Differential Privacy in Consumer Behavior Analysis

Haoxiang Wang, Xun Luo *and* Chenye Wu

***Abstract*—Consumer behavior analysis is the key enabler for many industrial applications. This is also true for the electricity sector. However, such analysis is based on huge amount of data, which raises the public concern over private information leakage. In this paper, we seek to understand how privacy preserving mechanism may affect the behavior analysis performance. Specifically, we use k-means clustering as an example of behavior analysis and define cluster stability from a probability theoretic viewpoint. We establish the relationship between different levels of privacy preserving requirement and cluster stability theoretically and empirically. Numerical studies highlight the value of our proposed analysis for both system operator and the consumer.**

***Index Terms*—Consumer Behavior Analysis, Differential Privacy, Clustering.**

I. Introduction

Data analytics is all the rage nowadays.. One important application of data analytics is consumer behavior analysis, which is also true for the electricity sector. Consumer behavior analysis is crucial to improve the overall power system efficiency [1]. It could also help the consumers achieve energy saving [2] and provide ambient assisted living [3].

However, such benefits come at the cost of private information leakage. The increasing public awareness of privacy preserving makes the consumer behavior analysis a rather challenging task. Specifically, most popular privacy preserving mechanisms adopt the notion of differential privacy (DP) and inject noise into the meter data. Such noisy data may significantly affect the performance of consumer behavior analysis. Our work targets to uncover the theoretical tension between the injected noise to the meter data and the performance of the consumer behavior analysis. This could inform the consumers the physical meanings of different levels of DP. Our work is also valuable to the system operators who may want to reexamine how to utilize the privacy preserving noisy data.

A. Related Works

To uncover the aforementioned theoretical tension, we use k-means clustering as an example of consumer behavior analysis, since k-means clustering oriented behavior analysis can be already valuable to the whole system: from enabling active demand side management [4], [5] to improving the electricity market design [6]. It could also be used to provide lifestyle suggestions to the consumers [7].

As such, we identify two major bodies of related literature. The first one examines the robustness of the clustering methods in consumer profiling and the other one designs the noise injection mechanism to achieve privacy preservation, both with an emphasis on the electricity sector.

The research works on examining the robustness of clustering methods applied in the electricity sector only appear recently. For example, Yilmaz *et al.* extensively compare different clustering approaches for the electricity load profile characterization-implications for demand side management and explicitly characterize the impact of noise in [8]. Motlagh *et al.* further propose a number of indexes to reflect the robustness of clustering methods in [9]. However, to the best of our knowledge, we are the first to theoretically investigate the impact of artificially injected noises on the robustness performance.

There is a growing body of research works, studying the privacy preserving mechanisms in the electricity sector. Just to name a few, Backes *et al.* theoretically analyze the mechanism to achieve different levels of privacy using storage system to physically inject noise in [10]. Zhang *et al.* further examine the cost effectiveness of a similar mechanism in [11]. Interested readers are referred to the survey [12] by Farokhi. However, most of the research works in this stream do not consider the influence of privacy preservation on consumer behavior analysis. Actually, there could be many other privacy mechanisms including masking with loads [13], encryption [14] or other information masking based on the optimization problems [15], [16]. But most of them are lack of the measurement for privacy. Most of these work focus on how to make the data different from the original or make it not identified by some algorithms with the lowest cost. But they could not control to achieve a specific level of privacy. Therefore, we consider differential privacy measurement first and use its corresponding mechanism to conduct our analysis effectively. In fact, most of other information masking could be converted to the differential privacy's framework. For example, some of works [17] analyzed by mutual information (MI) could be simply transformed to DP's measurement [18]. It shows the generality of our framework selected.

The most closely related works are privacy preserving non-intrusive load monitoring (NILM) mechanism performance assessment by Cao *et al.* [19] and our recent poster [20] (and subsequent journal publication [21]), which establishes a theoretical performance bound for NILM given different levels of injected noise. In contrast, our work seeks to provide both *theoretical* and *numerical* performance assessment of privacy preserving mechanism on *consumer behavior analysis*.

The rest of the paper is organized as follows. We evaluate

H. Wang is with Institute for Interdisciplinary Information Sciences, Tsinghua University. X. Luo is with School of Microelectronics, University of Science and Technology of China. C. Wu is with School of Science and Engineering, The Chinese University of Hong Kong, Shenzhen, and Shenzhen Institute of Artificial Intelligence and Robotics for Society. C. Wu is the correspondence author (email: chenyewu@yeah.net). This work was supported in part by Shenzhen Institute of Artificial Intelligence and Robotics for Society.

the performance of clustering methods for different granularity in Section II. Then, in Section III-A, we first revisit the concept of ϵ-DP as well as the corresponding Laplacian mechanism, and then based on this mechanism, we theoretically examine the impact of Laplace noise on behavior analysis. Next, we conduct numerical studies with field data and observe the empirical evidence in Section IV. Concluding remarks are given in Section V.

