Privacy in Smart Metering Systems

Document Version
Other version

Link to publication record in Manchester Research Explorer

Citation for published version (APA):

Citing this paper
Please note that where the full-text provided on Manchester Research Explorer is the Author Accepted Manuscript or Proof version this may differ from the final Published version. If citing, it is advised that you check and use the publisher's definitive version.

General rights
Copyright and moral rights for the publications made accessible in the Research Explorer are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

Takedown policy
If you believe that this document breaches copyright please refer to the University of Manchester’s Takedown Procedures [http://man.ac.uk/04Y6Bo] or contact uml.scholarlycommunications@manchester.ac.uk providing relevant details, so we can investigate your claim.
Privacy in Smart Metering Systems

Deniz Gündüz¹  Georgios Kalogridis²  Mustafa A. Mustafa³

¹Imperial College London
²Toshiba Research Europe (Telecommunications Research Lab).
³KU Leuven

IEEE WIFS 2015
Rome, 16 Nov 2015
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
1. Introduction

2. Smart Metering Privacy Analytics
   - Privacy Metrics
   - Knowledge extraction

3. Privacy-Preserving Smart Metering Techniques
   - Data modification: protocols
   - Energy modification: Information-theoretic

4. Conclusions
Table of Contents

1. Introduction

2. Smart Metering Privacy Analytics
   - Privacy Metrics
   - Knowledge extraction

3. Privacy-Preserving Smart Metering Techniques
   - Data modification: protocols
   - Energy modification: Information-theoretic

4. Conclusions
Smart Grid

Smart grid refers to the future energy grid that exploits information 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 Grid Entities

- Bulk Generation
- Distribution Lines
- Transmission Substation
- Consumer
- Smart Meter
- Appliances
- Renewable Energy Source
- Electric Vehicle
- In-Home Display
- Smart Meter
- Appliances
- Consumer

**Electricity flow**

**Data flow**

Introduction
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 providers/ grid operator and to promote services that facilitate energy efficiency within the home\(^1\).
Benefits for the Consumer

▶ Ability to track their own 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 of the household and equipment through better power quality and breakdown management,
▶ Home appliances failure detection, detection of waste, detection of unexpected activity or inactivity,
▶ Increase competition among energy providers due to ease of switching for customers.
Benefits for the Energy Provider/ Grid Operator

- Reduced cost of meter readings and back office rebilling processes,
- Misuse and fraud detection,
- Accurate sensing and monitoring capabilities to distribution network operators (DNOs)
- Possibility to introduce demand response management in order to reduce peak loads,
- Renewable integration and microgeneration management.
Advanced Metering Infrastructure (AMI)

AMI uses two-way communication to both transmit usage information and perform observation and maintenance tasks.
AMI in Great Britain
Smart Metering Market

- Global smart meters market is estimated to grow from $11.1 billion in 2014 to $18.2 billion by 2019, at a compound annual growth rate (CAGR) of 10.2% from 2014 to 2019.

- By 2024, there will be nearly 1.1 billion smart residential meters worldwide, with 57% market penetration.


- In UK, installation of 53m smart meters in 30m households by 2020 is expected to cost £10.9bn. Government estimates roll-out of smart meters will deliver £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 smart meters if it gave utilities greater access to data about their personal energy use
Smart Meter Privacy: Technical Angle

- Non-intrusive load monitoring (NILM) techniques using high frequency SM data

- Reveals information on user’s energy consumption behaviour: can track appliance usage patterns, home occupancy, even the TV channel user is watching ...
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

## Potential Risks

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

"Potential Privacy Impacts that Arise from the Collection and Use of Smart Grid Data," NIST, vol. 2, pp. 30–32.
Smart Meter Security

- **Security ≠ 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). In many cases 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
Many papers have reported serious security risks in the AMI architecture.

More recently: flaws in authentication mechanism of Open Smart Grid Protocol


Security Measures against Attackers

- Authentication and authorisation
- Secure networks and communication links
- Secure data storage
- Secure multi-party computing
- Encrypted functions
- Trusted platform module
- Physically unclonable functions

Are these measures sufficient to protect privacy?
Confidentiality and Authorisation vs. Privacy

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

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

In smart meters, privacy is not only against third parties/attackers, but also against the legitimate/authorised receiver of data.
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.
- Measurement data collected and stored in database of the operator.
- Trust in grid operators: consumers are protected mainly by guidelines, audits, codes of behaviour.

