# Privacy-Aware Smart Metering

Deniz Gündüz[1] Tobias Oechtering[2]

[1]Imperial College London

[2]KTH Royal Institute of Technology

Tutorial at

2018 IEEE Workshop on Information Forensic and Security

Hong Kong, Dec 10, 2018

# Acknowledgements

Our special thanks to our collaborators and students:
Gabriela Hug (ETHZ), Cedric Lauraudoux (INRIA), Henrik Sandberg (KTH), Ramana Reddy Avula (KTH), Giulio Giaconi (Imperial), Jesus Gomez-Vilardebo (CTTC), Zuxing Li (Supélec), Daniel Månsson (KTH), H. Vincent Poor (Princeton), Borzoo Rassouli (Imperial), Onur Tan (CTTC-Imperial), Yang You (KTH), Chin Jun Xing (ETHZ)

and funding agencies for their generous support:
Swedish Research Council, Engineering and Physical Sciences Research Council (EPSRC), CHIST-ERA, Swedish Energy Agency

# Scope

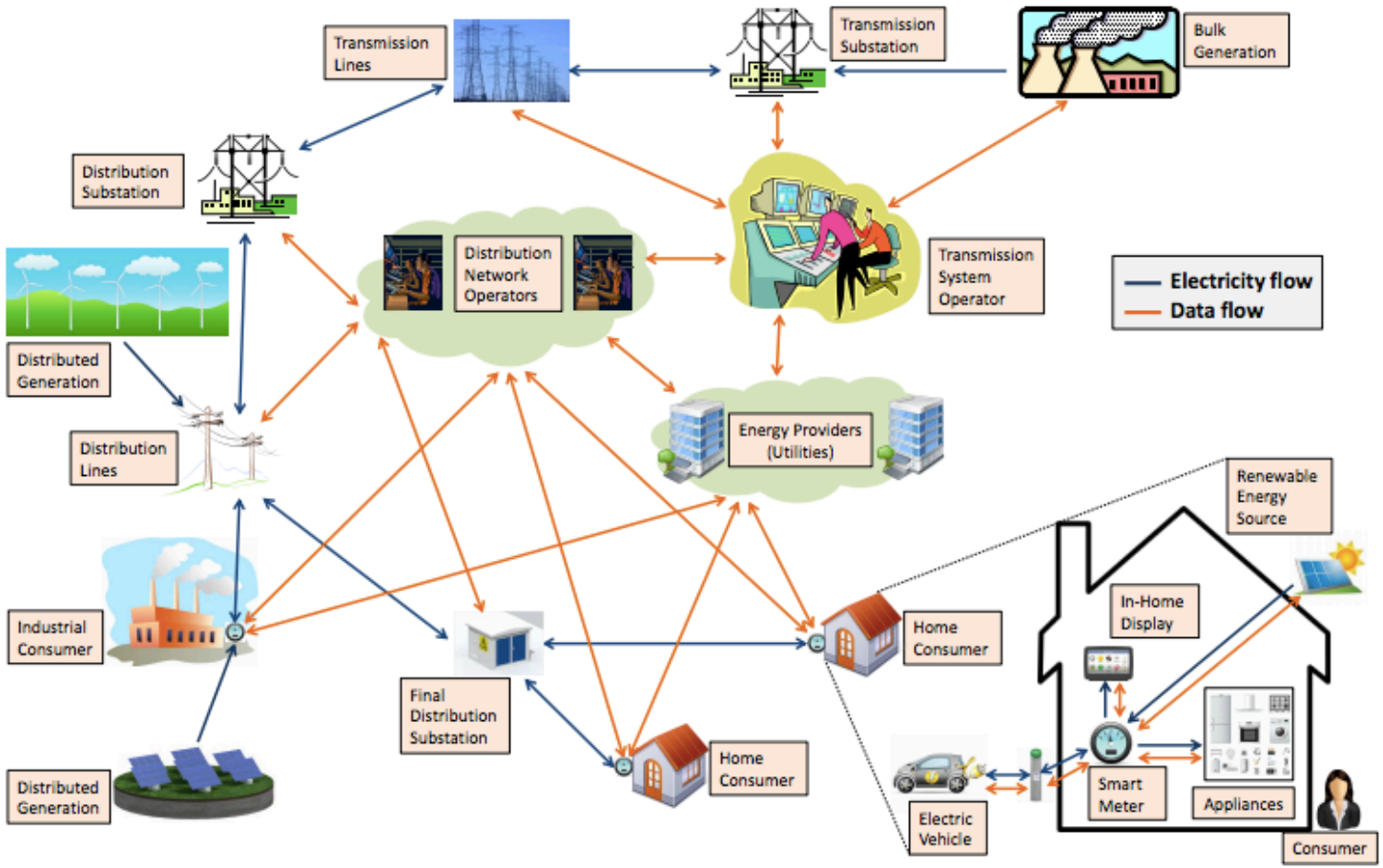
- What is the problem?
- What are the implications of privacy issues in smart meters?
- How to measure privacy in smart meter context?
- Existing approaches and solutions
- Remaining challenges, future research directions

# Smart Energy Grid

Smart grid refers to the future energy grid that exploits information and communication technologies

- to increase reliability,
- to increase efficiency and reduce carbon footprint,
- to incorporate renewable as well as traditional energy sources,
- to provide security,
- to introduce new services that cannot be foreseen today.

# Smart Energy Grid Entities



# Smart Energy Meters



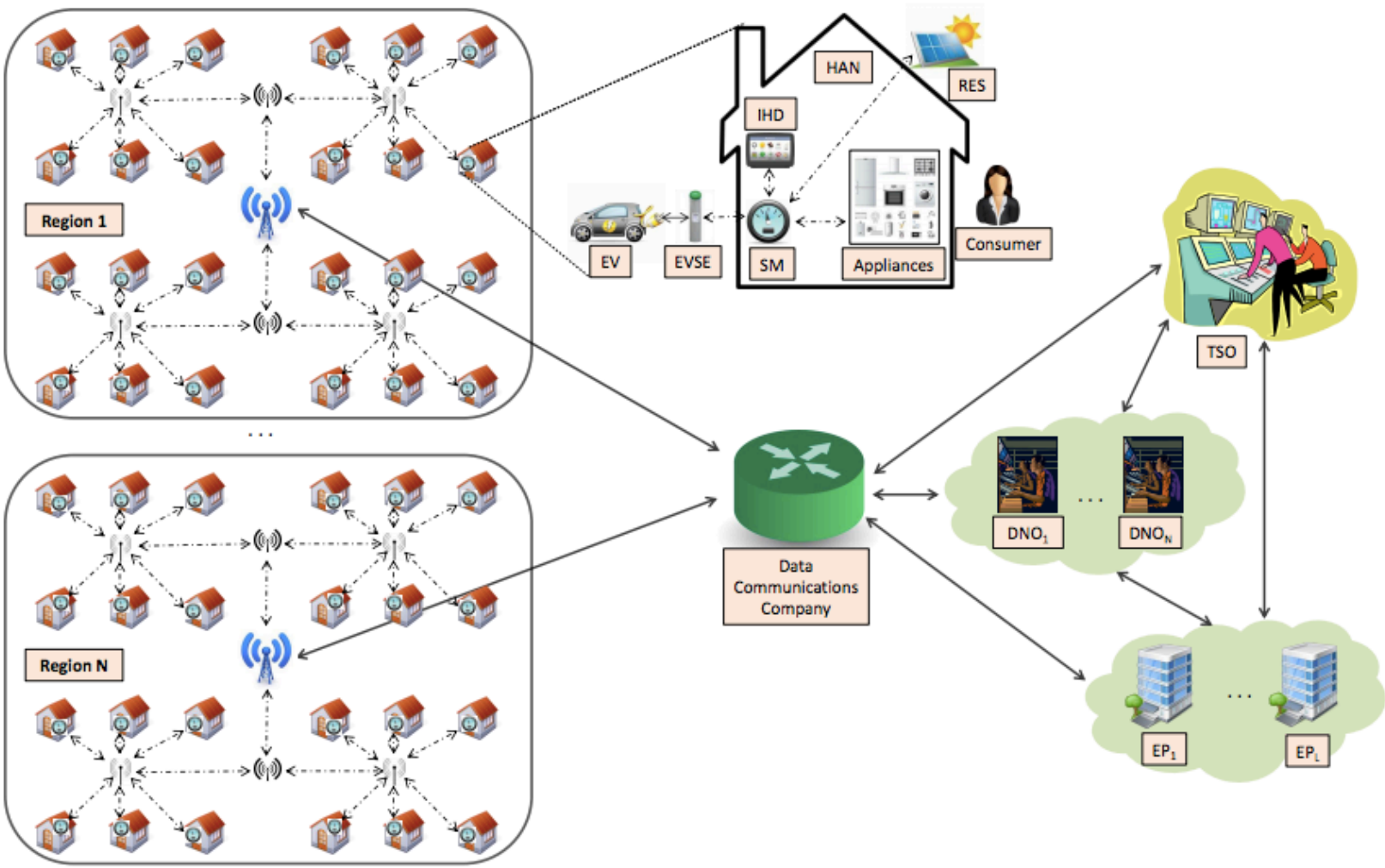
Smart meters (SMs) are an essential component of smart grids; they enable many "smart" grid functionalities.

SMs introduce the ability to provide bi-directional communication between consumers and the energy supplier/ grid operator and to promote services that facilitate energy efficiency within the home.

---

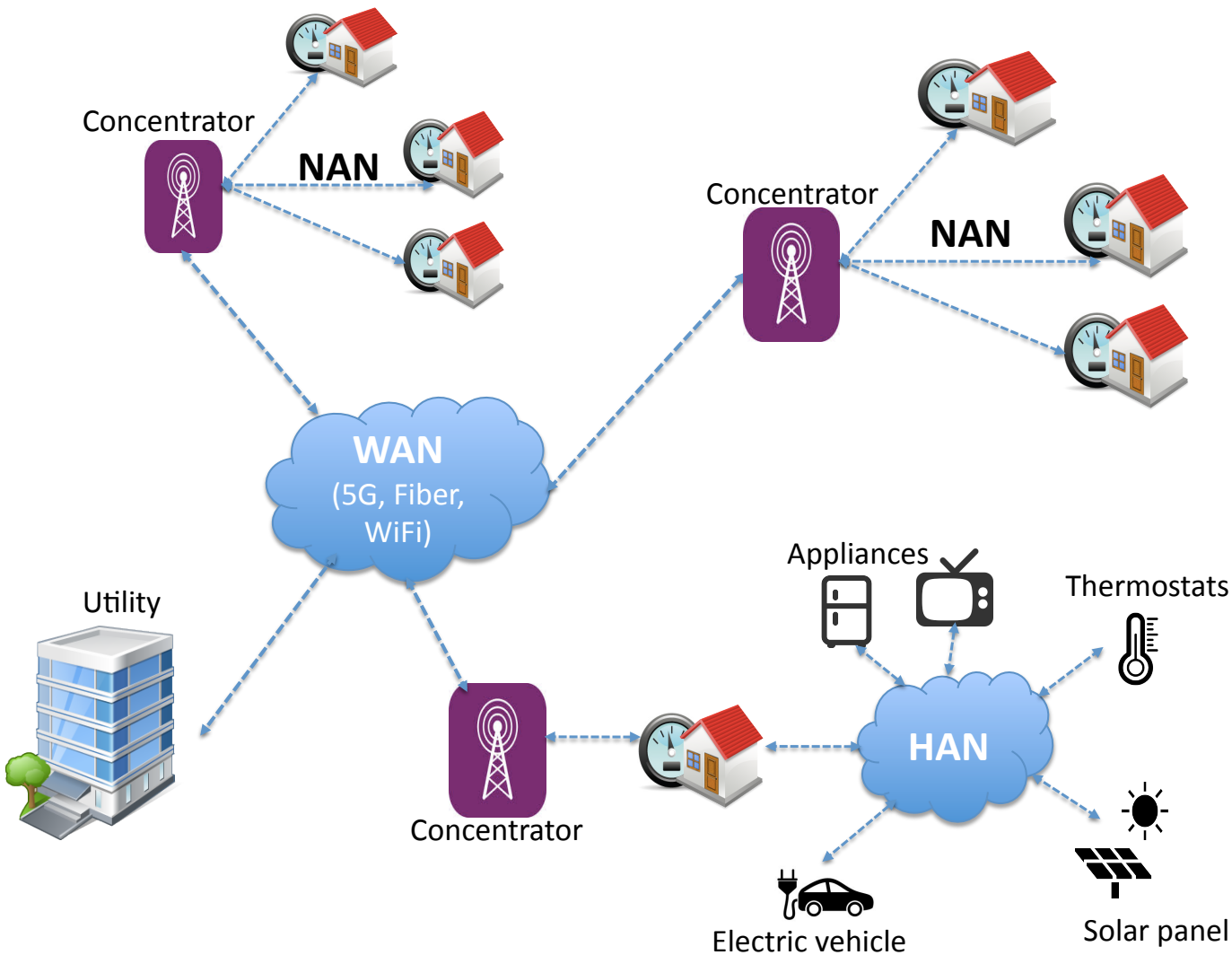
The European Commission's Interpretative Note on Directive 2009/72/EC.

# Advanced Metering Infrastructure (AMI)



# Advanced Metering Infrastructure (AMI)

AMI uses two-way communication to both transmit usage information and perform observation and maintenance tasks.



# What do Smart Meters (SMs) Measure?

SMs do more than measuring and reporting energy consumption:

- Readings of active, reactive, and apparent power and energy consumption (*4-quadrant metering*),
- Energy generated by the user and sold to the grid,
- Alerts about voltage quality measurements,
- Data for billing (e.g., time-of-use tariff, balance and debts),
- Tamper status,
- Security credentials for enabling cryptographic protocols,
- Firmware information and updates.

# Benefits to Consumers

- Ability to track energy consumption near real time, which leads to better energy usage management,
- More accurate and timely billing services,
- Possibility to benefit from demand flexibility and time-of-use (ToU) pricing,
- Possibility to introduce safety solutions through better power quality and breakdown management,
- Appliance failure detection, detection of waste, detection of unexpected activity or inactivity,
- Increase competition among energy providers due to ease of switching for customers,
- Integrate microgeneration and energy storage capabilities.

# Benefits to Energy Providers

- Reduced cost of meter readings,
- More accurate billings: Reduced customer complaints and back office rebilling,
- Energy theft detection,
- Introduce time-of-use pricing for demand management,
- Load-shaping to reduce peak loads thanks to improved demand forecasts.

# Benefits to Distribution System Operators (DSOs)

- Reduced operational costs,
- Improved fault detection possibilities,
- Increased grid efficiency, reduced energy losses,
- Better matching distributed resources to user demand and grid's power delivery,
- Improved distributed state estimation and Volt and Var control,
- Reduced need for additional generation.

# Smart Metering Standardization

## Open Smart Grid Protocol (OSGP)

European Telecommunications Standards Institute (ETSI) approved, OSGP Alliance (Mitsubishi, Schneider, Vattenfall, Ericsson, Oracle). Used with ISO/IEC 14908 control networking standard for smart grid applications. Uses power-line communications as physical layer. Over 40 million OSGP-based SMs deployed worldwide -most widely used standard.

## IEEE 802.15.4g

Wireless Neighborhood Area Networking (NAN) standard developed by IEEE Smart Utility Networks (SUN) Task Group (Elster, Itron, Landis+Gyr, NICT, and Silver Spring Networks).

## Telecommunications Industry Association (TIA)

TR-51 engineering committee, Smart Utility Networks, is also developing air-interface, network and conformance standards to support smart grids.

# Smart Metering Market

- Global smart meters market is estimated to grow from $12.79 billion in 2017 to $19.98 billion by 2022, at a compound annual growth rate (CAGR) of 9.3% from 2017 to 2022.
- Global market for SM analytics to reach $2.6 million by 2022.
- Global penetration to grow from 30% (2016) to 53% by 2025 with nearly 1.2 billion smart residential meters worldwide.
- China leads the market: 350 million installed meters
- Directive of the European Parliament requires 80% penetration by 2020: current installations 200 million.
- In UK, 53m meters in 30m households by 2020 is expected to cost £10.9bn. Government estimate: £7 billion net benefits to consumers, energy suppliers and networks over 20 years.

# Smart Meter Privacy Concerns



- Netherlands: Senate voted against mandatory roll-out of SMs, found to be against European Convention on human rights
- 9000 consumers polled in 17 countries: 1/3 discouraged from using SMs if it gave utilities access to their energy use

# Smart Meter Privacy Concerns

Dutch anti-smart meter logo; roughly equivalent to "Smart Metering Equals Spying"



- "Security experts warn that the smart meters can be infected with a virus that can spread between different devices, and cutting some individual energy supplies off. Others warn that they could even be hacked and used for terrorism."

---

https://www.telegraph.co.uk/money/consumer-affairs/six-reasons-say-no-smart-meter/ (accessed on 15 March 2018).

# Smart Meter Privacy Concerns

## Scots have topped a UK poll of box set bingers

The data from Scottish Gas shows that in 2015 entertainment energy usage in Scotland hit an annual high in April last year, coinciding with the release of Game of Thrones Season 5, as the nation powered up their TVs, laptops and tablets to follow the latest instalment from Jon Snow and friends.

The utility company collected the information from Smart meters which come with a smart energy monitor, which gives households a better understanding of their energy use by showing them exactly what energy they are using on entertainment devices.

---

http://www.brechinadvertiser.co.uk/news/scots-have-topped-a-uk-poll-of-box-set-bingers-1-4112286.

# Smart Meter Privacy Concerns

## Generating value from smart meter data

### Making the most of the smart meter roll-out

Programmers from CSE and the University of Bristol set out to develop a new computational system that would allow the extraction of commercially valuable patterns from smart meter data. They came up with a prototype 'Big Data' platform called 'Smart Meter Analytics, Scaled by Hadoop' (SMASH).

In parallel, a data mining team from the University of Bristol applied new, experimental techniques to a sample of real smart electricity meter data to identify interesting subgroups of consumers with statistically different consumption patterns. Scottish and Southern Energy and Western Power Distribution were partners in this project, providing an invaluable perspective from the electricity industry, and confirmation that the tools and techniques being developed had real business relevance for them. One key application they identified was that the tools would enable energy suppliers and District Network Operators to generate more accurate profiles of consumption, where before they were forced to generalise.

---

https://www.cse.org.uk/projects/view/1210.

# Smart Meter Privacy Concerns: USA

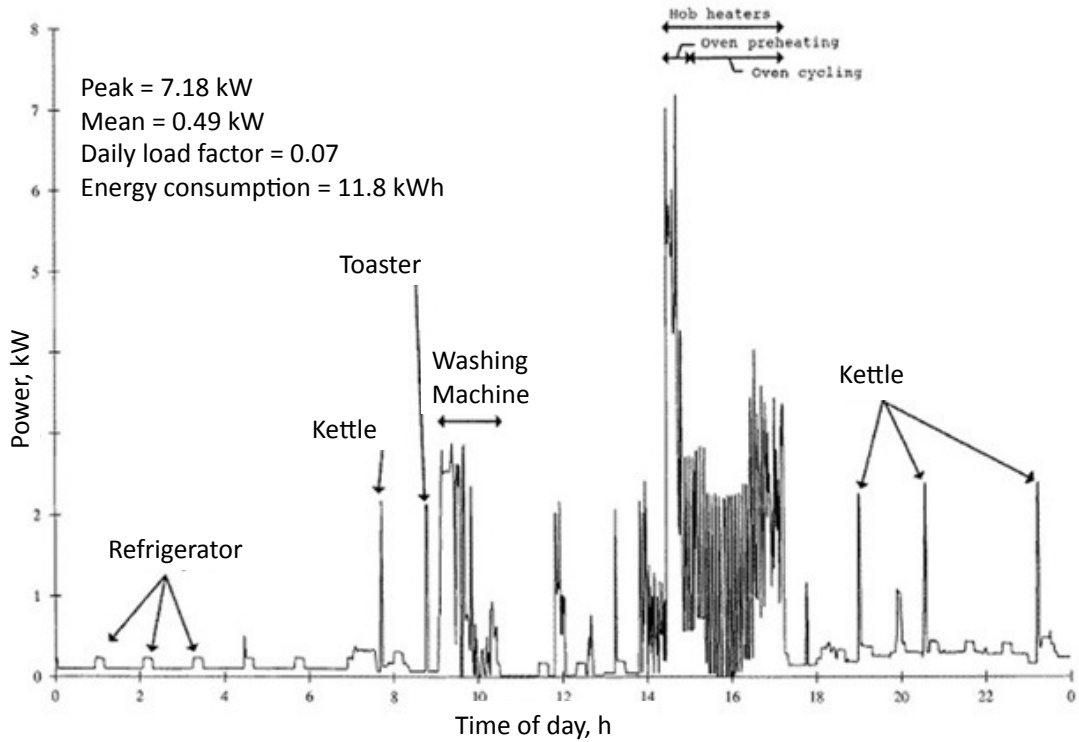

"Your smart meter data reveals binge TV viewing on Saturday nights and frequent use of an electric can opener. We thought you might enjoy an evening out."

Naperville Smart Meter Awareness v. City of Naperville: Court decides Fourth Amendment protects energy consumption data collected by SMs:
"Individuals have a reasonable expectation that SM data should remain private, and government's access of it constitutes a 'search' ".

---

https://bit.ly/2SENBI1

# Smart Meter Privacy: Technical Angle




- Non-intrusive load monitoring (NILM) techniques
- Can track appliance usage patterns, home occupancy, even the TV channel user is watching.

---

U. Greveler et al., "Multimedia content identification through smart meter power usage profiles," *Int'l Conf. on Information and Knowledge Eng.*, July 2012.

# Smart Meter Privacy: Social Angle

- **Patterns** (behaviour profiling)
  - Watching too much TV?
  - Another microwave meal?
- **Real-time surveillance**
  - Were you home last night?
  - Did your friend move in?
- **Non-grid use of data**
  - Advertising and spam
  - Insurance
  - Appliance warranties
- **Information leakage**
  - Phishing, pharming, fraud

"Guidelines for Smart Grid Cyber Security," National Institute of Standards and Technology (NIST), Privacy and the Smart Grid, vol. 2, NIST IR 7628 Rev. 1, Sep. 2014.

# Potential Risks

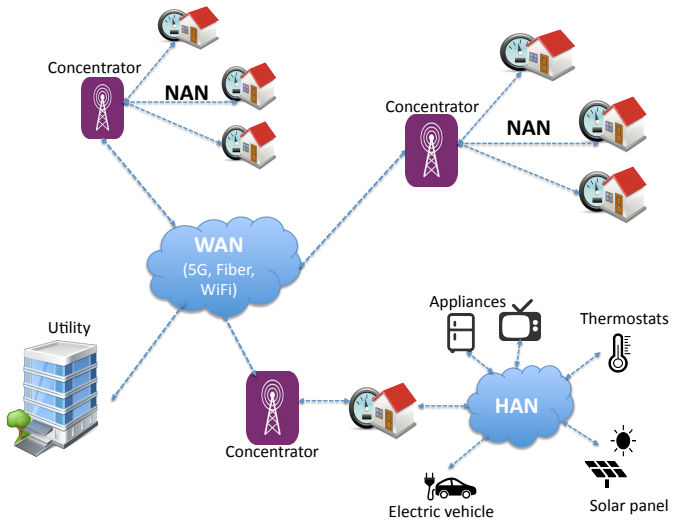
| **Who wants meter data?** | **How could it be used?** |
|---|---|
| Utilities | To monitor electricity usage and load; to determine bills |
| Advisory companies | To promote energy conservation and awareness |
| Insurance companies | To determine premiums based on unusual behaviors that might indicate illness |
| Marketers | To profile customers for targeted advertisements |
| Law enforcers | To identify suspicious or illegal activity |
| Civil litigators | To identify property boundaries and activities on premises |
| Landlords | To verify lease compliance |
| Private investigators | To monitor specific events |
| The press | To get information about famous people |
| Creditors | To determine behavior that might indicate creditworthiness |
| Criminals | To identify best times for a burglary, or valuable appliances to steal |

"Potential Privacy Impacts that Arise from the Collection and Use of Smart Grid Data," NIST, vol. 2.

# Smart Meter Security

- Security $\neq$ Privacy
- Remote switching off capability of smart meters opens up new vulnerabilities (Stuxnet type cyber attacks)
- Meters can be hacked by consumers or third parties to reduce/increase energy bill
  - a utility in Puerto Rico lost $400 million in annual revenue after criminals hacked into smart meters to under-report electricity usage.
- Smart meters are made to last (15-20 years). Encryption mechanisms are not adaptive, and cannot last as long.
- Highly connected AMI allows spread of malware
- Wireless transmission of meter readings is prone to eavesdropping and data injection attacks

# Smart Meter Security Problems




- Serious security risks reported in AMI architecture
- Flaws in authentication mechanism of Open Smart Grid Protocol
  - K. Kursawe and C. Peters, Structural Weaknesses in the Open Smart Grid Protocol, Cryptology ePrint Archive, Report 2015/088.
  - P. Jovanovic and S., Neves, Dumb Crypto in Smart Grids: Practical Cryptanalysis of the Open Smart Grid Protocol, Aug. 2015.
  - L. Feiten and M. Sauer, Extracting the RC4 secret key of the Open Smart Grid Protocol, IACR Cryptology ePrint Archive, 2016.

# Security Measures against Attackers

- Authentication and authorisation
- Secure networks and communication links
- Secure data aggregation
- Secure multi-party computing
- Encrypted functions
- Zero-knowledge-proof cryptography
- Physically unclonable functions

# Confidentiality and Authorisation vs. Privacy

## Confidentiality

set of rules that limit access or place restrictions on disclosure of information, e.g., by means of encryption. It ensures that access to information is restricted to authorized entities.

## Authorisation

limits access to certain entities. Authorization is usually coupled with authentication.

In SMs, privacy is not only against third parties/ attackers, but also against the legitimate/ authorised receiver of data.

# What is Privacy?

## Data privacy (OECD Glossary of Statistical Terms)

It is the status accorded to data which has been agreed upon between the person or organisation furnishing the data and the organisation receiving it and which describes the degree of protection which will be provided.

## Personal data (EU Data Protection Directive)

Any information relating to an identified or identifiable natural person should (among other things) a) "be collected for a specified purposes and not be further processed for other purposes", and b) "be merely adequate and not excessive for the purposes motivating its collection".

- Explains the notion of privacy
- Does not specify how privacy protection can be applied
- To protect privacy we first need to measure it

# Paradigm Shift: Privacy Against Energy Providers (EPs)/ Grid Operators

- Focus of current SMs is on protection against manipulation by customers.
- Grid operators/ EPs can remotely update crucial meter parameters (e.g., cryptographic keys, sampling frequency), install new software, or disconnect energy.
- Masurement data collected and stored in database of the operator.
- Trust in grid operators: customers are protected mainly by guidelines, audits, codes of behaviour.

# Privacy - Utility Trade-off

## Billing problem

EP needs to bill users. Perfect attribution and exactness required. Low sampling frequency sufficient.

## Grid management problem

Energy provider needs to manage the grid. High sampling frequency required, attribution exactness not necessary (i.e., can work with aggregate meter readings).

Meter data can leak sensitive information that should be kept private. There is a trade-off between utility and privacy.

