures and privacy-enabling technologies for SMs.



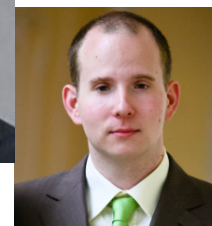
AWARD:

Dr. Giaconi's thesis titled "**Information-theoretic privacy in smart meters**" received the IEEE Information Theory Society UK and Ireland Chapter Best PhD Thesis Award in 2018.



- **Privatics team:**

- Cedric Lauradoux, lead WP4
- 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 Jun-Xing Chin



- Expertise in power systems modeling, operation and optimization
- Focus: Integration into energy management at residential level, interaction with the power grid

COPES Highlights

- 17 conference + 10 journal high quality research papers
 - 5 cross-partner papers
 - regular meetings in person (Stockholm, Zurich, London, Paris) and telcos (10) + visits, incl. 3 longer PhD student visits
 - Small scale demonstrator on how batteries can improve privacy
- 2 PhD graduations + 3 on the way
 - Giulio received best PhD thesis IT society UK award
 - MOOC on privacy (23000 registrations)
- Significant outreach and communication
 - 4 book chapters + online available tutorial
 - Reach out to several stakeholders: agencies, industry...
 - Communication at public events, incl. World Economic Forum'18, Davos
- 3 Follow up projects + proof-of-concept experiments in KTH Live-in lab in progress + experimental follow up project at ETH

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. Giaconì 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. Giaconì, T. Tinoco De Rubira, D. Gunduz and G. Hug, "Considering Time Correlation in the Estimation of Privacy Loss for Consumers with Smart Meters", Power Systems Computation Conference (PSCC), Dublin, Ireland, June 2018.
8. G. Giaconì, 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," IEEE SSP 2018.
12. R. Reddy, T. J. Oechtering, and D. Månsson, "Optimal Privacy-preserving Control Strategies for Smart Meters Including Energy Storage Losses," IEEE PES ISGT Europe 2018.
13. Z. Li and T. J. Oechtering, "Privacy and Utility Management of Hypothesis Tests," in Proc. IEEE ITW 2018.
14. B. Rassouli and D. Gunduz, Optimal utility-privacy trade-off with total variation distance as a privacy measure, IEEE Information Theory Workshop (ITW), Guangzhou, China, Nov. 2018
15. B. Rassouli, F. Rosas and D. Gunduz, Latent feature disclosure under perfect sample privacy, IEEE International Workshop on Information Forensics and Security (WIFS), Hong Kong, China, Dec. 2018.
16. J. Chin, T. Zufferey, E. Shyti, and G. Hug, "Load forecasting of privacy-aware consumers", accepted at IEEE PES PowerTech 2019.
17. R. Reddy, J. Chin, T. J. Oechtering, and G. Hug, "Smart Meter Privacy Control Strategy Including Energy Storage Degradation", accepted at IEEE PES PowerTech 2019.

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. Giacon, D. Gunduz and H. V. Poor, "Privacy-aware smart metering: Progress and challenges," revised, *IEEE Signal Processing Magazine*.
5. G. Giacon, 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*.
7. Z. Li, T. J. Oechtering and D. Gunduz, "Privacy against a Hypothesis Testing Adversary," to be published in *IEEE Transactions on Information Forensics & Security*, early access Nov 2018.
8. F. Farokhi and H. Sandberg, "Ensuring Privacy with Constrained Additive Noise by Minimizing Fisher Information", *Automatica*, vol. 99, pp. 275-288, Jan. 2019.
9. R. Avula, J.-X. Chin, T. J. Oechtering, D. Månsson, G. Hug, "Optimal Smart Meter Privacy Control Strategies Considering Energy Storage Aspects," to be submitted to *IEEE Trans. Smart Grids*, in preparation.
10. Y. Yang, Z. Li, T. J. Oechtering, "Privacy-enhancing and Cost-efficient Energy Management Strategies in Smart Grids," to be submitted to *IEEE Trans. Inform. Forensics and Security*, in preparation

Book chapters

1. Z. Li, Y. Yang, T. J. Oechtering "Privacy against Adversarial Hypothesis Testing: Theory and Application to Smart Meter Privacy Problem," in book with title "Privacy in Dynamical Systems" edited by Farhad Farokhi, planned to be published by Springer towards end of 2019.
2. F. Farokhi and H. Sandberg, "Fisher Information Privacy with Application to Smart Meter Privacy Using HVAC Units," in book with title "Privacy in Dynamical Systems" edited by Farhad Farokhi, planned to be published by Springer towards end of 2019.
3. E. Erdemir, P. L. Dragotti and D. Gunduz, "Information theoretic smart meter privacy," in book with title "Privacy in Dynamical Systems" edited by Farhad Farokhi, planned to be published by Springer towards end of 2019.
4. G. Giacon, D. Gunduz and H. V. Poor, "Privacy in smart grids," to appear in *Data Analytics for Power Systems*, edited by S. Perlaza, A. Tajer and H. V. Poor, Cambridge University Press.

