2021-03-04

DPNCT: A Differential Private Noise Cancellation Scheme for Load Monitoring and Billing for Smart Meters

Khadija Hafeez
Department of Computer Science, Munster Technological University, Bishopstown Campus, Cork, Ireland

Mubashir Husain Rehmani
Department of Computer Science, Munster Technological University, Bishopstown Campus, Cork, Ireland

Donna OShea
Department of Computer Science, Munster Technological University, Bishopstown Campus, Cork, Ireland

Recommended Citation

Khadija Hafeez, Mubashir Husain Rehmani, Donna O'Shea, 'DPNCT: A Differential Private Noise Cancellation Scheme for Load Monitoring and Billing for Smart Meters' to appear in IEEE International Conference on Communications (ICC) 2021 - Workshop on Communication, Computing, and Networking in Cyber-Physical Systems (IEEE CCN-CPS 2021), Montreal, Canada, June 2021.

2021-03-24

DPNCT: A Differential Private Noise Cancellation Scheme for Load Monitoring and Billing for Smart Meters

Khadija Hafeez

Mubashir Husain Rehmani

Donna OShea

DPNCT: A Differential Private Noise Cancellation Scheme for Load Monitoring and Billing for Smart Meters

Khadija Hafeez*, Mubashir Husain Rehmani*, Donna O'Shea*
* Munster Technological University (MTU), Cork, Ireland

***Abstract*—Reporting granular energy usage data from smart meters to power grid enables effective power distribution by smart grid. Demand Response (DR) mechanism incentivize users towards efficient use of energy. However, consumer's energy consumption pattern can reveal personal and sensitive information regarding their lifestyle. Therefore, to ensure users privacy, differentially distributed noise is added to the original data. This technique comes with a trade off between privacy of the consumer versus utility of the data in terms of providing services like billing, Demand Response schemes, and Load Monitoring. In this paper, we propose a technique - Differential Privacy with Noise Cancellation Technique (DPNCT) - to maximize utility in aggregated load monitoring and fair billing while preserving users' privacy by using noise cancellation mechanism on differentially private data. We introduce noise to the sensitive data stream before it leaves smart meters in order to guarantee privacy at individual level. Further, we evaluate the effects of different periodic noise cancelling schemes on privacy and utility i.e., billing and load monitoring. Our proposed scheme outperforms the existing scheme in terms of preserving the privacy while accurately calculating the bill.**

***Index Terms*—Differential Privacy (DP), Smart Grid (SG), Demand Side Management (DSM), Privacy Preservation.**

I. Introduction

The term Cyber Physical System (CPS) refers to large scale intelligent, reactive and highly configurable hybrid system which has both physical and computational properties. In smart grids, CPS is enabled through smart meters, which are entities that collect end user consumption data at high frequency in real time, transmitting this data to the utility grid provider. Such real time collection of end-user data facilitates Demand Response (DR) schemes which influence the customer demand of energy usage from peak time to off peak time for better distribution and generation of load. The issue is that such DR schemes and detailed collection of energy usage data can reveal sensitive and private information regarding consumer's life style [1].

Molina-Markham et al. [2] shows that the power consumption pattern can reveal personal information including, but not limited to, the time periods when the consumer is not at home, the type of electrical devices that are being used at a household, and any change in the habits of the consumer such as sleeping and eating. This information can be used for targeted marketing and can pose a serious security threat to the consumer.

In order to address the challenge of privacy invasion, Differential Privacy (DP) first proposed by Dwork et al. [3], is a mechanism that adds noise to the critical data in a way that addition, deletion or change in an individual record makes insignificant difference to the overall output. A central architectural component of DP is an aggregator which acts as an intermediary between smart meter and power grid, which collects the smart meter data at a network level and provides services, including but not limited to bill calculation of individuals, load monitoring, and enforcement of DR schemes. The goal of using DP for smart meter data is to release the statistics to the aggregator for critical decision making in DR schemes while preserving user's privacy. The challenge associated with this goal is how to provide a mechanism that preserves individual user privacy, enabling the aggregator to calculate total energy consumption of all smart meters in an area at an instant in time t and individual users over a period of time T.