# Non-Intrusive Load Monitoring (NILM)

**Content:**

- Introduction
  - Load categories, framework, features, ...
- Basic principles of some algorithmic approaches
  - Supervised vs. unsupervised learning
  - K-means clustering, neural networks
    naïve Bayes, hidden Markov models, ...
- Available datasets and toolboxes
  - Few numerical examples

---

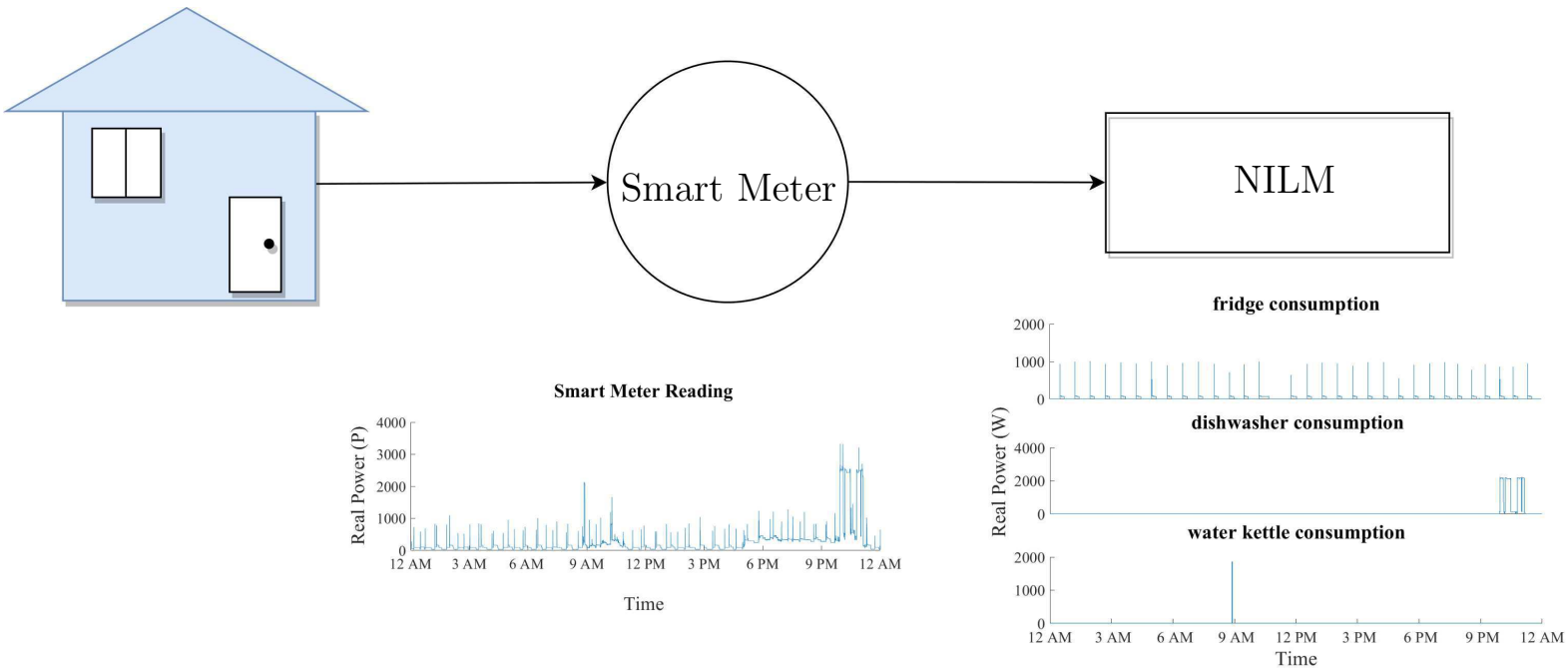
Zoha et al. "Non-intrusive load monitoring approaches for disaggregated energy sensing: A survey" 2012.
Klemenjak and Goldsborough "Non-Intrusive Load Monitoring: A Review and Outlook" 2016.

# Load Monitoring

- Load monitoring is the process of estimating the energy consumed by individual appliances.
- (Main) motivation and benefits
  - Consumer: Smart and reasonable energy consumption behaviour (e.g. for cost-saving)
  - Energy provider & grid operator: Efficient energy generation and management of the energy flows in the grid
- Approaches:
  - Intrusive load monitoring (ILM): Sensors measure consumption of appliance directly (intrusive, costly $\overset{\text{likely}}{\rightarrow}$ desired, consensual)
  - Non-intrusive load monitoring (NILM)

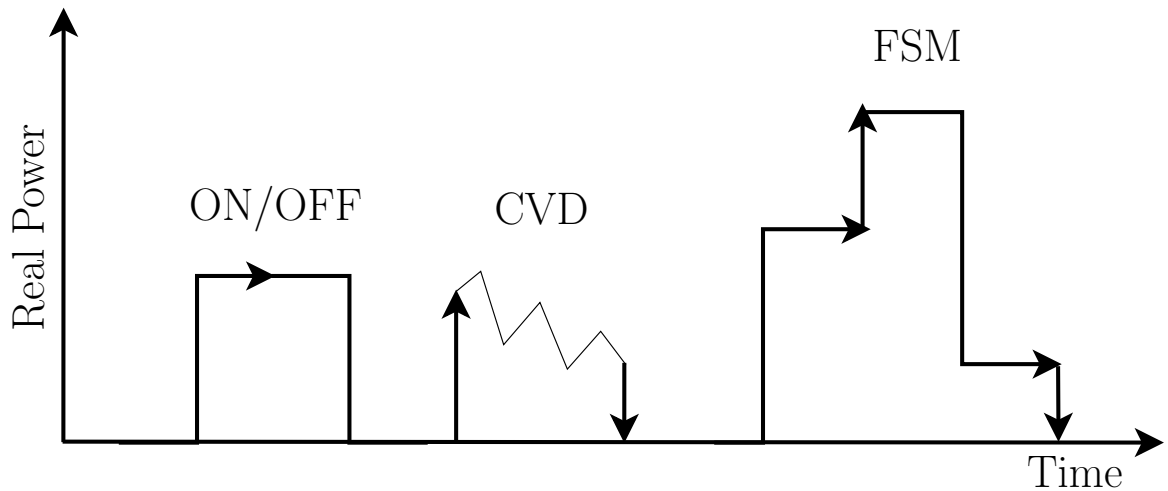
# Non-Intrusive Load Monitoring (NILM)

- SM readings
  - provide aggregated consumption profile $P(t)$ of all appliances
  - obtained non-intrusively $\rightarrow$ low cost $\rightarrow$ processing consensual?
  - used by NILM for disaggregation $P(t) = p_1(t) + p_2(t) + p_3(t)$



# Categories of Consumer Appliances

- Three main types of appliances
  - ON/OFF state machines, e.g. light,
  - Continuously variable devices (CVDs), e.g. heating device,
  - Finite state machines (FSM), e.g. fridge.

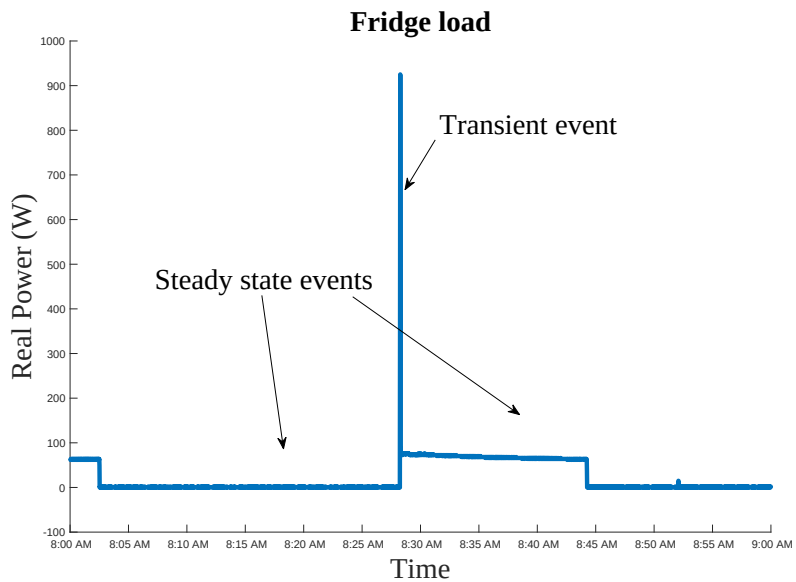


# NILM Framework

1. Data acquisition by smart meter
   - Low frequency readings
   - High frequency readings
2. Feature extraction
   - Steady state features
   - Transient state features
   - Non-traditional features
3. System training (initialization)
4. Inference and learning
   - Supervised learning (training with labeled load profile)
   - Unsupervised learning (training with unlabeled load profile)

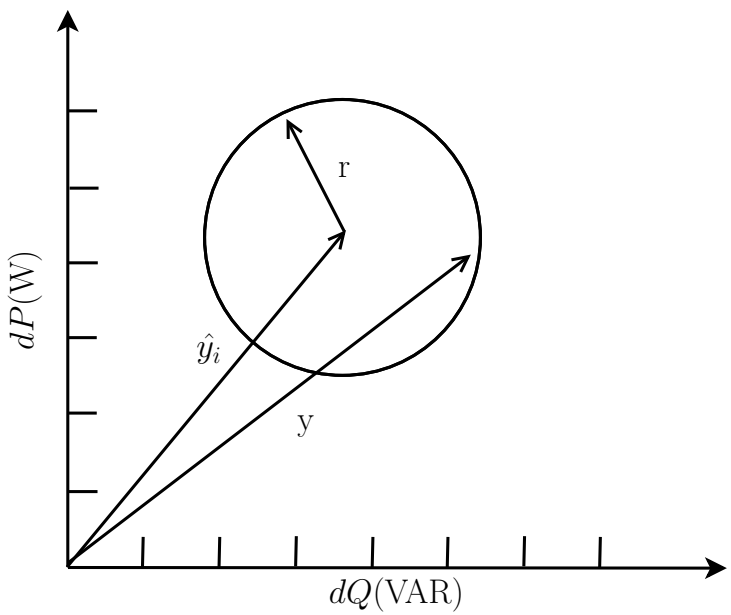
# Feature Extraction

- Steady state features: Power change, time and frequency domain characteristics of VI waveforms, etc.
- Transient features: Transient power, start-up current transients, etc.
- Non-traditional features: Time of the day, on-off duration distribution, frequency of appliance usage, etc.



# Supervised Learning - P-Q plane Classification

- Two-dimensional feature space
  - Real power (P) and reactive power (Q)
  - In order to identify ON/OFF events, changes in real power (dP) and reactive power (dQ) are often used.




- Distance-based classification
  - Given feature vector $y$ of an unknown load:
  - Identify a known load signature $\hat{y}_i$ (class) it matches best, i.e.,

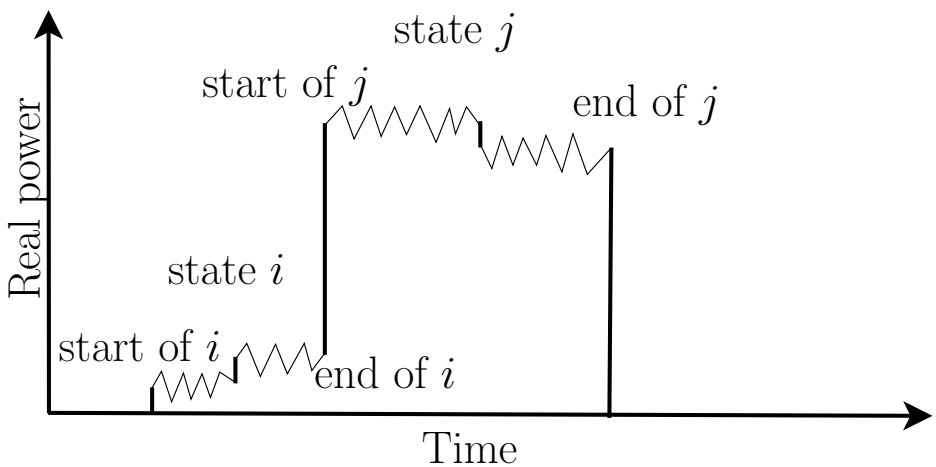
$$class\ i = \arg\min_i ||y - \hat{y}_i||$$

G.W. Hart "Non-intrusive appliance load monitoring," in *Proc. of the IEEE*, 1992.

# Supervised Learning - P-Q plane Classification Extension

Various extensions have been proposed:

- "Weiss" algorithm: Take **oscillations** during start up and shut down of an appliance into account.
  - Let $\overline{P_i^{start}}$, $\overline{P_i^{end}}$, $\overline{P_j^{start}}$ and $\overline{P_j^{end}}$ be the mean of several real power values from starting and ending periods of states $i$ and $j$




- Four different types of edges result in features with good performance:
  - $dP_1 = \overline{P_j^{start}} - \overline{P_i^{start}}$
  - $dP_2 = \overline{P_j^{start}} - \overline{P_i^{end}}$
  - $dP_3 = \overline{P_j^{end}} - \overline{P_i^{start}}$
  - $dP_4 = \overline{P_j^{end}} - \overline{P_i^{end}}$

M. Weiss et al."Leveraging smart meter data to recognize home appliances," in *IEEE Pervasive Comp.*, 2012.

# Supervised Learning - P-Q plane Classification Extension

## Improved distance-based classification in $(dQ, dP)$-space

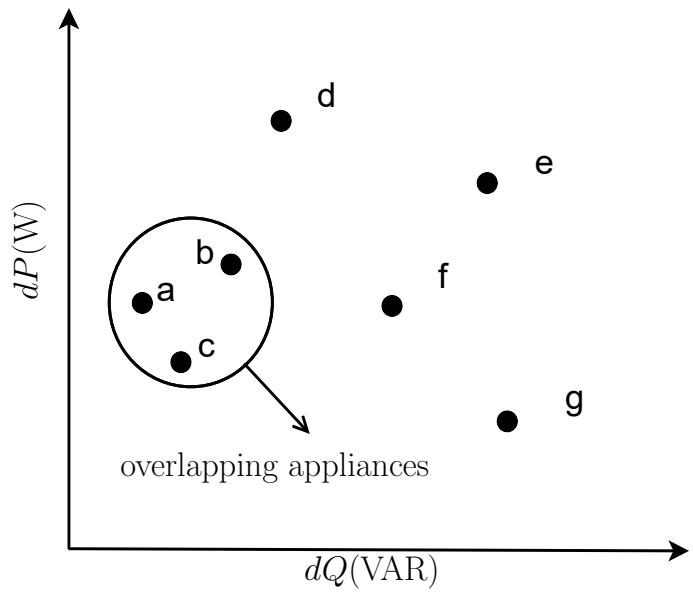
(Appliance-dependent) classification rule: $\hat{y}_k$ correct match if

$$||y - \hat{y}_k|| < \lambda ||\hat{y}_k|| + osc_k$$

with variable radius: $osc_k$ for oscillations, $\lambda$ scaling factor.

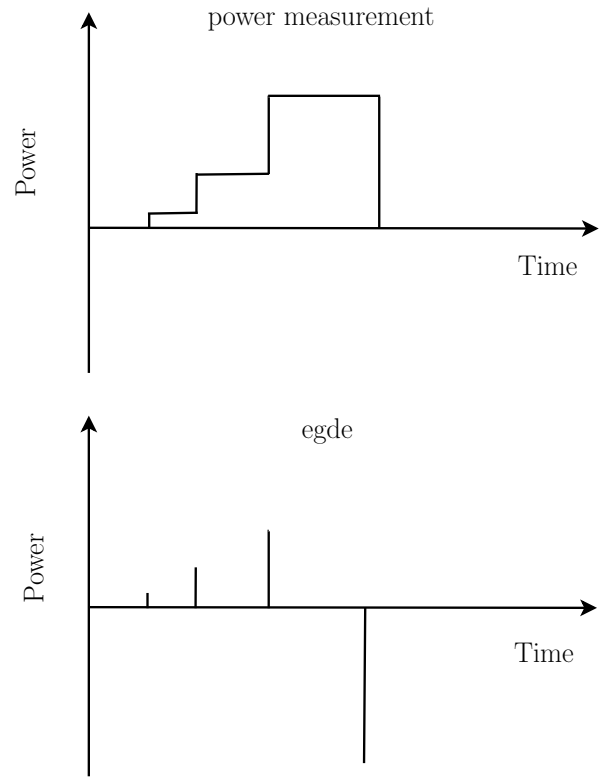
P-Q plane classification

- simple to implement
- fails when different appliances have overlapping $P - Q$ features



# Supervised Learning - Naïve Bayes Approach

- Features:
  - Total real power measurement $p$
  - Steady-state change $e$
- $S = \{D_1 = s_1, D_2 = s_2, \ldots D_n = s_n\}$ denotes **load signature**
  - $s_i$ state of appliance/device $D_i$
  - $\omega$ set of all load signatures $S$




## Optimal classifier (MAP rule)

$$\arg\max_{S \in \omega} P(S | \sum_{i=1}^{n} D_i = p \bigcap E = e)$$

Marchiori et al. "Circuit-Level Load Monitoring for Household Energy Management," *IEEE Pervasive Comp.*, 2011.

# Supervised Learning - Naïve Bayes Approach

- Equivalent formulation after applying Bayes rule:

$$\underset{S\in\omega,\sum_{i=1}^{n} D_i=p}{\arg\max} \quad P(E=e|S)P(S)$$

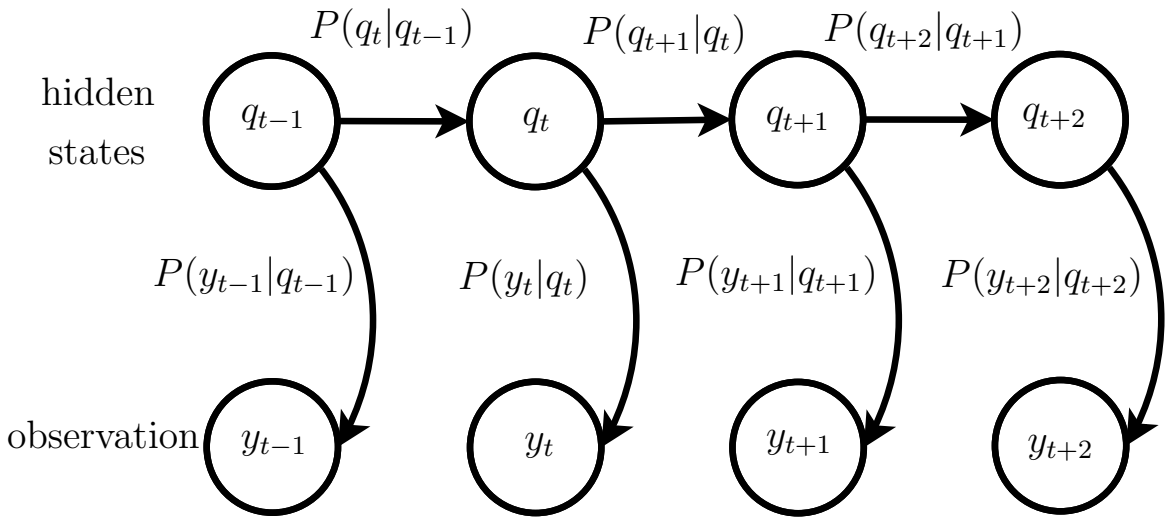
**Assumptions** to simplify computation of $P(E=e|S)$ and $P(S)$:

- Naïve approach[1]: Assume appliance states are independent of each other
  - Fair assumption in general, but devices such as a TV and a DVD player can have a highly correlated operation.
- Assume **only one device is changing at a time**.

$$P(S)=\prod_{i=1}^{n} P(D_i=s_i), \quad P(E=e|S)=\frac{\sum_{k\in E_S} I(k=e)}{|E_S|}$$

[1] Naïve Bayes approach often refers to assumption that features are conditionally independent given the class.

# Hidden Markov Model (HMM)




## Hidden Markov Model (HMM)

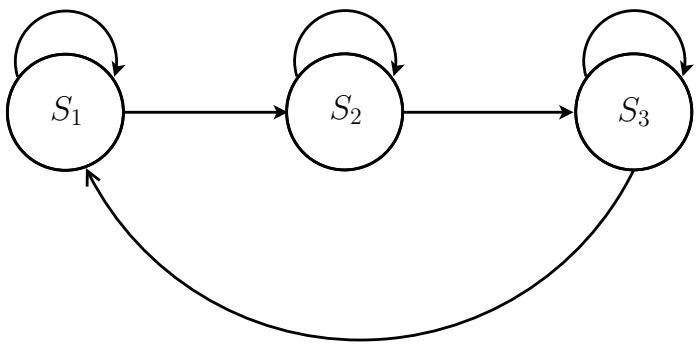
Statistical (system) model with

- hidden states described by an Markov process, and
- observations that are independent given hidden states.

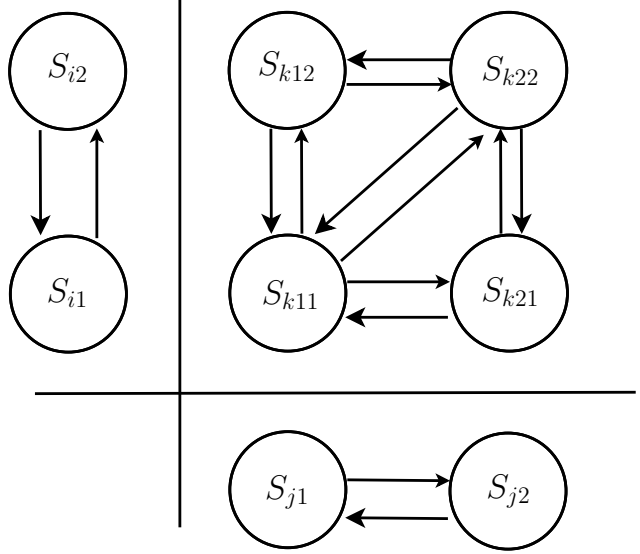
# Appliances as Hidden Markov Model

- HMM shown to be useful because
  1. Learning of HMM parameters $\lambda$ works well (i.e., $P(q_t|q_{t-1})$ and $P(y_t|q_t)$ for all $t$)
  2. Temporal and appliance state transitions can be well modeled
- Ergodic topology to model the state transition of appliances
- Left-to-right topology to model temporal development
- HMM can model individual or combined loads

Ergodic state transition topology of a fridge




4-State HMM of two appliances combination



# Supervised Learning - HMM Approach

## General HMM framework

1. **Decoding:** Given the HMM parameters $\lambda$, the observation sequence $Y = \{y_t\}$ and the set of states $\mathcal{S} = \{S_i\}$,
   - calculate the probability $P(Y, Q|\lambda)$ and
   - determine the most probable state sequence $Q = \{q_t\}, q_t \in \mathcal{S}$;
2. **Learning:** Given the observation sequence $Y$ and the set of states $\mathcal{S}$, learn the HMM parameters $\lambda$.

**Supervised learning of state transition probabilities** (labeled load signature and state transition of appliances given)

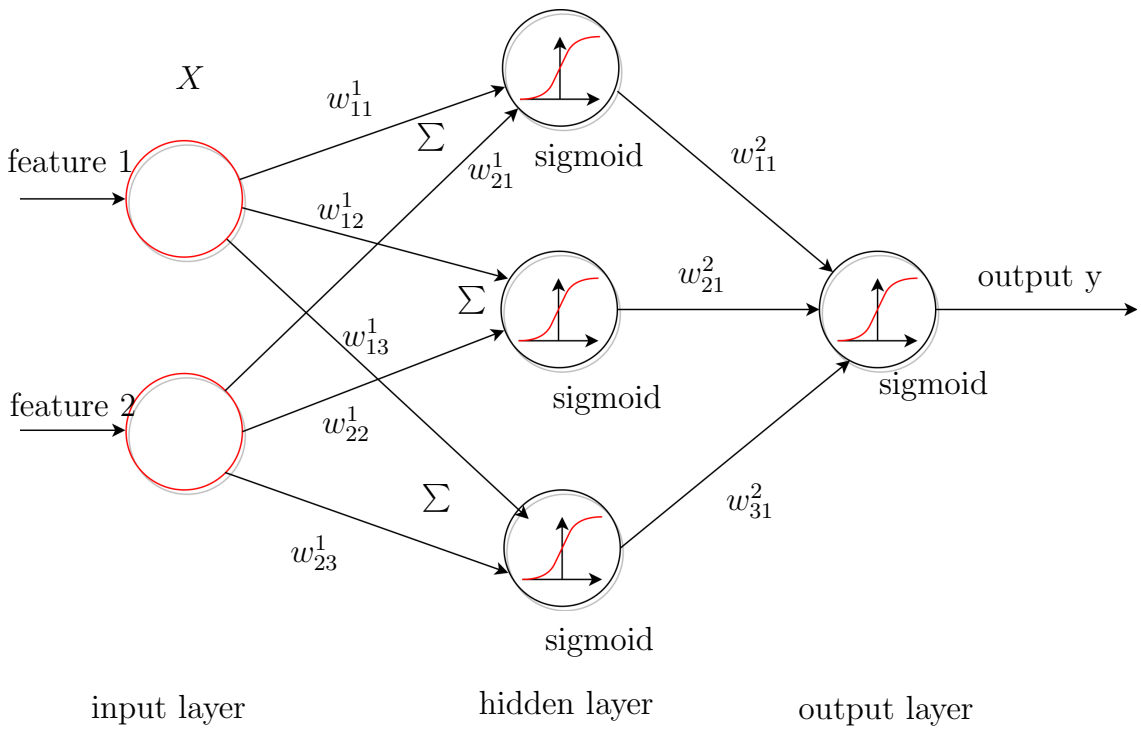
$$P(S_j|S_i) = \frac{\#: S_i \rightarrow S_j}{\#: \textit{all transitions from } S_i}$$

**Decoding:** Load disaggregation using Viterbi algorithm

T. Zia et al. "A hidden Markov model based procedure for identifying household electric loads," in *IECON 2011*.

# Supervised Learning - Neural Network Approach

- Advantage of neural networks:
  - extensibility to higher number of inputs, and
  - many types of values or dissimilar kind of data
- Feature vectors used as the input of a neural network to also train the classifier for different loads
  - output denotes probability that load belongs to a certain class



# Unsupervised Learning - K-means Clustering Approach

- What if labeled load signatures are not available?
  - **Unsupervised clustering approaches** such as K-means clustering

## K-means Clustering

Given a set of observation $\{x_1, x_2, ...., x_n\}$, partition the $n$ observations into $K$ sets $\mathcal{S} = \{\mathcal{S}_1, \mathcal{S}_2, ..., \mathcal{S}_K\}$ that minimizes the within-cluster sum of squares, i.e.,

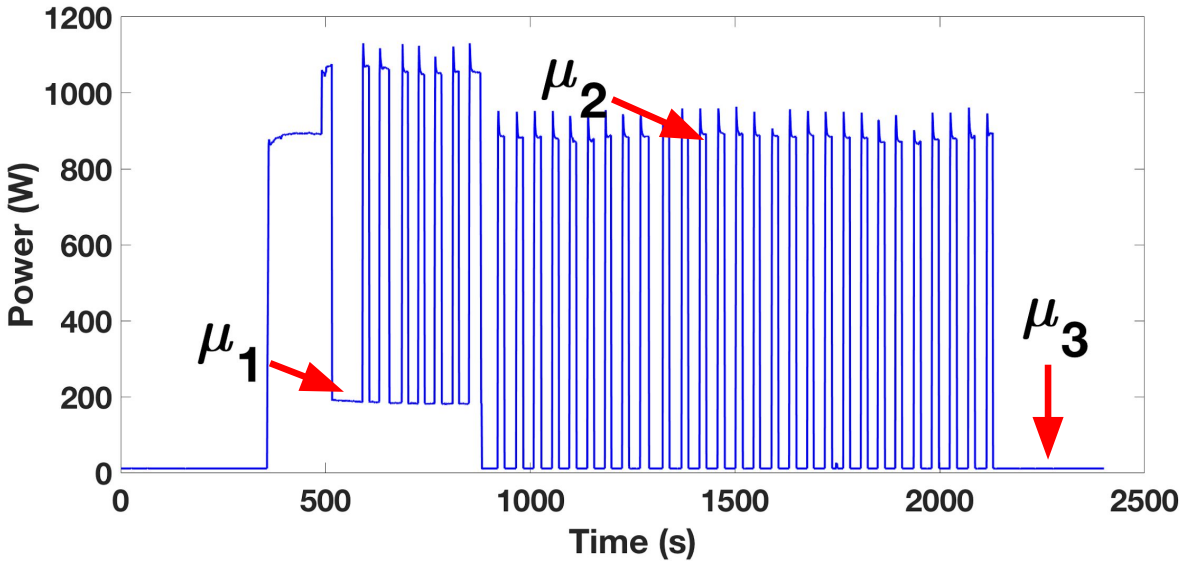
$$\arg\min_{\mathcal{S}} \sum_{i=1}^{K} \sum_{x \in \mathcal{S}_i} ||x - \mu_i||^2,$$

where $\mu_i$ is the mean of vectors in $\mathcal{S}_i$., i.e. $\mu_i = \frac{1}{|\mathcal{S}_i|} \sum_{x_k \in \mathcal{S}_i} x_k$.

- E.g., for $P$-$Q$ plane feature space, $x_i$ denotes $(p_i, q_i)$.

