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

iotdi

University of Massachusetts Amherst

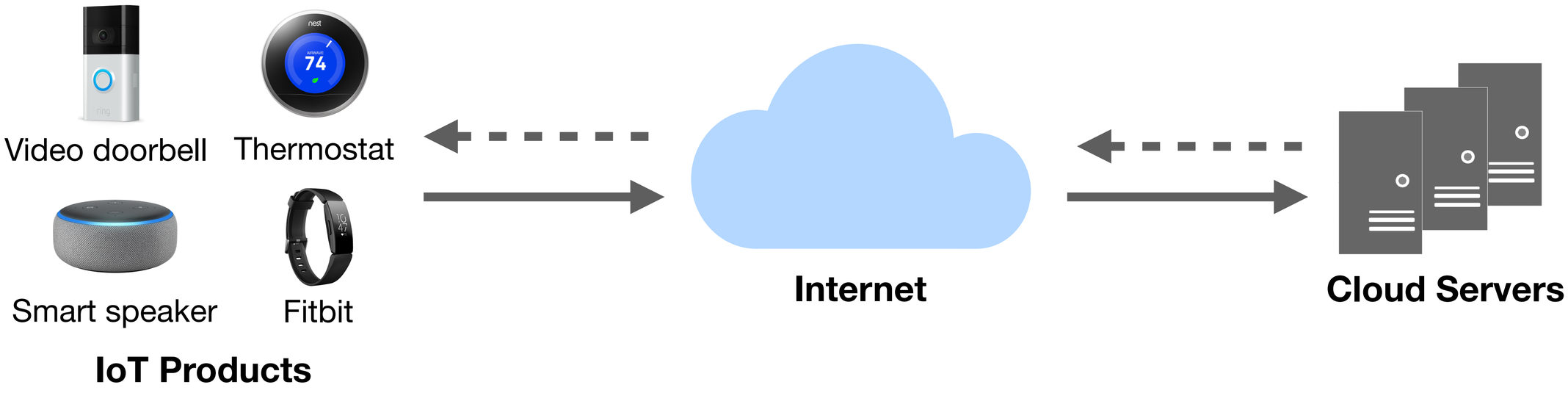
IoT in Smart Homes

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



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

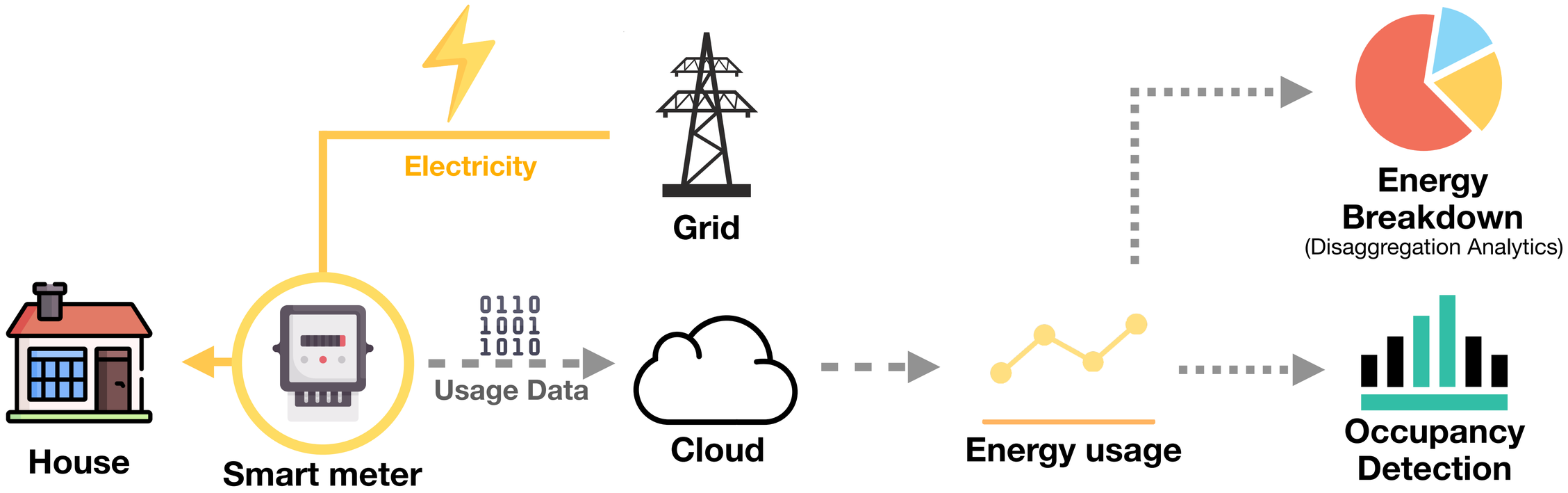
- **Traditional methods for IoT Privacy**
  I. **Data obfuscation** - obfuscate data before uploading
     - Suppress private information, cloud analytic impossible
  II. **Local processing** - no cloud transmission
     - Limited ability for sophisticated analytics