II. Effective Clustering for Behavior Analysis

Before diving into the theoretical and numerical studies, we first overview the dataset, and then trim the dataset for better consumer behavior analysis. Based on the trimmed dataset, we evaluate how to select the best granularity to enable the most effective behavior analysis.

A. Overview of the Dataset

We use the Pecan Street dataset [22], containing the load profile data of 1 minute resolution, collected from 400 users in Austin, Texas, from May 1 to October 30, 2015. We trim the dataset by removing all the data collected on August 9, 2015 due to too many missing data. To better characterize the diverse user behaviors, we combine the daily load profiles of all users into a single daily load profile dataset (containing 2,048 valid load profiles in total).

While it is commonly believed that more detailed data may contain more valuable information on the consumer behavior, too detailed data may lead to too many clusters, which negatively contributes to the value of clustering outcomes. In the subsequent analysis, we use numerical study to highlight this trade-off.

B. Granularity versus Effective Clustering

There are a number of metrics to evaluate the performance of clustering result (given the number of clusters), including clustering dispersion indicator (CDI) [23] and Davies-Bouldin indicator (DBI) [24], etc. As these indexes largely follow the same idea, we adopt CDI as a representative indicator.

Intuitively, CDI measures the average dispersion for all clusters. This indicator is negatively correlated with the performance of clustering result, i.e., the lower the CDI, the better the clustering result. Mathematically, for a clustering result of K clusters, we define $\hat{d}(C)$ the average Euclidean distance between every two central points and we define $\hat{d}(L^{(i)})$ the average Euclidean distance between every two load profiles of cluster i. Hence, CDI can be obtained as follows:

$$\text{CDI} = \frac{1}{\hat{d}(C)} \sqrt{\frac{1}{K} \sum_{i=1}^{K} \hat{d}^2 \left(L^{(i)}\right)} \tag{1}$$

Another set of metrics to evaluate the effectiveness of clustering can serve as guidelines to optimally choose the number of clusters. The most common method is to use the Elbow method [25].

The classical elbow method [26], [27] calculates the sum of the squared errors (SSE) of the clusters for different cluster numbers. In detail, if we have K clusters after K-means, the SSE could be calculated as follows:

$$SSE = \sum_{i=1}^{K} \sum_{p \in C_i} d(p, m_i), \tag{2}$$

where m_i is the center of cluster C_i. Then we could draw the SSE curve with the different K. We could find out the SSE decreases with K and the so-called elbow point is the point where the decreasing tendency becomes abruptly much smaller. This is a heuristic decision. It is the point where diminishing returns are no longer worth the additional cost. More precisely, the first clusters will add much information, but at some point the marginal gain will drop because the information has been reflected by the former clusters, giving an angle in the graph as an elbow. If we insist on adding more clusters, we might trap into overfitting and learn useless noise for our analysis. Therefore, the elbow point cluster could partly reflect the information or feature carried by the input data.

We plot the CDI and optimal number of clusters (dictated by Elbow method) for each granularity in Fig. 1. Since CDI is negatively correlated with the clustering performance, we plot its inverse (1/CDI) instead of CDI. It is clear when the granularity is too small, the optimal number of clusters remains the same but the performance (in terms of CDI) is getting worse. On the other hand, by choosing large granularity (e.g. 240 minutes), we may end up with too few clusters. Such result may carry limited information for behavior analysis purpose due to information loss incurred during the energy aggregation. This observation highlights the importance of examining the trade-off between granularity selection and performance of clustering, though a detailed theoretical analysis is beyond the scope of this paper. In the real application, when we derive the meter data and try to use it to conduct clustering for active demand side management, we need to reconsider whether we need to do transformation to the data or just give up the high granularity data. On the hand, a lower granularity could lead a bad clustering result, we might not identify the difference between different clusters of users clearly. On the other hand, if we receive the data with not enough low granularity, we need to be aware that we might suffer a great information loss and our clustering might not reflect the true differences between the users. Therefore, we need to empirically conduct numerical studies for real tasks such as Time of Use tariffs designing or load forecasting [8] with different granularity. Then we could check the final results for each tasks then find the optimal end-to-end granularity for application. In our paper, based on the numerical study, we select the granularity of 30 minutes to balance the clustering performance and information loss.

III. Main Results

Based on the trimmed dataset and the granularity selection in the last section, we study the impact of privacy preserving method on the behavior analysis. Hence, we first briefly revisit the concept of DP and its associated privacy preserving method. Then we numerically observe how privacy preserving

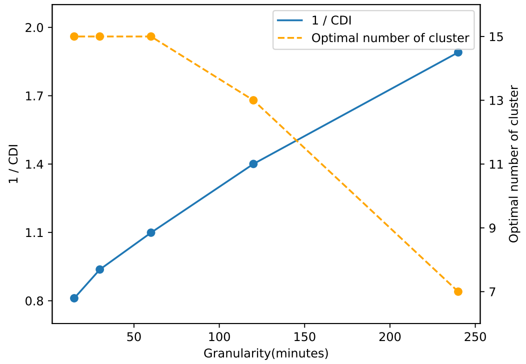

Fig. 1. Performance evaluation for clustering based on different granularity

method may affect the final outcome of k-means clustering. Finally, we theoretically study the underlying influential dynamics.

