

Private Memoirs of a Smart Meter

Nishad Gothoskar
ngothosk@andrew.cmu.edu

1: Summary

Privacy is an important but sometimes ignored factor of the entire "smart" future. Specifically, wide spread deployment of smart energy sensors has the ability to give a lot of insight into what's going on in the home. This paper is showing what kinds of privacy invasive things can be extracted from this data. This provides proof of the actual inspiration and then they go on to describe what ways they can protect against this.

The information leaks are dependent on the granularity of power measurements. Older meters only read once in a while, but our newer meters can get real-time measurements down to seconds. From this, newer generations of NILM algorithms can actually differentiate exact device usage patterns.

So what exactly are the privacy concerns of smart meters. Well they discuss some of the questions that could be answered by smart metering. Like were you home during sick leave? Did you leave late for work? While these might not seem extremely intrusive. A wide variety of these questions answered might together be intrusive. They just look for a simple patterns in our total and device usage to answer these questions and many times that is enough.

So the process the took was to label and tag power events. Then filter out automated appliances to leave just user initiated event changes. Finally map events to real life. Now you have a time series of all the events that were initiated by users. And then you can begin to develop a sense of routine. They use a density based clustering algorithm to do this mapping to real life.

Now they talking about privacy-enhancing architecture. The techniques they use include obfuscating the names, randomization, etc. In particular zero knowledge protocols would allow data transmission with anonymity.

2: Strengths

- Focus on privacy and proof that it is really an issue. Very thorough

3: Weaknesses

- Transmission of data section could be better

4: Future Directions

- Implementation of new version to see if you can still disambiguate