- **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**

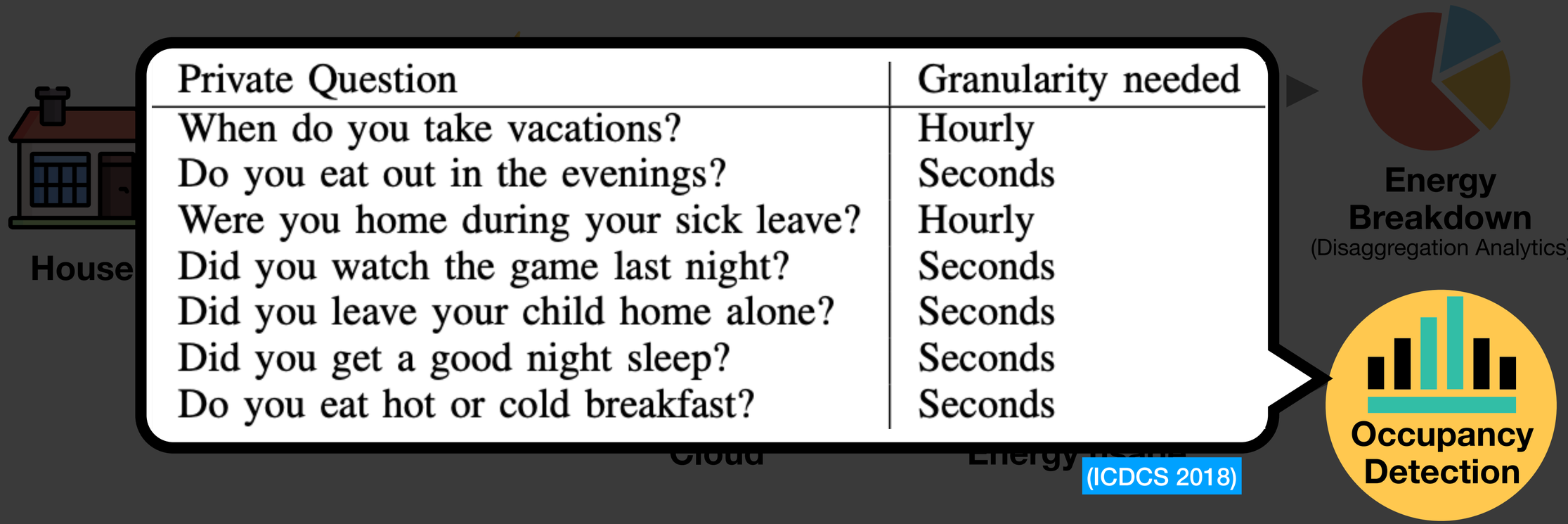
Utility Preserving Privacy for Energy

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



Utility Preserving Privacy for Energy

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



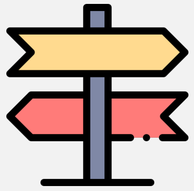
Utility Preserving Privacy for Energy

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

Key question:

> “How can we allow disaggregation analytics and prevent occupancy attacks?”