A. Revisit ϵ-Differential Privacy

We adopt the notion of ϵ-differential privacy (ϵ-DP), first proposed by Dwork *et al.* in [28]. It rigorously characterizes the probability of inability to differentiate two similar datasets. Formally, this notion is defined for a mapping $\mathscr{B}(D)$ from a dataset D to $\mathbb{R}$, and an associated query function $q : D \rightarrow \mathbb{R}$. For some distance metric $d(D, D')$ for two datasets D and D', we can further define neighbor datasets if and only if $d(D, D') = 1$.

Definition 1. If for all neighbor datasets D_1 and D_2, and for all measurable subsets $Y \subset \mathbb{R}$, the mapping $\mathscr{B}$ satisfies,

$$\frac{Pr(\mathscr{B}(D_1) \in Y)}{Pr(\mathscr{B}(D_2) \in Y)} \leq e^{\epsilon}, \tag{3}$$

we say the mechanism $\mathscr{B}$ achieves ϵ-DP [28].

To achieve ϵ-DP, one straightforward mechanism is to inject noise. It can be shown that it is enough to inject Laplace noise in the following way [28].

Theorem 1. We say a mechanism $\mathscr{B}$ achieves ϵ-DP, if $\mathscr{B}(D)$ satisfies

$$\mathscr{B}(D) = q(D) + n, \tag{4}$$

and n is Laplace noise with probability density function (pdf) $p(s)$:

$$p(s) = \frac{1}{2\lambda} e^{-\frac{|s|}{\lambda}}, \tag{5}$$

in which $\lambda = \frac{\Delta f(D)}{\epsilon}$ combines the privacy parameter ϵ that describes the level of the privacy and the sensitivity $\Delta f(D)$ satisfying $\Delta f(D) \geq \max \|q(D_1) - q(D_2)\|$ for all neighbor datasets D_1 and D_2.

Remark: In this theorem, actually the dataset D could denote the appliance state or consumer behavior at a certain time. Then query q could denote the meter reading for the whole appliances. There are many non-intrusive load monitoring algorithm [29], [30] to infer the state from the meter data. Therefore, according to our Theorem 1, we add a specific Laplacian noise to the meter reading to confuse the possible attacker and make him misjudge the appliances' state or hide some states for the specific appliances. We could achieve this because the distribution for different meter data after injecting noise could not differ much and the difference of the distribution could be controlled by the privacy parameter ϵ. The level of injecting Laplacian noise is depends on the sensitivity $\Delta f(D)$, which could be calibrated as the difference between different load patterns and the parameter ϵ. Theorem 1 shows that we need more efforts to inject higher noise for high privacy preservation or handling the states with huge differences.

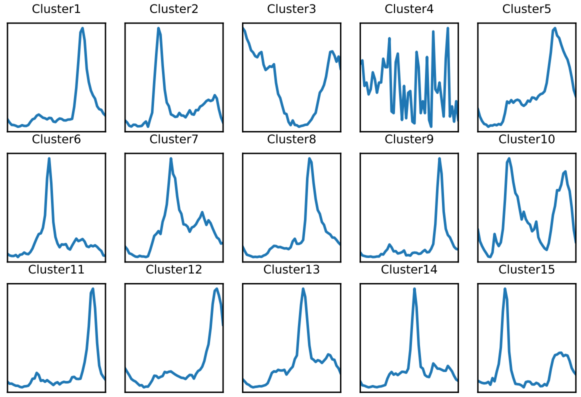

Fig. 2. The profile of the clustering center

In our setting, the sensitivity $\Delta f(D)$ could be calibrated as the difference between load patterns, and the parameters ϵ indicates the privacy requirement for the consumers. Our work targets to decipher the physical meaning of λ (combining the impact of parameter ϵ and Δf specified by the dataset) in practice.

B. Empirical Evidence

The injected noise may heavily impact the clustering result. We use trimmed dataset with 30 minute resolution. According to our analysis in Section II, we choose the number of clusters to be 15. Fig. 2 plots the center profiles of all the 15 clusters. Intuitively, they capture different life styles, which partially supports that Elbow method performs remarkably good in practice.

