A Differentially Private Data Sharing Mechanism for Smart Meters: An Approach for Longitudinal Data

Milad Hoseinpour
Dept. of Electrical and Computer Engineering
Tarbiat Modares University
Tehran, Iran

Mohammad Hoseinpour
Dept. of Electrical and Computer Engineering
Babol Noshrivani University of Technology
Babol, Iran

Mahmoud-Reza Haghifam
Dept. of Electrical and Computer Engineering
Tarbiat Modares University
Tehran, Iran

Digitalization has an instrumental role in the transition of power and energy systems towards decentralization and decarbonization. In this regard, digitalization rollout requires the deployment of smart meters, which are the key enabler for the integration of smart devices and demand response programs for domestic customers. Also, smart meters provide the possibility of logging and accessing granular consumption data of customers. Access to these rich and fine-grained data has a wide range of benefits for customers, grid operators, energy suppliers, policy makers, etc. Specifically, they facilitate the integration of Renewable Energy Sources (RESs) at the grid edge and operation of the grid under a high penetration level of RESs. Furthermore, the existence of smart meter data and their ease of access set the stage for the advent of new economic models and pricing schemes for electricity services. Nevertheless, concerns about the privacy and misuse of these data are a serious hurdle for the deployment of smart meters. For instance, non-intrusive load monitoring methods make it possible to decompose the load profile of domestic customers according to the type of consumption and appliances, which is a real privacy infringement for customers. Moreover, data privacy laws and regulations, e.g., General Data Protection Regulation (GDPR) passed by the EU, impose legal obligations on utilities to safeguard the sensitive information of domestic smart metering.

The main question motivating this paper is how to preserve the privacy of smart meter data while maintaining the utility of the data for social good. We aim to develop a data sharing mechanism for smart meters that guarantees anyone who has access to these data is not able to infer useful information at the individual level, without limiting the usefulness of that data for grid operation, statistical analysis, etc. To achieve our privacy goal, we implement the notion of Differential Privacy (DP), which gives us a framework to quantitatively reason about privacy. DP is a rigorous privacy notion used to bound the disclosure risk of the private information associated with an individual's participation in a computation. The literature for addressing the privacy concern of smart meters via DP mainly focuses on one-time smart meter data collection. However, the real challenge is to protect the privacy of a customer on a continual observation of the smart meter data. Indeed, smart metering infrastructure requires continuous publishing of the measurements that leads to a time series. As a result, due to the composition theorem of DP, the privacy loss of a customer adds up in the successive timestamps of the data sharing horizon. Thus, we should adopt an advanced privacy mechanism to bound the privacy loss of an individual caused by the smart meter longitudinal data.

In this regard, we implement the Randomized Aggregatable Privacy-Preserving Ordinal Response (RAPPOR) mechanism. RAPPOR is mainly developed to preserve the privacy of individuals in settings where data are collected repeatedly (or even infinitely) from the same individual, which is perfectly consistent with smart metering infrastructure. This paper provides an application of RAPPOR mechanism for preserving the privacy of smart meters time series data and demonstrates its privacy and utility guarantee. In numerical results, the practical deployment of this mechanism for real-world smart meters data is discussed.