Goncalves et al. "Unsupervised disaggregation of appliances using aggregated consump. data," *Proc. SustKDD'11.*

# Appliance Model: Temporal Correlations

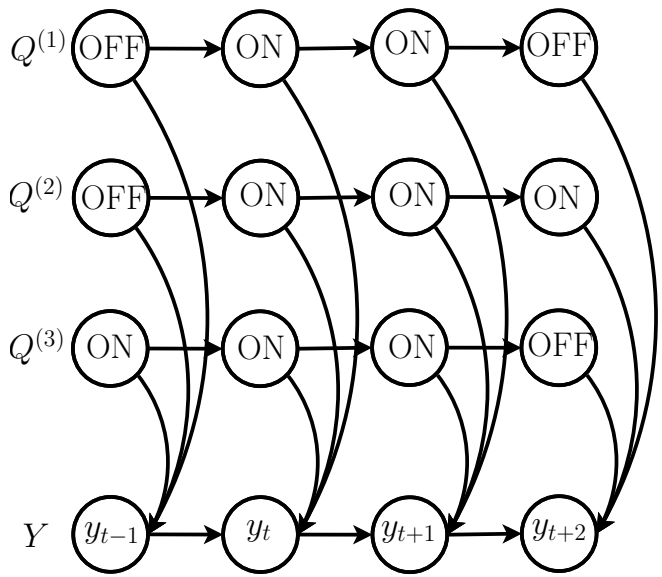



$$x_{570} = \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} \qquad x_{1475} = \begin{bmatrix} 0 \\ 1 \\ 0 \end{bmatrix} \qquad x_{2300} = \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix}$$

$$\mu^\top = \underbrace{\begin{bmatrix} 220, & 900, & 0 \end{bmatrix}}_{\text{average power}},$$

# Factorial HMM (FHHM)

- Use **factorial HMM** to characterize multiple underlying **independent causes or factors** of the total load
- Complexity grows exponentially with number of underlying appliances
- Standard approximation methods:
  - Markov chain Monte Carlo
  - Variational Bayes



# Unsupervised Learning - Expectation Maximization

- (F)HMM parameters can be iteratively updated by **expectation maximization algorithm** (EM):

$$\arg\max_{\lambda} \sum_{q} P(Y, Q|\lambda') \log P(Y, Q|\lambda)$$

  - $\lambda$ are the (F)HMM parameters to be estimated and $\lambda'$ are the parameters from the previous iteration
  - $Y$ is the observed aggregated load
  - $Q$ is the hidden sequence

- Decoding using Viterbi algorithm

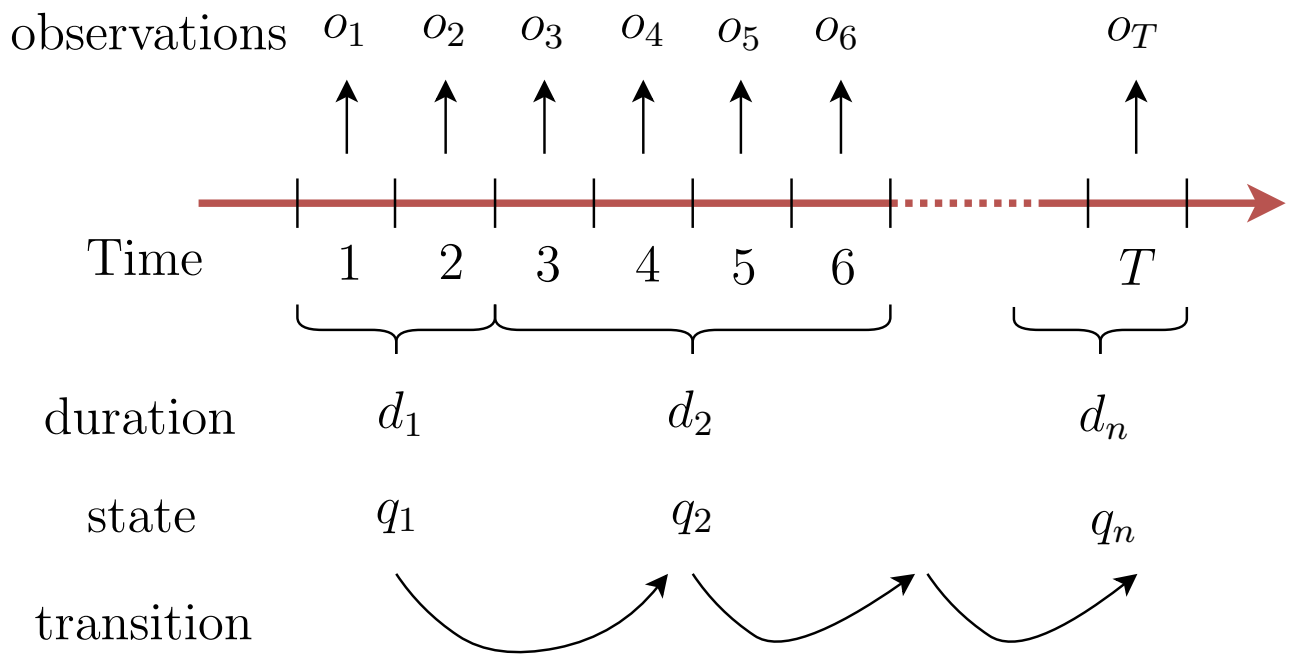
$$\arg\max_{Q} P(Y, Q|\lambda)$$

---

H. Kim et al, "Unsupervised disaggregation of low frequency power measurements," in *Proc. SIAM, 2011*.

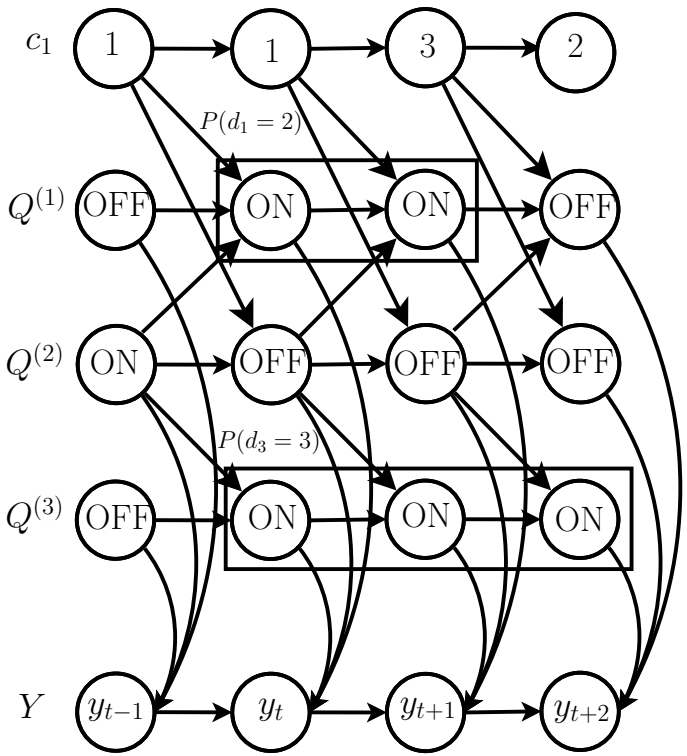
# Hidden Semi-Markov Model (HSMM)

- HSMM takes state occupancy duration into account
  - for appliances that stay in a certain state for some time



# Conditional Factorial Hidden Semi Markov Model

- **Conditional Factorial Hidden Markov Model** (CFHMM): Case when additional features affect the transition probability between different states (e.g. occupancy of home)



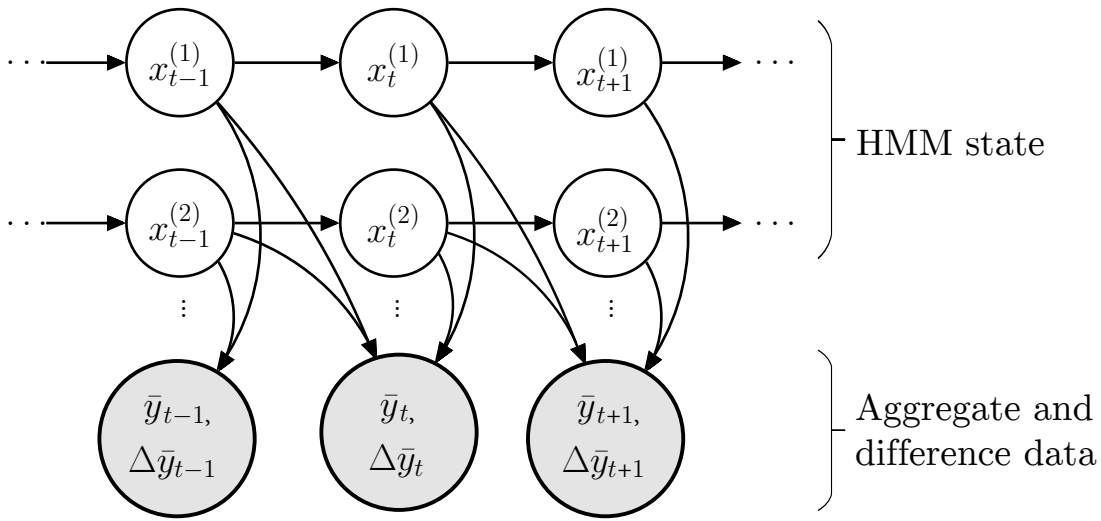

- **CFHSMM** model combines CFHMM and HSMM
  - often reasonable
- **Example** (left figure):
  - multiple appliances with on-off states,
  - number of people at home act as additional features,
  - the states dependency e.g. of a laptop and monitor.

H. Kim et al, "Unsupervised disaggregation of low frequency power measurements," in *Proc. SIAM, 2011*

# Unsupervised learning - AFAMAP

## Additive Factorial Approximate MAP (AFAMAP): unsupervised load disaggregation

- **Snippets**[2] of consumption data that likely correspond to an appliance's ON cycle are extracted.
- These snippets along with the total aggregate and difference aggregate data are together modeled as an ***additive* factorial hidden Markov model** (FHMM).




Kolter, Johnson, "REDD: A public data set for energy disaggregation research," in *Proc. SustKDD Workshop* '11.

[2] A snippet is a section of data where consumption increases over some threshold and then eventually returns to its original level.

# Unsupervised learning - AFAMAP (Cont.)

- Conditional likelihood of $\bar{y}_t$:

$$\bar{y}_t \mid x_t^{(1:N)} \sim \mathcal{N}\left(\sum_{i=1}^{N} \mu_{x_t^{(i)}}^{(i)}, \Sigma\right)$$

- Conditional likelihood of $\Delta\bar{y}_t$:

$$\Delta\bar{y}_t \mid x_t^{(1:N)}, x_{t-1}^{(1:N)}, \Delta z_t \sim \mathcal{N}\left(\sum_{i=1}^{N} \Delta\mu_{x_t^{(i)}, x_{t-1}^{(i)}} + \Sigma^{1/2}\Delta z_t, \Sigma\right)$$

  where $z_t$ is a mixture component with a Laplace prior to account for new and unmodeled devices.

- AFAMAP imposes a constraint that allows at most one HMM changes at any given time and infers the individual HMM states by maximizing the joint posterior of $\bar{y}_t$ and $\Delta\bar{y}_t$.

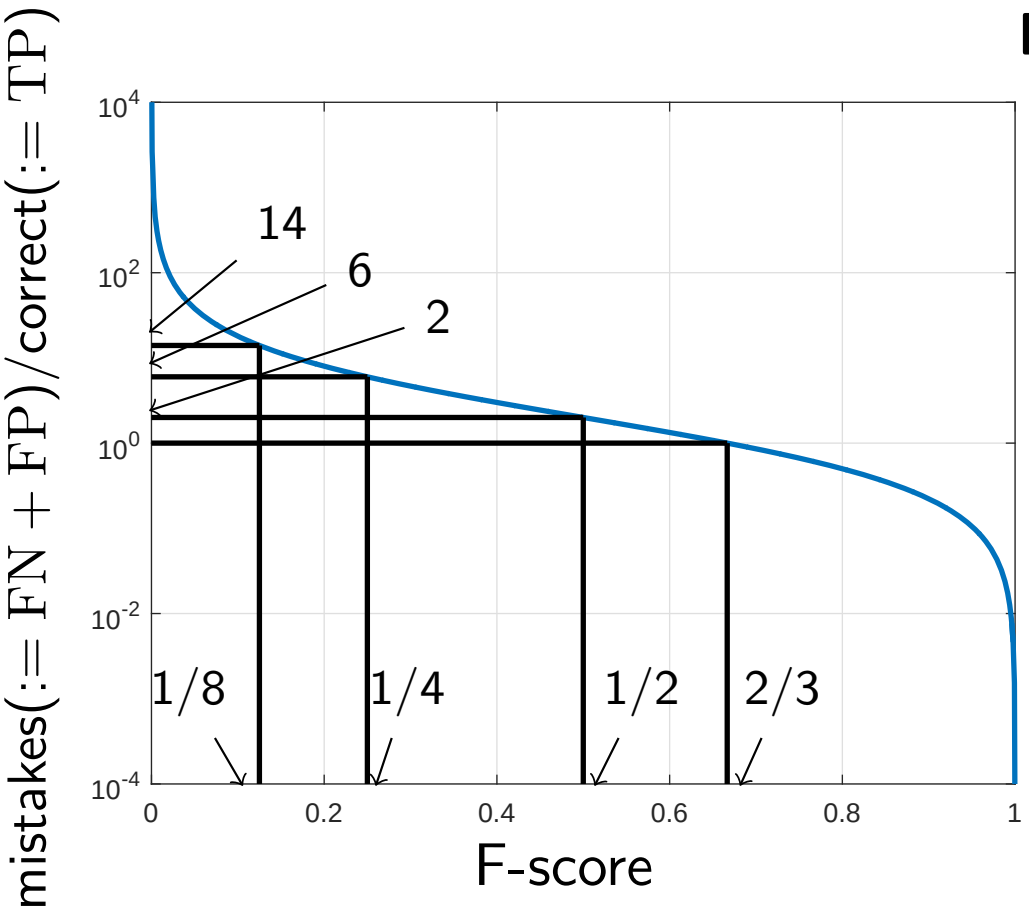
# Reference datasets for NILM

- Reference Energy Disaggregation Data Set (REDD)
  - Household-level and circuit level data from 6 US households over various durations in 2011
  - Lighting, fridge, microwave, oven, washer dryer, dish washer, kitchen outlets etc
  - Low frequency and high frequency data
- Electricity Consumption and Occupancy (ECO)
  - 6 Swiss households over a period of 8 months in 2012 - 13
  - Fridge, dryer, coffee machine, kettle, washing machine, PC, freezer, stove, tablet, lamp, entertainment (consists of TV and stereo), microwave, router etc
  - Only low frequency data but occupancy information for some houses is measured and provided

# Reference datasets for NILM (Cont.)

| Dataset | Locat. | Resolution | Features | Other data | Available Toolbox |
|---|---|---|---|---|---|
| REDD | USA | 15KHz (Aggr), 0.5 or 1Hz(Sub) | V and P (Aggr), P (Sub) | NA | NILMTK(Python) |
| BERDS | USA | 20sec | P,Q and S | climate data | NA |
| Smart | USA | 1Hz | P and S (Aggr), P (Sub) | on-site solar panels and wind turbines, outdoor weather, indoor temperature and humidity | NA |
| DRED | NL | 1Hz | P | indoor temperature, outside temperature, wind speed, pre-cipitation, humidity and occupancy | NILMTK(Python) |
| AMPDS | Canada | 1min | V, I, F, P, Q, S and P.F. | water and natural gas | NILMTK(Python) |
| AMPds2 | Canada | 1min | V, I, F, P, Q, S and P.F., real, reactive and apparent energies | water and natural gas, weather data and utility billing data. | NILMTK(Python) |
| UK-DALE | UK | 16KHz (Aggr), 1/6Hz (Sub) | P and switch status | NA | NILMTK(Python) |
| iAWE | India | 1Hz (Aggr), 1 or 6Hz (Sub) | V, I, F, P and phase | Water and ambient conditions | NILMTK(Python) |
| REFIT | UK | 8sec | P | Gas and environmental data | NILMTK(Python) |
| ECO | CH | 1Hz | P and Q | Occupancy information | NILMTK(Python), NILM-Eval(Matlab) |
| IHEP-CDS | France | 1min | V, I, P and Q | NA | NA |
| HES | UK | 2min | P | NA | NILMTK(Python) |

# Classification measure F-score



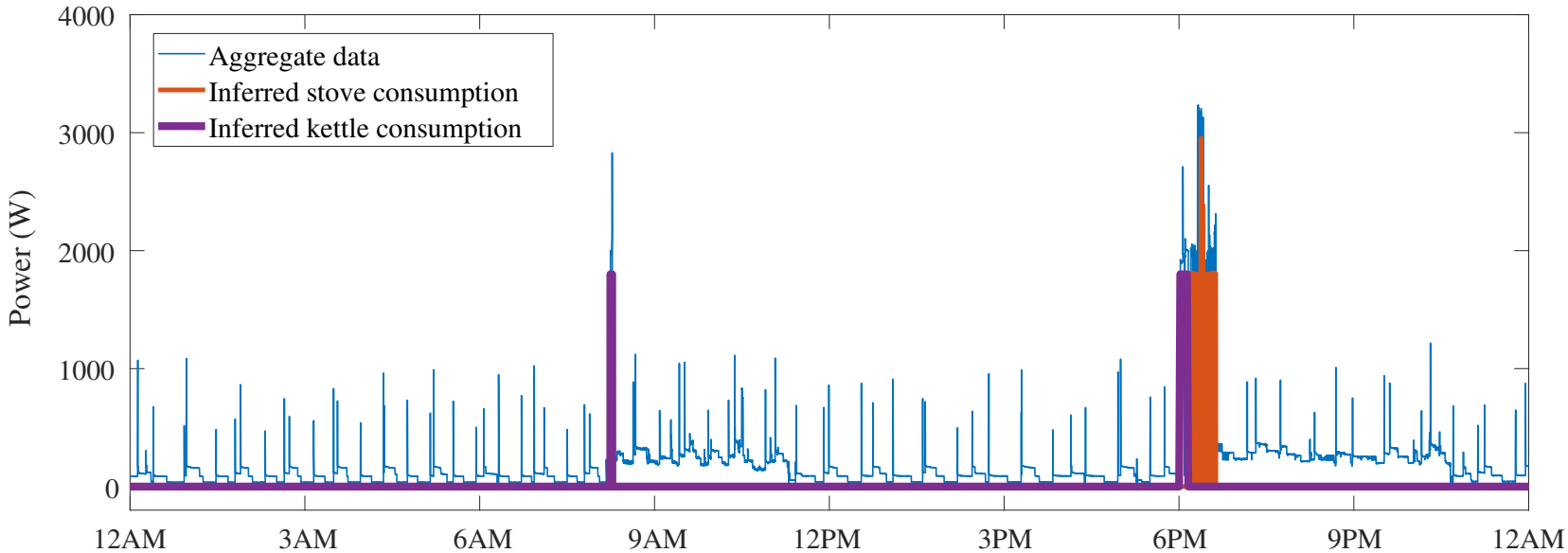

**F-score** is

- aka $F_1$ measure or F-measure
- a measure of test's accuracy
- defined as $\frac{1}{1+\frac{1}{2}\frac{\mathrm{FN}+\mathrm{FP}}{\mathrm{TP}}}$
- harmonic mean between recall and precision[3]

[3] precision$=\frac{TP}{TP+FP}$ (aka as sensitivity) and recall$=\frac{TP}{TP+FN}$ (aka positive predictive value), TP=True Positive, FP=False Positive, FN=False Negative

# Example disaggregation using NILM-Eval toolbox

- Dataset: ECO, Household 2 (Day 2012-06-02)
- Algorithm: Weiss'



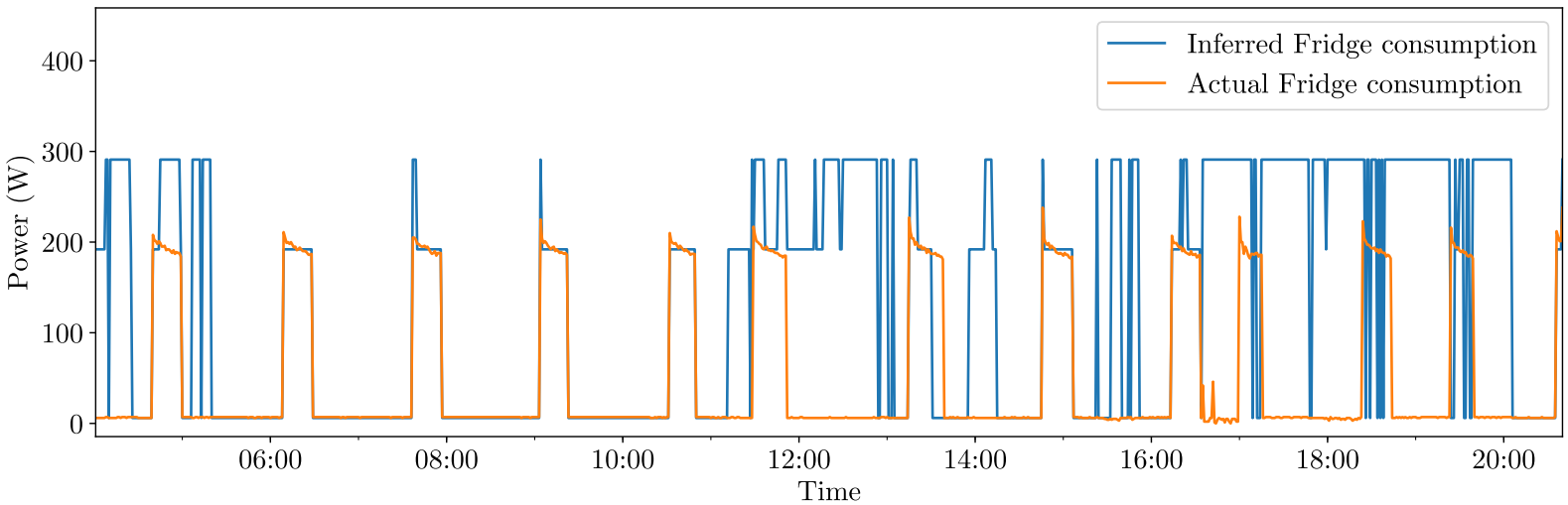

- Disaggregation accuracy:

| Appliance | Precision | Recall | F-Score[4] |
|---|---|---|---|
| Water Kettle | 1.0000 | 0.7500 | 0.8751 |
| Stove | 1.0000 | 1.0000 | 1.0000 |

[4] the higher the F-Score, the better is the accuracy of disaggregation

# Example disaggregation using NILMTK toolbox

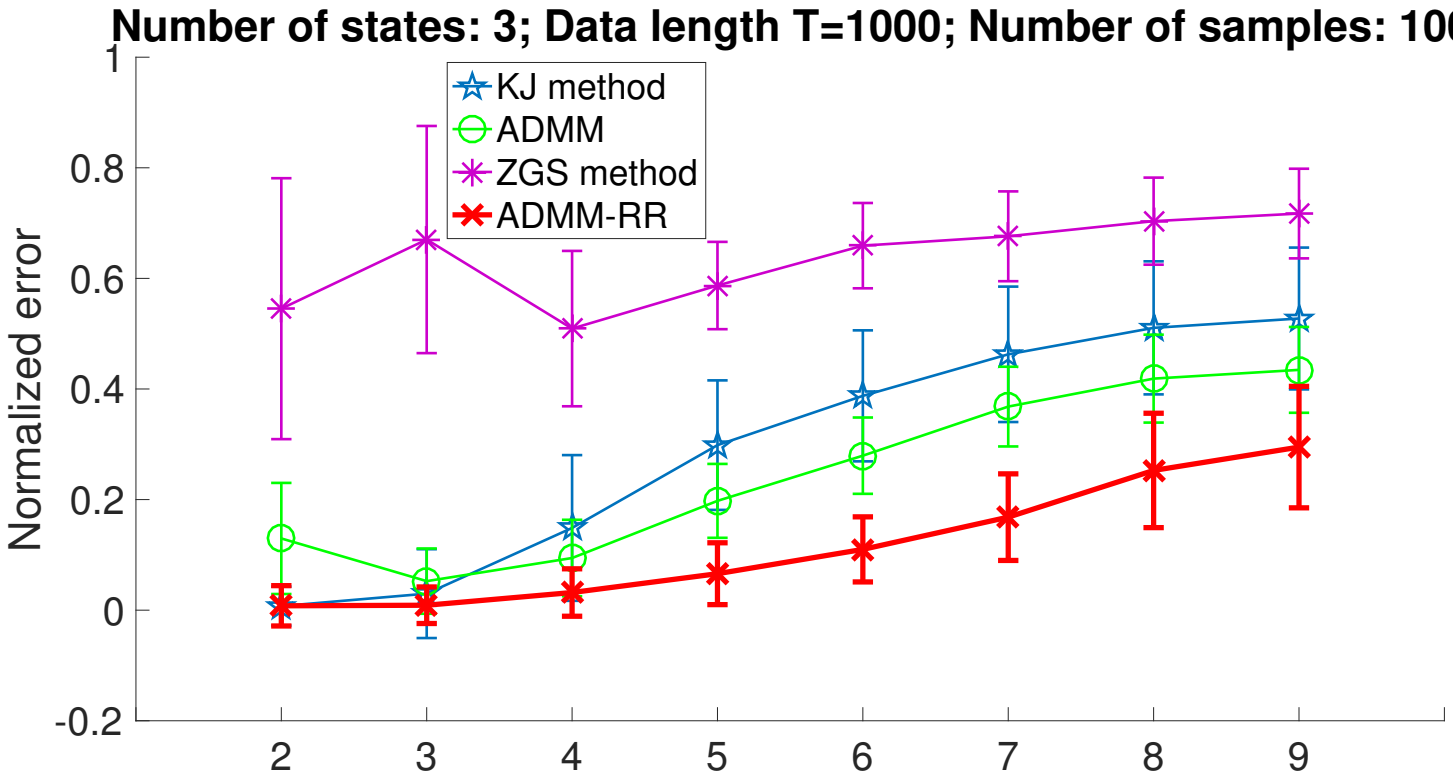
- Dataset: REDD
- Data: Household 1 (Day 2011-04-30)
- Algorithm: FHMM (Supervised learning)




- Disaggregation accuracy:

| Appliance | RMSE |
|---|---|
| Fridge | 98.30 |
| Microwave | 250.43 |
| Dish washer | 237.47 |
| Light | 82.26 |

# Synthetic Data Set: Disaggregation Error vs. Number of HMMs



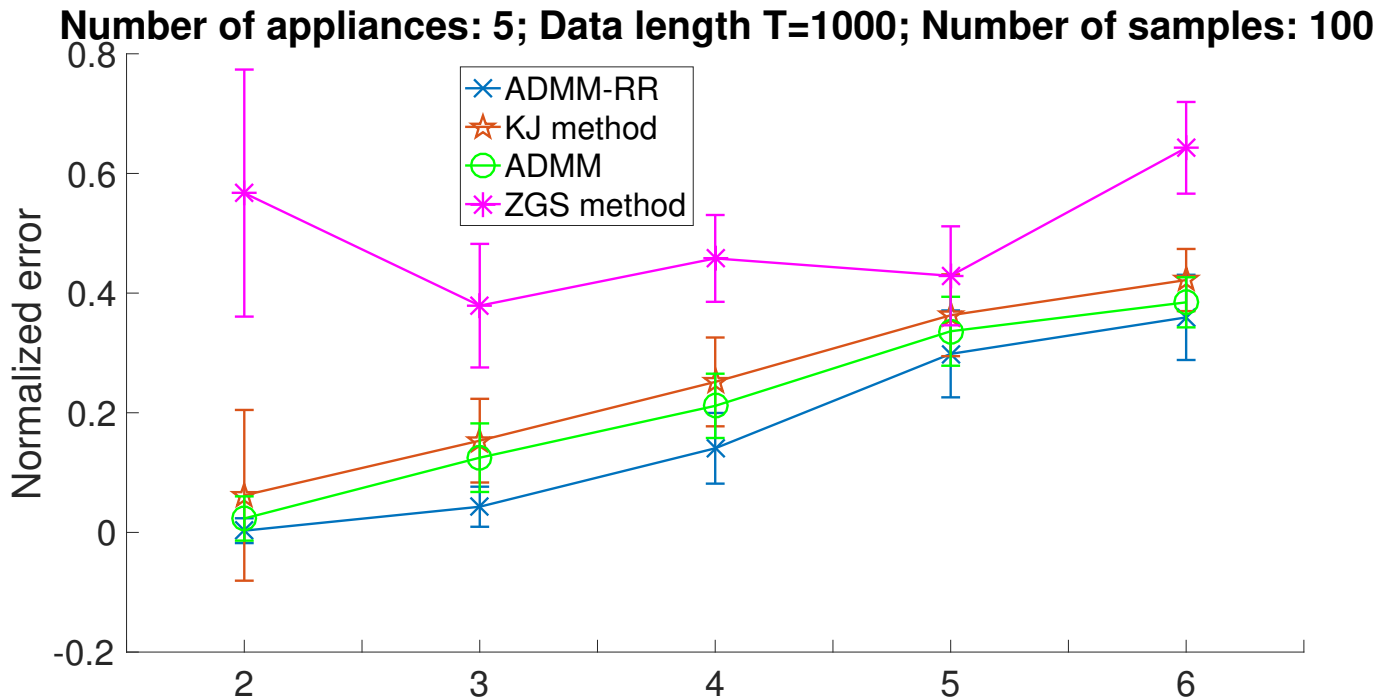


[KJ] Kolter and Jaakkola, Approximate inference in additive factorial HMMs with application to energy disaggregation, *AISTATS 2012*.