In the past, different proposals by Eibl et al [5] and Won et al [8] focus on providing privacy on aggregated data where differentialy perturbed noise is added at trusted aggregator level, protecting user's privacy in the aggregated data. For example, if adversary knows the aggregated data, it can not deduce sensitive information from it. The problem with this approach, is that privatizing aggregated data does not guarantee complete privacy of individuals as unprotected non private aggregated smart meter data can still reveal some critical information about the users [9]. To address this challenge Hassan et al. [6] introduced the Differentially Private Dynamic Pricing for Demand Response (DRDP) scheme, providing individual level privacy. In this scheme the smart meters send original data to the trusted aggregator which masks the data using distributed noise and reports the data to the utility grid along with the billing information. The trusted aggregator stores and calculates the bill according to the original data. The challenge with DRDP, is that it assumes the aggregator as a trusted entity, which introduces significant security risks.

Given the above context in this paper we propose a Differential Privacy with Noise Cancellation Technique (DPNCT) scheme, that assumes the aggregator entity is untrusted which may attempt to invade the privacy of users. In this paper, we will demonstrate how DPNCT achieves accuracy in billing and load monitoring ensuring users' privacy without the use of a trusted third party aggregator. As part of our analysis we

TABLE I: Comparison of Techniques for Privacy Preserving using Differential Privacy in smart meters

Ref. No	*Focus*	*Privacy Type*	*Working Mechanism*	*Limitation*
[4]	Differential Privacy without trusting third party	Differential Privacy with Encryption	Multiple exchange of encrypted messages with aggregator for differentially private data	Partial fault tolerance, Increased utilization of bandwidth, Privacy for aggregated data only
[5]	Infinite Divisibility of Laplacian Noise with post processing smoothing	Differential Privacy	Adding gamma distributed noise to each individual agent using infinite divisible laplace distribution	Privacy for Aggregated information only
[6]	Dynamic Pricing and Privacy	Differential Privacy	Dual Differential Privacy with Dynamic pricing using trusted third party	Too much trust on third party for storing real data and calculation of bills, No analysis on the usability of differentially private data at grid level
[7]	Privacy for Appliance Usage	Differential Privacy	Differential privacy using Laplacian noise with filtering attack analysis to preserve appliance usage privacy	Reduced accuracy in utility
[8]	Fault Tolerance	Differential Privacy with Encryption (Modular addition)	Differential privacy using Laplacian noise with current and future cipher text for fault tolerance with modular additive encryption	Computationally Complex, No privacy for individuals
[9]	Analysis of Accuracy vs Privacy	Differential Privacy	Finding balance at individual level privacy with increased data points for decrease in billing error	Reduced accuracy in utility
[10]	Privacy with State Estimation	Differential Privacy	Analysis of State estimation vs individual Privacy using differential privacy	Lack of analysis on the impact of differential noise on billing

have benchmarked DPNCT against DRDP [6] with different noise cancellation schemes (hourly, daily, and weekly) on total power consumption at an instant t for load monitoring and total consumption of an individual over a period of time T.

The rest of the paper is organized as follows. Section II discuss the related work and how our solution differs from them. In section III, we present our proposed solution along with algorithm and example. In section IV, we discuss the performance analysis of our scheme and finally conclude the discussion in section V.