To protect privacy we first need to measure it.
Table of Contents

1. Introduction

2. Smart Metering Privacy Analytics
   Privacy Metrics
   Knowledge extraction

3. Privacy-Preserving Smart Metering Techniques
   Data modification: protocols
   Energy modification: Information-theoretic

4. Conclusions
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
Privacy Measures for Smart Meters

- Privacy evaluation depends on the (data mining) task of extracting knowledge from the communicated smart metering data. We distinguish two main privacy approaches as such:
  - **Data privacy evaluation** – e.g. statistical analysis of aggregate data.
  - **Knowledge privacy evaluation** – e.g. analysis of inferred disaggregated data.
Privacy Metrics for Smart Meters

- **Relative entropy / Mutual information**: used for computing bounds on the achievable level of privacy, independent of technologic and computational capabilities of an attacker.

- **Cluster classification**: input data classified into clusters; known and hidden load cluster comparison may yield a possible privacy gain.

- **Regression analysis**: known and hidden loads are shifted until they align to their point of maximum cross-correlation.

- **Residual features**: features that appear both in the known and hidden profiles (i.e., an energy transition).

- **Exploratory Data Mining & Interestingness**: ensures that interesting data mining patterns (e.g., atypical TV or sleep patterns) remain hidden.

- **Differential privacy**: ensures that adding a single entry to a database (or deleting one from it) does not significantly change the answer given to some queries.
Privacy and Undetectability

Problem (Undetectability)

Suppose $G$ is an inference model that transforms a $p(t)$ smart metering trace into a hypothetical $e'(t)$ event trace. Suppose that we would like to protect a real event trace, $e(t)$. If $G$ offers (purposefully or not) $\alpha$ privacy protection, then how much is $\alpha$?

- Such a problem may be solved by means of evaluating the performance of the inference model. E.g. we may calculate the likelihood an event was occurred given a recorded load signature.

- A different approach concerns the use of similarity metrics to simply compare $e(t)$ with $e'(t)$.

- In the case of data perturbation, $e(t)$ would be the $p(t)$, and $e'(t)$ would be the perturbed metering data $p'(t)$.

- An event may be defined as a power edge:
  
  $$e'(t) = dp(t) = p(t) - p(t - 1)$$
  
  We also denote $dp_A(t)$ to be the original (real) trace of power edges $dp(t)$.
The relative entropy or Kullback Leibler distance is a well known information theoretic quantity which can be used to compare two sources of information:

\[ D(P \| Q) = \int_{x_{\text{min}}}^{x_{\text{max}}} f_P(x) \log \frac{f_P(x)}{f_Q(x)} \, dx. \]

▶ The bigger the \( D(P \| Q) \) the better the privacy protection.

Similarity metric 2: Cluster similarity

We consider a simple method of trace analysis to compute how close $dp_A(t)$ is to $dp(t)$.

1. Find the *silhouette optimal* $n$ for $dp_A(t)$.
2. Classify $dp_A(t)$ into set of clusters $\mathcal{A} = \{a_1, \ldots, a_n\}$.
3. Classify $dp(t)$ into set of clusters $\mathcal{B} = \{b_1, \ldots, b_n\}$.
4. Ignore cluster values corresponding to insignificant power changes.
5. Compute the ratio of ‘correct’ classifications in $\mathcal{B}$.
6. The smaller the cluster similarity the better the privacy protection.

Clustering-based graphical model similarity

An extension of clustering is to build a graphical model. The original and inferred graphical models may then be compared to evaluate privacy.
Similarity metric 3: Regression analysis

We may analyse the degree to which $dp(t)$ ‘predicts’ $dp_A(t)$ by *fitting* the traces and measuring their ‘distance’ in the time domain.

1. Estimate the error sum of squares $SS_E = \sum_t (dp(t) - \hat{dp}(t))^2$ and the regression sum of squares $SS_R = \sum_t (\hat{dp}(t) - \bar{dp})$.