Tutorial & Student Theses

Tutorials

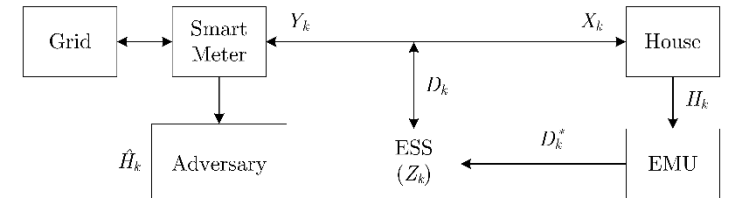
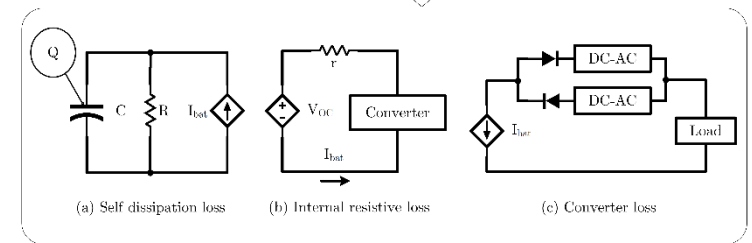
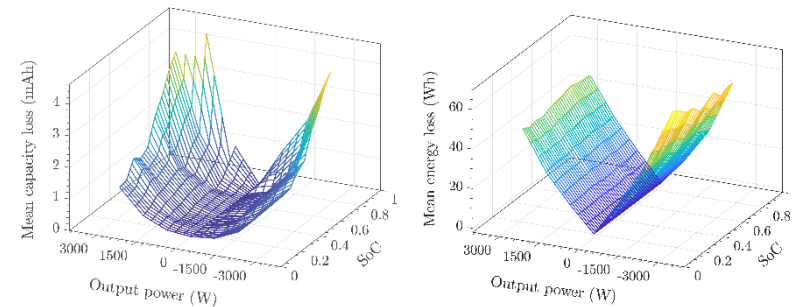
1. D. Gunduz and T. J. Oechtering, “Privacy in Smart Metering Systems,” scheduled at IEEE ICASSP 2018, Calgary, Canada & IEEE SmartGridCom 2018, Aalborg, Denmark.
2. D. Gunduz and T. J. Oechtering, “Privacy in Smart Metering,” IEEE WIFS 2018, Hong Kong. Slides available on T. Oechtering homepage: <https://people.kth.se/~oech/research.html>

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, 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. S. Jaichuen, “Data Mining / Machine Learning Techniques For Smart Grids,” Imperial College London, MSc thesis, Sep. 2017.
7. A. Asif,, “Load monitoring techniques for smart meters and privacy protection,” Imperial College London, MSc thesis, Jun. 2017.
8. F. Scherrer, “ The Identification of Household States using Smart Meter Data”, ETH Master’s project, Jan. 2019. Available online: <http://www.psl.ee.ethz.ch/Publications/SAMA.html>

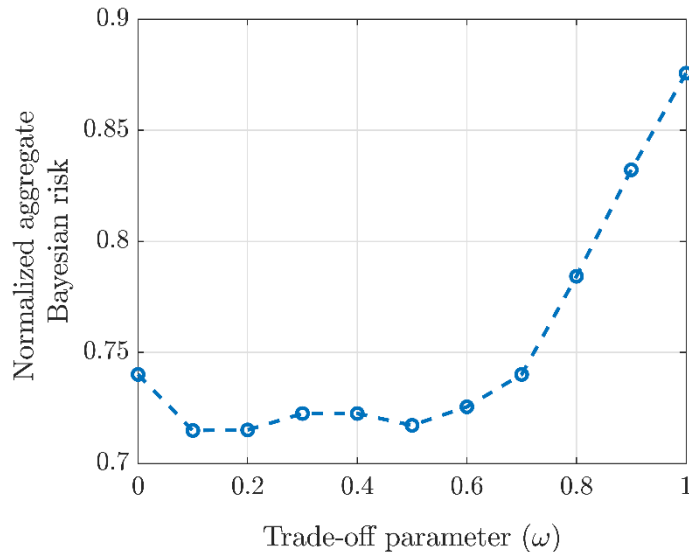
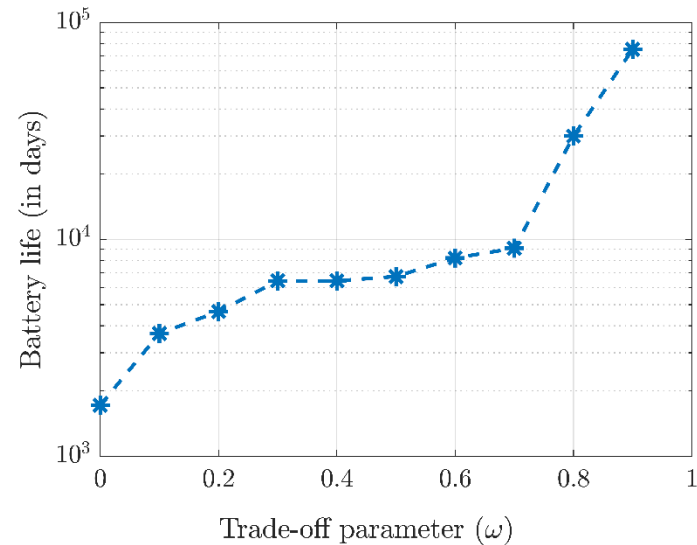
Energy storage aspects in Privacy-by-design

- **Privacy model:**
 - Markovian hypothesis
 - **Bayesian risk** as privacy metric.
- **Energy storage model:**
 - Three-circuit model to account for steady state energy losses
 - Slow **degradation of energy storage** modelled using Monte Carlo sampling of existing high-fidelity models.
- **Control strategy design:**
 - Objective is to minimize the weighted sum of privacy loss and storage usage cost.
 - Optimal strategy can be achieved by using partially observable Markov decision process.