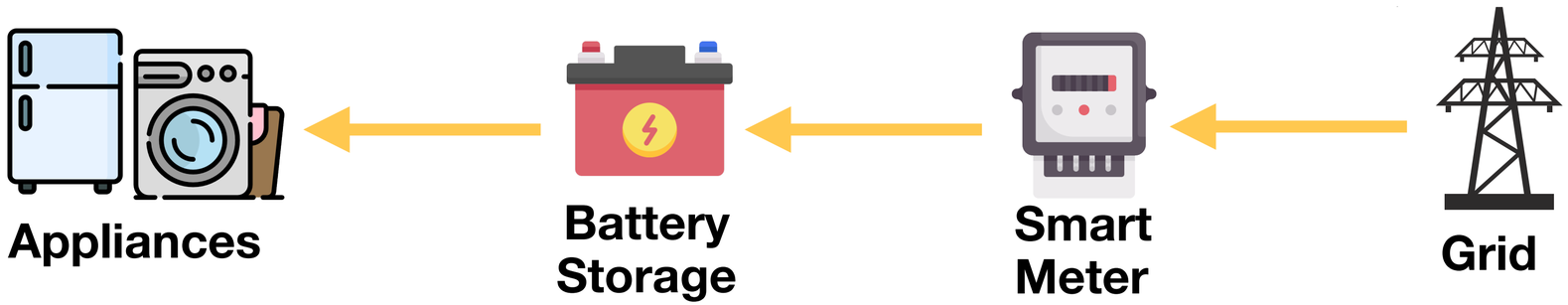
Talk Outline



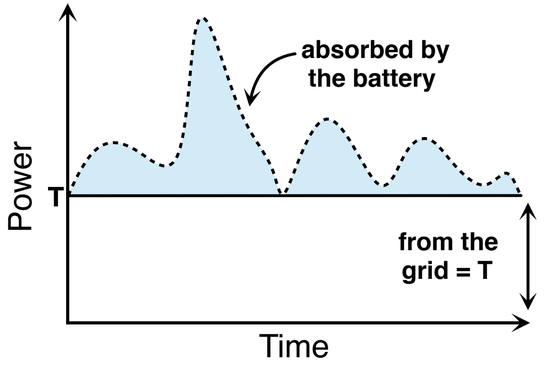
- Motivation
- **RepEL Utility Preserving Privacy**
- Experimental Results
- Conclusion

Smart Meter Privacy using a Battery

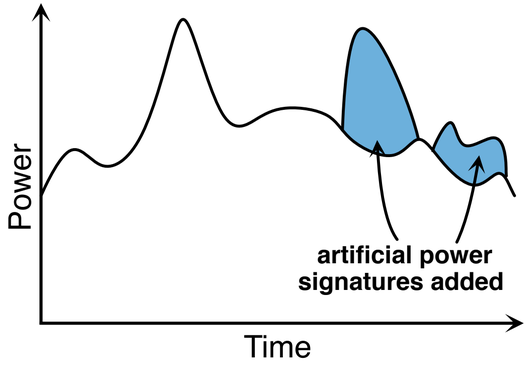
- **Key idea:** use a **battery storage** as energy buffer
  - Use charge/discharge to transform usage seen by smart meter



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



Flattening (Yang, et al.)



Noise injection (Chen., et al)

Our Approach: RepEL

(**Rep**lay **E**nergy **L**oad)

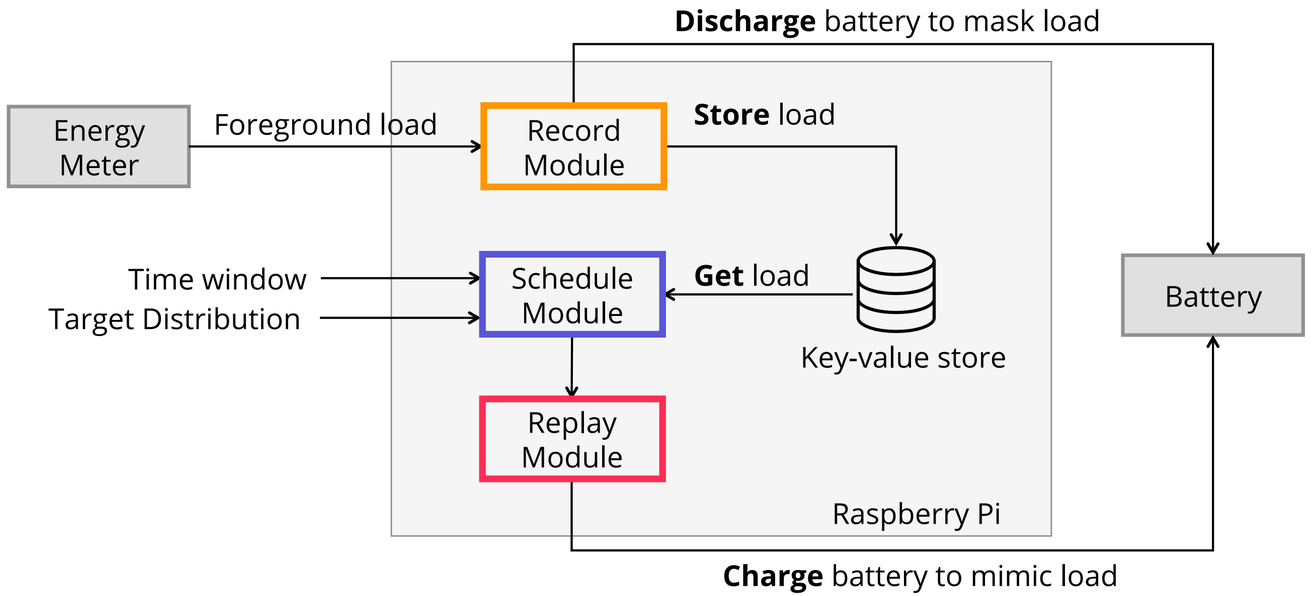
- **Key idea:** permute & randomize while retaining usage of each appliance
  - Use battery to suppress actual usage when it occurs
  - Record this usage
  - Use battery to replay usage at later time
- **Record and Replay**
  - Retains individual appliance usage
  - Permutes time order of usage as seen by meter