[ZGS] Zhong et al, Signal aggregate constraints in additive factorial HMMs with application to energy disaggregation, *NIPS 2014*.

[ADMM] and [ADMM-RR] Shaloudegi et al., SDP relaxation with radonmized rounding for energy diaggregation, *NIPS 2016*.

# Synthetic Data Set: Disaggregation Error vs. Number of States



# REDD Data Set: Precision/ Recall

| Appliance | ADMM-RR | KJ method | ZGS method |
|---|---|---|---|
| 1 Oven-3 | **61.70/78.30%** | 27.62/72.32% | 5.35/15.04% |
| 2 Fridge | **90.22/97.63%** | 41.20/97.46% | 46.89/87.10% |
| 3 Microwave | 12.40/74.74% | **13.40/96.32%** | 4.55/45.07% |
| 4 Bath. GFI-12 | **50.88/60.25%** | 12.87/51.46% | 6.16/42.67% |
| 5 Kitch. Out.-15 | **69.23/98.85%** | 16.66/79.47% | 5.69/26.72% |
| 6 Wash./Dry.-20-A | 98.23/93.80% | 70.41/98.19% | 15.91/35.51% |
| 7 Unregistered-A | 94.27/87.80% | 85.35/25.91% | 57.43/99.31% |
| 8 Oven-4 | 25.41/76.37% | 13.60/78.59% | 9.52/12.05% |
| 9 Dishwasher-6 | 54.53/90.91% | 25.20/98.72% | 29.42/31.01% |
| 10 Wash./Dryer-10 | **21.92/63.58%** | 18.63/25.79% | 7.79/3.01% |
| 11 Kitch. Out.-16 | 17.88/79.04% | 8.87/100% | 0.00/0.00% |
| 12 Wash./Dry.-20-B | 98.19/28.31% | 72.13/77.10% | 27.44/71.25% |
| 13 Unregistered-B | 97.78/91.73% | 96.92/73.97% | 33.63/99.98% |
| Average | **60.97/78.56%** | 38.68/75.02% | 17.97/36.22% |

- Phase A has 7 HMMs
- Phase B has 6 HMMs
- Spectral learning used for FHMM training

# REDD data set: Running time

In real-data experiments, with approximately 1 million decision variables for each day:

| | ADMM-RR | ADMM | KJ |
|---|---|---|---|
| Memory | 6 GB | 6 GB | 14 GB |
| Time | 5 hours | 2 hours | 5 minutes |
| Solver | MATLAB | MATLAB | MOSEK |

- An optimized C++ version of ADMM-RR achieves a comparable running time.

# NILM Concluding Remarks

- Only basic principles shown
  - underlying model, underlying features, learning & decoding alg
- Conditional HMM exploit auxiliary information state
  - could be directly privacy sensitive
- Algorithmic advances in machine learning improve disaggregation performance
  - significant research takes place at (start-up) companies
- *Off-the-shelf* algorithms and reference databases exist that can be used for numerical experiments and benchmarks

# Privacy Preservation Techniques for Smart Meters

Two family of approaches to SM privacy problem:

1. Modify SM data before being reported to EP.
   - Aggregation with/ without trusted third party (TTP), i.e., summing measurements over a group of users,
   - Obfuscation, i.e., adding noise to data,
   - Anonymization with/ without TTP, i.e., using pseudonyms instead of real identities.
2. Modify energy consumption:
   - Through storage devices, i.e., filtering energy consumption,
   - Exploiting other energy sources (renewables, uninterrupted power supplies),
   - Through elastic energy consumption (e.g., heating),
   - Reducing sampling frequency.

# Aggregation with Trusted Third Party (TTP)

- SM readings sent to a TTP over secure links.
- TTP reports to EP:
  - instantaneous sum consumption for a group of SMs (e.g., neighborhood),
  - sum consumption of each user over billing period.
- EP learns exactly what it needs to learn, not more.
- TTP does not need to know real identities of users, but has to be trusted.

---

J.-M. Bohli, C. Sorge, and O. Ugus, "A privacy model for smart metering," in IEEE Int'l Conf. on Comm. Workshops, Cape Town, South Africa, May 2010.

# Aggregation without Trusted Third Party (TTP)

- How to add a user's data to the aggregate without revealing it to other users?
- SMs have trusted elements (e.g., smart card or secure USB stick) that cannot be controlled by the grid operator (i.e., it cannot change keys remotely).
- These trusted elements provide secure storage and basic cryptographic functionality
- Common tool: homomorphic encryption, thanks to its additive homomorphic property.
- Proposed approaches differ mainly in:
  - Who performs the aggregation,
  - How keys are managed.

# Homomorphic Encryption

- Neighborhood groups of size $N$.
- Each node prepares $N$ shares of its measurements.
- Encrypts one share with the public key of each user (N-1 users) and sends to the collector (except own share).
- The collector, using the properties of homomorphic encryption, sums all $N-1$ ciphertexts intended for a user and sends the resulting ciphertext to her to decrypt.
- Each user adds its own share and sends the final result back to the concentrator unencrypted.

---

F. D. Garcia and B. Jacobs, Privacy-friendly energy-metering via homomorphic encryption, in Proc. Int'l Conf. on Security and Trust Management, 2011.

# Obfuscation

- Users add zero-mean independent noise to their readings before forwarding to EP.
- Average sum consumption remains same at each period.
- Goal: low confidence for individual measurements (high variance noise component), and high-confidence for total consumption (too many users aggregated together: 99.9% confidence requires aggregating 3.8 million users.)
- Meters should be tamper-proof.

---

J.-M. Bohli, C. Sorge, and O. Ugus, "A privacy model for smart metering," in IEEE Int'l Conf. on Comm. Workshops, May 2010.

# Information Theoretic SM Privacy

- Energy consumption of user is modeled as a sequence of real numbers, $X^n$.
- SM readings, $Y^n$, represents information available to EP.
- Privacy is measured by average information leakage, defined as average mutual information between $X^n$ and $Y^n$:

$$\begin{aligned}\frac{1}{n}I(X^n;Y^n) &= \frac{1}{n}\left[H(X^n) - H(X^n|Y^n)\right] \\ &= \frac{1}{n}\sum_{(x^n,y^n)\in\mathcal{X}^n\times\mathcal{Y}^n} p(x^n,y^n)\log\frac{p(x^n,y^n)}{p(x^n)p(y^n)}\end{aligned}$$

# Reporting Quantized Energy Consumption

- SM maps $X^n$ to a predefined set of meter readings:

$$\text{Encoder}: X^n \rightarrow \mathcal{SMR} = \{SMR_1, \ldots, SMR_M\}$$

- No matter what real consumption is, EP will receive $Y^n \in \mathcal{SMR}$, one of $M$ readings,
- The closer $Y^n$ to $X^n$, the more useful it is for grid estimation/ monitoring, and the more data is leaked.
- There is a fundamental trade-off between privacy and utility of reported SM readings

---

D. Rebollo-Monedero et al., "From t-Closeness-Like Privacy to Postrandomization via Information Theory," *IEEE Trans. Knowl., Data Eng.*, Nov. 2010.

Sankar et al., "Smart Meter Privacy: A Theoretical Framework," IEEE Trans. Smart Grid, Jun. 2013.

# Privacy- Utility Trade-off

- Utility: The closer the estimates, the higher the utility:

$$\Delta = \mathbb{E}\left[\frac{1}{n}\sum_{i=1}^{n} d(X_i, Y_i)\right]$$

  $d(\cdot,\cdot)$: given distortion measure (distance between real energy consumption and EP's estimation)

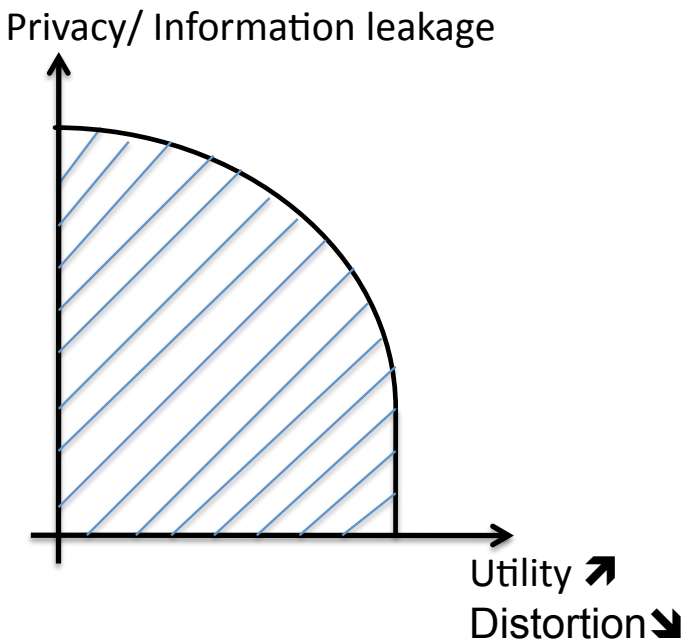
- Average information leakage:

$$\mathcal{I} = \frac{1}{n} I(X^n; Y^n)$$

- Question: What is the set of feasible $(\Delta, \mathcal{I})$ pairs?

# Privacy- Utility Trade-off

- For given utility $\Delta$, minimum information leakage is obtained by the rate-distortion function $R(\Delta)$
- Rate-distortion function, $R(D)$: Minimum number of bits per symbol that should be transmitted to a receiver, so that the source (input signal) can be approximately reconstructed within a given distortion, $D$ (lossy data compression).



# Differential Privacy

- Introduced to privately release statistical queries on data sets
- Differential privacy measures privacy by parameter $\epsilon$ that bounds the log-likelihood ratio of the output for two databases that **differ in only a single entry**.

## Definition

*A probabilistic algorithm $F$ taking values in set $\mathcal{T}$ provides $\varepsilon$-differential privacy if*

$$\Pr(F(\mathcal{D}) \in \mathcal{S}) \leq e^{\varepsilon} \cdot Pr(F(\mathcal{D}') \in \mathcal{S})$$

*for all $\mathcal{S} \in \mathcal{T}$, and all data sets $\mathcal{D}$ and $\mathcal{D}'$ that differ in a single entry.*

---

C. Dwork, Differential privacy, in Automata, Languages and Programming, vol. 4052 of LNCS, 2006.

# Approximate Differential Privacy

## Definition

*A probabilistic algorithm $F$ taking values in set $\mathcal{T}$ provides $(\varepsilon, \delta)$-differential privacy if*

$$\Pr(F(\mathcal{D}) \in \mathcal{S}) \leq e^{\varepsilon} \cdot Pr(F(\mathcal{D}') \in \mathcal{S}) + \delta$$

*for all $\mathcal{S} \in \mathcal{T}$, and all data sets $\mathcal{D}$ and $\mathcal{D}'$ that differ in a single entry.*

- Weaker than $\varepsilon$-differential privacy (equivalent when $\delta = 0$)

---

C. Dwork, K. Kenthapadi, F. McSherry, I. Mironov, and M. Naor. Our data, ourselves: Privacy via distributed noise generation. In Proc. 25th International Cryptology Conference (EUROCRYPT), 2006.

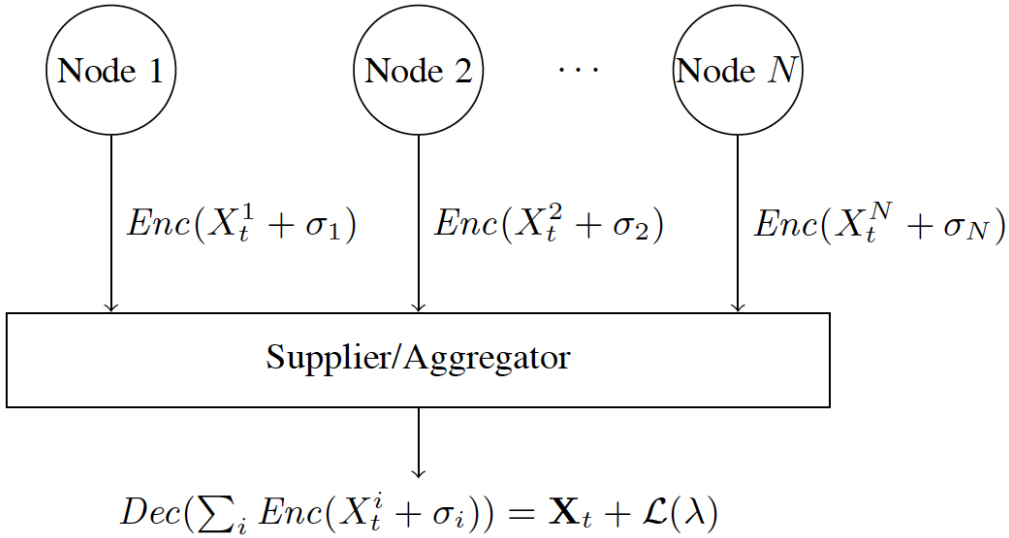
# Differentially Private Billing

- Even billing information can reveal private data in the presence of additional side information
- Users add noise (only positive) to meter measurements to create privacy
- Noise = Money: Users minimize noise (trade-off between additional cost and privacy)
- Discrete noise: Geometric distribution (instead of Laplacian)
  - Geometric distribution maximizes uncertainty for given mean
- Rebates: With additional encrytion tools (zero-knowledge proof, anonymous payment) added cost can be reimbursed to customer
- Negative noise can be possible by introducing deposit payment in advance

---

G. Danezis, M. Kohlweiss, A. Rial, Differentially Private Billing with Rebates. IACR Cryptology ePrint Archive, 2011, p. 134.

# Differentially Privacy + Modulo Encryption




- Group SMs into clusters.
- $X_t^i$ : Consumption of user $i$ at time slot $t$
- EP interested only in sum consumption of a cluster: $\sum_{i=1}^{N} X_t^i$
- Each user adds noise, and encrypts noisy measurement before sending to EP.

---

G. Acs and C. Castelluccia, I have a DREAM! (DiffeRentially privatE smArt Metering), 13th Information Hiding Conference, 2011.

# Distributed Noise Addition

- User $i$ calculates $\hat{X}_t^i = X_t^i + \Gamma_1(N, \lambda) - \Gamma_2(N, \lambda)$ in slot $t$ and sends it to the aggregator.
- $\Gamma_1(N, \lambda)$ and $\Gamma_2(N, \lambda)$ independently drawn from gamma distribution with shape parameter $1/N$ and scale parameter $\lambda$.

$$\begin{aligned}\sum_{i=1}^{N} \hat{X}_t^i &= \sum_{i=1}^{N} X_t^i + \sum_{i=1}^{N} [\Gamma_1(N, \lambda) - \Gamma_2(N, \lambda)] \\ &= \sum_{i=1}^{n} X_t^i + [\Gamma_1(1, \lambda) - \Gamma_2(1, \lambda)] \\ &= \sum_{i=1}^{n} X_t^i + [\mathrm{Exp}(\lambda) - \mathrm{Exp}(\lambda)] \\ &= \sum_{i=1}^{n} X_t^i + \mathcal{L}(\lambda)\end{aligned}$$

$\mathcal{L}(\lambda)$ : Laplace distribution

# Modulo Encryption

- Each SM is configured with a private key, and gets the corresponding certificate from a trusted third party.
- Generate pairwise keys between each pair of SMs.
- Modulo addition based encryption: EP can only decode noisy aggregate data (since it does not know pairwise keys).
- Aggregate noise enough to provide differential privacy to each consumer.

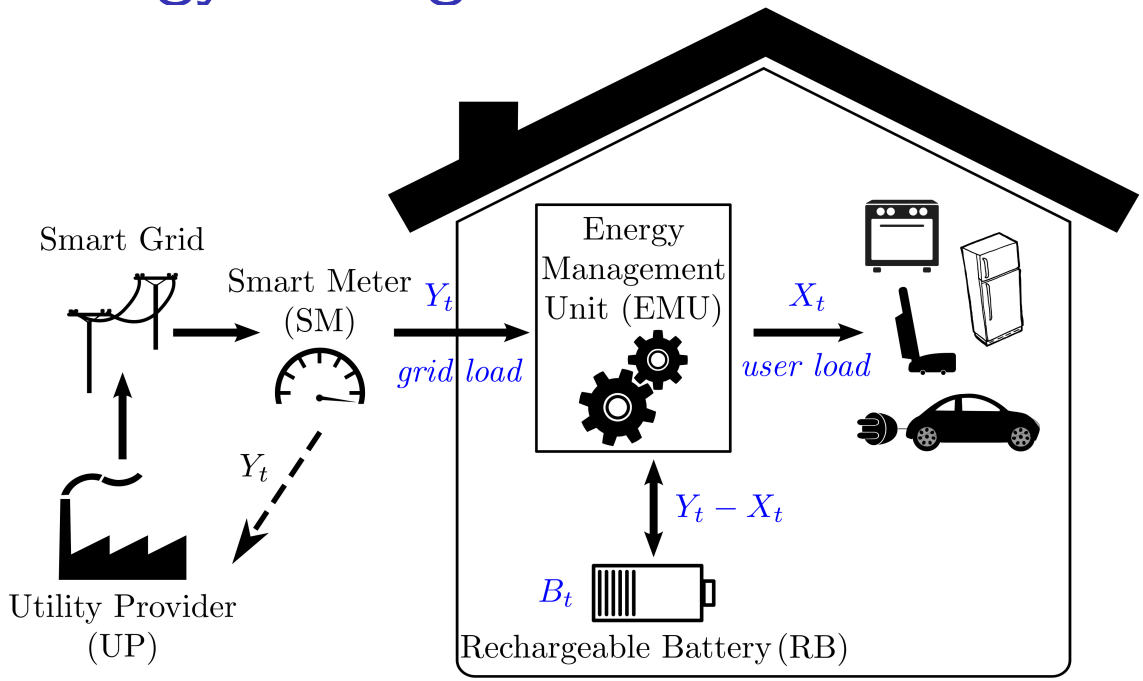
---

G. Acs and C. Castelluccia, I have a DREAM! (DiffeRentially privatE smArt Metering), 13th Information Hiding Conference, 2011.

# Privacy Through Energy Consumption Manipulation

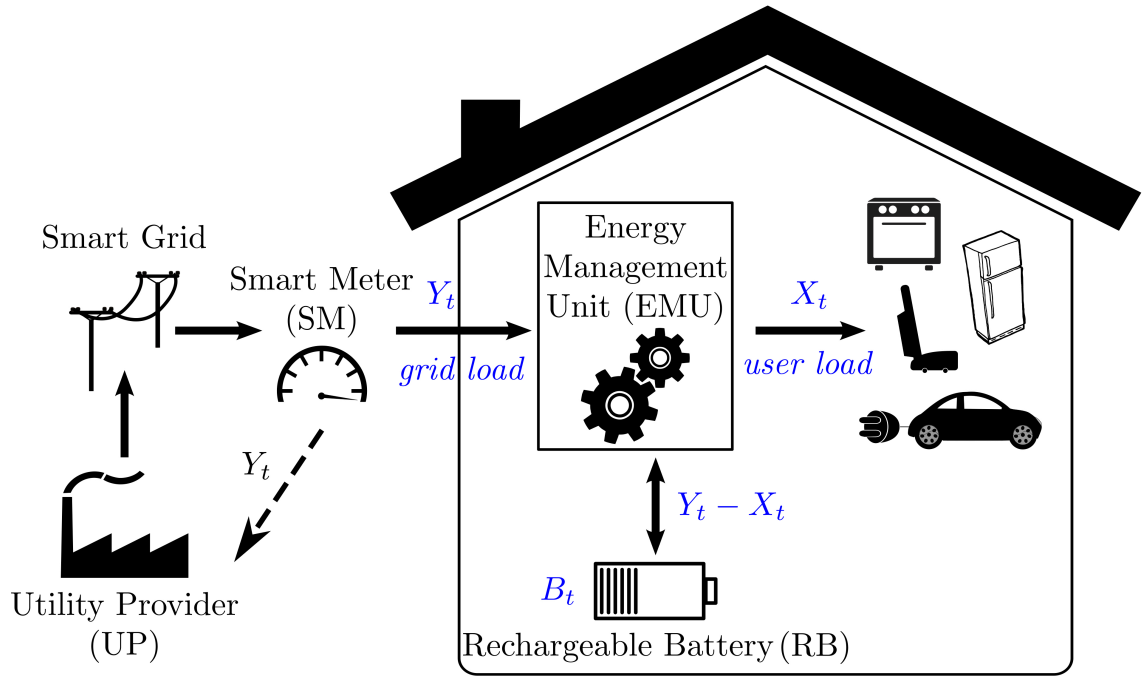
- *Physical* approach to privacy, rather than *cyber*.
- Previous techniques do not provide full privacy. Grid operator owns the grid, and has many other sensors, measurement mechanisms that can provide some level of information.
- Obfuscation, data aggregation, etc. limit operator's capabilities to monitor grid for failures, energy quality changes, renewable integration, etc.
- **Alternative solution:** Consumers manipulate energy consumption over time by exploiting storage devices, renewable energy sources, uninterruptible power supplies, or elastic energy consumption.

# Privacy with an Energy Storage Device




- Rechargeable battery (**RB**) with capacity $B$ (kWh).
- Discrete-time consumption and pricing model
- Consider $N$ time slots that span time frame $[0, T]$
- Duration of time slot $i$, $\tau_i \triangleq t_i - t_{i-1}$ (sec)
- Total power consumption $X(t)$ within time slot $i$: $X_i$ (kW)
- Cost of unit energy $C(t)$ within time slot $i$: $C_i$ (cent/kWh)

# Energy Management Unit




- Energy Management Unit (EMU) satisfies

$$X(t) = Y(t) + P(t)$$

- $Y(t) \geq 0$ (kW): power drawn from smart grid
- $P(t)$ (kW): power charged to, or discharged from RB
- SM reports average $Y(t)$ for each time slot to EP

# Energy Management (EM) Policy

- EM policy, i.e., $Y(t)|_{t=0}^{T}$, jointly optimizes privacy and cost
- Assume user load known for following $N$ time slots

## Privacy measure:

- Flat power demand leads to perfect privacy
- Average power demand, $\bar{E} \triangleq \frac{1}{T} \sum_{i=1}^{N} \tau_i \cdot X_i$
- Perfect privacy: $Y(t) = \bar{E}, \forall t \in [0, T]$
- Privacy measured by Load Variance: $\mathcal{V} \triangleq \frac{1}{T} \int_0^T (Y(t) - \bar{E})^2 dt$

## Cost measure:

- Average Energy Cost: $\mathcal{C} \triangleq \frac{1}{T} \int_0^T Y(t) C(t) dt$

---

O. Tan, D. Gündüz, H. V. Poor, "Increasing smart meter privacy through energy harvesting and storage devices," *IEEE Journal on Selected Areas in Communications*, Jul. 2013.

# Constraints

- Appliances should not incur any outages (no load shifting):

$$\int_0^t X(u)du \leq \int_0^t Y(u)du, \forall t \in [0, T] \tag{1}$$

- Finite RB capacity, energy cannot be wasted (no battery overflow):

$$\int_0^t (Y(u) - X(u))du \leq B, \quad \forall t \in [0, T] \tag{2}$$

- $(\mathcal{V}, \mathcal{C})$ pairs under (1) and (2) form a convex region
- Sufficient to characterize Pareto boundary of achievable $(\mathcal{V}, \mathcal{C})$ pairs

# Optimal Energy Management (EM) Policy

## Optimization problem

$$\min_{Y(t)\geq 0} \int_0^T \left[\theta\left(Y(t)-\bar{E}\right)^2 + (1-\theta)Y(t)C(t)\right] dt$$

s.t. (1) and (2)

- $0 \leq \theta \leq 1$ is the trade-off parameter.

# Optimal Energy Management (EM) Policy

## Dimensionality reduction

- Cost and demand constant within a time slot
- Due to convexity optimal $Y(t)$ constant within a TS
- Number of variables = Number of time slots ($N$)
- Optimize over $Y_1, \ldots, Y_N$

## Convex optimization problem

$$\min_{P_i \geq 0} \sum_{i=1}^{N} \left[ \theta \cdot \tau_i \cdot (Y_i - \bar{E})^2 + (1-\theta) \cdot \tau_i \cdot Y_i C_i \right]$$

$$\text{s.t.} \quad \sum_{i=1}^{n} \tau_i \cdot X_i \leq \sum_{i=1}^{n} \tau_i \cdot Y_i, \qquad n = 1, \ldots, N, \tag{3}$$

$$\sum_{i=1}^{n} \tau_i \cdot (Y_i - X_i) \leq B, \qquad n = 1, \ldots, N. \tag{4}$$

# Optimal EM policy

- $\theta = 0$: Linear program
- For $0 < \theta \leq 1$, applying KKT optimality conditions:

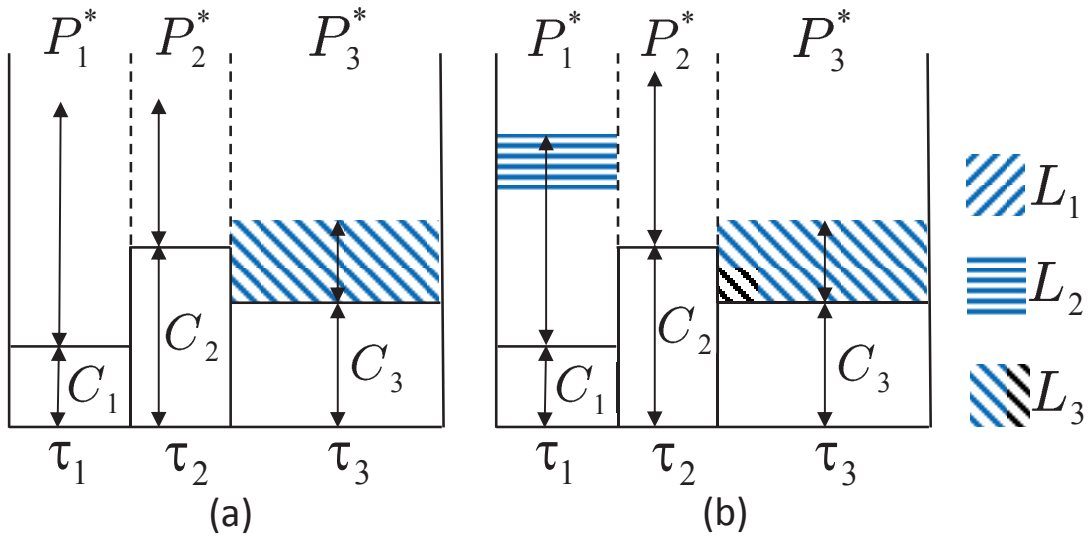
$$Y_i^* = \left[\alpha_i - \frac{(1-\theta)C_i}{2\theta}\right]^+, \quad 0 < \theta \leq 1 \quad , \forall i$$

where

$$\alpha_i \triangleq \frac{\sum_{j=i}^{N}(\lambda_j - \mu_j)}{2\theta} + \bar{E}, \quad 0 < \theta \leq 1 \quad , \forall i.$$

  - $\lambda_i$ and $\mu_i$ are Lagrange multipliers associated with (3) and (4), respectively.