Reference: R.R.Avula, J.Chin, T.J.Oechtering and G.Hug "Smart Meter Privacy Control Strategy Including Energy Storage Degradation", accepted to IEEE PES PowerTech, 2019.

Privacy and storage degradation trade-off



- By including the degradation losses in the design, **significant improvement in battery lifetime can be achieved**, at the expense of some privacy loss.

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

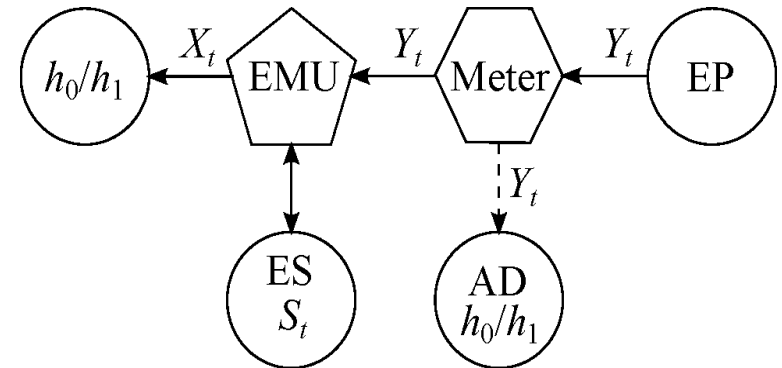
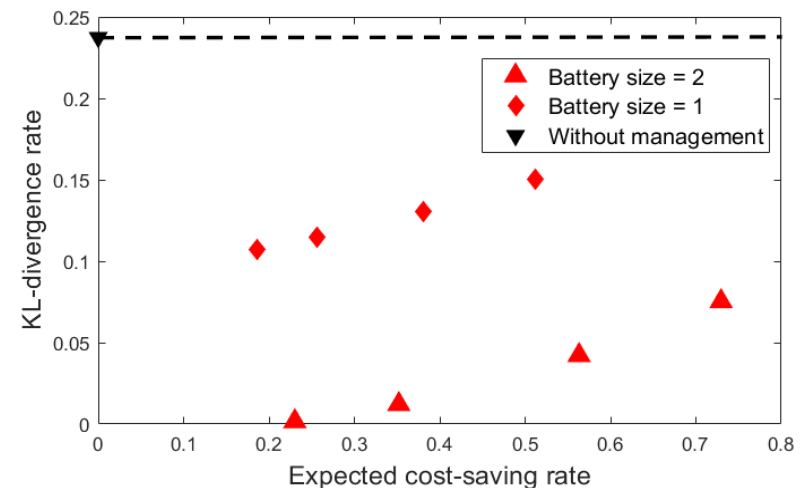
- **System setting:**
 - Binary energy consuming hypothesis
 - Random energy demand and price
 - Finite-capacity energy storage
- **Objectives:** Minimize weighted sum of
 - Privacy leakage rate:

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

- 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
 - Reinforcement learning



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

Fisher-information-based Privacy

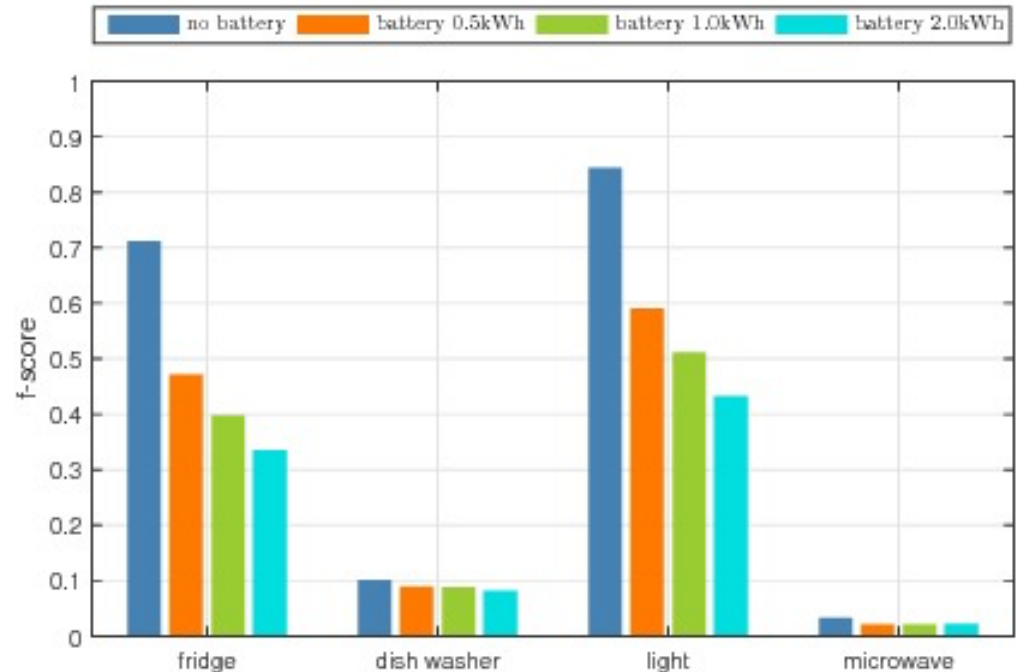
- Run battery or HVAC system to make **estimation of privacy-sensitive information** as hard as possible given SM data

- Cramér-Rao bound* provides a lower operational bound for adversary's estimation quality:

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

- We developed efficient schemes to run battery or HVAC units to **make Fisher information as small as possible**.