2. Compute the *coefficient of determination*:
$$R^2 = 1 - \frac{SS_E}{SS_R + SS_E}, \quad 0 \leq R^2 \leq 1.$$

- $R^2 = 1 \Rightarrow$ predictions are fully explained by the model
- $R^2 \rightarrow 0 \Rightarrow$ (higher privacy protection) when
  - $SS_E \gg SS_R$ (the noise increases), or
  - or when $SS_R \rightarrow 0$ ($dp(t)$ is similar to $\bar{dp}$).

Purpose: Extract knowledge from or give insights about the data without answering specific questions.

Pattern type: Groups of features (time) that exhibit a common power consumption profile.

For example, such an exploration may follow the detection of consumption profiles (e.g. via clustering).

This corresponds to finding cliques in a graph.
Learning consumption profiles and features

Density based clustering and dynamic optimisation can help extract consumption profiles and their features.

1-2-3-stage clustering: 74-52-12 clusters.
Pattern type: Windows of time with a common power consumption profile.

This may be done with bi-clique mining algorithms.

This may provide insights to hidden or interesting patterns.

But how can this be interesting from a privacy point of view?
Mining more complex (interesting) patterns

- Washier
- TV
- Boiler
- Cooker
- Kettle
- Swimming pool

Day 1
Day 7
...
Week 1
Week 52
...
5-10m
>2hrs
...
1-5m

Metrics 34/100
Pattern type: Consumption profiles that appear in the same windows of time at the same days of the week, for the same length of time.

Pattern syntax: find Maximal Complete Connected Subsets of patterns (MCCS).

Simple pattern mining: divide and conquer depth 1st search.
Interestingness

- Interestingness of a pattern may be assessed as a trade-off between the self-information and the description length.
- Self information: this may be calculated by calculating the entropy of mutually exclusive subsets of the pattern.
- Description length: this measures how conceisely the pattern conveys this information.

\[
\text{Interestingness}(\gamma) = \frac{\text{Self Information}(\gamma)}{\text{Description Length}(\gamma)}
\]

Ranking patterns based on interestingness:

\{TV\} ↔ \{Kettle\} ↔ \{02-04h\} ↔ \{Sat.\} ↔ \{30–60m\} ↔ \{Swimming Pool\} ↔ \{1–2h\}
Data mining for privacy

- A variety of models may be used to infer information from the data.
- A variety of metrics to evaluate privacy . . .
- A data mining / anomaly detection inspired method:
  - Analyse the variability of activity occurrence probability distributions with different time features.
  - Focus on significant variability as an indication of anomaly and privacy alert.

![Exploratory Data Mining Diagram]

- Clustering
- Frequent pattern mining
- HMM based pattern recognition
- Information Visualisation
Subset data mining

Example:

- Detected appliance profiles: TV, Microwave, Cooker
- Event space: all possible subsets of \{TV, Microwave, Cooker, Zero/Other\}
- \(2^N - 1\) subsets (excluding the empty set).
- Data mining: sequential batch window.
- Types of behaviour: 1) duration of appliance usage, and 2) frequency of switch-ON appliance event.
We characterise a behaviour profile with an empirical probability distribution (EPD) of sets of concurrent events: there are $2^M$ possible events.

An interval EPD, $P_p$, and an expected EPD, $Q_p$, may be obtained by counting across a constraint or a sufficiently large number of sample paths.

**Atypicality**: $\text{Kdiv}(P_p \| Q_p) := \sum_b P_p(b) \log \frac{2P_p(b)}{P_p(b) + Q_p(b)}$.

The probability of any given sequence of $p$ is given by

$$Q^n_p(p) = |X|^{-n(H(P_p) + D(P_p \| Q_p))},$$

where $X$ is the set of all possible events, $D(P_p \| Q_p)$ signifies relative entropy, and $H(P_p)$ is the Shannon’s entropy.

Kdiv-inspired privacy metric

- Is privacy protected when the atypicality is large?
- Is privacy protected when atypicality is small?