Then we try to observe how different levels of injected noise may affect the clustering result. In Fig. 3, the directed arrows track the cluster interchanges. The color of each node indicates the frequency that such interchanges happen in the corresponding cluster. The yellow color infers that the cluster is more stable in terms of less interchanges happen while the red color represents the unstable cluster. It reflects that in the results of K-means clustering, we could find some clusters in which the consumers' profile have higher probability not to change. This characteristic could be useful when we want to choose the consumers with low variability for the following

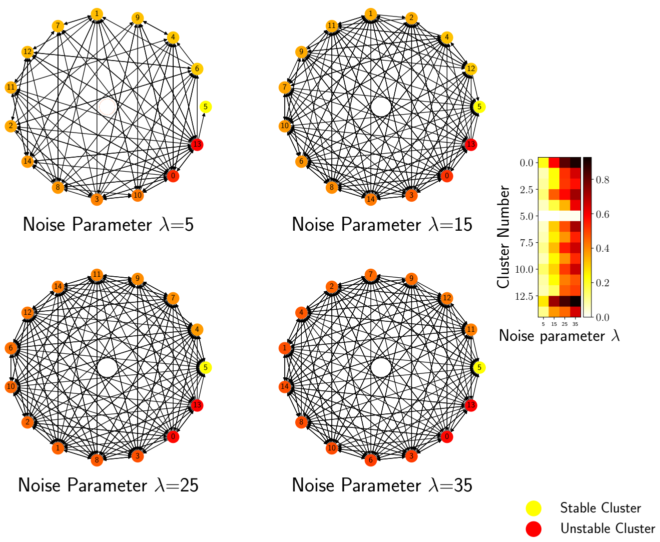

Fig. 3. The clusters interchanges influenced by different levels of noise injection

tasks like demand response. Fig 3 captures such interchange dynamics for 4 kinds of injected noises, with parameter λ ranging from 5 to 35, with a step size of 10. It is self-evident that higher λ leads to higher frequency that consumers may deviate from its true cluster. Such empirical evidence may render the consumer behavior analysis based on clustering problematic. In the remainder of this section, we seek to mathematically establish the relationship between the stability of each cluster and the parameter λ of the injected noise, which offers practical insights on how to explain the DP parameters.

C. Cluster Stability Characterization

We characterize the cluster stability from a probability theoretic view. For each consumer, we can examine its load profile $\mathbf{d} \in \mathbb{R}^T$, where T is 48 in our setting. Denote the injected noise into this profile by $\mathbf{n} \in \mathbb{R}^T$. Hence, to achieve ϵ-DP, the pdf of $\mathbf{n}$ is as follows:

$$\mathbf{Pr}(\mathbf{n} = \mathbf{s}) = \frac{1}{(2\lambda)^T} \exp\left(-\frac{\|\mathbf{s}\|_1}{\lambda}\right). \tag{6}$$

This allows us to denote the noisy load profile by $\mathbf{d}^{'} = \mathbf{d} + \mathbf{n}$. For clustering results with K clusters, we denote the center of each cluster i as $\tilde{\boldsymbol{d}}_{\boldsymbol{i}}$, $i \in \{0, 1, .., K-1\}$. Without loss of generality, we assume the center of the cluster which the consumer of interest belongs to is $\tilde{\boldsymbol{d}}_{\mathbf{0}}$.

We make the following technical alignment assumption for the ease of subsequent analysis.

Assumption 1. $\|\tilde{\boldsymbol{d}}_{\boldsymbol{i}}\|_0 = T, \ \ \forall i \in \{0, 1, .., K-1\}$.

Remark: This assumption simply requires the center load profile of each cluster contains all non-zero elements. This is generally true as most load profiles contain background energy consumption, which renders the center load profiles easy to satisfy this assumption.

We further denote the radius of cluster 0 by r:

$$r = \frac{1}{2} \min_{i \in \{1,\ldots,K-1\}} \|\tilde{\boldsymbol{d}}_{\mathbf{0}} - \tilde{\boldsymbol{d}}_{\boldsymbol{i}}\|_2. \tag{7}$$

We can show that

Theorem 2. If Assumption 1 holds, the probability that the consumer would stay in his original cluster after Laplace noise injection (with parameter λ) is lower bounded by

$$C_0(r)\lambda^{-T+1} \exp\left(\frac{-C(r)}{\lambda}\right), \tag{8}$$

where C_0 and C are constants related to the radius r.

Our Theorem 2 shows that, if the assumption 1 holds which means the center of K-mean could not be the extreme cases, we could derive that probability of the points staying his original clusters after injecting noise could be higher than the form of Eq. 8, where r denotes the radius of the clusters. It actually comes from some mathematical manipulations of the probability function. It shows the staying probability could be related to the noise parameter λ and the radius r. We could know that if we have a higher privacy requirement, we could have a higher λ and the staying probability could decrease. Then we could also find when λ is large, if our r increases, we could derive higher staying probability because the clusters become closer.

Remark: This lower bound characterization is not always tight. In the numerical study, we use this lower bound to construct a more useful empirical asymptotic approximation. In fact, we intend to examine how to construct a much tighter lower bound in our future work, which could provide more theoretical insights on the influential dynamics between ϵ-DP and cluster stability.

IV. Numerical Studies and Practical Discussion

A. Numerical Studies

Based on the aforementioned trimmed Pecan Street dataset, we illustrate how to effectively utilize our proposed lower bound to establish the asymptotic approximation for characterizing the evolution of cluster stability with increasing level of DP.