- Figure:** Fisher-info-optimal battery use 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

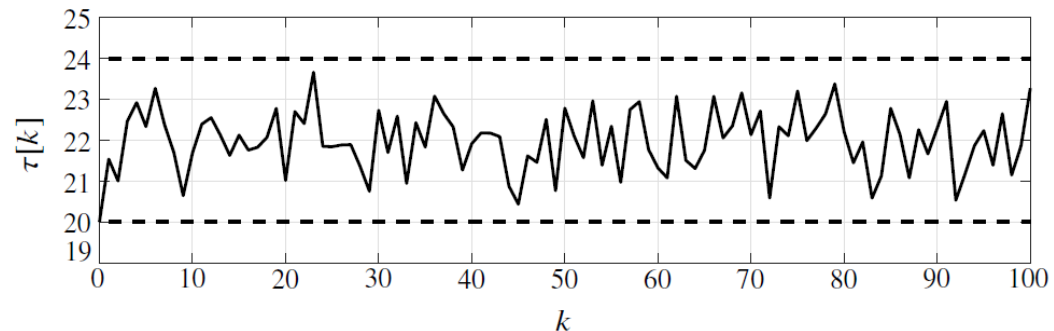
TP = True positives

Fisher-information-based Privacy Using HVAC-units

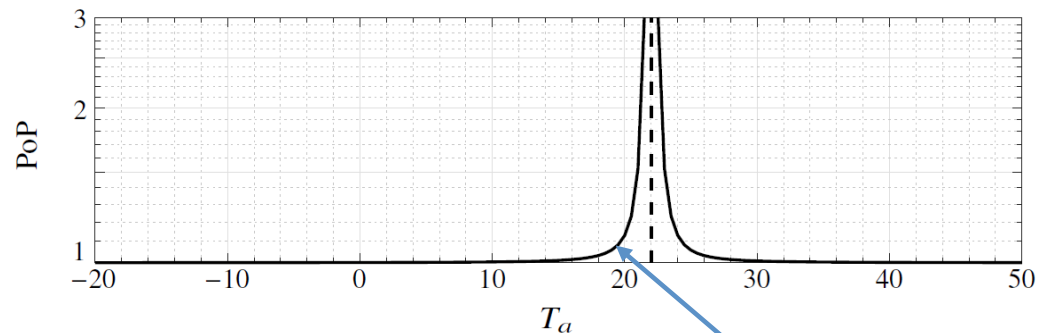
Problem: Choose HVAC-unit consumption $w[k]$ (times $k=0,1,2,\dots$) to make estimation of privacy-sensitive data as hard as possible, while maintaining temperature $\tau[k]$ within comfort constraints.

Solution: Compute such sequence $w[k]$ minimizing Fisher information.

*Example of
resulting room
temperature:*

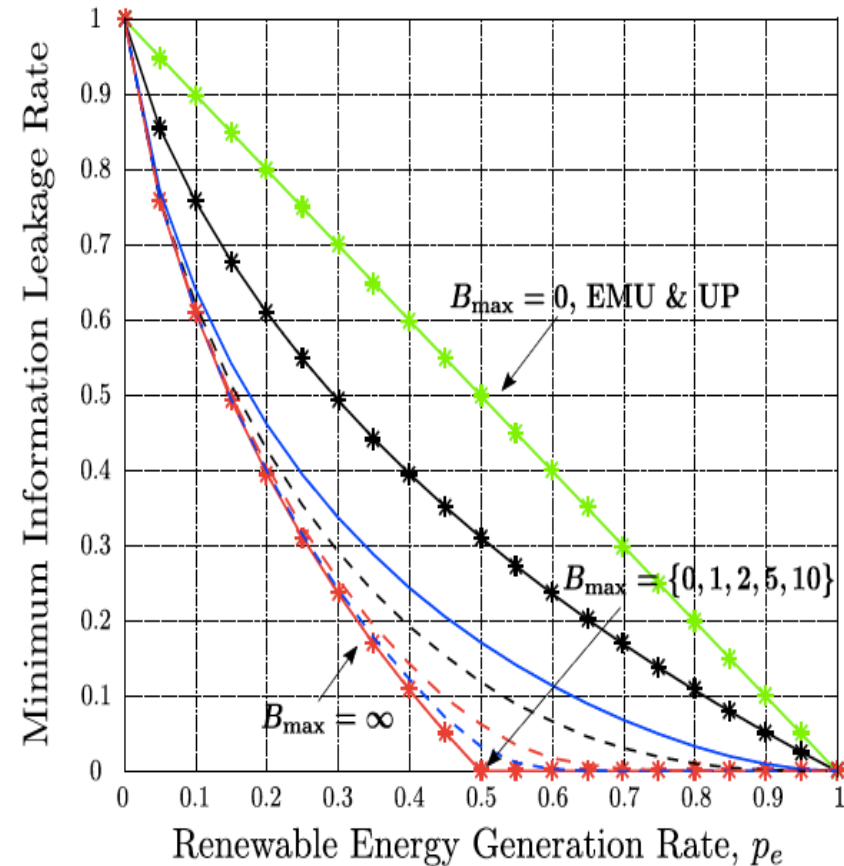


*Relative Price of Privacy vs
ambient temperature (T_a):
(At $T \approx 22^\circ\text{C}$ HVAC not a
needed for temp. control at all,
so all energy use is for privacy)*