- Simple privacy alarms:

  \[
  \text{Crest factor(Kdiv)} > th1 \quad \text{Max(Kdiv)} > th2
  \]

<table>
<thead>
<tr>
<th></th>
<th>Y</th>
<th>N</th>
</tr>
</thead>
<tbody>
<tr>
<td>Anomaly detection</td>
<td>Y</td>
<td>N</td>
</tr>
<tr>
<td>Incongruence</td>
<td>N</td>
<td>Y</td>
</tr>
<tr>
<td>Data perturbation</td>
<td>Y</td>
<td>Y</td>
</tr>
</tbody>
</table>

Subset atypicalities

Atypicality of all distinct bags of duration of operation (On-On) appliance events:

- Explore the variability of atypicality in all possible event spaces.
- Particular subsets produce higher atypicalities (darker color).
- Continuous high atypicality: incongruent data → non-behavioural problem (false alarm).
- Exclusion of the zero event intensifies atypicality.
Example of an alarm

- Suppose an alarm is triggered when atypicality exceeds a threshold value (e.g. set to 0.5).
- Privacy alarms of different bags of events for both the appliance duration and switch-on events.
- More frequent privacy alarms when the TV or microwave, and no other appliance is considered.

<table>
<thead>
<tr>
<th>House No.</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
<th>7</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cook</td>
<td>0 &amp; 0</td>
<td>3 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
</tr>
<tr>
<td>Micro</td>
<td>0 &amp; 0</td>
<td>3 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
</tr>
<tr>
<td>TV</td>
<td>0 &amp; 0</td>
<td>3 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
</tr>
<tr>
<td>Zero</td>
<td>8 &amp; 0</td>
<td>15 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
</tr>
<tr>
<td>TV,Zero</td>
<td>9 &amp; 25</td>
<td>0 &amp; 1</td>
<td>8 &amp; 18</td>
<td>68 &amp; 27</td>
<td>0 &amp; 0</td>
<td>4 &amp; 29</td>
<td>10 &amp; 7</td>
<td>50 &amp; 76</td>
</tr>
<tr>
<td>Micro,Zero</td>
<td>0 &amp; 25</td>
<td>15 &amp; 15</td>
<td>0 &amp; 0</td>
<td>27 &amp; 27</td>
<td>0 &amp; 0</td>
<td>11 &amp; 22</td>
<td>15 &amp; 15</td>
<td>125 &amp; 24</td>
</tr>
<tr>
<td>Micro,TV</td>
<td>4 &amp; 0</td>
<td>0 &amp; 0</td>
<td>33 &amp; 33</td>
<td>54 &amp; 14</td>
<td>0 &amp; 0</td>
<td>4 &amp; 28</td>
<td>8 &amp; 0</td>
<td>20 &amp; 105</td>
</tr>
<tr>
<td>Cook,Zero</td>
<td>4 &amp; 0</td>
<td>14 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
</tr>
<tr>
<td>Cook,TV</td>
<td>9 &amp; 0</td>
<td>0 &amp; 8</td>
<td>18 &amp; 19</td>
<td>41 &amp; 41</td>
<td>0 &amp; 0</td>
<td>4 &amp; 13</td>
<td>10 &amp; 13</td>
<td>46 &amp; 31</td>
</tr>
<tr>
<td>Cook,Micro</td>
<td>7 &amp; 0</td>
<td>11 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
</tr>
<tr>
<td>Cook,Micro,Tv</td>
<td>0 &amp; 0</td>
<td>3 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
</tr>
<tr>
<td>Cook,Micro,Zero</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
</tr>
<tr>
<td>Cook,TV,Zero</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
</tr>
<tr>
<td>Micro,TV,Zero</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>42 &amp; 42</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
</tr>
<tr>
<td>Cook,Micro,TV,Zero</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
<td>0 &amp; 0</td>
</tr>
</tbody>
</table>

Metrics

42/100
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 $T$ provides $\epsilon$-differential privacy if

$$\Pr(F(D) \in S) \leq e^\epsilon \cdot \Pr(F(D') \in S)$$

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

Approximate Differential Privacy

Definition

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

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

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

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

The fundamental privacy metrics may also apply after smart metering data is processed to extract knowledge.

For example, knowledge may simply be represented as a categorical table with multiple dimensions (columns).

A particularly important knowledge, from a privacy perspective, concerns metering data at an appliance level.

This leads us to the problem of appliance disaggregation, the *alter ego* of privacy protection.