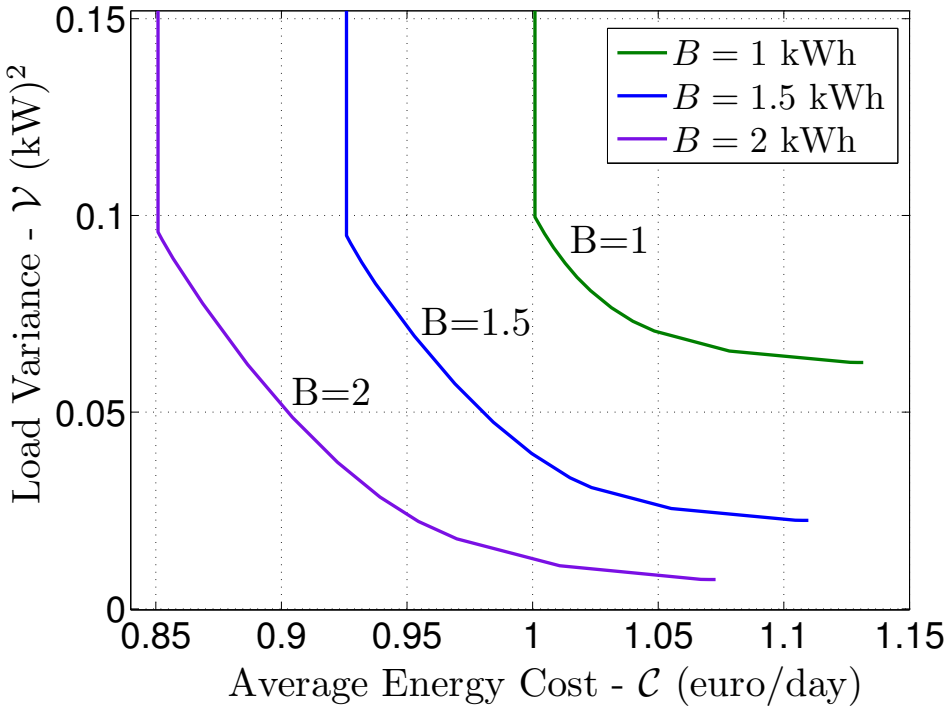
# Backward Water-filling




- Backward water-filling algorithm for optimal EM policy with (a) infinite, and (b) finite capacity RB, and $\theta = 1/3$.

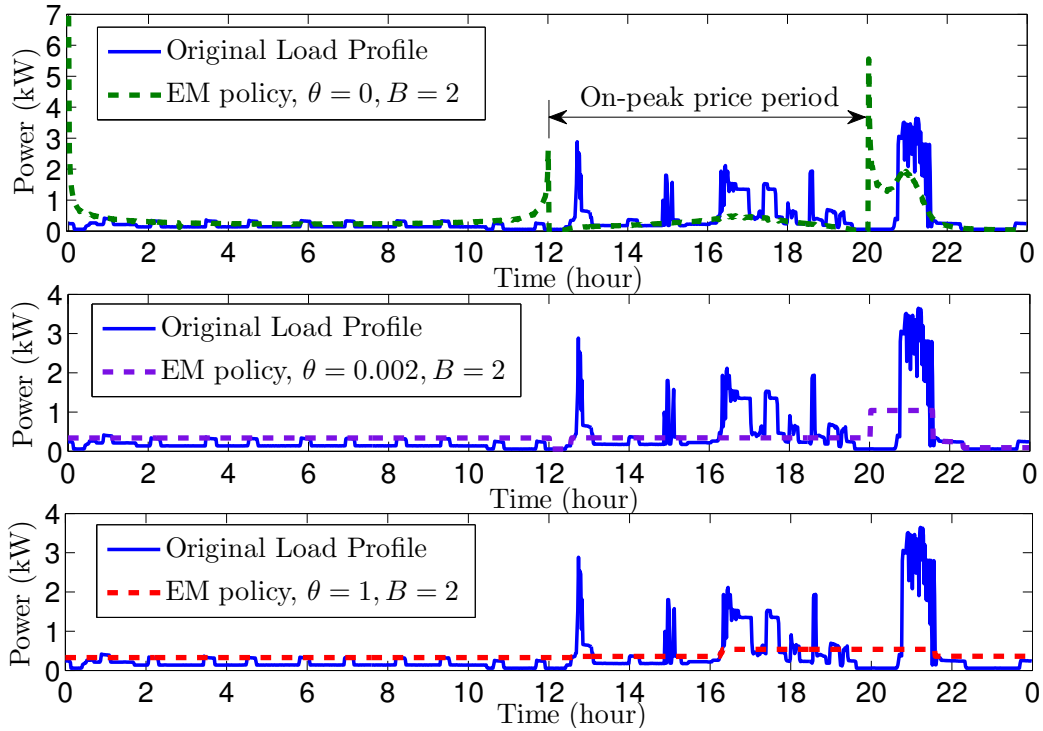
# Real Consumption Data

- A whole-day real power consumption data of a household
- Real pricing tariffs,
  - The off-peak price (00:00 – 12:00) is 5 (cent/kWh).
  - The on-peak price (12:00 – 20:00) is 20 (cent/kWh).
  - The medium-peak price (20:00 – 00:00) is 10 (cent/kWh).



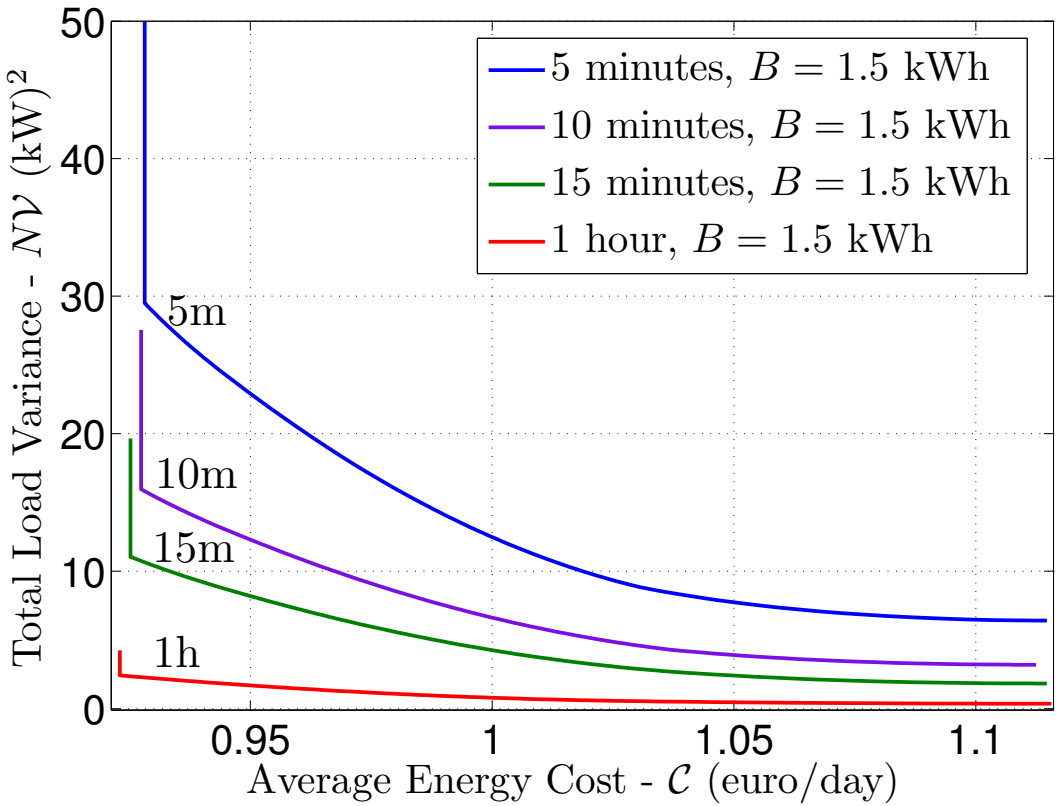

- Pareto optimal trade-off curves obtained varying $\theta$ from 0 to 1.
- Trade-off moves towards origin as RB capacity increases.

# Energy Consumption Profile



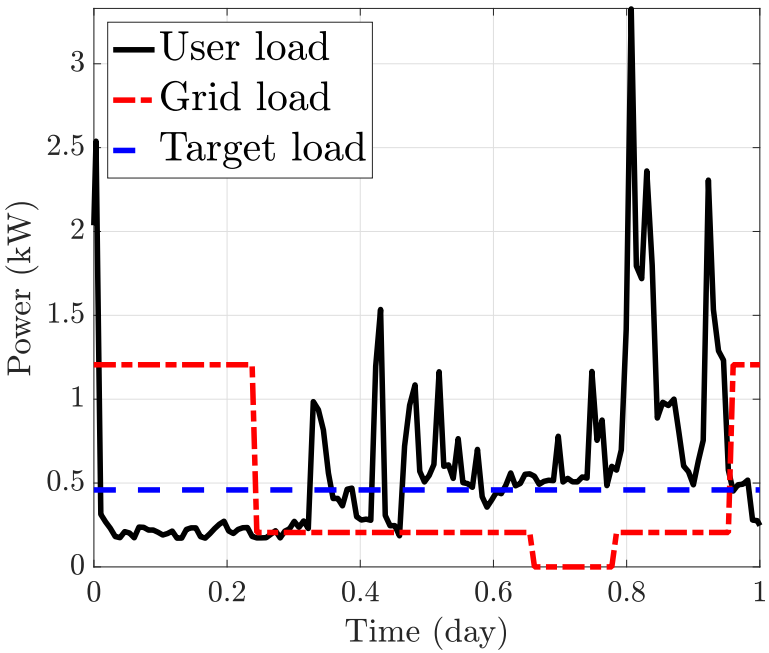

- $\theta = 0$: EM policy minimizes only the energy cost
  - Extra energy is stored in RB in the off-peak price period
  - Peak demand satisfied from RB as much as possible
- $\theta = 1$: EM policy maximizes only the privacy
  - A smooth load profile is generated
  - Peaks in the original load profile are masked

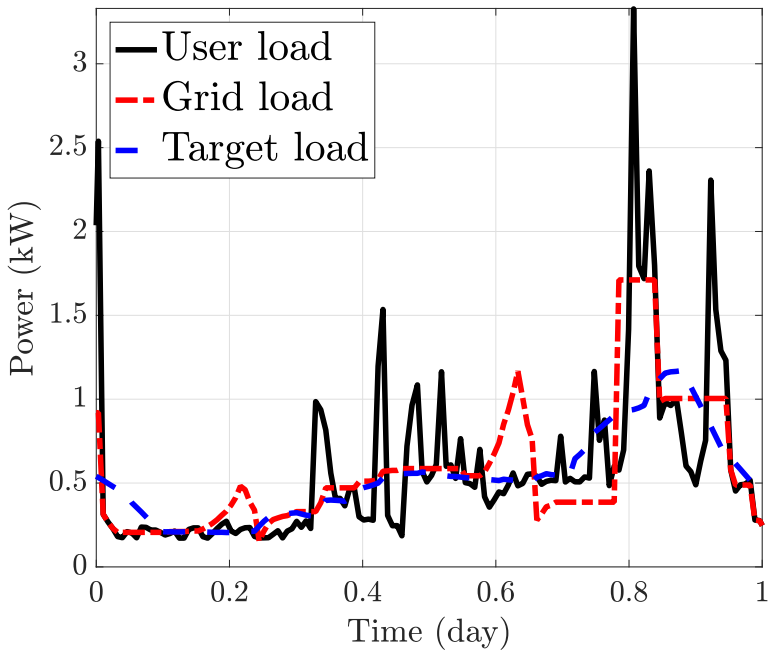
# Impact of Measurement Resolution




- Measurement time resolutions 5, 10, 15 minutes, and 1 hour.
- Optimal boundary moves downwards as SM resolution decreases
- Higher privacy with decreasing meter resolution

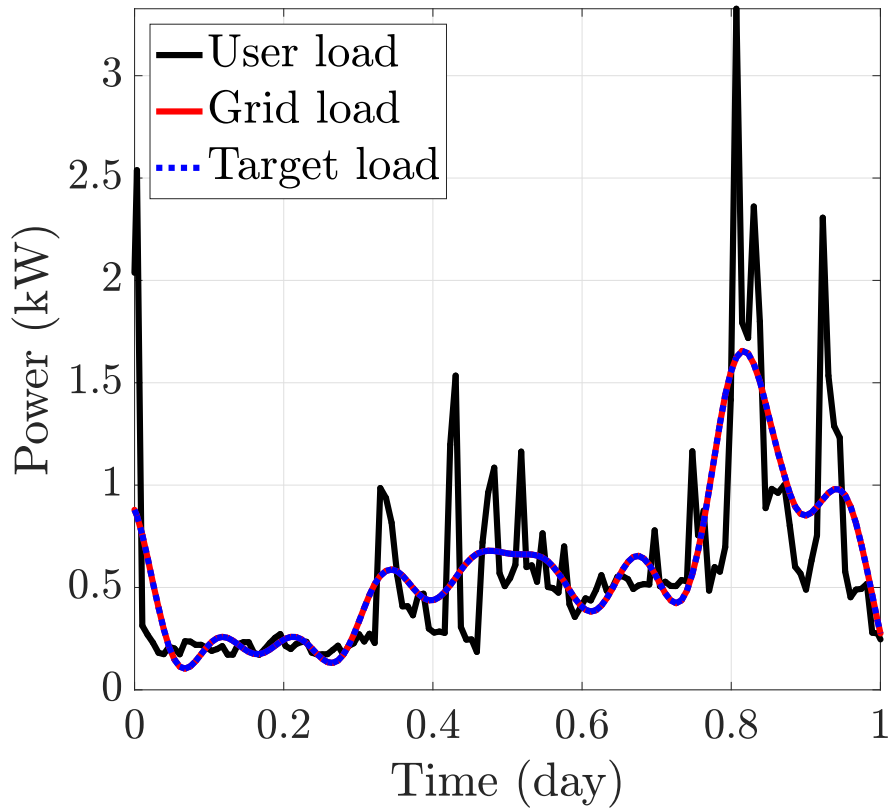
# Limited Prediction Horizon




- EMU can predict demand only for a limited future horizon

# Filtered Target Load Profile




- Fixed target load equivalent to keeping the dc response
- We can keep more low-frequnecy components
- Most information in high-frequency components

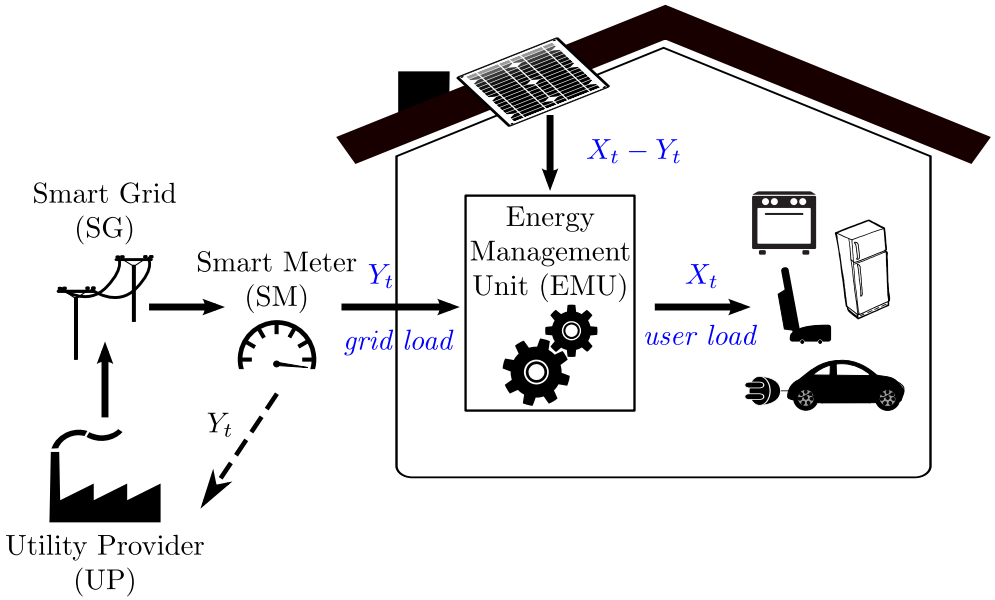
# Statistical Privacy Measures

- Treat user load as a random sequence
- Grid load is also random, and depends on the energy management (EM) policy
- Privacy can be measured by the *similarity* between the two time series
- Perfect privacy achieved when grid load is *independent* of user load
- With no EM, grid load = user load: maximum leakage

# Statistical Privacy Measures

- Treat user load as a random sequence
- Grid load is also random, and depends on the energy management (EM) policy
- Privacy can be measured by the *similarity* between the two time series
- Perfect privacy achieved when grid load is *independent* of user load
- With no EM, grid load = user load: maximum leakage
- We will first consider information theoretic privacy measure: mutual information between user and grid loads

# Privacy with a Renewable Energy Source




- Discrete time model:
  - Energy demand (user load): $X_t$
  - Energy from grid (grid load): $Y_t$
  - Remainder from renewable energy source(RES): $X_t - Y_t$
- SM measures and reports $Y_t$

---

J. Gomez-Vilardebo and D. Gunduz, "Smart meter privacy for multiple users in the presence of an alternative energy source," *IEEE Transactions on Information Forensics and Security*, Jan. 2015.

# Energy Management Policy

- Energy management policy: $f_t : \mathcal{X}^t \times \mathcal{Y}^{t-1} \to \mathcal{Y}$, s.t.

$$0 \leq X_t - Y_t \leq \bar{P}$$

- Privacy: Information leakage rate

$$I_n \triangleq \frac{1}{n} I(X^n; Y^n)$$

- Average power from RES:

$$P_n = \mathbb{E}\left[\frac{1}{n}\sum_{t=1}^{n}(X_t - Y_t)\right]$$

- For given $\bar{P}$, pair $(I, \hat{P})$ is achievable if there exist energy management policies with $\lim_{n\to\infty} I_n \leq I$ and $\lim_{n\to\infty} P_n \leq \hat{P}$.
- Privacy-power function, $\mathcal{I}(\bar{P}, \hat{P})$, is the minimum achievable information leakage rate under peak power $\bar{P}$, and average power $\hat{P}$ constraints on renewable energy generation rate.

# Privacy- Power Function

- Assume independent identically distributed (i.i.d.) input power sequence $X^n$ with distribution $p_X$

## Theorem (Privacy-Power Function)

*Privacy - power function for an i.i.d. input load $X$ with distribution $p_X(x)$ is given by*

$$\mathcal{I}(\bar{P},\hat{P}) = \inf_{\substack{p_{Y|X}(y|x):\mathrm{E}[X-Y]\leq\hat{P}\\ 0\leq X-Y\leq\bar{P}}} I(X;Y)$$

- Privacy - power function is a non-increasing convex function of $\bar{P}$.
- Optimal energy management policy is memoryless and stochastic: randomly generate output load based on instantaneous input load.

# Rate-Distortion Interpretation

Privacy-power function is a rate-distortion function with difference distortion measure:

$$d(x,y) = \begin{cases} x-y & \text{if } 0 \le x-y \le \bar{P}, \\ \infty & \text{otherwise.} \end{cases}$$

- No digital interface: $Y^n$ is direct output of "encoder", rather than the reconstruction of the decoder based on the transmitted index
- EMU does not operate over blocks: $Y_t$ decided instantaneously based on previous input/output loads
- If all future energy demands were known, same privacy could be achieved by deterministic block-based energy management policy

# Continuous Grid Load

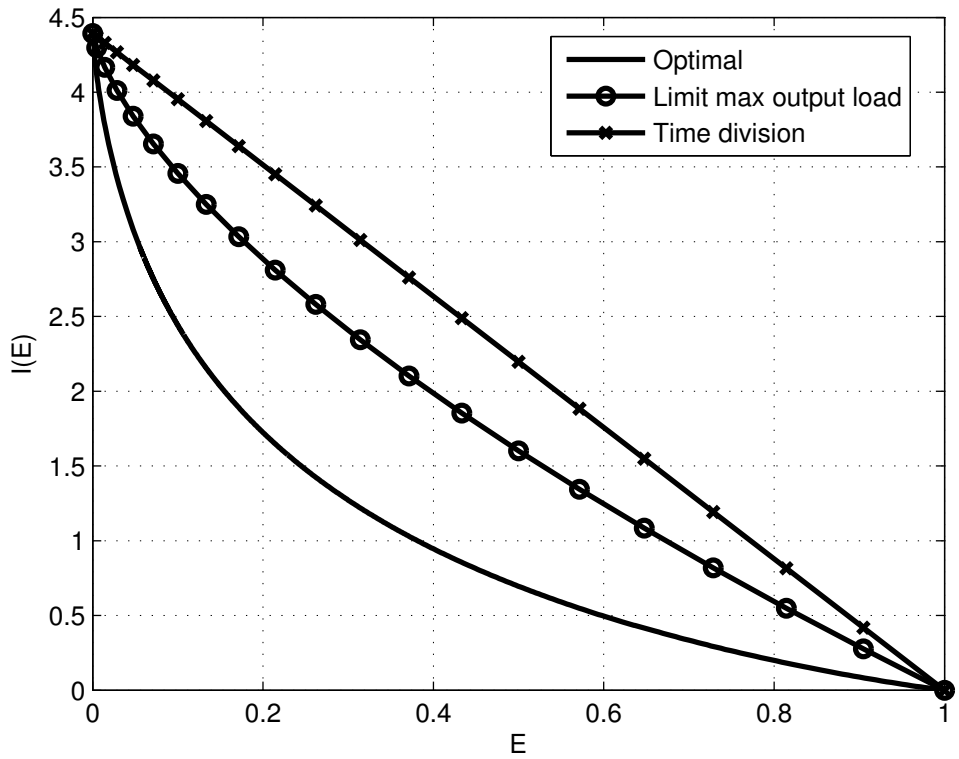
- Continuous grid load alphabet: Infinitely many variables

**Theorem**

*Without loss of optimality grid load alphabet $\mathcal{Y}$ can be constrained to the user load alphabet, i.e., $\mathcal{Y} = \mathcal{X}$.*

- Discrete user/ grid load alphabets: Convex optimization problem
- Blahut-Arimoto algorithm

# Uniform Grid Load




- Uniform demand over $\{0, c, 2c \ldots, 20c\}$, such that $E[X] = 1$
- Time division: Either from RES or grid
- Limit max output load: $Y(t) \leq C$

# Continuous User Loads

- Continuous user and grid load alphabets
- No efficient numerical computation method (infinite dimensional optimization problem)
- Shannon Lower Bound (SLB):

$$\mathcal{I}(P) \geq (\mathrm{h}(X) - \ln(P))^{+} \text{ nats}$$

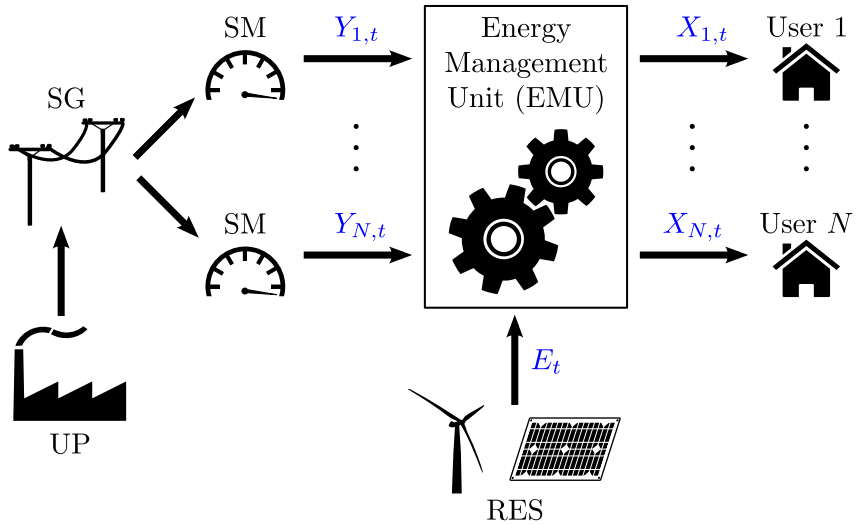
- Not tight in general
- Exponential input load, $X \sim exp(\lambda)$: SLB is tight
- Achieved by $f_{Y_i|X_i}(y|x) = \frac{P_{X_i}}{P_i} e^{-\frac{(x-y)}{P_i}} e^{\frac{x}{P_{X_i}}} f_{Y_i}(y)$, where $f_{Y_i}$ is a mixture of a continuous and a discrete distribution specified by

$$f_{Y_i}(y) = \left(1 - \frac{P_i}{P_{X_i}}\right) \frac{1}{P_{X_i}} e^{-\frac{y}{P_{X_i}}} + \frac{P_i}{P_{X_i}} \delta(y),$$

where $\delta(y)$ is the Dirac delta function.

$$\mathcal{I}(P) = \left(\ln\left(\frac{\lambda}{P}\right)\right)^{+} \text{ nats.}$$

# Shared Storage




- $N$ independent appliances sharing a common RES
- Input load of appliance $i$: $X_i$
- Goal: Minimize the total (or weighted) information leakage:

$$\mathcal{I}(P) = \inf_{\sum_{i=1}^{N} P_i \leq P} \sum_{i=1}^{N} \mathcal{I}_{X_i}(P_i).$$

---

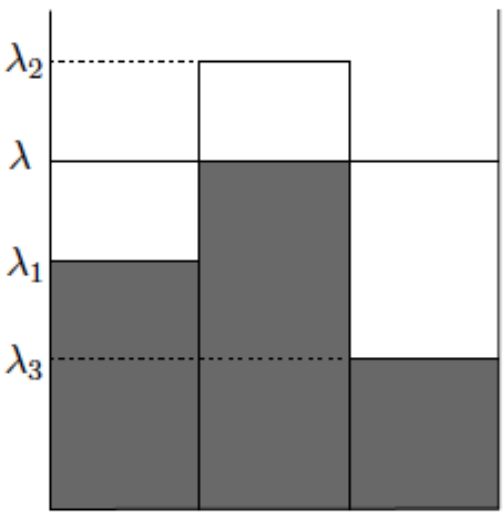
J. Gomez-Vilardebo and D. Gunduz, "Smart meter privacy for multiple users in the presence of an alternative energy source," IEEE Trans. on Information Forensics & Security, Jan. 2015.

# Exponential User Loads

- Let $X_i \sim \text{Exp}(P_{X_i})$
- Optimal power allocation obtained by reverse water-filling:

$$P_i^* = \begin{cases} \lambda, & \text{if } \lambda < P_{X_i}, \\ P_{X_i}, & \text{if } \lambda \geq P_{X_i}, \end{cases}$$

where $\lambda$ is chosen such that $\sum_{i=1}^{N} P_i^* = P$.




- Satisfy all energy demands with average load below $\lambda$ from RES
- Others receive exactly power $\lambda$ from the RES, and remainder of their demand from the grid

J. Gomez-Vilardebo and D. Gunduz, Smart meter privacy for multiple users in the presence of an alternative energy source, IEEE Trans. on Information Forensics & Security, vol. 10, no. 1, pp. 132-141, Jan. 2015.

# Instantaneous Power Constraints

- We have considered average power constraint: Appropriate for alternative energy sources such as micro-grids,
- For RES, energy is generated online with some statistics
- For finite RB capacity, we have instantaneous constraints
- In general, a Markov decision process (MDP)
- We will first look at special cases

# RES with an Infinite Battery ($B_{max} = \infty$)

- Cumulative energy constraints ($E_t$ random process):

$$\sum_{t=1}^{n}(X_t - Y_t) \leq \sum_{t=1}^{n} E_t, \qquad \forall n.$$

**Theorem**

*If $B_{max} = \infty$, minimum information leakage rate $\mathcal{I}_\infty$ for average renewable energy generation rate $\bar{P}_E$, is*

$$\mathcal{I}_\infty \triangleq \mathcal{I}(\bar{P}_E, \infty)$$

- Scenario equivalent to average-power-constrained case. Lower bound on minimum information leakage under battery constraints.

---

G. Giaconi, D. Gunduz, and H. V. Poor, "Smart meter privacy with renewable energy and an energy storage device," *IEEE Trans. on Information Forensics & Security,* Jan. 2018.

# Achievable Schemes for $B_{max} = \infty$

## Store-and-Hide Scheme

- Initial storage phase of duration $h(n)$: requests satisfied only from grid, no privacy.
- Consecutive hiding phase of duration $n - h(n)$. Energy from grid and battery. Privacy achieved.
- Assumptions: $h(n) \in o(n)$, with $\lim_{n\to\infty} h(n) = \infty$, and $\lim_{n\to\infty} n - h(n) = \infty$.
- Constraints satisfied if $\mathbb{E}[X - Y] < \bar{P}_E$. No information about recharge process required.

## Best-Effort Scheme

- No initial charging phase. Same stochastic policy of hiding phase. If $S_t + E_t \geq X_t - Y_t$, decide whether to take energy from battery or from grid.
- Battery update: $S_{t+1} = S_t + E_t - (X_t - Y_t) \cdot \mathbf{1}(S_t + E_t \geq X_t - Y_t)$, where $\mathbf{1}(x) = 1$ if $x$ holds, and 0 otherwise.
- If $\mathbb{E}[X - Y] < \bar{P}_E$, $S_t + E_t < X_t - Y_t$ holds only for finitely many time slots as $n \to \infty$.