Information theoretic privacy with demand shaping

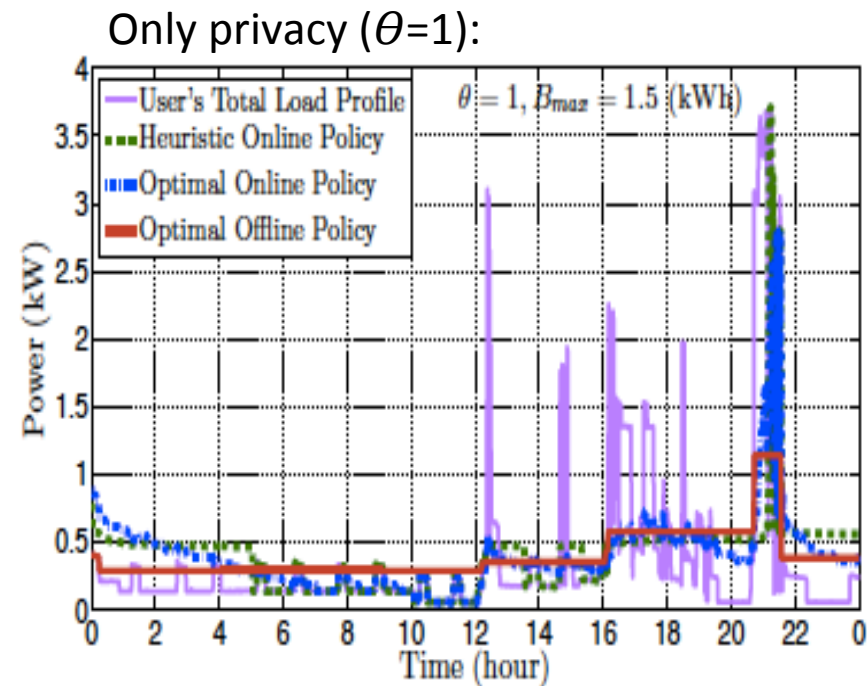
- Information theoretic smart meter privacy with **battery** and **renewable energy source**
 - Leakage rate measured by **mutual information** between real demand and what is received from the grid
 - Optimal characterization for extreme cases of zero or infinite battery capacity
 - Low-complexity general solutions



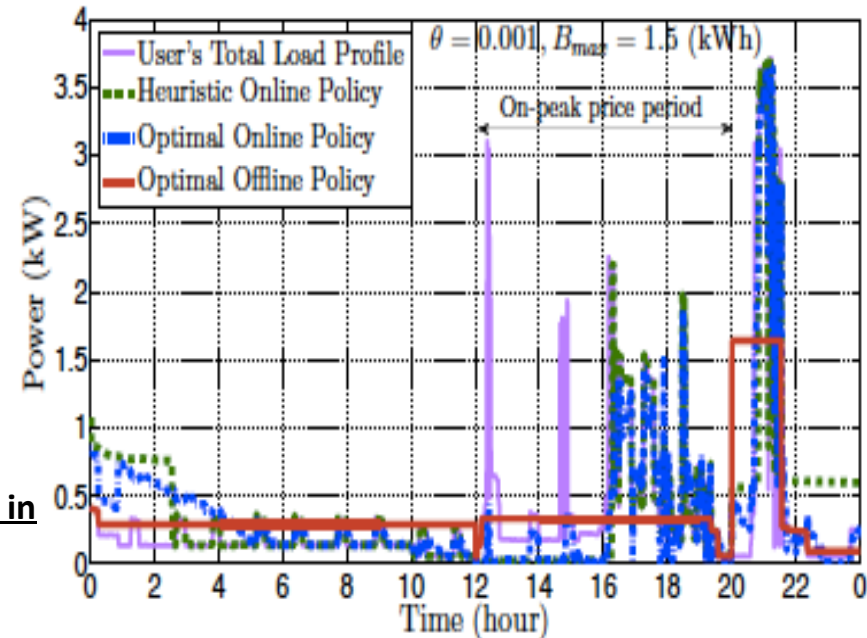
Battery capacity: $B_{\max}$

Privacy-cost tradeoff

- Privacy measured by load variance (perfect privacy when completely flat consumption profile)
- Convex optimization problem
- Water-filling like solution



(a)



(b)

O. Tan, J. Gomez-Vilardebo, and D. Gunduz, **Privacy-cost trade-offs in demand-side management with storage**, *IEEE Transactions on Information Forensics & Security*, no. 6, pp. 1458-1469, Jun. 2017.

New privacy measure: total variation distance

- Total variation distance between distributions p_X and q_X :

$$\delta(p_X, q_X) \triangleq \frac{1}{2} \|\mathbf{p} - \mathbf{q}\|_1$$

- Privacy leakage about X by revealing U measured as

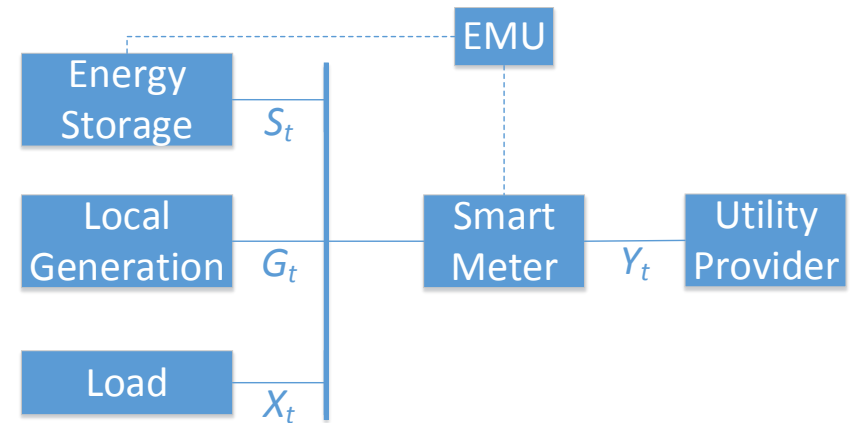
$$T(X; U) \triangleq \frac{1}{2} \sum_u p_U(u) \|\mathbf{p}_{X|u} - \mathbf{p}_X\|_1$$