Specifically, we focus on analyzing the load profile of 30-minute resolution, and employ the standard k-means clustering method to obtain 15 clusters. All follow the discussion in Section II.

Based on the noisy data, we observe the cluster interchange for these 1,000 consumers and empirically calculate the cluster stability. For each DP parameter λ (ranging from 15 to 50, with a step size of 5), we repeat the simulation for 100 times, which help us obtain the percentile information of empirical stability. We plot such information in Fig. 4. In the figure, the yellow full line with yellow percentile denotes the empirical mean frequency of the consumers staying in the original clusters after adding noise and its 10% and 90% quantiles. We could view that for the probability of the consumer staying in his

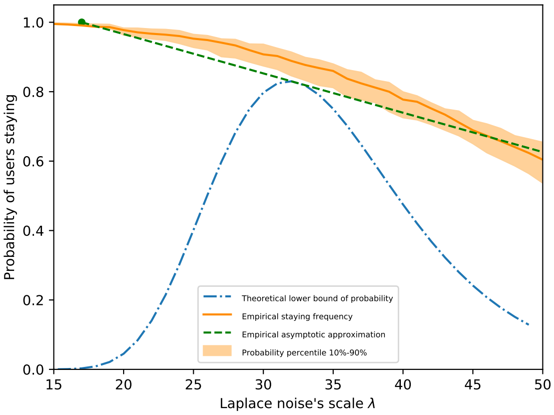

Fig. 4. The relationship between λ and staying probability

original clusters could decrease with the λ, which is consistent with the observation in Fig. 3.

Next, we examine the tightness of our theoretical bound. To fully characterize the bound, we set the overall constant τ [1] to be 490 according to the load profile, and set the radius r to be 0.492. Thus, the lower bound is indicated by the blue dash dot curve on Fig. 4. It is self evident that this bound is not always tight. In fact, it is only tight at its peak point (when λ is 33). The bound is not tight when λ is small due to the use of union bound. It is not tight either when λ is large due to the conservative cluster region selection. Nonetheless, from perspective of magnitude, this bound indicates the polynomial decreasing rate at the tail, which coincides with the numerical results.

Noting the tight bound at the peak point, we can make use of it to construct the asymptotic approximation (green dash line). The straightforward way is to identify another point $(0, 1)$ (the cluster stability is 1 when there is no noise injection), which is a tight lower bound at $\lambda = 0$. Connecting this point and the peak could serve as a better asymptotic approximation. In fact, we can further improve this asymptotic approximation. The key is to observe a breaking point, beyond which the injected noise starts to take effect (in terms of driving the cluster stability significantly away from 1). In our numerical study, this breaking point is $(17, 1)$. When λ is smaller than 17, the stability is almost 1. These three points construct a piece wise linear asymptotic approximation (shown by the dashed green curve in Fig. 4) of the numerical results. Such approximation is often good enough for the consumers to better understand what DP means to them. It is also good enough for the system operator to estimate the impact of injected noise on behavior analysis.

B. Discussion about the practical application

We propose the DP and corresponding mechanism and analyze the influence on the K-means clustering above. In practice, we could use it to measure the variability of the consumer. If we derive the results of clustering, we could analyze for each consumer the probability that he stays in his original cluster under different privacy levels.

For practical applications, we could view from two perspectives. From the consumer's perspective, when he receives the privacy service for a certain privacy level, he would know the risk that he could be treated as another type of consumers. He might be viewed as a nightbird and charged more in the daytime but he is actually a daytime worker. Then he could calculate the probability and expectation he could pay then decide a more rational privacy requirement.

Then from the view of system operator, it could estimate the probability of each consumer's cluster changing through our theoretical bound or empirically constructed asymptotic approximation. Then it could know the potential effectiveness loss caused by the changing. For example, if the system operator uses the tariffs to reduce the peak. If the households exhibiting high evening peak demand are jumping to the noon peak, the higher tariffs at the evening could be less effective. Therefore, the system operator needs to know the possible privacy preservation mechanism for the consumers in detail and then after estimating through our framework, it could design a better tariffs mechanism considering the variability. The same manipulations could also be conducted for the load forecast if we simply assume the probability of changing to different clusters is the same and we could construct the possible distribution of the load. Moreover, for the demand response, the targets selected should considered with the probability. Kwac et al. [31] show that it could be easier to target demand response programmes to a more stable household. Therefore, we could select the target with the enough high probability to stay in the original clusters through our empirically asymptotic approximation, which could be constructed by the break point and the peak of theoretical lower bound.

In general, our proposed framework could be applied into different scenario to help the consumer to accept a suitable privacy service or the system operator to measure the possible risk coming from the privacy preservation and make better decisions.

V. Conclusion

Our paper targets to understand how noise injection mechanism to achieve ϵ-DP may affect the performance of a classical behavior analysis technique: k-means clustering. We first study the granularity selection issue for the dataset, and submit that higher granularity data may not always lead to better results. Then, we examine our core focus from both theoretical and empirical points of view.