❌ **Time-based occupancy attack**

✅ **Usage-based cloud analytics**

RepEL Architecture

- **Re**play **E**nergy **L**oads in **3** steps



Step1: Record - record energy consumption of foreground appliance

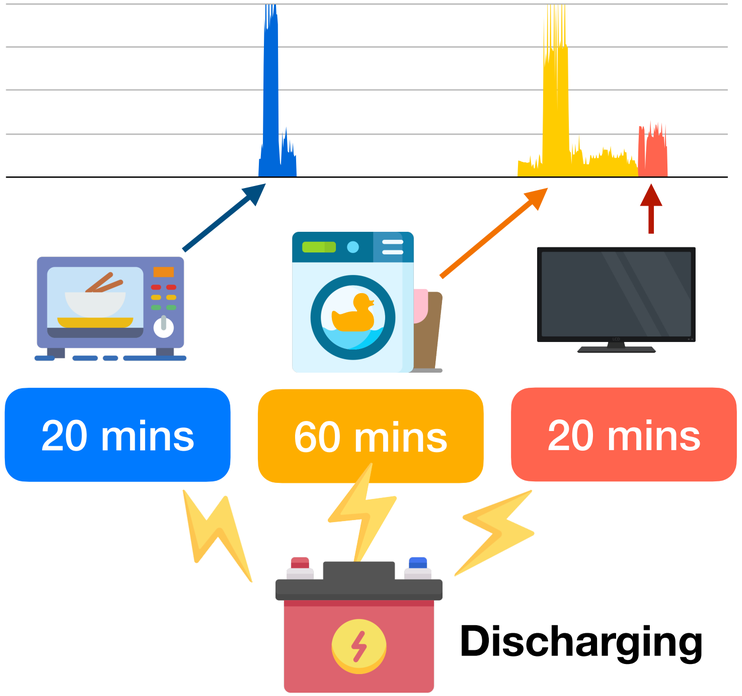
Step2: Schedule - schedule the time to replay using a target distribution