# RES without Battery ($B_{max} = 0$)

- $E_t$ serves as a peak power constraint on the energy requested from RES. Energy constraint:

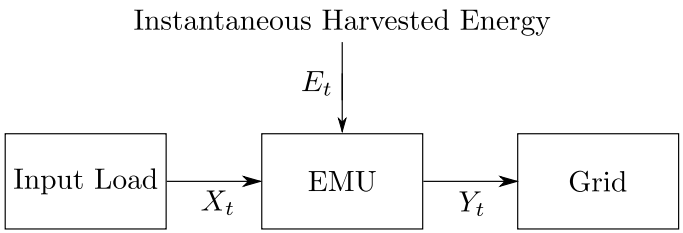
$$0 \leq X_t - Y_t \leq E_t, \qquad t = 1, ..., n.$$

  **Remark**: past has no influence.

- For random $E_t$, two scenarios: RES state known only by EMU, and known also by EP.

# No Battery ($B_{max} = 0$)

## RES State Known only by EMU

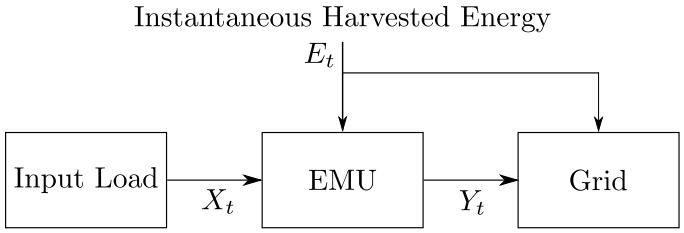



- UP still knows $p_E$.

  If $B_{max} = 0$, and RES is i.i.d. with $p_E$, minimum information leakage rate

$$\mathcal{I}_0 \triangleq \inf_{p_{Y|X,E}(y|x,e):0\leq X-Y\leq E} I(X;Y)\,.$$

## RES State Known also at UP




- Worst case scenario.

  If $B_{max} = 0$ and RES state known at the UP, minimum information leakage rate:

$$\bar{\mathcal{I}}_0 \triangleq \inf_{p_{Y|X,E}(y|x,e):0\leq X-Y\leq E} I(X;Y|E)\,.$$

- It is possible to prove $\bar{\mathcal{I}}_0 \geq \mathcal{I}\left(\bar{P}_E, \infty\right) = \mathcal{I}_\infty$ hold, and $\mathcal{I}_0 \leq \bar{\mathcal{I}}_0$.

# Binary Input Load

$\mathcal{X} = \{0, 1\}$,
$X \sim \text{Bern}(q_x)$,
$\Pr\{X = 1\} = q_x$.
$\mathcal{E} = \{0, 1\}$,
$E \sim \text{Bern}(p_e)$,
$\Pr\{E = 1\} = p_e$.

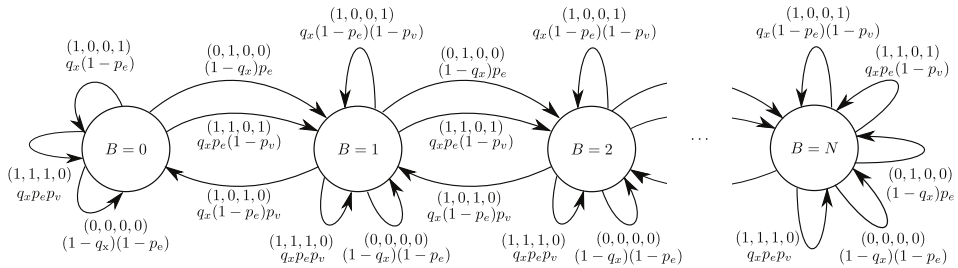



Figure 1: Finite battery model.

$q_x = 0.7$

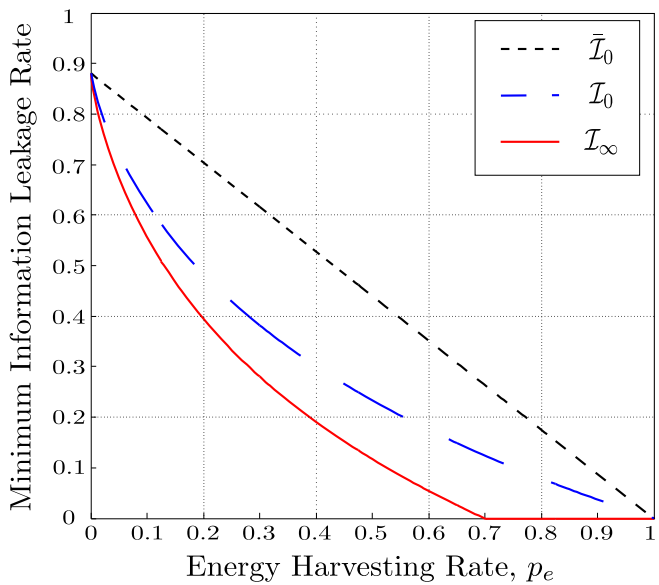



Figure 2: Privacy w.r.t. $p_e$.

$q_x = 0.5$

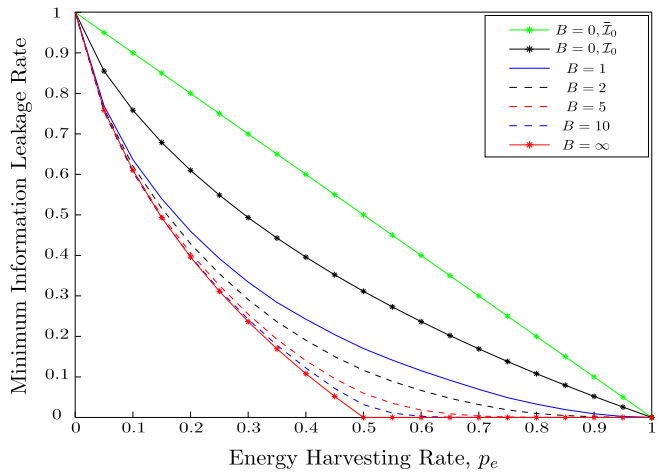


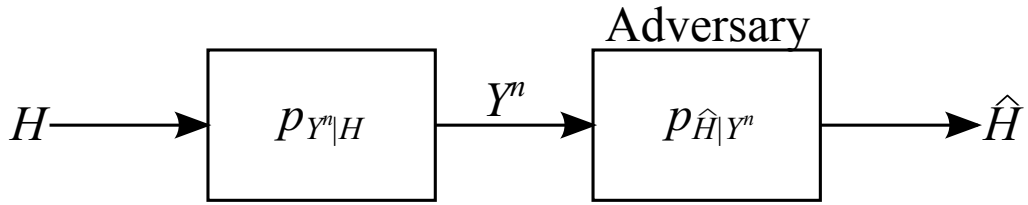

Figure 3: Privacy w.r.t. $p_e$.

# Energy Manipulation against Statistical Inference Attacks

**Content:**

- Statistical inference based approaches based on
  - **unauthorized hypothesis detection** (Bayesian/Neyman-Pearson approach)
  - **unauthorized state estimation** (Fisher information-based approach)
- Problem modeling and recapitulations, privacy-by-design approach based on worst-case asymptotics, fundamental bounds, algorithmic design based on Markov-decision process framework, ...
  - Methods are applied to smart meter privacy problem, but readily extend to other settings
  - Binary hypothesis testing can be straightforwardly extended to multiple hypotheses.

# Privacy Leakage as a Neyman-Pearson Test




- **Neyman-Pearson hypothesis test**
  - Binary hypothesis $H$ (e.g., watching TV or not)
  - Observation $Y^n$ and likelihood $p_{Y^n|H}$
  - Decision $\hat{H}$
  - Type I prob. of error $p_{\mathrm{I}} = p_{\hat{H}|H}(h_1|h_0)$ (false alarm, false neg.)
  - Type II prob. of error $p_{\mathrm{II}} = p_{\hat{H}|H}(h_0|h_1)$ (miss, false positive)

## Neyman-Pearson test approach

$$p^*_{\hat{H}|Y^n} = \arg\min_{p_{\hat{H}|Y^n}} p_{\mathrm{II}}, \text{ s.t. } p_{\mathrm{I}} \leq \phi$$

# Privacy Leakage as a Neyman-Pearson Test (cont.)

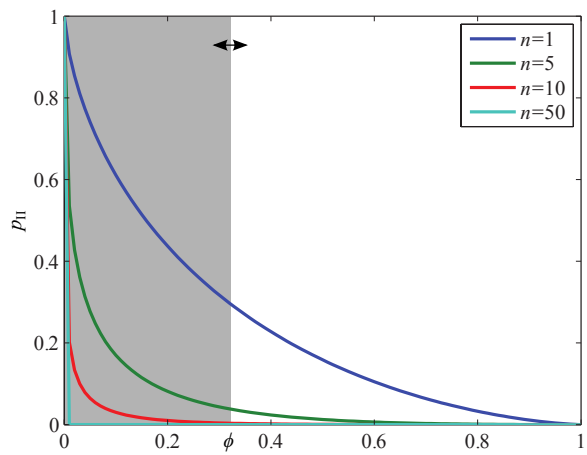
- **Privacy leakage measure:** Minimal Type II probability of error

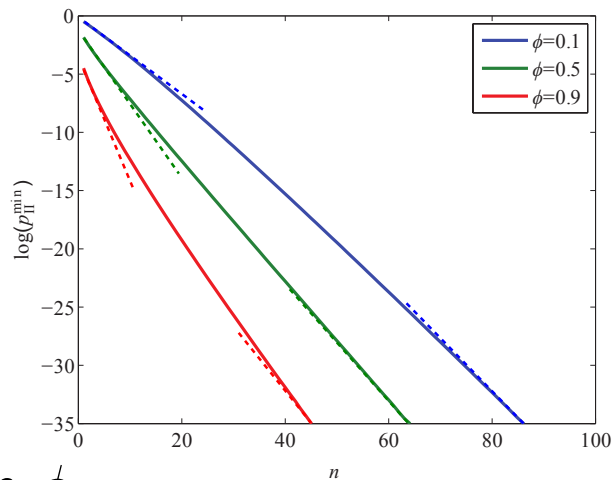
$$p_{\mathrm{II}}^{\min} = \min_{\gamma:\mathcal{Y}^n\to\mathcal{H}} p_{\mathrm{II}}, \text{ s.t. } p_{\mathrm{I}} \le \phi$$

## Stein's Lemma: Asymptotic privacy leakage measure

Let $Y^n$ be i.i.d. sequence under each hypothesis, i.e., $\sim p_{Y|h_0}$ or $\sim p_{Y|h_1}$,

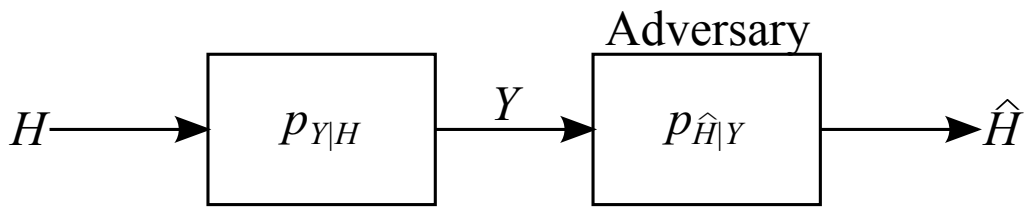
$$r_{\mathrm{II}} = \lim_{n\to\infty} -\frac{\log p_{\mathrm{II}}^{\min}}{n} = \mathrm{D}(p_{Y|h_0}||p_{Y|h_1})$$




- Note that $r_{\mathrm{II}}$ does not depend on $\phi$.

# Privacy Leakage as a Bayesian Hypothesis Test




- **Bayesian hypothesis test**
  - Hypothesis $H$ and prior distribution $p_H$
  - Observation $Y$ (smart meter reading) and likelihood $p_{Y|H}$
  - Decision $\hat{H}$ and decision cost $c(\hat{h}, h)$
  - Bayesian risk $r = \mathbb{E}\{c(\hat{H}, H)\}$ (expected decision cost)

## Bayesian test approach

$$p^*_{\hat{H}|Y} = \arg\min_{p_{\hat{H}|Y}} r$$

# Bayesian Testing Modeled Privacy Leakage (cont.)

- **Design objective** of the adversary: Minimize the Bayesian risk

$$r = \sum_{h,\hat{h}\in\mathcal{H}} c(\hat{h},h)p_{\hat{H},H}(\hat{h},h) = \sum_{y\in\mathcal{Y}}\sum_{\hat{h}\in\mathcal{H}} p_{\hat{H}|Y}(\hat{h}|y)\sum_{h\in\mathcal{H}} c(\hat{h},h)p_{Y|H}(y|h)p_H(h).$$

  - *Deterministic likelihood test* are sufficient for optimality

$$\gamma^*(y) = \arg\min_{\hat{h}\in\mathcal{H}} \sum_{h\in\mathcal{H}} c(\hat{h},h)p_{Y|H}(y|h)p_H(h)$$

- **Privacy leakage measure:** Minimal Bayesian risk of the adversary

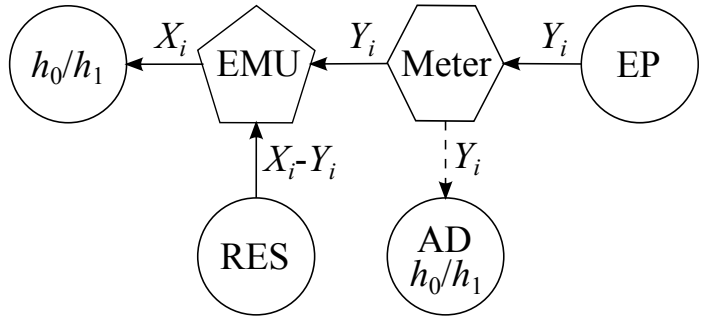
$$r^{\min} = \min_{\gamma:\mathcal{Y}\to\mathcal{H}} r = \sum_{y\in\mathcal{Y}} \left\{ \min_{\hat{h}\in\mathcal{H}} \left\{ \sum_{h\in\mathcal{H}} c(\hat{h},h)p_{Y|H}(y|h)p_H(h) \right\} \right\}$$

# Adversarial Hypothesis Testing - Overview

- Assumptions on the adversary
  - Informed about the smart metering system, access to smart meter readings and knowledge on statistics
  - Adversarial behavior: Neyman-Pearson or Bayesian hypothesis testing
- Problem settings
  - Worst-case analysis[5]
  - Consumer energy demands: i.i.d. or Markov model
  - Distortion source: renewable energy supplies (RES) or rechargeable battery
- Objectives of Studies
  - Privacy-enhancing energy management design
  - Fundamental bounds on the privacy performance

[5] Flipping the processing order of attacker and defender, i.e., attacker manipulates observation leads to zero-sum game theoretic formulation of adversarial signal processing approaches, e.g. [Barni, Tondi '13, '16].

# SM System with Renewable Energy Supply




- **Binary** hypothesis $h_0/h_1$ (e.g. using the oven or not)
- i.i.d. energy demands $X^n|h_0$ or $X^n|h_1$
- EMU: Random instantaneous energy management policy

$$Y_i = \gamma_i(x^i, y^{i-1}, h), \text{ s.t. } y_i \leq x_i.$$

- RES with a sufficiently-large energy storage
- EMU policy over $n$-slot horizon $\gamma^n(s) = \{\gamma_i\}_{i=1}^n$ satisfying

$$\mathrm{E}\left[\frac{1}{n}\sum_{i=1}^{n}(X_i - Y_i)\middle| h_j\right] \leq s, \quad \forall j = 0, 1$$

# Adversarial Neyman-Pearson Hypothesis Test Design

- Informed adversary
- **Operational** privacy leakage measure:

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

where $\mathcal{A}_n$ and $\mathcal{A}_n^c$ denote decision regions for $h_0$ and $h_1$ of the AD.

## Design objective for privacy enhancement

$$\beta(n, \varepsilon, s) \triangleq \max_{\gamma^n(s) \in \Gamma^n(s)} \{\beta(n, \varepsilon, \gamma^n(s))\}.$$

Li, Oechtering, Gündüz, "Smart meter privacy based on adversarial hypothesis testing," in *Proc. IEEE ISIT 2017*.

# Infimum Kullback-Leibler Divergence Rate

- Infimum Kullback-Leibler divergence rate[6] $\theta(s)$ is defined as

$$\theta(s) \triangleq \inf_{k\in\mathbb{Z}_+} \left\{ \inf_{\gamma^k(s)\in\Gamma^k(s)} \left\{ \frac{1}{k} \mathrm{D}(p_{Y^k|h_0} || p_{Y^k|h_1}) \right\} \right\}.$$

## Lemma 1

$$\theta(s) = \lim_{k\to\infty} \inf_{\gamma^k(s)\in\Gamma^k(s)} \left\{ \frac{1}{k} \mathrm{D}(p_{Y^k|h_0} || p_{Y^k|h_1}) \right\}.$$

- The proof follows from the subadditive sequence of $\inf_{\gamma^k(s)\in\Gamma^k(s)} \left\{ \mathrm{D}(p_{Y^k|h_0} || p_{Y^k|h_1}) \right\}$ and Fekete's Lemma[7].
- Thus, the **infimum is obtained in the limit.**

[6] KL-divergence is defined as $D(p||q) = \sum_i p(i) \log \frac{p(i)}{q(i)}$.

[7] Fekete Lemma: For every subadditive sequence $\{a_n\}_{n=1}^{\infty}$, the limit $\lim_{n\to\infty} \frac{a_n}{n}$ exists and is equal to $\inf_n \frac{a_n}{n}$.

# Asymptotic Privacy-Enhancement Performance Bounds

- Operational meaning of $\theta(s)$ for given $s > 0$:

## Theorem 1

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

$$\lim_{\varepsilon\to 1} \liminf_{n\to\infty} \frac{1}{n} \log \frac{1}{\beta(n,\varepsilon,s)} \geq \theta(s).$$

- Proof ideas:
  - Use the maximization(sup)/minimization(inf) and the definition of $\beta(n,\varepsilon,s)$ to derive upper/lower bound;
  - Use Stein's lemma, information spectrum, and Lemma 1 to relate with the Kullback-Leibler divergence rate $\theta(s)$.

# Robustness: Worst Scenario with $\varepsilon \to 1$

- Uncertainty about chosen $\varepsilon$ at AD
  - $\varepsilon \to 1$ is most conservative assumption
  - $\varepsilon \to 1$ means Type I probability of error does not matter for the AD.
- The bounds in Theorem 1 are tight when $\varepsilon \to 1$.

## Corollary 1

Given $s > 0$,

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

# Memoryless Hypothesis-Aware Policy

- Why memoryless energy management policy?
  - Generally, $\theta(s)$ is difficult to evaluate and achieve.
  - Memoryless policy is easy to design and implement in practice.

- Random instantaneous **memoryless hypothesis-aware policy**:

$$Y_i = \pi_i(x_i, h), \text{ s.t. } y_i \leq x_i.$$

- Memoryless hypothesis-aware policy over $n$-slot horizon $\pi^n(s) = \{\pi_i\}_{i=1}^n$ satisfying

$$\mathrm{E}\left[\frac{1}{n}\sum_{i=1}^{n}(X_i - Y_i)\middle| h_j\right] \leq s, \forall j = 0, 1$$

# Asymptotic Privacy-Enhancement Performance of $\pi^n(s)$

- **Design objective** for privacy enhancement policy:

$$\beta_{\mathsf{L}}(n,\varepsilon,s) \triangleq \max_{\pi^n(s)\in\Pi^n(s)} \{\beta(n,\varepsilon,\pi^n(s))\}.$$

  - $\Pi^n(s)$ denotes set of all memoryless policies $\pi^n(s)$.

- Define an infimum Kullback-Leibler divergence rate $\theta_{\mathsf{L}}(s)$ as

$$\theta_{\mathsf{L}}(s) \triangleq \inf_{k\in\mathbb{Z}_+} \left\{ \inf_{\pi^k(s)\in\Pi^k(s)} \left\{ \frac{1}{k} \mathsf{D}(p_{Y^k|h_0} || p_{Y^k|h_1}) \right\} \right\}.$$

## Corollary 2

Given $s > 0$,

$$\lim_{\varepsilon\to 1} \lim_{n\to\infty} \frac{1}{n} \log \frac{1}{\beta_{\mathsf{L}}(n,\varepsilon,s)} = \theta_{\mathsf{L}}(s).$$

- *Any single-letter expression?*

# Single-Letter Expression

- Given $s_0,\ s_1 > 0$, define

$$\phi(s_0, s_1) \triangleq \min_{(p_{Y|X,h_0}, p_{Y|X,h_1}) \in \mathcal{P}(s_0,s_1)} \left\{ \mathsf{D}(p_{Y|h_0} || p_{Y|h_1}) \right\}.$$

- **Lemma**: $\phi(s_0, s_1)$ is a non-increasing, continuous, and jointly convex function for $s_0 > 0$ and $s_1 > 0$.

## Theorem 2

Given $s > 0$,

$$\lim_{\varepsilon \to 1} \lim_{n \to \infty} \frac{1}{n} \log \frac{1}{\beta_{\mathsf{L}}(n, \varepsilon, s)} = \theta_{\mathsf{L}}(s) = \phi(s, s).$$

- The proof is based on the chain rule of Kullback-Leibler divergence and properties summarized in the above lemma.

**Remark**: $\phi(s, s)$ can be achieved with an *i.i.d.* memoryless policy.

# Hypothesis-*Unaware* Policy *with Memory*

- The EMU may not have access to the correct hypothesis.
- Random instantaneous **hypothesis-unaware policy with memory**:

$$Y_i = \rho_i(x^i, y^{i-1}), \text{ s.t. } y_i \leq x_i.$$

- Hypothesis-unaware policy with memory over $n$-slot horizon $\rho^n(s) = \{\rho_i\}_{i=1}^n$ satisfying

$$\mathsf{E}\left[\frac{1}{n}\sum_{i=1}^{n}(X_i - Y_i)\middle| h_j\right] \leq s, \forall j = 0, 1$$

# Asymptotic Privacy-Enhancement Performance of $\rho^n(s)$

- **Design objective** for privacy enhancement:

$$\beta_{\mathrm{M}}(n,\varepsilon,s) \triangleq \max_{\rho^n(s)\in P^n(s)} \{\beta(n,\varepsilon,\rho^n(s))\}.$$

- Define an infimum Kullback-Leibler divergence rate $\theta_{\mathrm{M}}(s)$ as

$$\theta_{\mathrm{M}}(s) \triangleq \inf_{k\in\mathbb{Z}_+} \left\{ \inf_{\rho^k(s)\in P^k(s)} \left\{ \frac{1}{k} \mathrm{D}(p_{Y^k|h_0} || p_{Y^k|h_1}) \right\} \right\}.$$

## Corollary 3

Given $s > 0$,

$$\lim_{\varepsilon\to 1} \lim_{n\to\infty} \frac{1}{n} \log \frac{1}{\beta_{\mathrm{M}}(n,\varepsilon,s)} = \theta_{\mathrm{M}}(s).$$

- *Which information is more useful for the asymptotic energy management? Correct hypothesis information or previous data?*

# Comparison of Policies

## Theorem 3

Given $s > 0$,

$$\theta_{\mathrm{M}}(s) \leq \phi(s, s).$$

- Proof idea: Construct a two-phase hypothesis-unaware policy with memory and bound its asymptotic performance by $\theta_{\mathrm{M}}(s)$, $\phi(s, s)$.
  - At the end of the first phase, the EMU makes a hypothesis test.
  - The energy management in the second phase depends on the decision of the EMU.
  - The EMU may make a wrong decision which can lead to a violation of the expected RES energy generation constraint.

# Adversarial Bayesian Hypothesis Testing

- Assume that the informed AD also knows the hypothesis prior probabilities $p_0$ and $p_1$.
- Operational privacy leakage measure:

$$\alpha(n, \gamma^n(s)) \triangleq \min_{\mathcal{A}_n \subseteq \mathcal{Y}^n} \left\{ p_0 \cdot p_{Y^n|h_0}(\mathcal{A}_n^c) + p_1 \cdot p_{Y^n|h_1}(\mathcal{A}_n) \right\},$$

with $\mathcal{A}_n$ and $\mathcal{A}_n^c$ decision regions for $h_0$ and $h_1$ of the AD.

## Design objective for privacy enhancement

$$\alpha(n, s) \triangleq \max_{\gamma^n(s) \in \Gamma^n(s)} \{\alpha(n, \gamma^n(s))\}.$$

- Lowest asymptotic exponent $D^* = \lim_{n \to \infty} -\frac{1}{n} \log \alpha(n, s)$

Li, Oechtering, Gündüz, "Privacy against a Hypothesis Testing Adversary," to be published IEEE T-IFS.
See also KTH PhD thesis of Z. Li (2016).

# Adversarial Bayesian Hypothesis Testing (cont.)

## Theorem (Chernoff)

$$D^* = D(p_{\lambda^*}||p_{Y^n|h_0}) \overset{(x)}{=} D(p_{\lambda^*}||p_{Y^n|h_1})$$

with $p_\lambda(y^n) = \dfrac{p^\lambda_{Y^n|h_0}(y^n)p^{1-\lambda}_{Y^n|h_1}(y^n)}{\sum\limits_{\hat{y}^n\in\mathcal{Y}^n} p^\lambda_{Y^n|h_0}(\hat{y}^n)p^{1-\lambda}_{Y^n|h_1}(\hat{y}^n)}$ and $\lambda^*$ the value of $\lambda \in [0,1]$ such that $(x)$ holds.

- It can be shown that $D^*$ is equal to the **Chernoff information** $C(p_{Y^n|h_0}, p_{Y^n|h_1}) = -\min\limits_{0\le\lambda\le 1} \log \sum_{y^n} p^\lambda_{Y^n|h_0}(y^n)p^{1-\lambda}_{Y^n|h_1}(y^n)$
- Similar results are obtained while the asymptotic performances are characterized by **Chernoff information rates** and **single-letter Chernoff information**.
  - Optimization of $\lambda$ is new and needs to be handled.

# Reduction of Energy Supply Alphabet

## Theorem 4

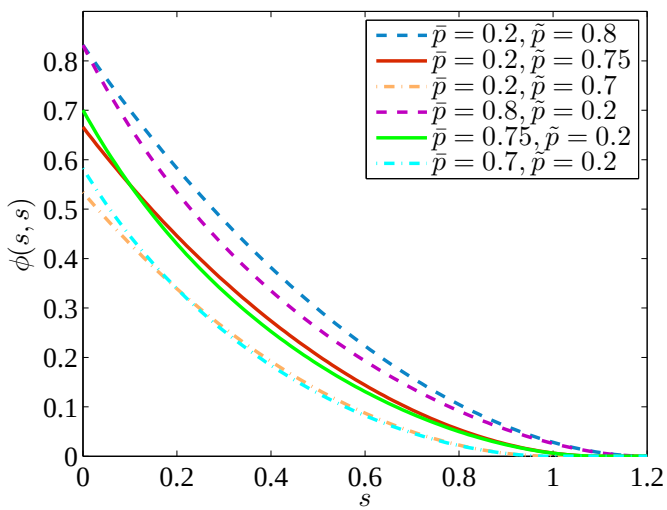
The **energy supply alphabet $\mathcal{Y}$ can be limited to the energy demand alphabet $\mathcal{X}$** under both hypotheses without loss of optimality for the evaluations of $\phi(s,s)$ and $\nu(s,s)$.

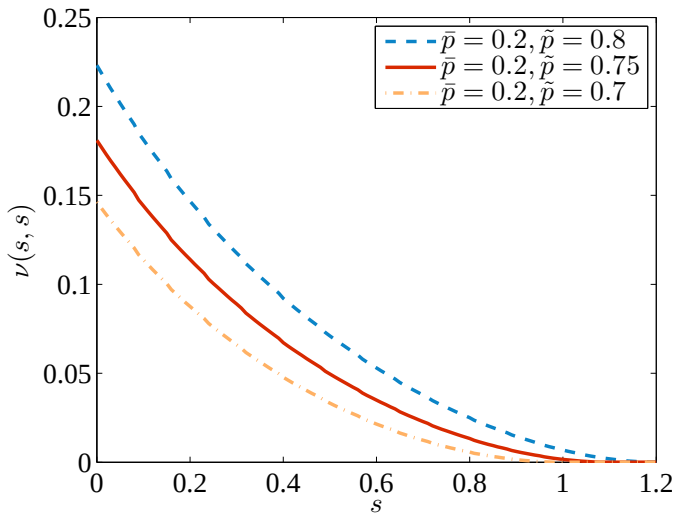
Proof outline:

- Let $\{p^*_{Y|h_i}\}_{i=0,1}$ be minimizer of $D(p^*_{Y|h_0}||p^*_{Y|h_1})$.
- Use certain quantization that maps $y$ to $\hat{y} \in \mathcal{X}$.
  - Always next higher level in $\mathcal{X}$.
- Let $\{p_{\hat{Y}|h_i}\}_{i=0,1}$ denote concatenation of $\{p^*_{Y|h_i}\}_{i=0,1}$ and quantization, then " $=$ " follows from
  - $D(p^*_{Y|h_0}||p^*_{Y|h_1}) \leq D(p_{\hat{Y}|h_0}||p_{\hat{Y}|h_1})$ since $\{p^*_{Y|h_i}\}_{i=0,1}$ is a minimizer, and
  - $D(p^*_{Y|h_0}||p^*_{Y|h_1}) \geq D(p_{\hat{Y}|h_0}||p_{\hat{Y}|h_1})$ due to data processing inequality for KL-divergence.