Our work could be extended in many interesting ways. From the theoretical point of view, it is interesting to derive a tighter lower bound for the cluster stability. From a practical point of view, it is valuable to examine if our conclusions can be generalized to other privacy preserving mechanisms as well as other behavior analysis techniques.

[1] See Appendix A for more detailed definition of τ, and how it could help decide the constant C_0 and C, together with r.

References

[1] G. W. Hart, "Residential energy monitoring and computerized surveillance via utility power flows," *IEEE Technology and Society Magazine*, vol. 8, pp. 12–16, June 1989.

[2] M. Fell, H. Kennard, G. Huebner, M. Nicolson, S. Elam, and D. Shipworth, "Energising health: A review of the health and care applications of smart meter data," *London, UK: SMART Energy GB*, 2017.

[3] J. R. Herrero, Á. L. Murciego, A. L. Barriuso, D. H. de La Iglesia, G. V. González, J. M. C. Rodríguez, and R. Carreira, "Non intrusive load monitoring (nilm): A state of the art," in *International Conference on Practical Applications of Agents and Multi-Agent Systems*, pp. 125–138, Springer, 2017.

[4] A. Capozzoli, M. S. Piscitelli, and S. Brandi, "Mining typical load profiles in buildings to support energy management in the smart city context," *Energy Procedia*, vol. 134, pp. 865–874, 2017.

[5] S. Lin, F. Li, E. Tian, Y. Fu, and D. Li, "Clustering load profiles for demand response applications," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 1599–1607, 2017.

[6] M.-A. Milton, C.-O. Pedro, S.-G. Xavier, and E.-E. Guillermo, "Characterization and classification of daily electricity consumption profiles: Shape factors and k-means clustering technique," in *E3S Web of Conferences*, vol. 64, p. 08004, EDP Sciences, 2018.

[7] A. Ozawa, R. Furusato, and Y. Yoshida, "Determining the relationship between a household's lifestyle and its electricity consumption in japan by analyzing measured electric load profiles," *Energy and Buildings*, vol. 119, pp. 200–210, 2016.

[8] S. Yilmaz, J. Chambers, and M. K. Patel, "Comparison of clustering approaches for domestic electricity load profile characterisation-implications for demand side management," *Energy*, vol. 180, pp. 665–677, 2019.

[9] O. Motlagh, A. Berry, and L. O'Neil, "Clustering of residential electricity customers using load time series," *Applied Energy*, vol. 237, pp. 11–24, 2019.

[10] M. Backes and S. Meiser, "Differentially private smart metering with battery recharging.," *IACR Cryptology ePrint Archive*, vol. 2012, p. 183, 2012.

[11] Z. Zhang, Z. Qin, L. Zhu, J. Weng, and K. Ren, "Cost-friendly differential privacy for smart meters: Exploiting the dual roles of the noise," *IEEE Transactions on Smart Grid*, vol. 8, no. 2, pp. 619–626, 2017.

[12] F. Farokhi, "Review of results on smart-meter privacy by data manipulation, demand shaping, and load scheduling," *IET Smart Grid*, 2020.

[13] W. Yang, N. Li, Y. Qi, W. Qardaji, S. McLaughlin, and P. McDaniel, "Minimizing private data disclosures in the smart grid," in *Proceedings of the 2012 ACM conference on Computer and communications security*, pp. 415–427, 2012.

[14] Y. Lu and M. Zhu, "Privacy preserving distributed optimization using homomorphic encryption," *Automatica*, vol. 96, pp. 314–325, 2018.

[15] K. Wada and K. Sakurama, "Privacy masking for distributed optimization and its application to demand response in power grids," *IEEE Transactions on Industrial Electronics*, vol. 64, no. 6, pp. 5118–5128, 2017.

[16] A. R. Borden, D. K. Molzahn, B. C. Lesieutre, and P. Ramanathan, "Power system structure and confidentiality preserving transformation of optimal power flow problem," in *2013 51st Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pp. 1021–1028, 2013.

[17] S. R. Rajagopalan, L. Sankar, S. Mohajer, and H. V. Poor, "Smart meter privacy: A utility-privacy framework," in *2011 IEEE international conference on smart grid communications (SmartGridComm)*, pp. 190–195, IEEE, 2011.

[18] W. Wang, L. Ying, and J. Zhang, "On the relation between identifiability, differential privacy, and mutual-information privacy," *IEEE Transactions on Information Theory*, vol. 62, no. 9, pp. 5018–5029, 2016.

[19] H. Cao, S. Liu, L. Wu, Z. Guan, and X. Du, "Achieving differential privacy against non-intrusive load monitoring in smart grid: A fog computing approach," *Concurrency and Computation: Practice and Experience*, vol. 31, no. 22, p. e4528, 2019.

