RepEL: A Utility-preserving Privacy System for IoT-based Energy Meters

Phuthipong Bovornkeeratiroj, Srinivasan Iyengar, Stephen Lee, David Irwin, and Prashant Shenoy

University of Massachusetts Amherst, Microsoft Research India, University of Pittsburgh

April 22, 2020
IoT in Smart Homes

Many IoT products for smart homes
- Smart light bulbs, voice assistants, thermostats, fridges, etc.

Cloud-based IoT architecture
- Send data to cloud servers for analytics

IoT Products
- Video doorbell
- Thermostat
- Smart speaker
- Fitbit

Internet

Cloud Servers
Privacy of IoT Data

- **Cloud analytics of IoT data**
  - Useful services to user
  - e.g. safety monitoring
- **Privacy Leakage**
  - Data reveals privacy information
  - e.g. continuously stream all activity in the house

*Graphics from: canary.is*
Utility Preserving Privacy

• Traditional methods for IoT Privacy
  I. Data obfuscation - obfuscate data before uploading
     - Suppress private information, cloud analytic impossible
  II. Local processing - no cloud transmission
     - Limited ability for sophisticated analytics

• Trade-off: Utility of data analytics vs. Privacy of user

• Utility-preserving Privacy: how to intelligently transform IoT data such that
  - Private information suppressed ✔ Privacy
  - Non-private information retained ✔ Analytics
Utility Preserving Privacy for Energy

- **Smart meter** - Monitor electricity usage at fine time granularity
Utility Preserving Privacy for Energy

- **Smart meter** - Monitor electricity usage at fine time granularity

<table>
<thead>
<tr>
<th>Private Question</th>
<th>Granularity needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>When do you take vacations?</td>
<td>Hourly</td>
</tr>
<tr>
<td>Do you eat out in the evenings?</td>
<td>Seconds</td>
</tr>
<tr>
<td>Were you home during your sick leave?</td>
<td>Hourly</td>
</tr>
<tr>
<td>Did you watch the game last night?</td>
<td>Seconds</td>
</tr>
<tr>
<td>Did you leave your child home alone?</td>
<td>Seconds</td>
</tr>
<tr>
<td>Did you get a good night sleep?</td>
<td>Seconds</td>
</tr>
<tr>
<td>Do you eat hot or cold breakfast?</td>
<td>Seconds</td>
</tr>
</tbody>
</table>

Energy Breakdown (Disaggregation Analytics)

Occupancy Detection

(ICCDS 2018)
Utility Preserving Privacy for Energy

- **Smart meter** - Monitor electricity usage at fine time granularity

Key question:

"How can we **allow disaggregation analytics** and **prevent occupancy attacks**?"
Talk Outline

- Motivation

RepEL Utility Preserving Privacy

- Experimental Results
- Conclusion
Smart Meter Privacy using a Battery

- **Key idea:** use a battery storage as energy buffer
  - Use charge/discharge to transform usage seen by smart meter

- **Current state of art:** data obfuscation using battery

![Diagram showing the relationship between appliances, battery storage, smart meter, and grid.](image)
Our Approach: **RepEL**

(Replay Energy Load)

- **Key idea:** permute & randomize while retaining usage of each appliance
  - Use battery to suppress actual usage when it occurs
  - Record this usage
  - Use battery to replay usage at later time

- **Record and Replay**
  - Retains individual appliance usage
  - Permutes time order of usage as seen by meter

- **Time-based occupancy attack**

- **Usage-based cloud analytics**
RepEL Architecture

- **Replay Energy Loads in 3 steps**

  1. **Step1: Record** - record energy consumption of foreground appliance
  2. **Step2: Schedule** - schedule the time to replay using a target distribution
  3. **Step3: Replay** - replay recorded trace based on schedule and policies

---

**Diagram:**

- **Energy Meter** connected to **Foreground load**
- **Record Module** connected to **Schedule Module**
- **Schedule Module** connected to **Replay Module**
- **Battery** connected to **Discharge battery to mask load**
- **Store load** connected to **Key-value store**
- **Charge battery to mimic load** connected to **Battery**
- **Raspberry Pi** connecting **Schedule Module** and **Replay Module**
- **Time window** and **Target Distribution** connecting **Schedule Module**

---

Step1: Record - record energy consumption of foreground appliance
Step2: Schedule - schedule the time to replay using a target distribution
Step3: Replay - replay recorded trace based on schedule and policies
RepEL Algorithm Pipeline

**Record**

Time window #1

- 20 mins
- 60 mins
- 20 mins

Discharging

no original load seen

**Schedule**

Time window #2

Schedule 3 start times

- 3 AM
- 8 AM
- 1 PM

**Replay**

Time window #2

- Charging
- 20 mins
- 60 mins
- 20 mins

Result in randomization & permutation
RepEL Replay

- **RepEL** use **MCMC sampling** method called **Metropolis-Hasting Algorithm** to mimic any distribution during schedule step.

  - **Vacation mode**
    - Long absence periods means **nothing to record**
    - **Replay random loads** from previous week
Talk Outline

- Motivation
- RepEL Utility Preserving Privacy
- Experimental Results
- Conclusion
Experimental Setup

Metrics

• Privacy leakage rate = \(100 \times \frac{\sum_{i=1}^{N} is\_leak(i)}{N}\)

• Device usage change = \(100 \times \frac{\sum_{i=1}^{N} (replay\_profile_i - energy\_profile_i)}{\sum_{i=1}^{N} energy\_profile_i}\)

Dataset

• Dataport from Pecan Street Inc. - 19 houses, 1 month, minute-level data

• ECO from ETH Zurich - 4 houses, 22-36 days, second-level data
RepEL Privacy vs Utility

**Result:** RepEL provides <10% privacy leakage with <3% error in usage
Disaggregation analytics accuracy

Comparison with LS2

<table>
<thead>
<tr>
<th>Metric</th>
<th>LS2</th>
<th>RepEL</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAPE</td>
<td>64.25</td>
<td>6.53</td>
</tr>
<tr>
<td>MSE</td>
<td>4.07e+11</td>
<td>1.36e+10</td>
</tr>
</tbody>
</table>
Result: RepEL has reasonable good privacy property but slightly worse than LS2
But LS2 cannot preserve utility information
Conclusion

• Proposed a utility-preserving privacy system (RepEL) for smart meter

• Implemented and evaluated on two plug-level home energy trace dataset

• Our results show:
  - RepEL can prevent adversaries from inferring behavioural patterns
  - Also RepEL can preserve utility information in the trace
Thank you

Contact us:
phuthipong@cs.umass.edu