This is also known as Non-intrusive Appliance Load Monitoring (NIALM) and may be further distinguished into low frequency NIALM and high frequency NIALM.
High frequency signatures

- Original idea based on a clustering of active & reactive power edges.
- Recent techniques based on Harmonics pattern recognition (~90% accuracy).
- High frequency NIALM assumes specialised metering device.
Low frequency (smart metering) NIALM

- Machine Learning models; Input: 1”–15’ power readings.
- Open source NIALM: https://github.com/nilmtk/nilmtk
- Typically runs in the backend (Energy provider).
NIALM ML performance

- Depends on how performance is assessed.
- A typical FHMM model may achieve 70-80% accuracy of the task of appliance ON-OFF detection, assuming an average household energy usage profile.
- An active area of research; almost exponential increase of research publication is in recent years.
Poor-man’s real-time & low-cost NIALM

Application of the knapsack algorithm (as opposed to expensive HMM training):

- maximise $W(t) = \sum_{i=1}^{N} \sum_{j=1}^{s} w_{i,j}(t)z_{i,j}$, subject to $\Delta Q_t - Q_n \leq W(t) \leq \Delta Q_t + Q_n$, where $\Delta Q_t$ is the observed smart meter power reading, $N$ is the number of appliances, $s = 2$ the number of appliance states, $Q_n$ is a tolerance value, and $w_{i,j}(t)$ takes values from $\{0, 1\}$ with the constrain that $\sum_{i=1}^{s} w_{i,j}(t) = 1$, for all $j$, at any time $t$.

- We set $Q_n = x - L$, where $L$ is a detected minimum power (vampire power), and $0 \leq x \leq x_{\text{max}}$.

For real-time (fast) detection, we construct a lookup table by sorting the solutions that correspond to a choice of $w_{i,j}(t)$ and the associated $W(t)$.
NIALM and knowledge / privacy ramifications

- Appliance disaggregation may be used to infer Activities of Daily Living (ADLs).
- ADLs may furnish more sensitive personal data such as healthcare.
Table of Contents

1. Introduction

2. Smart Metering Privacy Analytics
   - Privacy Metrics
   - Knowledge extraction

3. Privacy-Preserving Smart Metering Techniques
   - Data modification: protocols
   - Energy modification: Information-theoretic

4. Conclusions
Main Approaches

1. Real energy consumption is not modified, **meter data is modified** before being reported to EP.
   
   ▶ Anonymization with/ without TTP, i.e., using pseudonyms instead of real identities.
   
   ▶ Aggregation with/ without trusted third party (TTP), i.e. summing measurements over a group of users,
   
   ▶ Obfuscation, i.e., adding noise to data,

2. **Energy consumption is modified**:

   ▶ Through storage devices, i.e., filtering energy consumption,
   
   ▶ Through alternative energy sources (renewables, uninterrupted power supplies),
   
   ▶ Sampling approach, i.e., reducing sampling rate of measurements.
Anonymization with Trusted Third Party (TTP)

- SM readings sent to a TTP over secure links.
- TTP removes the identities of users from the tuples received and sends only the SM readings to EP.
- EP learns the SM readings, but not their origin.
- However, TTP learns the SM readings too.

Anonymization with STTP

- SM readings are encrypted with the public key of EP.
- Instead of real identities, users use pseudonyms.
- STTP sends only the encrypted SM readings to EP.
- EP decrypts and learns the SM readings, but not their origin.
- STTP does not learn the SM readings nor the real identities of users.

Anonymisation: Customer Data vs. Technical data

▶ EU SM standards recommendation to define two types of data for smart metering:

▶ **Customer data**: Attributable data, e.g. for billing and account management purposes → Low-frequency data, e.g. every few days/weeks.

▶ **Technical data**: “Anonymous” data, e.g. for power network management and demand response → High-frequency data, e.g. every few minutes.

▶ There is no real reason why the high-frequency data can’t be anonymous and still serve the purposes of the utility and the power distribution network.

▶ Smart meter uses both eponymous and anonymous IDs (and related crypto keys) for customer and technical data, respectively.

▶ The utility knows that the anonymous ID is located within a certain area, but not which specific house.
Anonymisation evaluation

- Anonymity level achieved depends on the size of the “anonymity set”, i.e. how hard it is to associate a given anonymous (ADP) with an eponymous customer (CDP) profile / security key.

- The use of random time intervals in the ADP setup protocols is crucial.