- Satisfies post-processing and linkage inequalities, which makes it consistent with an intuitive notion of a privacy measure
- Optimal utility-privacy trade-off solved by standard linear program
- Provides a bound on leakage measured by mutual information and maximal leakage

B. Rassouli and D. Gunduz, **Optimal utility-privacy trade-off with total variation distance as a privacy measure**, *IEEE Transactions on Information Forensics & Security*, to appear.

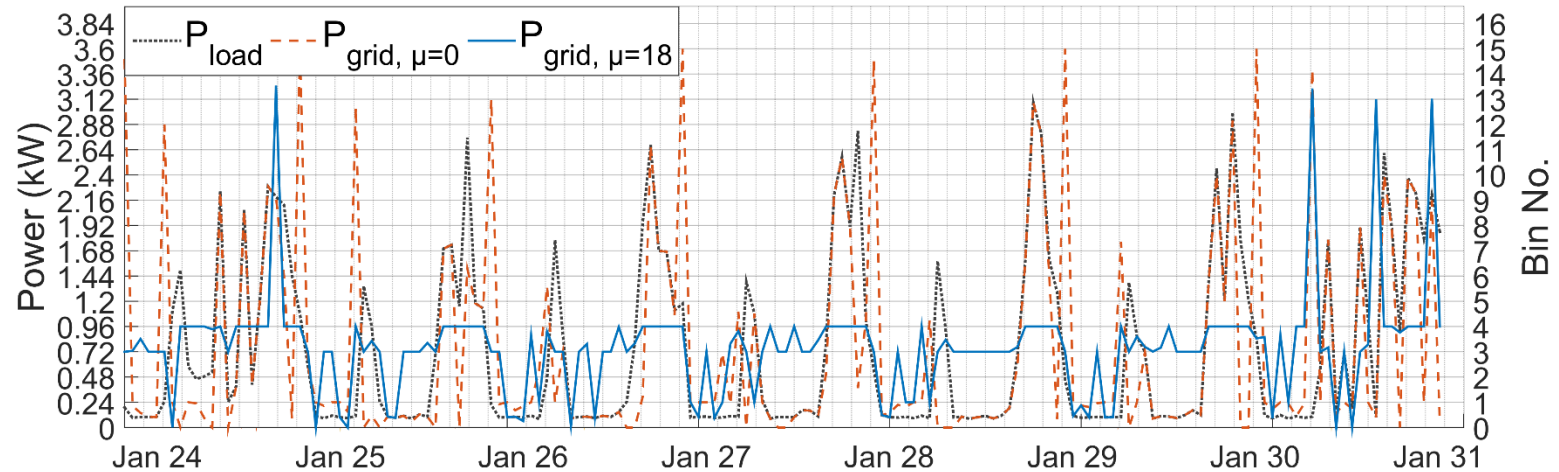
Privacy-Protecting Energy Management Unit through Model-Distribution Predictive Control

- Developed an approach based on **Model Predictive Control**
- 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

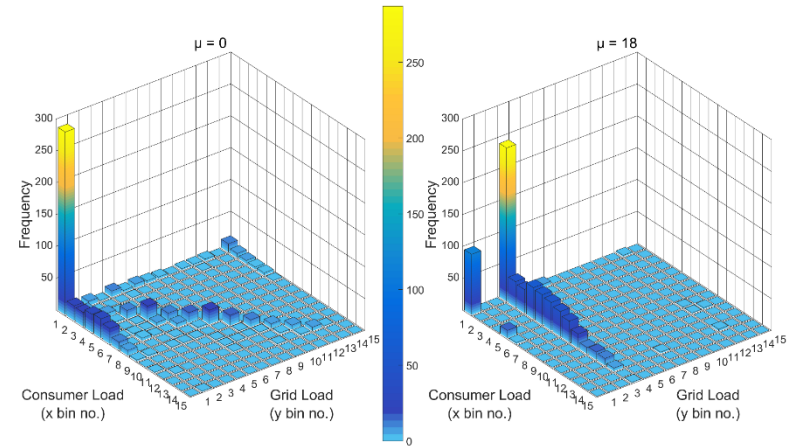
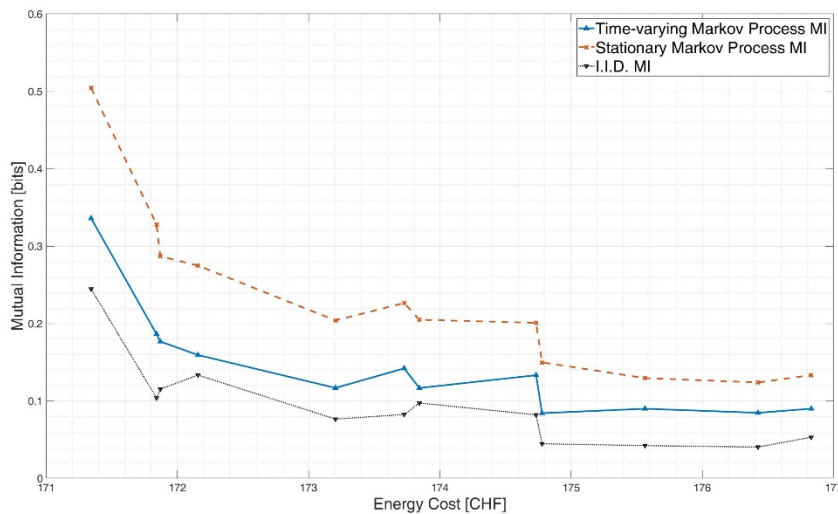
Resultant Grid-Visible Load



- 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.

