Differential Privacy in Non-Intrusive Load Monitoring

Background: Advanced metering devices are generating huge amount of data every second. This raises significant public concern on privacy protection since advanced machine learning techniques have shown the potential to infer user behavior from metered data (non-intrusive load monitoring). One possible solution is to inject noises to the metered data to achieve differential privacy.

Challenges: Though promising, the embedded parameters in differential privacy do not provide any intuition of the physical implications, e.g., what is the level of privacy guarantee that a differential privacy with certain parameter can provide. This sets a significant barrier for the wide application of differential privacy techniques.

Our Idea: We use non-intrusive load monitoring (NILM) as an example to understand differential privacy in the electricity sector. The goal of NILM is to infer user behaviors through metered data. We consider a simplified task, one shot NILM inference, which only seeks to infer the appliance switching events of a particular user for the next time slot. Assuming certain sparsity in the switching events, such inference can be cast int the compressive sensing framework [1]. We establish the lower bound of the inference accuracy in this framework.

This lower bound can also be interpreted as the performance guarantee of using compressive sensing for NILM inference. We observe that injecting Laplace noise into the metered data can achieve ϵ-differential privacy. The parameter ϵ will affect the variance of Laplace noise, which in turn will affect the lower bound of inference accuracy!

We offer explicit characterization for this process. We find that a higher level of differential privacy (larger ϵ) leads a decreased performance guarantee (the lower bound of the inference accuracy) at the rate of $O(1/\epsilon^2)$ [2].

Future Work: It will be interesting to derive the upper bound, or a tighter lower bound for the inference accuracy. We also intend to understand the role of DP parameters in other inference schemes for NILM with better performance than compressive sensing.

References

[1] J. Candes, J. Romberg, and T. Tao, Stable signal recovery from incomplete and inaccurate measurements, Communications on Pure and Applied Mathematics, vol. 59, no. 8, pp. 1207–1223, 2006

[2] Haoxiang Wang, **Chenye Wu***, "Understanding Differential Privacy in Non-Intrusive Load Monitoring", in submission to IEEE Power Engineering Letters, Initial Submission: Dec. 2019.