# Example

- Binary demand $\mathcal{X} = \{0, 2\} \Rightarrow$ binary supply $\mathcal{Y} = \{0, 2\}$.
- $\bar{p} = p_{X|h_0}(0)$, $\tilde{p} = p_{X|h_1}(0)$.



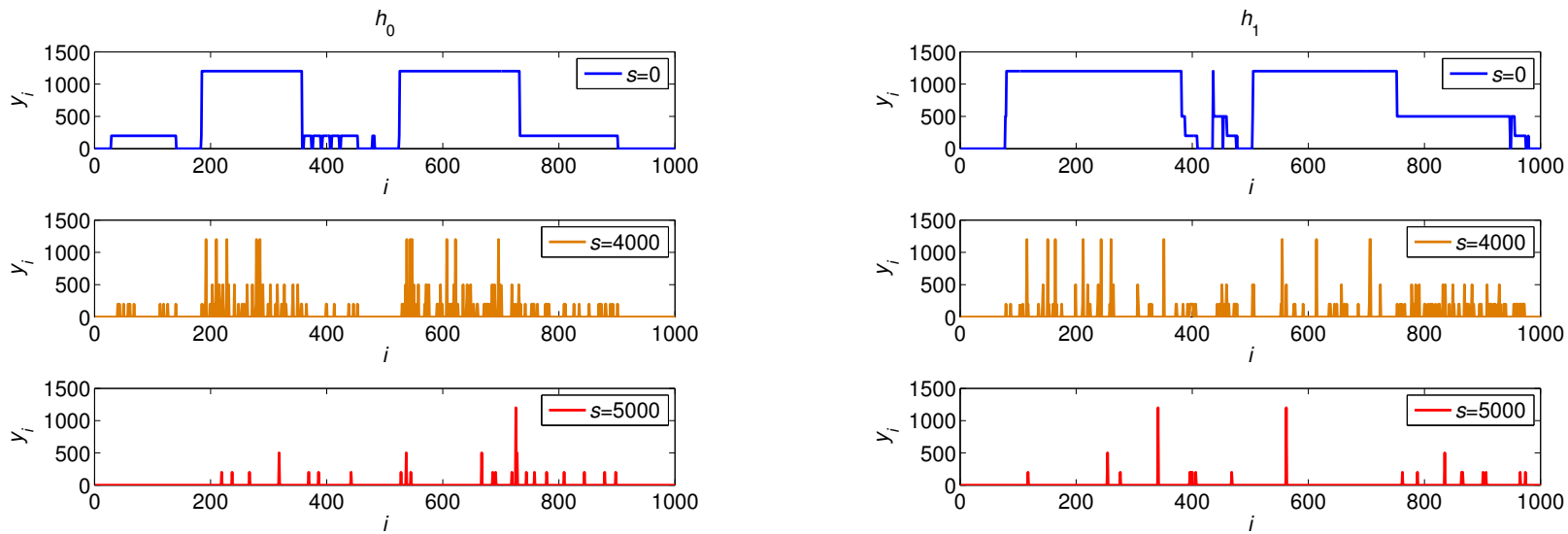




- Higher average renewable supply improves the privacy enhancement.
- Similar energy demand profiles improve the privacy enhancement.

# REDD Dataset Numerical Experiment

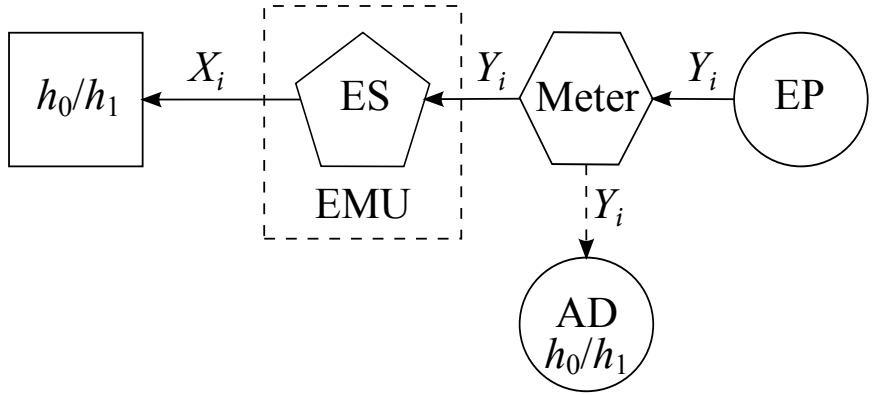
- $h_0$: Type A dishwasher is used. $h_1$: Type B dishwasher is used.
- The optimal i.i.d. memoryless hypothesis-aware policy is used.

| $p_{X\|h}$ : $h$ \ $x$ (W) | 0 | 200 | 500 | 1200 |
|---|---|---|---|---|
| $h_0$ (Type A) | 0.2528 | 0.3676 | 0 | 0.3796 |
| $h_1$ (Type B) | 0.1599 | 0.0579 | 0.2318 | 0.5504 |




Kolter, Johnson, "REDD: A public data set for energy disaggregation research," in *Proc. SustKDD Workshop'11*.

# SM System with a Powerful Energy Storage




- Binary hypothesis $H$
- i.i.d. energy demand $X_i$ under each hypothesis
- i.i.d. energy management: $p_{Y_i|H,X_i}$
  $\Rightarrow$ i.i.d. energy supply $Y_i$ under each hypothesis
- Powerful energy storage device assumption: **Infinite** capacity
- Dependency: $p_{X_i,Y_i|X^{i-1},Y^{i-1},H} = p_{X_i,Y_i|H} = p_{Y_i|X_i,H} \cdot p_{X_i|H}$

Li, Oechtering, "Privacy on hypothesis testing in smart grids," in *Proc. IEEE ITW 2015.*

# Adversarial Neyman-Pearson Hypothesis Testing

- Set of feasible energy management policies:

$$\mathcal{P}_{Y|X,H} = \left\{ p_{Y_i|X_i,H} : \begin{array}{l} \mathrm{E}(Y_i|h_0) = \mathrm{E}(X_i|h_0) = f_0 \\ \mathrm{E}(Y_i|h_1) = \mathrm{E}(X_i|h_1) = f_1 \end{array} \right\},$$

  i.e., asymptotic balance $\frac{1}{n}\sum_{i=1}^{n} Y_i \overset{a.s.}{\to} \mathrm{E}(X)$ under each hypothesis.

## Design objective for privacy enhancement

$$r_{\mathrm{II}}^* = \min_{p_{Y_i|X_i,H} \in \mathcal{P}_{Y|X,H}} \mathrm{D}(p_{Y_i|h_0} || p_{Y_i|h_1})$$

**Observations**:

- Sufficient to optimize $p_{Y_i|H}$ instead of $p_{Y_i|X_i,H}$ since both the objective and constraints depend on $p_{Y_i|H}$ only.
- Equal support condition: $\mathcal{S}(p^*_{Y_i|h_0}) = \mathcal{S}(p^*_{Y_i|h_1}) = \mathcal{Y}^*$. Adversary otherwise knows directly hypothesis for $y_i \notin \mathcal{S}(p^*_{Y_i|h_0}) \cap \mathcal{S}(p^*_{Y_i|h_1})$.

# Cardinality Bound of Energy Supply

## Theorem 1

The optimal energy management policy requests **at most two supply states**, i.e., $|\mathcal{Y}^*| \leq 2$.

Proof outline:

- The problem $\min_{p_{Y|H} \in \mathcal{P}_{Y|H}} \mathrm{D}(p_{Y|h_0} || p_{Y|h_1})$ is a convex optimization and satisfies Slater's condition.
  - Optimal $p^*_{Y|H}$ has to satisfy KKT conditions.
- Conditions of stationarity and complementary slackness lead to

$$\exp(-\lambda^* y - 1 - \nu_0^*) = w^* y + \nu_1^*, \ \forall y \in \mathcal{Y}^*.$$

  Denote the solution set of this equation by $\mathcal{Y}_\mathsf{s}$.
- $|\mathcal{Y}^*| \leq |\mathcal{Y}_\mathsf{s}|$. Then, bound $|\mathcal{Y}_\mathsf{s}|$.

# Optimal Energy Management

## Corollary 1

If $|\mathcal{Y}^*| = 1$, then we have equal expected energy demands for both hypotheses $f_0 = f_1 = f \in \mathcal{Y}$, $\mathcal{Y}^* = \{f\}$ and $r_{\text{II}}^* = 0$ (**perfect privacy**).

## Theorem 2

If $|\mathcal{Y}^*| = 2$, then $\mathcal{Y}^* = \{\min \mathcal{Y}, \max \mathcal{Y}\}$ with

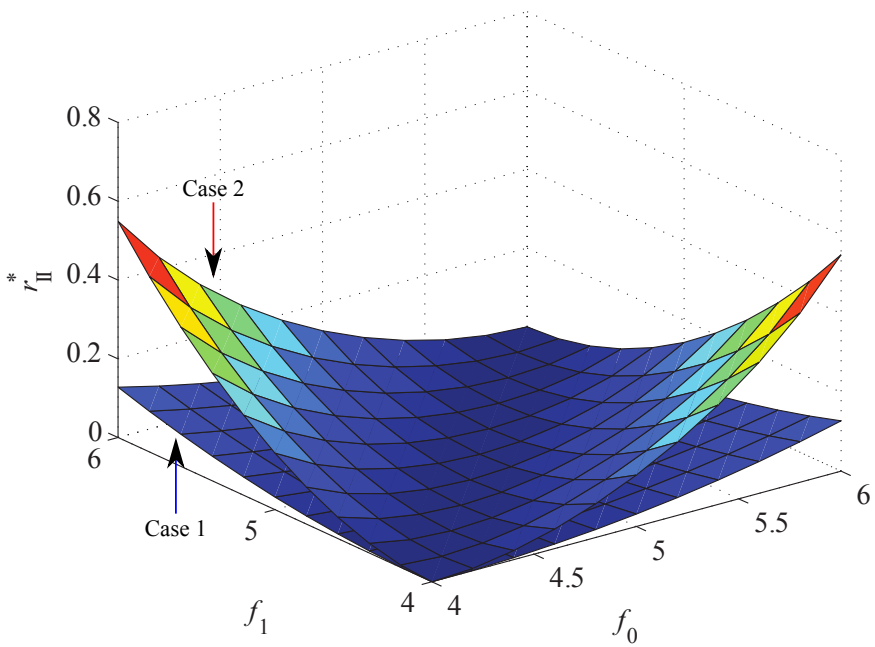
$$p^*_{Y_i|h_j}(\min \mathcal{Y}) = \frac{\max \mathcal{Y} - f_j}{\max \mathcal{Y} - \min \mathcal{Y}},$$

$$p^*_{Y_i|h_j}(\max \mathcal{Y}) = 1 - p^*_{Y_i|h_j}(\min \mathcal{Y}),$$

$j \in \{0, 1\}$ and $r_{\text{II}}^* = \frac{f_0 - \min \mathcal{Y}}{\max \mathcal{Y} - \min \mathcal{Y}} \log \frac{f_0 - \min \mathcal{Y}}{f_1 - \min \mathcal{Y}} + \frac{\max \mathcal{Y} - f_0}{\max \mathcal{Y} - \min \mathcal{Y}} \log \frac{\max \mathcal{Y} - f_0}{\max \mathcal{Y} - f_1}$.

# Numerical Example

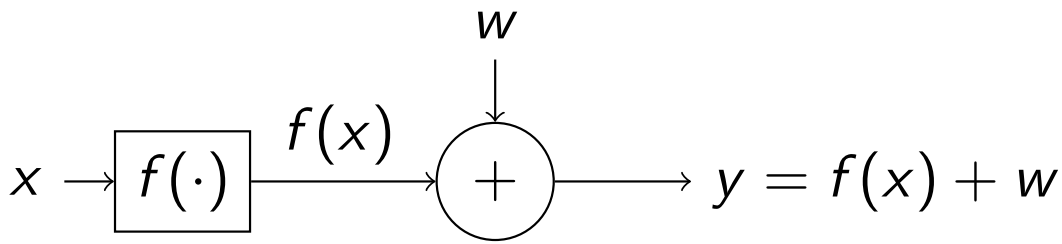
- $f_0, f_1 \in [4, 6]$.
- Case 1: $\min \mathcal{Y} = 1$, $\max \mathcal{Y} = 9$
- Case 2: $\min \mathcal{Y} = 3$, $\max \mathcal{Y} = 7$




Two ways to suppress the privacy risk:

- Increase the difference $\max \mathcal{Y} - \min \mathcal{Y}$.
- Decrease the difference $|f_0 - f_1|$.

# Adversarial State Estimation Approach




- Consumption sequence $x \in \mathcal{X} \subseteq \mathbb{R}^n$
- Continuously differentiable $f : \mathbb{R}^n \to \mathbb{R}^m$
- Additive noise $w \in \mathcal{W}(x) \subseteq \mathbb{R}^m$
  - Conditional probability density function $\gamma(w|x) \in \Gamma$
- Adversarial state estimation $\hat{x}(y)$

$$\gamma^* \in \arg\max_{\gamma \in \Gamma} \mathbb{E}\{\|x - \hat{x}(y)\|_2^2\}$$

Farokhi, Sandberg, "Fisher Information as a Measure of Privacy: Preserving Privacy of Households with Smart Meters Using Batteries," to be published in *IEEE Trans. on Smart Grid*. *Thanks for providing material.*

# Adversarial State Estimation Approach (cont.)

- Let $\mathcal{I}(x)$ denote the *Fisher Information*

## Cramér-Rao Bound

- $\mathbb{E}\{\hat{x}(y)\} = x \quad \Rightarrow \quad \mathbb{E}\{\|x - \hat{x}(y)\|_2^2\} \geq \text{trace}(\mathcal{I}^{-1}(x))$
- $\mathbb{E}\{\hat{x}(y)\} = g(x) \Rightarrow$
  $\mathbb{E}\{\|x - \hat{x}(y)\|_2^2\} \geq \text{trace}(G(x)^\top \mathcal{I}^{-1}(x) G(x)) + \|x - g(x)\|_2^2$

## Privacy-by-design problems:

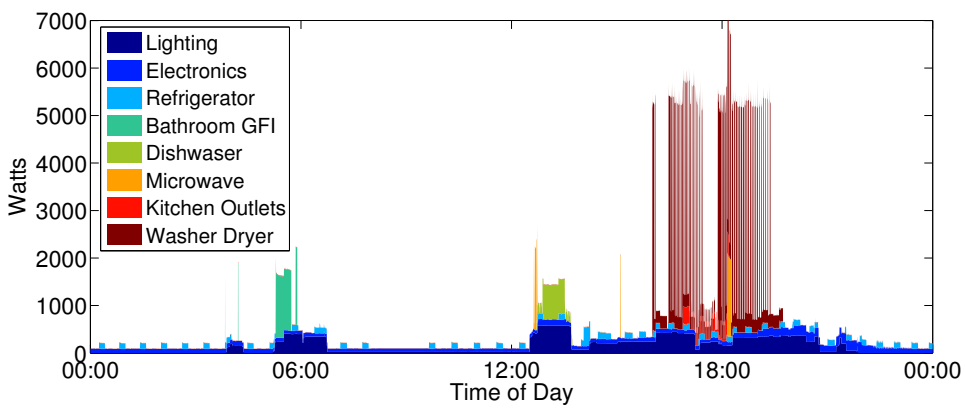
$$\gamma^* \in \arg\max_{\gamma \in \Gamma} \text{trace}(\mathcal{I}^{-1}(x)) \qquad \mathcal{I}^{-1}(x) \text{ not concave}$$

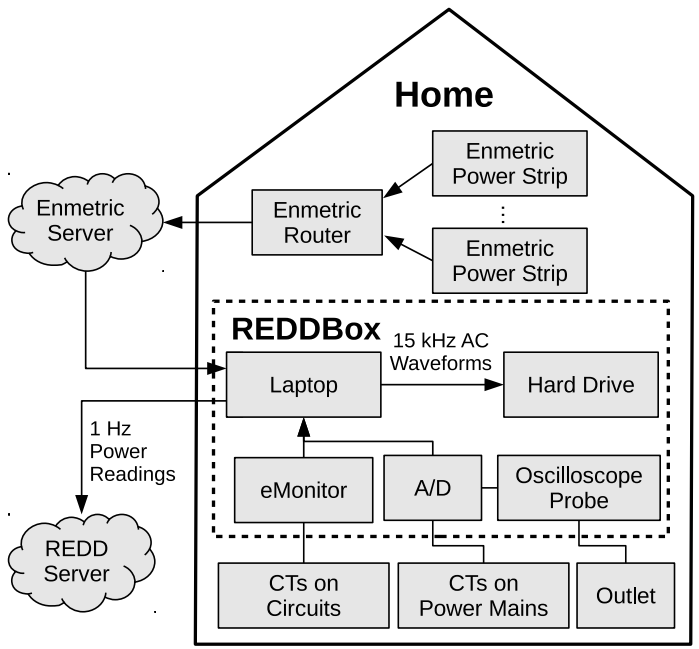
$$\gamma^* \in \arg\min_{\gamma \in \Gamma} \text{trace}(\mathcal{I}(x)) \qquad \text{relaxed problem}$$

- Solution of linear partial differential equation provides solution (noise distr.) to relaxed problem sometimes even explicitly.

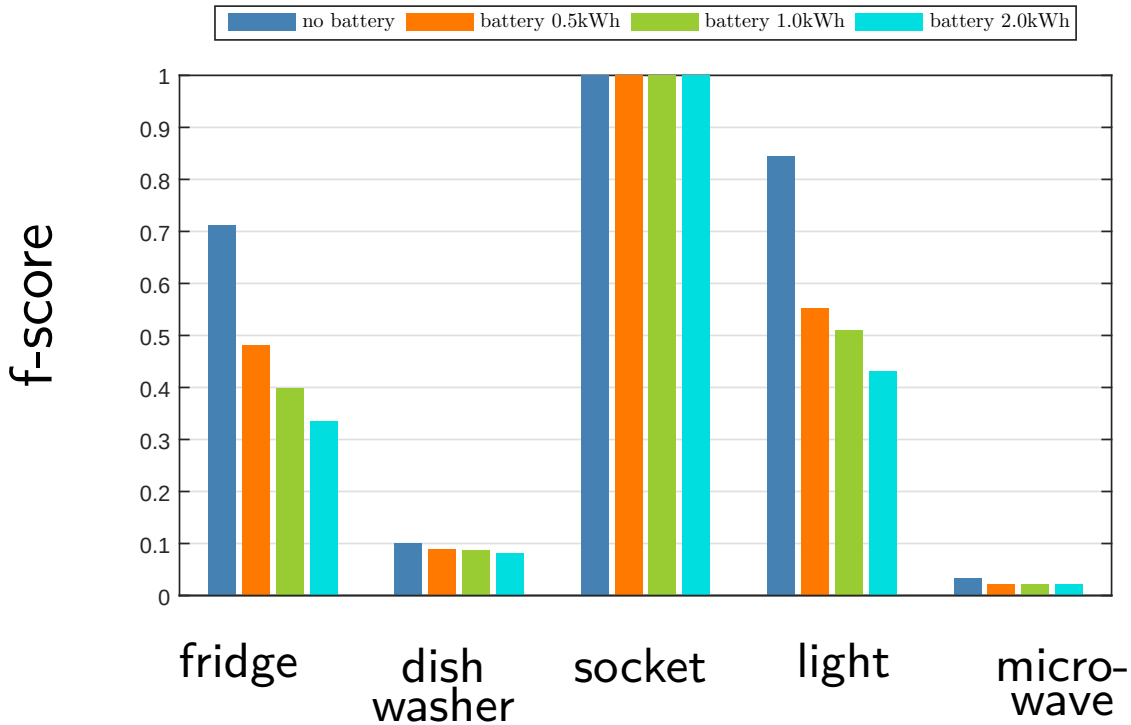
# Numerical Study Setup

- Real consumption data (April 23-May 21, 2011) from REDD database [Kolter & Johnson, 2011]
- State-of-the-art non-intrusive load monitoring algorithm in NILMTK toolbox [Kim, et al, 2011] [Barta, et al, 2014]
- Data over April 23-30 is used for learning and the rest is used for evaluation



# Numerical Study




- Resolution of the policy of the battery is an hour
- The appliance connected to the socket was always on during the experiment

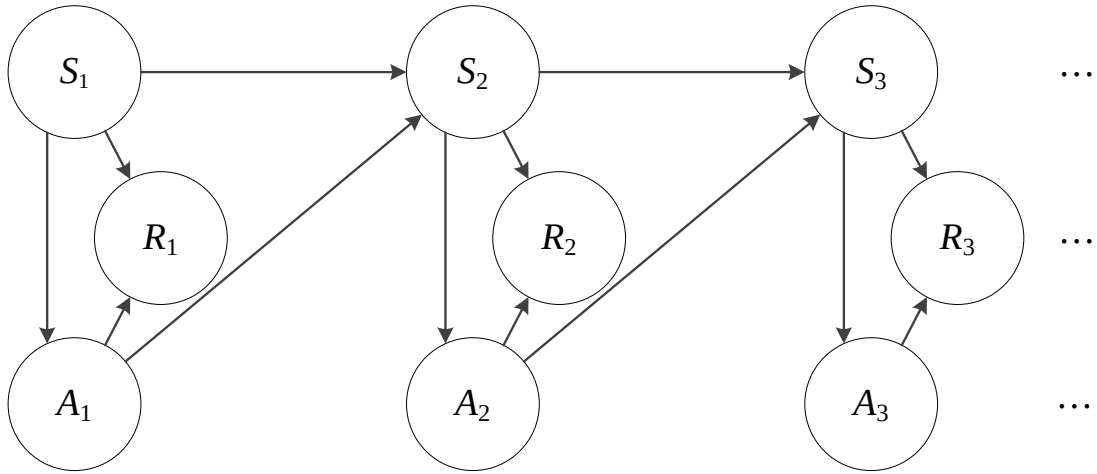
# Energy-flow Control Strategies Based on MDP Framework

- Concept of **Markov decision process (MDP)** provides a framework with well-developed tools for the design the optimal energy-flow control strategies
- MDP has been used with a *reward function* based on
  - information-theoretic motivated privacy measures
    - conditional entropy [Yao et al.2015]
    - mutual information [G. Giaconi et al., 2016], [S. Li et al, 2016]
  - statistical inference motivated privacy measures
    - Bayesian risk [Z. Li et al, 2017]
    - KL divergence [Y. Yang et al, 2018]

Yao, Venkit., "On the privacy-cost tradeoff of an in-home power storage mechanism," in *Allerton*, 2013.
Giaconi, Gündüz, "Smart Meter Privacy with Renewable Energy and a Finite Capacity Battery," in *SPAWC 2016.*
Li, Khisti, & M., "Privacy-optimal strategies for smart metering syst. w. a rechargeable battery," in *ACC*, 2016.
Li, Oechtering, Skoglund, "Privacy-preserving energy flow control in smart grids," in *Proc. IEEE ICASSP 2016*.
Yang, et al., "Optimal Privacy-enhancing and Cost-efficient Energy Management ...," in *Proc. IEEE SSP 2018*.

# Markov Decision Process (MDP)

- MDP is a process with Markov property



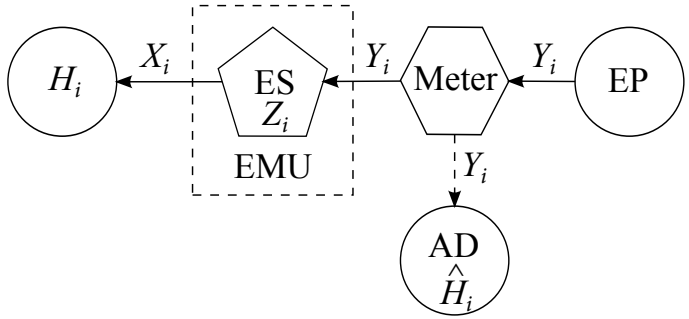

  - **Task:** Find optimal (decision) policies $\{\delta_i : \mathcal{S} \to \mathcal{A}\}_{i \in \mathbb{Z}_+}$ to optimize an objective in terms of rewards $\{R_i\}_{i \in \mathbb{Z}_+}$.
    - Decision on an action $A_i \in \mathcal{A}$ is based on the current state $S_i \in \mathcal{S}$ and influences the reward $R_i$ and next state $S_{i+1}$.
  - **Framework** with established computational methods exists
  - Suitable for modeling problems with Markov property setting

Krishnamurthy, "Partially Observed Markov Decision Processes: From Filtering to Controlled Sensing," 2016.

# Belief State Markov Decision Process

- Extension: **Belief state**
  - Posterior distributions of the state $S_i$ conditioned on different realizations of historical observations
  - *Belief state* formulation allows the partially observed MDP to be formulated as a standard (fully-observed) MDP
- **Action**
  - For energy management, action $a_i$ decides on the amount of energy supply based on the current state
  - **Deterministic action**
    - Certain energy supply at each state deterministically chosen.
  - **Random action**
    - Decide on *different* amounts of energy supply according to a certain distribution at each state.

# SM System with a Finite Capacity Storage




- Markov random hypothesis $H_i$ with *time-invariant* transition $p_{H_i|H_{i-1}}$
- Generation of $X_i$ follows *time-invariant* pmf $p_{X_i|H_i,X_{i-1}}$.
- Energy management policy $\gamma_i = p_{Y_i|X_i,Z_i}$ satisfies the constraint $z_i - z_{i+1} + y_i = x_i$, i.e.,
  (i) demand $x_i$ is always satisfied and (ii) no energy is wasted.
- Dependency setting:

$$P_{H_i,X_i,Z_i,Y_i|H^{i-1},X^{i-1},Z^{i-1},Y^{i-1}}$$
$$= p_{Y_i|X_i,Z_i} \cdot p_{X_i|H_i,X_{i-1}} \cdot p_{Z_i|X_{i-1},Z_{i-1}} \cdot p_{H_i|H_{i-1}}$$

Li, Oechtering, Skoglund, "Privacy-preserving energy flow control in smart grids," in *Proc. IEEE ICASSP 2016*.

# Belief State MDP Formulation

- *Belief State Markov Decision Process:*
  - Current "reward" $r_i$ depends on "action" $\gamma_i$ and "belief state" $p_{H_i,X_i,Z_i}$.
  - Next "belief state" $p_{H_{i+1},X_{i+1},Z_{i+1}}$ depends on current "action" $\gamma_i$ and "belief state" $p_{H_i,X_i,Z_i}$.

## Belief state MDP elements

- State: $s_i = (h_i, x_i, z_i)$
- Belief state: $b_i = p_{H_i,X_i,Z_i} \in \mathcal{B}$
- Action (energy management policy): $a_i = \gamma_i = p_{Y_i|X_i,Z_i} \in \mathcal{A}$
- Reward: $r_i(b_i, a_i)$
- Policy $\delta_i$: $\mathcal{B} \to \mathcal{A}$
- Belief state transition: $b_{i+1}(b_i, a_i)$

# Adversarial Bayesian Hypothesis Testing

- Informed adversary makes decision $\hat{H}_i$ based on $Y_i$.
- Instantaneous Bayesian risk of the adversary:

$$r_i = \sum_{y_i} \left\{ \min_{\hat{h}_i} \left\{ \sum_{h_i, x_i, z_i} c(\hat{h}_i, h_i) p_{Y_i|X_i,Z_i}(y_i|x_i, z_i) p_{H_i,X_i,Z_i}(h_i, x_i, z_i) \right\} \right\}$$

  - **Observations:** Depending on policy $\gamma_i$ and "belief" $p_{H_i,X_i,Z_i}$ instead of $(h_i, x_i, z_i)$

# Infinite Horizon Energy Management

Privacy leakage: **Accumulated discounted minimal Bayesian risk**

$$\text{Given initial "belief" } p_{H_1,X_1,Z_1}, \qquad J(p_{H_1,X_1,Z_1}) = \sum_{i=1}^{\infty} \beta^{i-1} r_i$$

where $0 < \beta < 1$ is a discount factor

- Applicable to the scenarios where privacy leakage risk decays with time, e.g., considering the time-increasing exposure probability of the adversary

## Privacy-enhancing energy management

$$J^*(p_{H_1,X_1,Z_1}) = \max_{\{\gamma_i\}} J(p_{H_1,X_1,Z_1})$$

Current energy management affects the future!

$$p_{H_{i+1},X_{i+1},Z_{i+1}|H_i,X_i,Z_i} = p_{Z_{i+1}|X_i,Z_i} \cdot p_{X_{i+1}|H_{i+1},X_i} \cdot p_{H_{i+1}|H_i}$$

# Optimal Policies

## Bellman equation

$$J^*(b_i) = \max_{a_i \in \mathcal{A}} r_i(b_i, a_i) + \beta \cdot J^*(b_{i+1}(b_i, a_i))$$

$$\delta_i^*(b_i) = \arg\max_{a_i \in \mathcal{A}} r_i(b_i, a_i) + \beta \cdot J^*(b_{i+1}(b_i, a_i))$$

- Optimal policy $\delta_i^*$ is time-invariant.
- Established algorithms, e.g., value iteration (on the next slide), policy iteration
- How an optimal energy management operates:
  At time slot 1, implement an instantaneous energy management policy $\gamma_1 = \delta_1^*(p_{H_1,X_1,Z_1})$; and update $p_{H_2,X_2,Z_2}$. Repeat the two steps at the remaining slots.