Step3: Replay - replay recorded trace based on schedule and policies

RepEL Algorithm Pipeline

Record

Time window #1

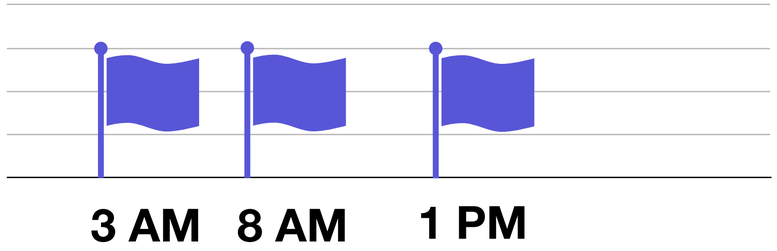


no original load seen

Schedule

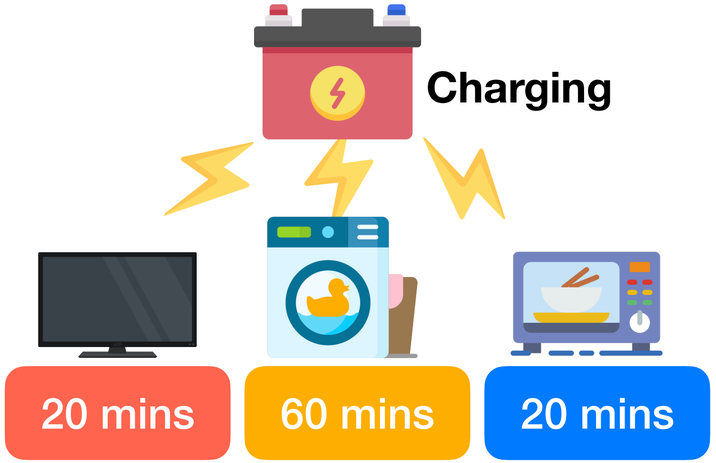
Time window #2

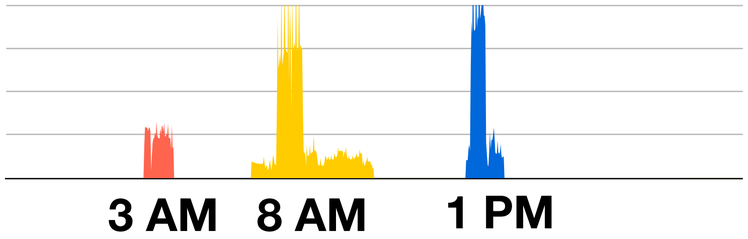
Schedule 3 start times



Replay

Time window #2

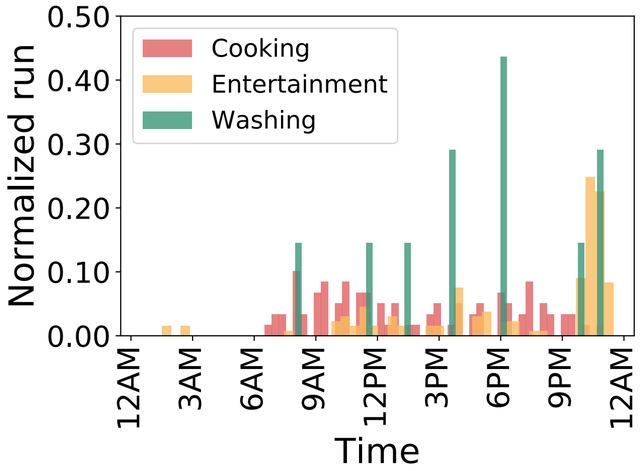




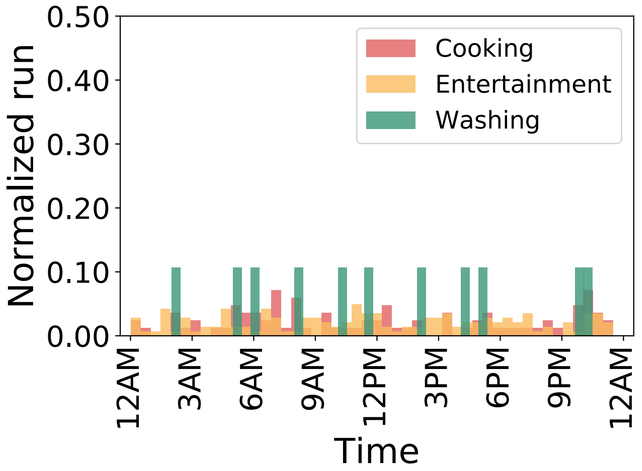
Result in randomization & permutation

RepEL Replay

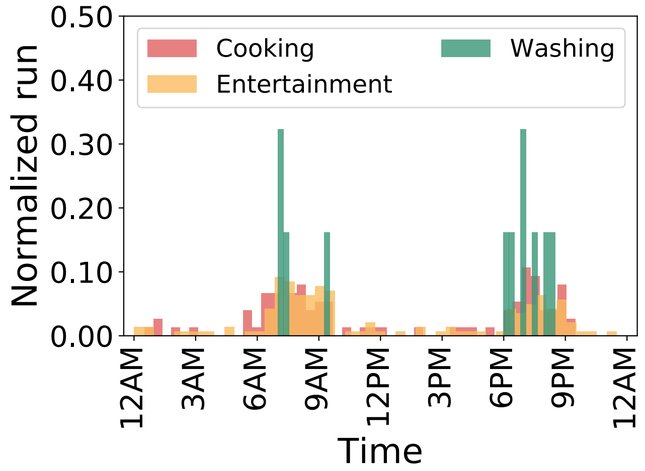
- **RepEL** use **MCMC sampling** method called **Metropolis-Hasting Algorithm** to **mimic any distribution** during schedule step