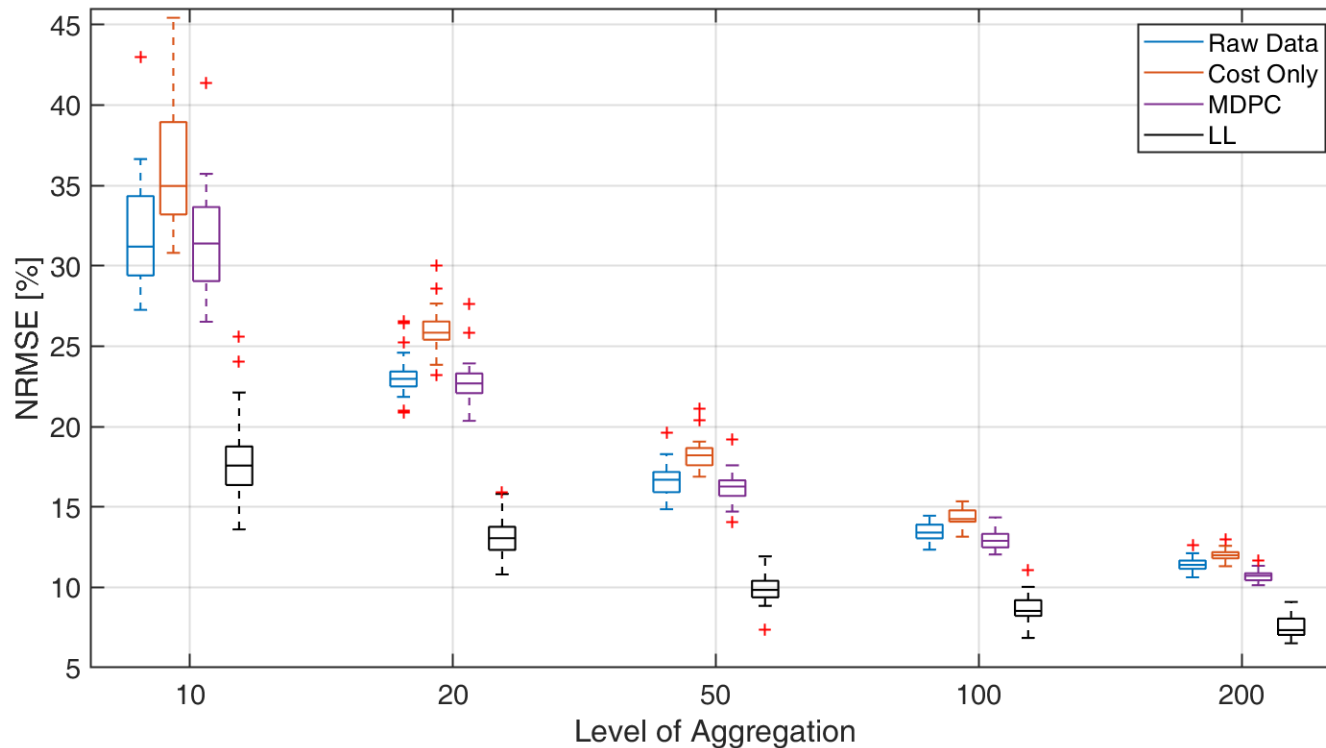
Consumer and Grid-Visible Loads

Energy Cost and Privacy Centric Statistics:
Consumer load statistics are masked



Time-varying Markov process MI estimation
better captures actual consumer privacy-loss

Impact of Privacy Protection on Load Forecasts

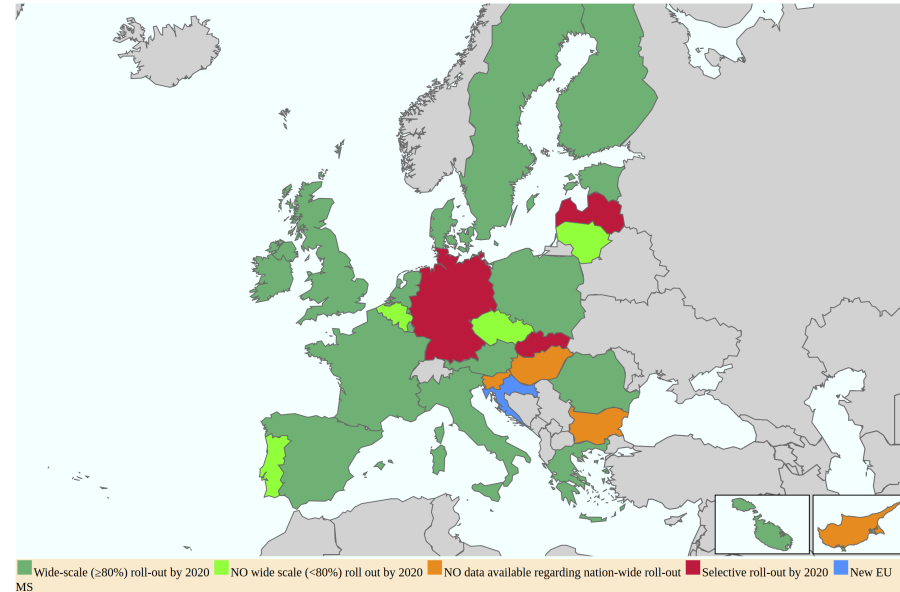


Privacy-Protection can have negligible impact on short-term load forecasting

May even improve forecast accuracy!