Anonymization with off-line TTP

- Each SM has two IDs, one for sending low frequency readings, LFID, and one for sending high frequency readings, HFID.
- Only TTP is aware of the connection between a valid HFID/LFID pair.
- TTP is involved only in the SM registration (setup) stage.
- EP knows only the connection between a valid LFID/real user ID pair, but not the connection between HFID/LFID.

Anonymization & Data Splitting

- Each SM splits its data into shares and sends each share to a different concentrator.
- Each concentrator replaces the real ID of the user with a pseudonym and forwards the data to EP.
- EP sums all the shares attached with the same pseudonym.
- EP knows the SM readings, but not their origin.

Aggregation with Trusted Third Party (TTP)

- SM readings sent to a TTP over secure links.
- TTP reports to EP:
  - sum consumption for a group of SMs (e.g., neighbourhood),
  - 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.

Each SM splits its data into $w$ shares using $(w, t)$ secret sharing scheme; sends each share to a different concentrator.

Each concentrator sums the received shares and sends the aggregated shares to EP.

EP sums at least $t$ of the received aggregated shares to obtain the aggregated data of all SMs.

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 with Aggregation done by Collector

- Each SM encrypts its data with the homomorphic public key of EP and sends the ciphertext to the collector.
- The collector aggregates the received ciphertexts and sends the aggregated ciphertext to EP.
- The EP decrypts the aggregated ciphertext to obtain the aggregated data of all SMs.

Homomorphic Encryption with Aggregation done by EP

- Each SM chooses random key $k$ of bihomomorphic encryption scheme.
- Keys are aggregated within SM group by electing random SM as key aggregator (KA) through a secure channel that provides anonymity for every SM.
- KA computes aggregated key $K$ and sends it to EP.
- Every SM sends its data, encrypted with its key to EP via a secure channel.
- EP aggregates all received encrypted values, then obtains the aggregated energy consumption by decrypting the aggregated encrypted value using $K$.
- SMs updates their keys at every data reporting round such that $K$ remains the same.

Homomorphic Encryption & Data Splitting

- Neighbourhood 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 EP (except own share).
- The EP, 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 EP unencrypted.
- EP sums all the received results.

SM data encrypted with DNO’s homomorphic public key.

At collectors ciphertexts are aggregated based on EP.

At DCC ciphertexts are aggregated based on DNO and EP.

DNO recovers the data and random number from ciphertexts, sends both items to EP, sums all data and sends to TSO.

EP performs ciphertext-based verification of the data.

 Computations executed by the customer without disclosing raw meter readings.

 Correctness can be guaranteed.

 If the raw data is needed, secure aggregation can be used.

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 uses aggregated together: 99.9% confidence requires aggregating 3.8 million users.)
► Meters should be tamper-proof.

Main Approaches

1. Real energy consumption is not modified, meter data is modified before being reported to EP.
   - Anonymization with/without TTP, i.e., using pseudonyms instead of real identities.
   - Aggregation with/without trusted third party (TTP), i.e., summing measurements over a group of users,
   - Obfuscation, i.e., adding noise to data,

2. Energy consumption is modified:
   - Through storage devices, i.e., filtering energy consumption,
   - Through alternative energy sources (renewables, uninterrupted power supplies),
   - Sampling approach, i.e., reducing sampling rate of measurements.
Privacy - Utility Trade-off

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

Grid management problem
Energy provide 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.
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 $Y^n$:

$$
\frac{1}{n} I(X^n; Y^n) = \frac{1}{n} [H(X^n) - H(X^n|Y^n)]
$$

$$
= \frac{1}{n} \sum_{(x^n, y^n) \in X^n \times Y^n} p(x^n, y^n) \log \frac{p(x^n, y^n)}{p(x^n)p(y^n)}
$$
Reporting Quantized Energy Consumption

- SM maps $X^n$ to a predefined set of meter readings:
  \[ \text{Encoder} : X^n \rightarrow \text{SMR} = \{ SMR_1, \ldots, SMR_M \} \]

- No matter what real consumption is, EP will receive $Y^n \in \text{SMR}$, 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

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).
Privacy Through Energy Consumption Manipulation