Original distribution



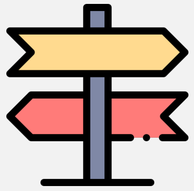
Uniform distribution



Bimodal distribution

- **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

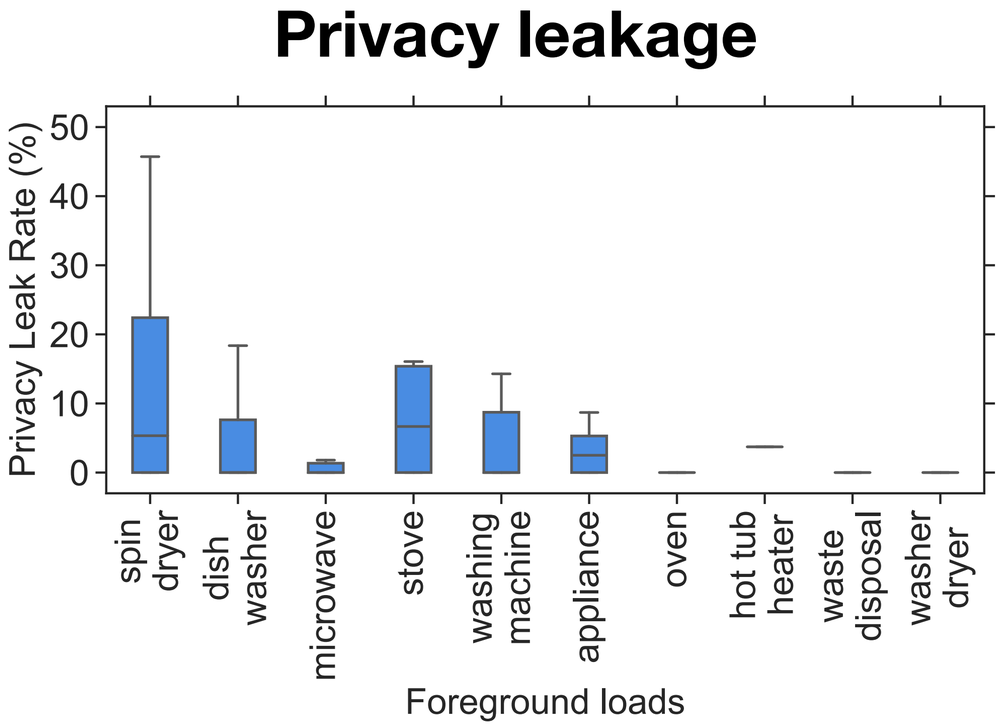
Metrics

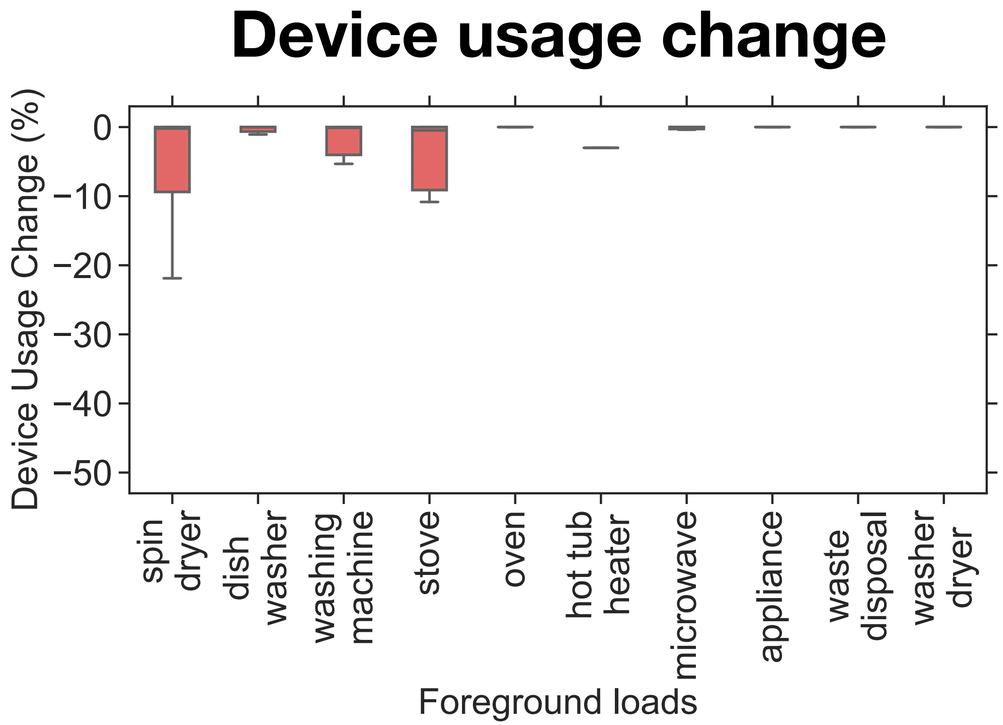
- **Privacy leakage rate** $= 100 \times \sum_{i=1}^{N} \frac{is\_leak(i)}{N}$
- **Device usage change** $= 100 \times \frac{\sum_{i=1}^{N} (replay\_profile_i - energy\_profile_i)}{\sum_{i=1}^{N} energy\_profile_i}$