GDPR and Smart-meters (I)

- **Smart-meters are deployed in the European Union:**
 - Directive 2006/32/CE,
 - Directive 2009/72/CE.
- In France, Enedis is in charge of deploying the LINKY smart-meter.



- Source: JRC "SMART ELECTRICITY SYSTEMS AND INTEROPERABILITY"

- **Since May 2018, the GDPR has been enforced.**
- **How does the GDPR apply to smart-meters data collection ?**

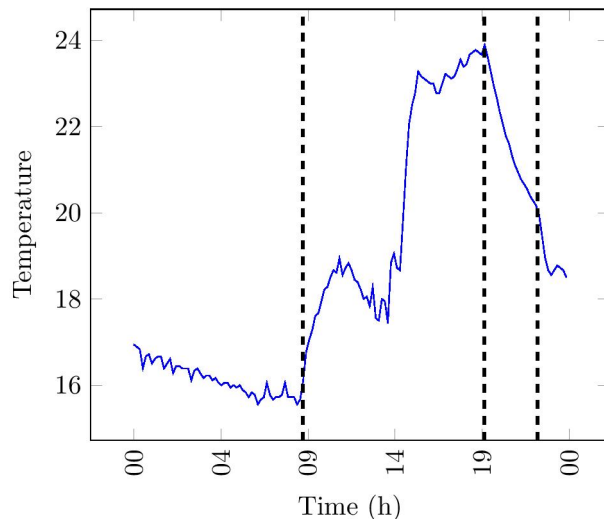
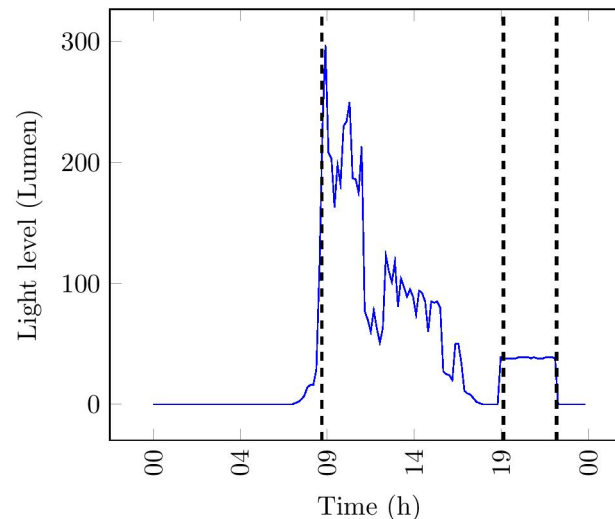
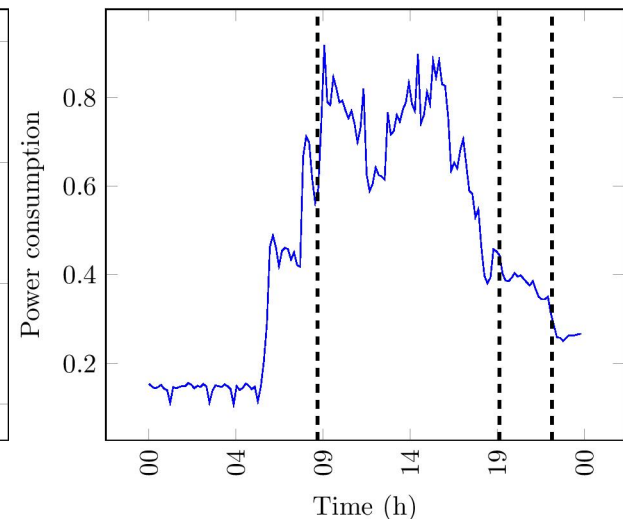
GDPR and Smart-meters (II)

- **Our power consumption profile is:**
 - a personal data ?
 - **or a sensitive data ?**
- **The frequency of the data collection is the key metric:**
 - Every seconds → **sensitive**
 - Every hour → **sensitive**
 - Every day → **not sensitive**
- At least according to CNIL and ENEDIS...
- ...but can it be challenged ?

**From day to day profile,
it is still possible to recover your religion !**

Activities → Sensors → Power consumption

- **We gather two month of data for 1 office in a smart-building**
 - Light, temperature, fan mode...
 - **and power consumption.**
- **We re-identify human activities.**



Dissemination

- 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
 - to research institutes such as National Renewable Energy Laboratory, Electric Power Research Institute, Aug 2018
 - 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

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

Dissemination

- 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 (23000 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.
 - Panel event on future research direction in IFS at WIFS 2019
 - at KTH Campus 100 year celebration to the general public
 - to industry: Vattenfall, Northvolt
 - at several stakeholder events 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 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



- + additional discussions within COPES on additional funding opportunities