- *Physical* approach to privacy, rather than *cyber*.
- Previous techniques assume grid operator depends solely on SM readings for load monitoring.
- However, grid operator owns the grid, and has many other sensors, measurement mechanisms that can provide some level of information.
- Moreover, obfuscation, data aggregation, etc. limit operators' capabilities to monitor grid for failures, energy quality changes, renewable integration, etc.
- Alternative solution: Consumers manipulate their energy consumption over time by exploiting storage devices or alternative energy sources (renewable sources, uninterruptible power supply, etc.).
Alternative Energy Source

Discrete time model:
- Energy demand (input load): $X_t$
- Energy from grid (output load): $Y_t$
- Remainder from alternative energy source (AES): $X_t - Y_t$

SM reads and reports $Y_t$


Simple alternative energy-based system

Naive (best-effort) privacy algorithm: Perturbs electrical events while improving energy efficiency.

<table>
<thead>
<tr>
<th>Privacy Detection &amp; Protection</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Smart Grid Optimisation</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Original: ( p_A(t) )</th>
<th>Modified: ( p(t) )</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kettle detected</td>
<td>Kettle hidden</td>
</tr>
<tr>
<td>Peaks &amp; variability</td>
<td>Peaks and variability mitigated</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Battery</th>
<th>0 kWh</th>
<th>4 kWh</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protection level</td>
<td>0%</td>
<td>99%</td>
</tr>
<tr>
<td>PAPR</td>
<td>8</td>
<td>6</td>
</tr>
</tbody>
</table>

Privacy Protection System

Event detection → Privacy algorithm → Energy control

\[
p_A(t) \rightarrow p(t) = p_A(t) - p_U(t) - p_B(t)
\]

Smart Meter

Utility

\( p(t) \)

\( p_A(t) \)

(Smart) Appliances

Micro-generation

Rechargeable Batteries

\( p_B(t) > 0 \)

(discharging)

\( p_B(t) < 0 \)

(charging)
Battery friendly privacy algorithm

Algo 1 (selective use of battery):
- If a rare event occurs (e.g. kettle at 1am): discharge battery to hide it.
- If an expected event does not occur (e.g. lights at 9pm): recharge battery to simulate it.

Algo 2 (selective allocation per appliance):
- Allocate battery energy quotas to different appliances (e.g. protect privacy of TV, but not Kettle).
- Detect appliance (e.g. NIALM algorithm)
- Apply best-effort (water filling) algorithm for each appliance and its allocated sub-battery resources.

Utility friendly privacy algorithm

Energy Capping algo:

- Objective: consume a certain amount of energy (CAP) every $T = 30$ minutes.
- If prediction $> \text{CAP}$, then battery power is used (best effort).
- If prediction $< \text{CAP}$, then the battery is charged.
- Benefits
  - (Grid-scale effect) mitigate peaks & rebound peaks
  - (Uncertainty) reduce demand uncertainty,
  - complementary to demand response signal.

G. Kalogridis and S. Dave, “PeHEMS: Privacy enabled HEMS and load balancing prototype”, IEEE SmartGridComm12
Energy Management Policy

- **Energy management policy:** $f_t : \mathcal{X}^t \times \mathcal{Y}^{t-1} \rightarrow \mathcal{Y}$, 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 AES:**
  $$P_n = \mathbb{E} \left[ \frac{1}{n} \sum_{t=1}^{n} (X_t - Y_t) \right]$$
Energy Management Policy

- Energy management policy: \( f_t : \mathcal{X}^t \times \mathcal{Y}^{t-1} \rightarrow \mathcal{Y} \), 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 AES:
  \[
  P_n = \mathbb{E}\left[\frac{1}{n} \sum_{t=1}^{n} (X_t - Y_t)\right]
  \]

- For given \( \bar{P} \), pair \((I, \hat{P})\) is achievable if there exist energy management policies with \( \lim_{n \rightarrow \infty} I_n \leq I \) and \( \lim_{n \rightarrow \infty} P_n \leq \hat{P} \).

- Privacy-power function, \( \mathcal{I}(\bar{P}, \hat{P}) \), is the minimum achievable information leakage rate for given peak power \( \bar{P} \), and average power \( \hat{P} \).
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

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

Lemma

Privacy - power function is a non-increasing convex function of $P$.