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



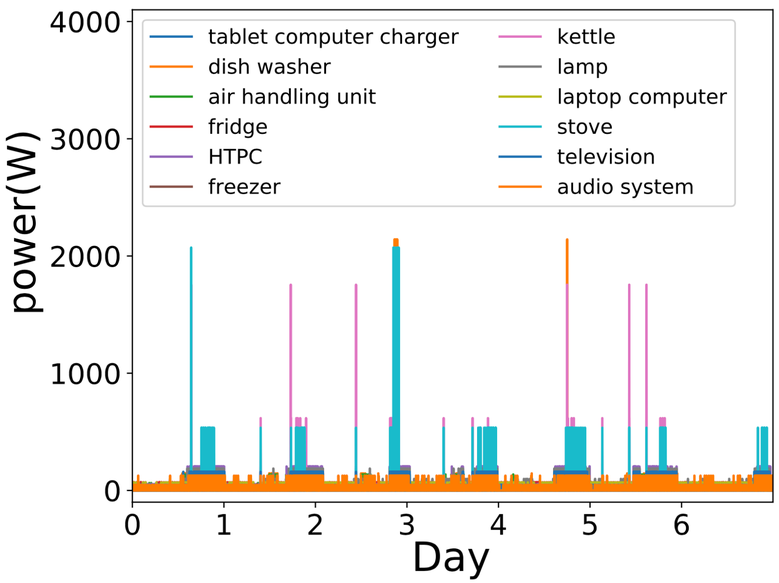


Result: RepEL provides **<10% privacy leakage** with **<3% error in usage**

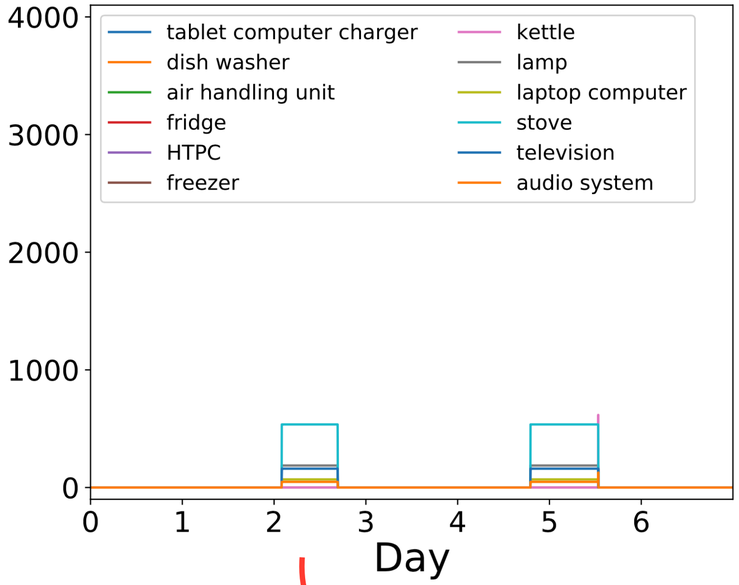
Disaggregation analytics accuracy

Comparison with LS2