[20] H. Wang and C. Wu, "Understanding differential privacy in non-intrusive load monitoring," in *Proceedings of the Eleventh ACM International Conference on Future Energy Systems*, e-Energy '20, (New York, NY, USA), p. 401–403, Association for Computing Machinery, 2020.

[21] H. Wang, J. Zhang, C. Lu, and C. Wu, "Privacy preserving in non-intrusive load monitoring: A differential privacy perspective," *IEEE Transactions on Smart Grid*, 2020.

[22] Pecan Street INC., "Pecan street data." http://www.pecanstreet.org.

[23] C. G, N. R, P. P, S. M, and T. C, "Customer character-isation options for improving the tariff offer," *IEEE Trans. Power Syst*, vol. 18(1), no. 381-7, 2003.

[24] D. DL and B. DW, "A cluster separation measure," *IEEE Trans. Pattern AnalMachine Intelligence*, vol. PAM-1(2), no. 224-7, 1979.

[25] M. A. Syakur, B. K. Khotimah, E. M. S. Rochman, and B. D. Satoto, "Integration k-means clustering method and elbow method for identification of the best customer profile cluster," *IOP Conference Series: Materials Science and Engineering*, vol. 336, 2018.

[26] R. L. Thorndike, "Who belongs in the family?," *Psychometrika*, vol. 18, no. 4, pp. 267–276, 1953.

[27] M. A. Syakur, B. K. Khotimah, E. M. S. Rochman, and B. D. Satoto, "Integration k-means clustering method and elbow method for identification of the best customer profile cluster," *IOP Conference Series: Materials Science and Engineering*, vol. 336, 2018.

[28] C. Dwork, F. Mcsherry, K. Nissim, and A. Smith, "Calibrating noise to sensitivity in private data analysis," *Lecture Notes in Computer Science*, pp. 265–284, 2006.

[29] H. Kim, M. Marwah, M. Arlitt, G. Lyon, and J. Han, "Unsupervised disaggregation of low frequency power measurements," in *Proceedings of the 2011 SIAM International Conference on Data Mining*, pp. 747–758, 2011.

[30] S. Makonin, F. Popowich, I. V. Bajic, B. Gill, and L. Bartram, "Exploiting hmm sparsity to perform online real-time nonintrusive load monitoring," *IEEE Transactions on Smart Grid*, vol. 7, no. 6, pp. 2575–2585, 2016.

[31] J. Kwac, J. Flora, and R. Rajagopal, "Household energy consumption segmentation using hourly data," *IEEE Transactions on Smart Grid*, vol. 5, no. 1, pp. 420–430, 2014.

[32] A. Olde Daalhuis, D. Lozier, B. Schneider, R. Boisvert, C. Clark, B. Miller, B. Saunders, *et al.*, "Nist digital library of mathematical functions," 2016.

[33] E. Neuman, "Inequalities and bounds for the incomplete gamma function," *Results in Mathematics*, vol. 63, no. 3-4, pp. 1209–1214, 2013.

Appendix

A. Proof for Theorem 2

We fix $\lambda = \frac{\delta}{2\epsilon}$ according to Theorem 1. Denote the original load profile by $\boldsymbol{d}$, and then we could use a normalized vector $\boldsymbol{s} \in \mathbb{R}^T$ to define the pdf $q(\cdot)$ for the normalized demand after noise injection:

$$q(\boldsymbol{s}) = \int_0^{+\infty} \frac{k^{T-1}}{(2\lambda)^T} \exp\left(-\frac{\|k\mathbf{s}-\mathbf{d}\|_1}{\lambda}\right) dk \qquad (9)$$

Then we denote the cluster stability by PL. Specifically, if the profile vector $\boldsymbol{s}$ such that $\|\boldsymbol{s}-\tilde{\boldsymbol{d_0}}\|_2 \leq r$, the profile belongs to cluster 0. This is due to the following triangle inequality:

$$\begin{aligned} \|\boldsymbol{s}-\tilde{\boldsymbol{d_i}}\|_2 \ &\geq \left| \|\boldsymbol{s}-\tilde{\boldsymbol{d_0}}\|_2 - \|\tilde{\boldsymbol{d_i}}-\tilde{\boldsymbol{d_0}}\|_2 \right| \\ &\geq r \geq \|\boldsymbol{s}-\tilde{\boldsymbol{d_0}}\|_2 \end{aligned} \qquad (10)$$

Thus, define $\Theta = \{\boldsymbol{s} | \|\boldsymbol{s}-\tilde{\boldsymbol{d_0}}\|_2 \leq r, \|\boldsymbol{s}\|_2 = 1\}$ as the cluster region for $\tilde{\boldsymbol{d_0}}$. We could derive the lower bound for PL by $PL \geq \int_\Theta q(\boldsymbol{s}) d\boldsymbol{s}$. We need to define a constant τ for all $\boldsymbol{s}$ in Θ, such that $\tau \boldsymbol{s} \geq \boldsymbol{d}$ for all dimensions.