# Value Iteration

- Consider a finite discretized belief state alphabet $\mathcal{B} = \{b_{(1)}, \ldots, b_{(||\mathcal{B}||)}\}$.

---

1: input: a reward vector $[J^*(b_{(1)}), \ldots, J^*(b_{(||\mathcal{B}||)})]$

2: **while** the update of reward vector does not satisfy convergence criterion **do**

3: **for** $k \in \{1, \ldots, ||\mathcal{B}||\}$ **do**

4:

$$J(b_{(k)}) \leftarrow \max_{a_i \in \mathcal{A}} r_i(b_{(k)}, a_i) + \beta \cdot J^*(b_{i+1}(b_{(k)}, a_i))$$

$$\delta_i^*(b_{(k)}) \leftarrow \arg\max_{a_i \in \mathcal{A}} r_i(b_{(k)}, a_i) + \beta \cdot J^*(b_{i+1}(b_{(k)}, a_i))$$

$$J^*(b_{(k)}) \leftarrow J(b_{(k)})$$

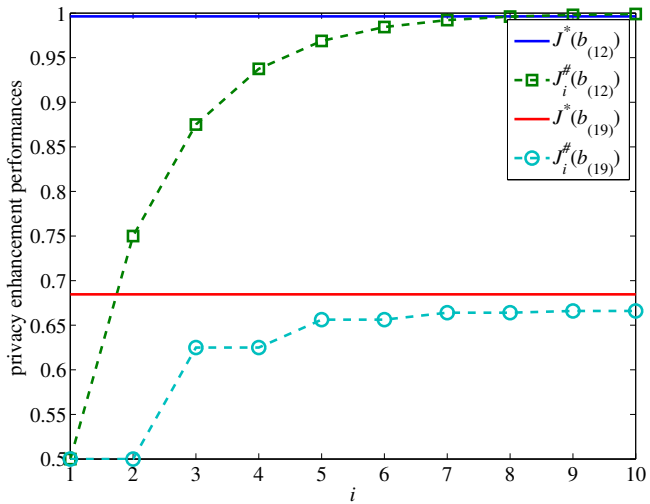
5: **end for**

6: **end while**

7: output: $[J^*(b_{(1)}), \ldots, J^*(b_{(||\mathcal{B}||)})]$ and $[\delta_i^*(b_{(1)}), \ldots, \delta_i^*(b_{(||\mathcal{B}||)})]$

---

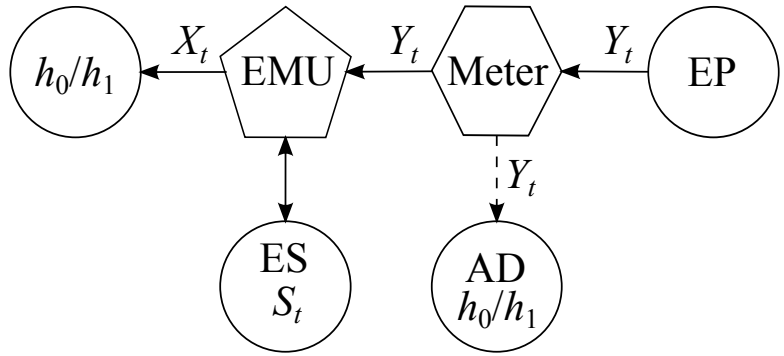
# Numerical Example




- Binary hypotheses $H_i$
- $x_i, z_i \in \{0, 1\}$, $y_i \in \{0, 1, 2\}$
- $\beta = 0.5$
- A finite number of belief states (an approx.)

- Instantaneous optimal energy management policy ($J^{\#}$), i.e., a policy always maximizes instantaneous reward *without considering impact on the future*
- Policy considering future impact $\Rightarrow$ Privacy-enhancing improvement

# Privacy-Cost Trade-off



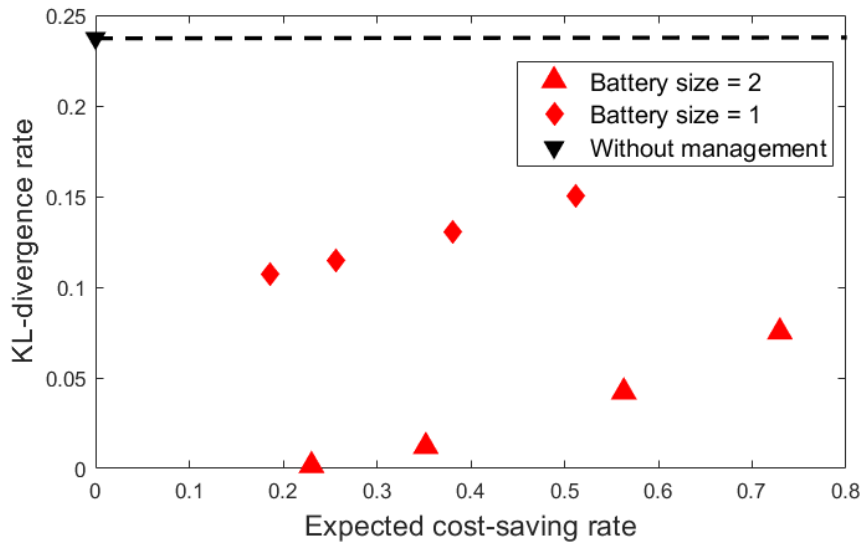

- Energy storage (ES) is also used for **energy cost savings**
  - What is the policy $f$ that achieves the optimal trade-off?
- Battery level evolves as $S_{t+1} = S_t + Y_t - X_t$, $0 \leq S_t \leq s_{\max}$
- **Privacy measure:** $L(f) = \frac{1}{T} D(P^f_{Y^T,P^T|h_0} \| P^f_{Y^T,P^T|h_1})$
- **Cost-saving rate** with dynamic pricing $P_t$: $V(f) = \frac{1}{T} \sum_{t=1}^{T} \{\mathbb{E}^f[(X_t - Y_t)P_t|h_0]P(h_0) + \mathbb{E}^f[(X_t - Y_t)P_t|h_1]P(h_1)\}$

Yang, Li, Oechtering, "Optimal Privacy-enhancing and Cost-efficient Energy Management Strategies for Smart Grid Consumers," in *Proc. IEEE SSP 2018*.

# Belief-state MDP Design Approach

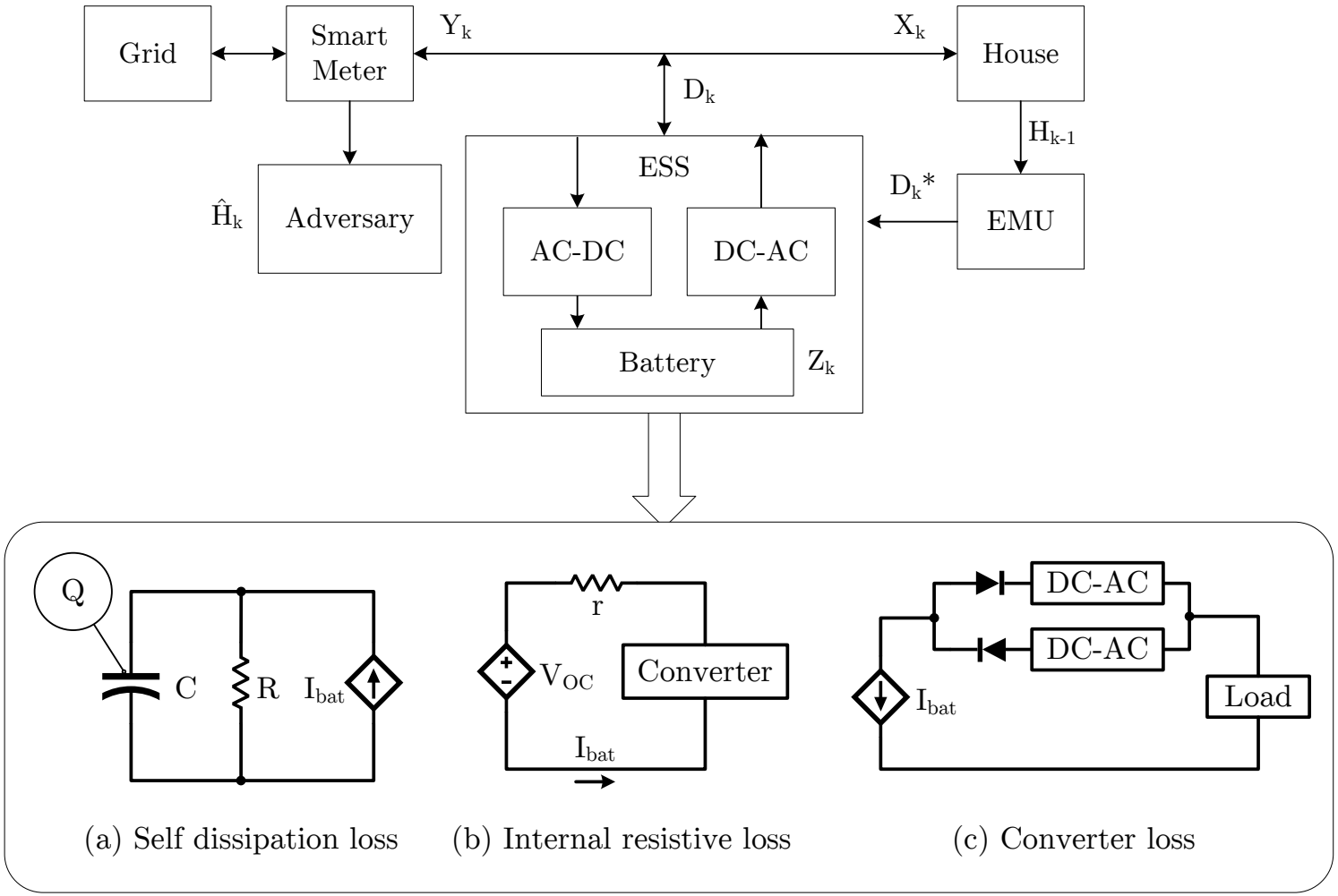
- Design objective: $\min_{f \in \mathcal{F}} C(f, \lambda) = \min_{f \in \mathcal{F}} \lambda L(f) - (1 - \lambda) V(f)$
- **Solution approach:** Belief-state MDP formulation & finite horizon backward dynamic programing

- Decomposition of $f_t$ in
  - policy $a_t = \pi_t(y^{t-1}, p^{t-1})$
  - actions $a_t \in \{P_{Y_t|X_t,S_t,P_t}\}$
- Belief state: $P_{X_t,S_t,P_t|Y_1^{t-1},P_1^{t-1},A_1^{t-1},h_i}$
- Per-step expected cost $C_t(\pi_t, \lambda, Y^{t-1}, A^{t-1}, P^{t-1})$




Binary power levels toy problem

# Energy Losses due to Privacy Control




Reddy, Oechtering, Månsson, "Optimal Privacy-preserving Control Strategies for Smart Meters Including Energy Storage Losses," IEEE PES Innovative Smart Grid Technologies Conference Europe (ISGT-Europe), 2018.

# Energy Loss Aware Bayesian Hypothesis Testing

- With energy loss accounted in battery state estimation[8]

$$Z_{t+\Delta t} = (1-\gamma)\cdot Z_t + \beta\left(\sqrt{V_{OC}^2 + 4r\cdot D_t\cdot\delta_t} - V_{OC}\right)$$

- Optimal control strategy:

$$\mu^* = \underset{\{\mu_1,\cdots,\mu_N\}}{\arg\max} \sum_{k=1}^{N} \mathcal{R}_k^*(b_{k-1}, z_{k-1}, \mu_k)$$

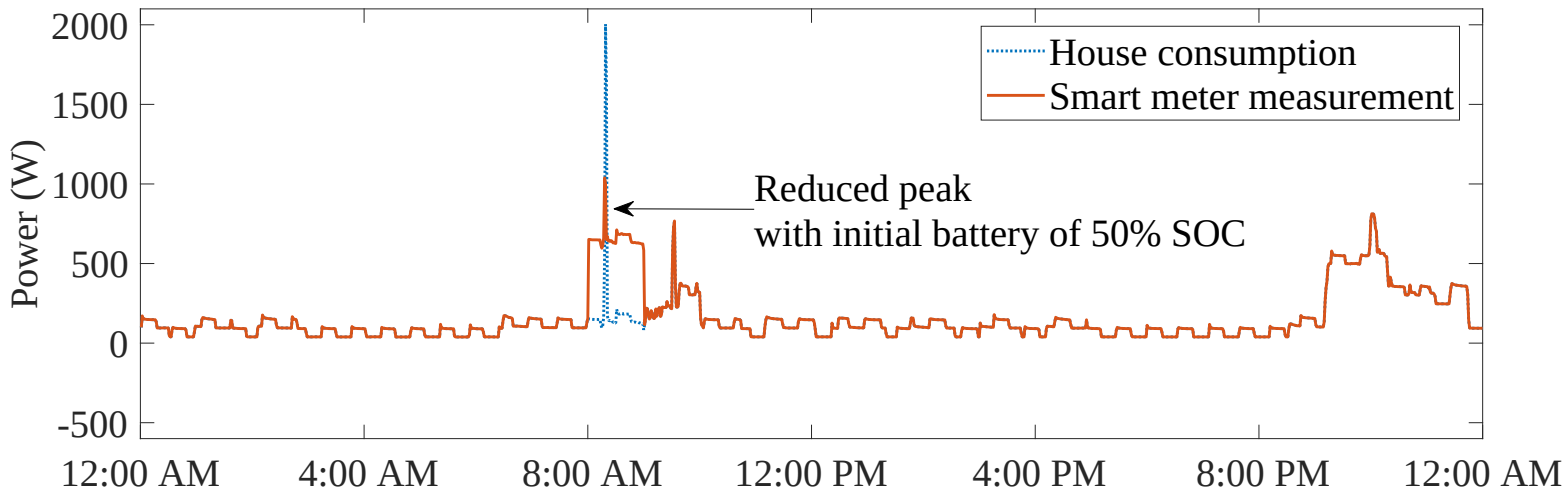
where the instantaneous minimum Bayesian risk is given as

$$\mathcal{R}_k^*(b_{k-1}, z_{k-1}, \mu_k) = \sum_{y\in\mathcal{Y}} \min_{\hat{h}\in\mathcal{H}} \Bigg\{ \sum_{g,h,x\in\mathcal{H}^2\times\mathcal{X}} C(\hat{h}, h)\cdot P_{Y_k|X_{k-1},Z_{k-1}}(y \mid x, z)\cdot P_{X_{k-1}|H_{k-1}}(x \mid g)\cdot P_{H_k|H_{k-1}}(h \mid g)\cdot P_{H_{k-1}}(g)\Bigg\}$$

[8] where $\gamma$, $r$, $\beta$, $V_{OC}$ are model parameters and $D_t\cdot\delta_t$ is control variable.

# Numerical Experiment

- The EMU when tasked to protect the events of a water kettle between 8 AM and 9 AM in Household 2 of ECO dataset using 12V 100Ah battery:




| Initial battery SOC (%) | Energy loss (Wh) | Accumulated minimum Bayesian risk (AMBR)[9] |
|---|---|---|
| Without battery | 0 | 0 |
| 0 | 40.421 | 152.57 |
| 50 | 36.230 | 153.51 |
| 100 | 9.779 | 148.89 |

[9] The higher the AMBR, the better is the privacy control

# Differentially Private Battery Recharging

- Modify household's consumption profile (first proposer of this approach) by adding noise using a rechargeable battery to achieve privacy in the sense of *differentially privacy*
  - Use battery as buffer to apply Laplacian noise to the consumption (either discharging or charging)
  - Taking battery capacity and throughput (energy charged/retrieved per time) into account **differential privacy in resource-bounded setting**
    - bounded mechanism (noise, can be high)
    - $(\epsilon, \delta)$-differential privacy guarantees with revised (increased) $\delta$ due to restrictions (without recharging, one step result)
  - Battery recharging mechanism, noise generation via cascading
    - Idea: Consider energy to be recharged as function that should be made differentially private
- Formally only one activation of one device is protected

---

M. Backes, S. Meiser, "Differentially Private Smart Metering with Battery Recharging," Proc. DPM 2013.

# Summary & Conclusion PET Approaches

- There exist several *Privay Enhancing Technology (PET)* design approaches based on
  - load signature manipulations
  - various privacy measures objectives
  - sources of distortion
  - control policy design approaches
- A few fundamental results
  - based on simplified settings
  - applicable to other applications
- A lot of opportunities for further research!

# In Summary

- Privacy is an important concern for smart meter roll-outs
- Privacy should be part of design, not something to be fixed retrospectively
- "Physical layer privacy" for energy networks
- Hard to quantify and guarantee privacy
- Fundamental privacy - utility trade-off
- Information theory and signal processing provide powerful tools to study this trade-off
- Based on known statistics: Provable guarantees vs. Data-dependent approaches

# What Next?

- Some fundamental principles and concepts have been developed, but for further developments of the technology readiness we need to study:
  - Technological implementation aspects, e.g., real energy storage aspects
  - Impact of privacy-enhancing methods on the power grid, e.g., energy management
  - Incentives for its integration, e.g., dual use of (car) batteries
- Mostly initial studies have been pursued, refinements and extensions are needed
- Comparison and assessment of different approaches should be done

# Closing remarks

- Epochal change where AI advancements create more and more information from data
  - Protection of sensitive information to make it sustainable
  - Legally enforced, e.g., European GDPR
- Privacy-by-design is an exciting research field
  - Smart-meter privacy is a prominent prototype problem
  - Concepts, methods, and approaches transfer to other privacy problems
- Many open research questions at the intersection of computer science, power systems, control theory, signal processing and information theory.

THANK YOU!

Deniz Gunduz
Imperial College London
d.gunduz@imperial.ac.uk

Tobias Oechtering
KTH Royal Institute of Technology
oech@kth.se

# References


M. Backes and S. Meiser,

"Differentially private smart metering with battery recharging"

in *Proc. Int. Workshop Data Privacy Management and Autonomous Spontaneous Security,* Egham, UK, Sep. 2013, pp. 194–212.

M. Barni and B. Tondi,

"The source identification game: An information-theoretic perspective,"

in *IEEE Trans. Inform. Forensics and Security,* no. 3, pp. 450-463, 2013.

M. Barni and B. Tondi,

"Source distinguishability under distortion-limited attack: An optimal transport perspective,"

in *IEEE Trans. Inform. Forensics and Security,* no. 10, pp. 2145-2159, 2016.

C. Beckel, W. Kleiminger, R. Cicchetti, T. Staake and S. Santini,

"The ECO Data Set and the Performance of Non-Intrusive Load Monitoring Algorithms,"

in *arXiv* vol. abs/1703.00785, 2017

preprint available online: https://arxiv.org/abs/1703.00785

# References


J.-M. Bohli, C. Sorge, and O. Ugus,

"A privacy model for smart metering,"

in *Proc. IEEE Int. Conf. on Commun.*, Cape Town, South Africa, May 2010.

J. X. Chin, G. Giaconi, T. T. De Rubira, D. Gunduz, and G. Hug,

"Considering time correlation in the estimation of privacy loss for consumers with smart meters,"

in *Proc. Power Systems Computation Conference,* Dublin, Ireland, Jun. 2018.

J. X. Chin, T. T. D. Rubira, and G. Hug,

"Privacy-protecting energy management unit through model-distribution predictive control,"

in *IEEE Trans. Smart Grid,* Nov 2017.

F. Farokhi and H. Sandberg,

"Fisher Information as a Measure of Privacy: Preserving Privacy of Households with Smart Meters Using Batteries,"

to be published in *IEEE Trans. on Smart Grid*.

# References


A. Faustine, N. H. Mvungi, S. Kaijage and K. Michael,

"A Survey on Non-Intrusive Load Monitoring Methodies and Techniques for Energy Disaggregation Problem,"

in *Proc. BuildSys 2014*, pp. 80-89.

G. Giaconi, D. Gunduz and H. V. Poor,

"Privacy-aware smart metering: Progress and challenges,"

to appear in *IEEE Signal Processing Magazine*.

G. Giaconi, D. Gunduz, and H. V. Poor,

"Smart meter privacy with renewable energy and an energy storage device,"

in *IEEE Trans. on Information Forensics & Security,* Jan. 2018.

G. Giaconi, D. Gunduz, and H. V. Poor,

"Optimal demand-side management for joint privacy-cost optimization with energy storage,"

in *IEEE Int'l Conf. on Smart Grid Comms.,* Dresden, Germany, Oct. 2017.

# References


G. Giaconi and D. Gündüz,

"Smart meter privacy with renewable energy and a finite capacity battery,"

in *Proc. IEEE SPAWC 2016*, pp. 1-5.

J. Gomez-Vilardebo and D. Gunduz,

"Smart meter privacy for multiple users in the presence of an alternative energy source,"

in *IEEE Trans. on Information Forensics & Security,* Jan. 2015.

H. Goncalves, A. Ocneanu, and M. Berges,

"Unsupervised disaggregation of appliances using aggregated consumption data,"

in *Proc. SustKDD*, 2011.

U. Greveler, P. Glosekotter, B. Justus, and D. Loehr,

"Multimedia content identification through smart meter power usage profiles,"

in *Proc. of Int'l Conf. on Information and Knowledge Eng. (IKE),* July 2012.

# References


G. W. Hart,

"Nonintrusive appliance load monitoring,"

in *Proc. IEEE*, 1992, vol. 80, no. 12, pp. 1870-1891.

D. Jurafsky and J. Martin,

"Speech and language processing,"

London:: Pearson, 2014.

G. Kalogridis, C. Efthymiou, S. Denic, T. Lewis, and R. Cepeda,

"Privacy for smart meters: Towards undetectable appliance load signatures,"

in *Proc. IEEE Int. Conf. on Smart Grid Commun.*, Gaithersburg, MD, Oct. 2010, pp. 232–237.

G. Kalogridis, Z. Fan, and S. Basutkar,

"Affordable privacy for home smart meters,"

in *Proc. IEEE Int. Symposium on Parallel and Distributed Process. with Applicat. Workshops,* Busan, Korea, May 2011, pp. 77–84.

# References


H. Kim, M. Marwah, M. Arlitt, G. Lyon and J. Han,

"Unsupervised disaggregation of low frequency power measurements,"

in *SIAM International Conference on Data Mining*, 2011, pp. 747-758.

C. Klemenjak1 and P. Goldsborough,

"Non-Intrusive Load Monitoring: A Review and Outlook,"

GI-Jahrestagung 2016.

J. Z. Kolter and T. Jaakkola,

"Approximate inference in additive factorial hmms with application to energy disaggregation,"

in *Artificial Intelligence and Statistics 2012*, pp. 1472-1482.

J. Z. Kolter and M. J. Johnson,

"REDD: A public data set for energy disaggregation research,"

in *Proc. Workshop on Data Mining Applications in Sustainability,* 2011.

V. Krishnamurthy,

"POMDP: From Filtering to Controlled Sensing,"

Cambridge University Press, 2016.

# References


S. Li, A. Khisti, and A. Mahajan,

"Information-Theoretic Privacy for Smart Metering Systems with a Rechargeable Battery,"

in *IEEE Trans. on Information Theory*, May 2018.

Z. Li,

"Privacy-by-Design for Cyber-Physical Systems,"

PhD dissertation, KTH Royal Institute of Technology, 2017.

Online: http://kth.diva-portal.org/smash/get/diva2:1131655/FULLTEXT01.pdf

Z. Li and T. J. Oechtering,

"Privacy on hypothesis testing in smart grids,"

in *Proc. IEEE ITW 2015 Fall*, pp. 337-341.

Z. Li, T. J. Oechtering, and M. Skoglund,

"Privacy-preserving energy flow control in smart grids,"

in *Proc. IEEE ICASSP 2016*, pp. 2194-2198.

# References


Z. Li, T. J. Oechtering, and D. Gündüz,
"Smart meter privacy based on adversarial hypothesis testing,"
in *Proc. IEEE ISIT 2017*, pp. 774-778.

Z. Li, T. J. Oechtering, and D. Gündüz,
"Privacy against a Hypothesis Testing Adversary,"
early access in *IEEE Trans. Inform. Forensic and Security*.

F. Li, B. Luo, and P. Liu,
"Secure and privacy-preserving information aggregation for smart grids,"
in *Int. Journal of Security and Networks*, Apr. 2011.

A. Marchiori, D. Hakkarinen, Q. Han and L. Earle,
"Circuit-Level Load Monitoring for Household Energy Management,"
in *IEEE Pervasive Computing*, 2011, vol. 10, no. 1, pp. 40-48.

# References


A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin,
"Private memoirs of a smart meter,"
in *ACM Work. Embedded Sensing Sys. for Energy-Eff. in Building*, Nov. 2010.

D. Rebollo-Monedero, J. Forne, J. Domingo-Ferrer,
"From t-Closeness-Like Privacy to Postrandomization via Information Theory,"
*IEEE Trans. Knowl., Data Eng.*, Nov. 2010.

R. Reddy Avula, T. J. Oechtering , D. Månnson,
"Privacy-Preserving Smart Meter Control Strategy Including Energy Storage Losses,"
in Proc. *IEEE PES Innovative Smart Grid Technologies Conf. Europe*, 2018.

L. Sankar, S. Rajagopalan, S. Mohajer, and H. V. Poor,
"Smart meter privacy: A theoretical framework,"
in *IEEE Trans. Smart Grid,* Jun. 2013.

K. Shaloudegi, A. György, C. Szepesvári, and W. Xu,
"SDP relaxation with radonmized rounding for energy diaggregation,"
in *NIPS* 2016.

# References


O. Tan, J. Gomez-Vilardebo, and D. Gunduz,

"Privacy-cost trade-offs in demand-side management with storage,"

in *IEEE Transactions on Information Forensics & Security*, Jun. 2017.

O. Tan, D. Gunduz and H. V. Poor,

"Increasing smart meter privacy through energy harvesting and storage devices,"

in *IEEE Journal on Selected Areas in Communications: Smart Grid Communications*, vJul. 2013.

D. Varodayan and A. Khisti,

"Smart meter privacy using a rechargeable battery: Minimizing the rate of information leakage,"

in *Proc. IEEE ICASSP 2011*, pp. 1932-1935.

M. Weiss, A. Helfenstein, F. Mattern and T. Staake,

"Leveraging smart meter data to recognize home appliances,"

in *IEEE PerCom*, 2012, pp. 190-197.

Y. Yang, Z. Li, and T.J. Oechtering,

"Optimal Privacy-enhancing and Cost-efficient Energy Management Strategies for Smart Grid Consumers,"

Proc. IEEE Statistical Signal Processing Workshop (SSP), June 2018

# References


J. Yao and P. Venkitasubramaniam,

"On the privacy-cost tradeoff of an in-home power storage mechanism,"

in *Allerton*, 2013, pp. 115-122.

T. Zia, D. Bruckner, and A. Zaidi,

"A hidden Markov model based procedure for identifying household electric loads,"

in *IEEE IECON*, 2011, pp. 3218-3223.

A. Zoha, A. Gluhak, M.A. Imran, and S. Rajasegarar,

"Non-intrusive load monitoring approaches for disaggregated energy sensing: A survey,"

in *Sensors*, 2012, pp. 16838-16866.

M. Zhong, N. Goddard, and C. Sutton

"Signal aggregate constraints in additive factorial HMMs with application to energy disaggregation,"

in *NIPS* 2014.