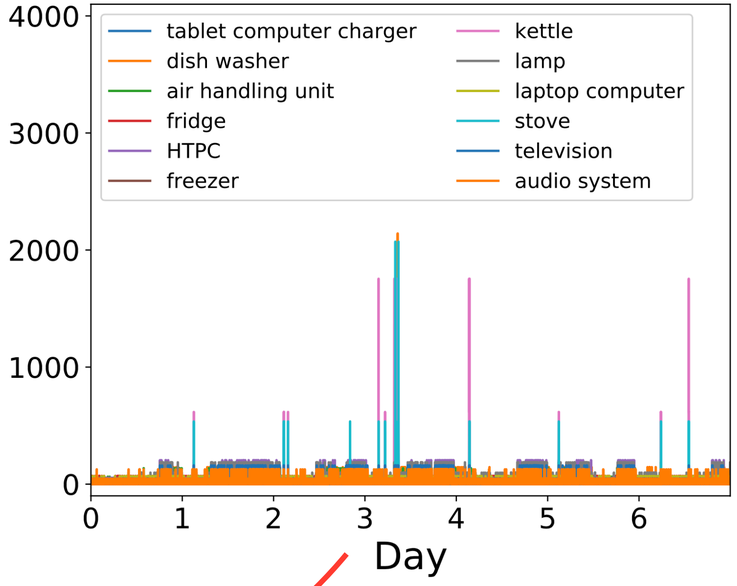
Original disaggregation



LS2 disaggregation

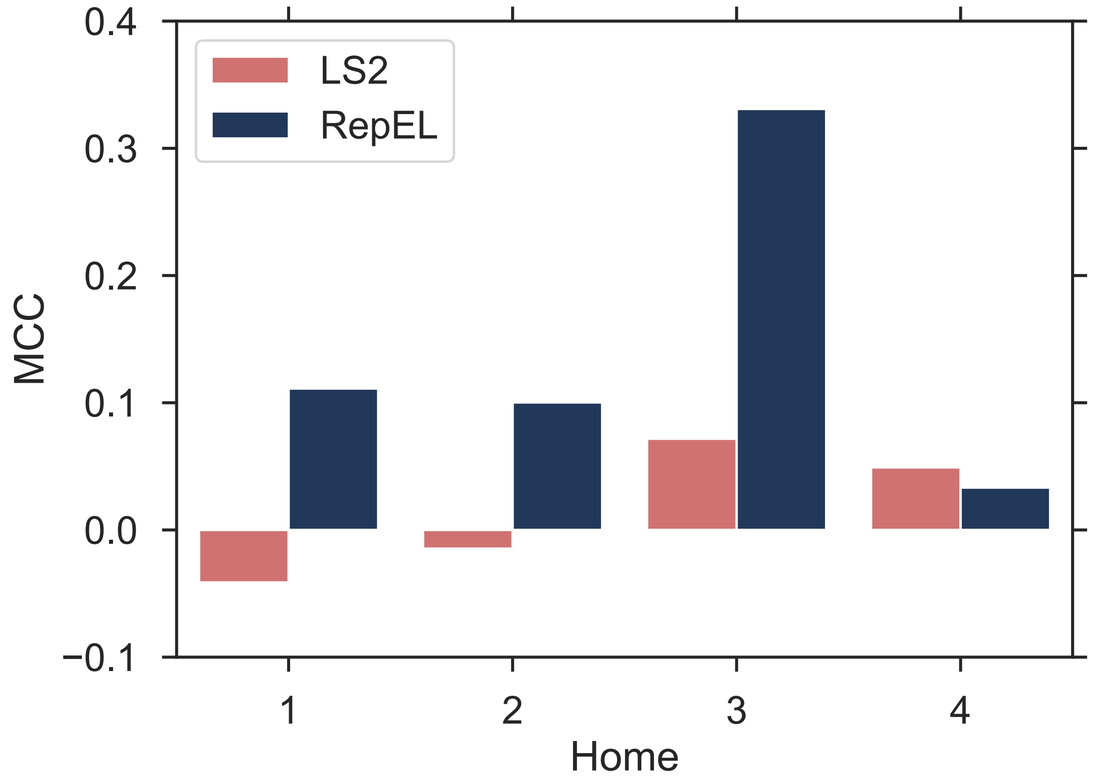


RepEL disaggregation



Metric	LS2	RepEL
MAPE	64.25	6.53
MSE	4.07e+11	1.36e+10

Occupancy Detection Accuracy



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