We first derive a lower bound for $q(\boldsymbol{s})$ for $\boldsymbol{s} \in \Theta$. It holds:

$$
\begin{aligned}
q(\boldsymbol{s}) = &\frac{1}{(2\sqrt{T})^T}\exp\left(\frac{\|\mathbf{d}\|_1}{\lambda}\right)\times\\
&\int_{\frac{\tau\sqrt{T}}{\lambda}}^{+\infty}\frac{(k\sqrt{T})^{T-1}}{\lambda^{T-1}}\exp\left(-\frac{k\sqrt{T}}{\lambda}\right)d\left(\frac{k\sqrt{T}}{\lambda}\right)\\
&+\int_0^{\tau}\frac{k^{T-1}}{(2\lambda)^T}\exp\left(-\frac{\|k\mathbf{s}-\mathbf{d}\|_1}{\lambda}\right)dk \qquad (11)\\
\geq &\frac{1}{(2\sqrt{T})^T}\exp\left(\frac{\|\mathbf{d}\|_1}{\lambda}\right)\left(\frac{\tau\sqrt{T}}{\lambda}\right)^{T-1}\exp\left(-\frac{\tau\sqrt{T}}{\lambda}\right)\\
&+\int_0^{\tau}\frac{k^{T-1}}{(2\lambda)^T}\exp\left(-\frac{\|k\mathbf{s}\|_1+\|\mathbf{d}\|_1}{\lambda}\right)dk
\end{aligned}
$$

The inequality is again due to triangle inequality. This expression motivates us to utilize the Leonhard Euler's gamma function [32]. With the characteristics of incomplete Gamma function [33], we have

$$
\begin{aligned}
q(\boldsymbol{s}) \geq &\frac{\tau^{T-1}}{2^T\lambda^{T-1}\sqrt{T}}\exp\left(\frac{\|\mathbf{d}\|_1-\tau\sqrt{T}}{\lambda}\right)\\
&+\frac{1}{(2\sqrt{T})^T}\exp\left(\frac{-\|\mathbf{d}\|_1}{\lambda}\right)\times\\
&\int_0^{\frac{\tau\sqrt{T}}{\lambda}}\frac{(k\sqrt{T})^{T-1}}{\lambda^{T-1}}\exp\left(-\frac{k\sqrt{T}}{\lambda}\right)d\left(\frac{k\sqrt{T}}{\lambda}\right)\\
&\geq\frac{\tau^{T-1}}{2^T\lambda^{T-1}\sqrt{T}}\exp\left(\frac{\|\mathbf{d}\|_1-\tau\sqrt{T}}{\lambda}\right)\\
&+\frac{1}{(2\sqrt{T})^T}\exp\left(\frac{-\|\mathbf{d}\|_1}{\lambda}\right)\frac{(\frac{\tau\sqrt{T}}{\lambda})^T}{T}\exp\left(\frac{-T\sqrt{T}\tau}{\lambda(T+1)}\right)\\
&=\frac{\tau^{T-1}}{2^T\lambda^{T-1}\sqrt{T}}\exp\left(\frac{\|\mathbf{d}\|_1-\tau\sqrt{T}}{\lambda}\right)\\
&+\frac{\tau^T}{(2\lambda)^T T}\exp\left(-\frac{\|\mathbf{d}\|_1}{\lambda}-\frac{T\sqrt{T}\tau}{\lambda(T+1)}\right)
\end{aligned}
\tag{12}
$$

Note that the n-dimensional volume for Euclidean ball with radius r is $V_n(r)=\frac{\pi^{n/2}}{\Gamma(\frac{n}{2}+1)}r^n$. This helps us to construct the lower bound for PL as follows:

$$
\begin{aligned}
PL \geq &\int_{\Theta} q(\boldsymbol{s})d\boldsymbol{s}\\
&\geq\frac{\tau^{T-1}\pi^{\frac{T-1}{2}}r^{T-1}}{2^T\lambda^{T-1}\sqrt{T}\Gamma(\frac{T+1}{2})}\exp\left(\frac{\|\mathbf{d}\|_1-\tau\sqrt{T}}{\lambda}\right)\\
&+\frac{\tau^T\pi^{\frac{T-1}{2}}r^{T-1}}{(2\lambda)^T T\Gamma(\frac{T+1}{2})}\exp\left(-\frac{\|\mathbf{d}\|_1}{\lambda}-\frac{T\sqrt{T}\tau}{\lambda(T+1)}\right)\\
&\geq C_0(r)\lambda^{-T+1}\exp\left(\frac{-C(r)}{\lambda}\right),
\end{aligned}
\tag{13}
$$

where

$$
C_0=\frac{\tau^{T-1}\pi^{\frac{T-1}{2}}r^{T-1}}{2^T\sqrt{T}\Gamma(\frac{T+1}{2})},\ \text{and}\ C=\tau\sqrt{T}-\|\mathbf{d}\|_1. \tag{14}
$$

This completes the proof of Theorem 2 .