- 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:

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

- 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
Numerical Analysis

- Continuous output alphabet: Infinitely many variables

**Theorem**

*Without loss of optimality output load alphabet \( \mathcal{Y} \) can be constrained to input alphabet, i.e., \( \mathcal{Y} = \mathcal{X} \).*

- Discrete input/output alphabets: Convex optimization problem
- Blahut-Arimoto algorithm
Uniform Input Load

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

PP Techniques 83/100
Continuous Input Loads

- Continuous input and output alphabets
- No efficient numerical computation method (infinite dimensional optimization problem)
- Shannon Lower Bound (SLB):
  \[ I(P) \geq (h(X) - \ln(P))^+ \text{ nats} \]

- Not tight in general
- Exponential input load, \( X \sim \exp(\lambda) \): SLB is tight
  \[ I(P) = \left( \ln \left( \frac{\lambda}{P} \right) \right)^+ \text{ nats.} \]

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 encryption tools (zero-knowledge proof, anonymous payment) added cost can be reimbursed to customer
- Negative noise can be possible by introducing deposit payment in advance

Group SMs into clusters.

$X^i_t$ : Consumption of user $i$ at time slot $t$

Energy provider (EP) interested only in sum consumption of a cluster within a time slot: $\sum_{i=1}^{N} X^i_t$

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 \( \lambda \).

\[
\sum_{i=1}^{N} \hat{X}_t^i = \sum_{i=1}^{N} X_t^i + \sum_{i=1}^{N} [\Gamma_1(N, \lambda) - \Gamma_2(N, \lambda)]
\]

\[
= \sum_{i=1}^{n} X_t^i + [\Gamma_1(1, \lambda) - \Gamma_2(1, \lambda)]
\]

\[
= \sum_{i=1}^{n} X_t^i + [\text{Exp}(\lambda) - \text{Exp}(\lambda)]
\]

\[
= \sum_{i=1}^{n} X_t^i + \mathcal{L}(\lambda), \quad \mathcal{L}(\lambda) : \text{Laplace distribution}.
\]

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

1. Introduction

2. Smart Metering Privacy Analytics
   Privacy Metrics
   Knowledge extraction

3. Privacy-Preserving Smart Metering Techniques
   Data modification: protocols
   Energy modification: Information-theoretic

4. Conclusions
In summary

- **PEMS**: Privacy-enabled Energy Management System
- Data anonymisation (escrow protocol)
- Secure aggregation, key management (network security)
- Policy, Regulations, Access Control (Standards)
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. Over 4 million OSGP based SMs deployed worldwide - most widely used standard.

IEEE 802.15.4g
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 Standardisation II

EU / EC

EC set up Smart Grids Task Force (SGTF) in 2009. Key recommendations: User should have choice e.g. opt-in, opt-out. SGTF Expert Group 2 (EG2) and SGIS work-programme included Data protection impact assessment (DPIA) and Cyber-security assessment.

UK

The Department of Energy and Climate Change (DECC) has assessed that the UK Data Protection Act (DPA) protection is not enough; PIA (privacy impact assessment): data storage, communication and access control should be protected by means of cryptography. Data may be aggregated. The consumer should choose in which way data shall be used and by whom, with the exception of regulated duties.

Germany

The BSI, the federal agency for IT security, has developed a “smart meter protection profile” specification (2010). Smart meter data are stored in home Gateway. Stakeholders are authenticated and authorised by the Gateway. The consumer may choose in which way consumption data shall be accessed and by whom, with the exception of regulated duties.
Future Directions

▶ An exciting research field
▶ Many open questions at the intersection of computer science, power systems, control theory, signal processing and information theory.
▶ What is the relationship of different privacy definitions?
  ▶ k-Anonymity.
  ▶ Information leakage.
  ▶ Anomaly detection & Atypicality.
  ▶ Knowledge extraction (data mining & Machine learning).
  ▶ Differential privacy.
▶ How else can privacy be defined and measured?
▶ How much does the user care about privacy? What is the future of privacy with IoT and big data?
Take away message

- Privacy is a fundamental value; in a future of complex (smart city) systems, security and trust (policies) is not enough...

- To protect privacy we need to measure it.

- Diverse privacy preservation techniques may be based on information theory, multiple source energy engineering, and cryptographic network protocols. Which one to use?
THANK YOU!
References


"Potential Privacy Impacts that Arise from the Collection and Use of Smart Grid Data," NIST, vol. 2, pp. 30–32.


References


References

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