II. Literature Review

Table I, gives an overview of the comparison of different privacy solutions for smart grid using DP. [5], [8] provides privacy for the aggregated data only using infinite divisibility of Laplacian distribution. As previously mentioned the challenge with these approaches is that protected aggregated data still can leak useful information regarding individuals. In order to address this issue, Acs et al [4] use cryptography schemes, which relies on users sharing cryptographic keys or $ciphertexts$ with each other, which is difficult to manage as the systems scales. Won et al. [8] builds upon the solution provided by [4] to address the scalability issue and provides fault tolerance by introducing modular additive encryption. Using this approach, smart meters send private data with current and future $ciphertexts$ to cater for future transmission failure, helping system to run smoothly even in scenarios when smart meter fails to share its $ciphertext$. The challenge with the solutions outlined above is that even though they provide DP, their implementation makes them computationally complex and expensive. The most relevant work in smart grid privacy using purely differential privacy is [6], [7], [9] where they used Laplacian distribution for generation of noise for individual level privacy. Barbosa et al. [7] used filtering time series attack to validate appliance usage privacy of individual consumers. Trajectory level privacy technique is used by Hale et al. [9] which protects sensitive smart meter data over a period of time at an individual level and analyze the cost of privacy over accuracy in billing and aggregated load monitoring. By not using a trusted third party [7], [9], introduce a certain level of inaccuracy in bills for the users as a cost of privacy. The authors from [6] provide usage based dynamic billing along with differential privacy at aggregator level. The noise is generated at the aggregator level and then added to individual data points before sending it to the grid utility. For dynamic billing, the aggregated load is compared with peak allowed load and only the individuals who are responsible for peak load are charge. However, they depend on a trusted third party and assume a "curious but honest" aggregator to provide privacy. In contrast, in our approach we do not make this assumption, and instead we provide individual level privacy at the smart meter level, before it reaches the aggregator component. In addition, our solution also includes a noise cancellation technique to deal with the error in dynamic billing and load monitoring.

III. Proposed Solution: DPNCT

In this section we present our novel solution along with preliminary information of DP as privacy preserving technique.

A. System Model

Our model illustrated in Figure 1, shows three main physical entities: smart meters, aggregators, and utility grid. To calculate total energy consumption in an area at an instant t, the aggregator receives differentialy private energy consumption data of each user transmitted by smart meters. However, this data alone does not provide accurate information of total load

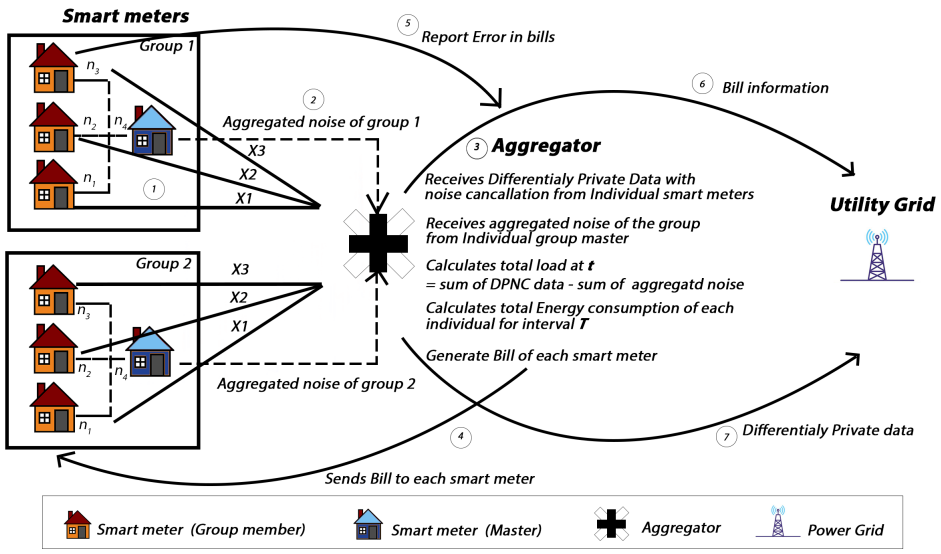


Fig. 1: System Model: All smart meters send DPNCT masked data to aggregator and group master sends aggregated noise of the group to the aggregator which is subtracted from total masked data to get true aggregated load.

TABLE II: Key Notations and their Description used in Algorithm 1 and 2

Key	Description	Key	Description
$mIDs$	IDs of all master smart meters	Er_{T-1}	Error in previous bill reported by smart meters
N	Total number of smart meters	N_K	Aggregated group noise
x_t	Original load consumption of the household at time t	Δt	chosen scheme in DPNCT (Hourly, Daily, Monthly)

at an instant t due to the addition of noise in the data at smart meter level. To deal with this issue, smart meters send their added noise at time t to a randomly selected master smart meter shown as blue house in the Figure 1. The master smart meter then accumulates this noise from all member smart meters in the group and sends it to the aggregator where this accumulated noise gets subtracted from aggregated private data. This process gives an accurate information of total energy consumption at an instant t for load monitoring. To calculate total energy consumption of an individual we propose a noise cancelling DP mechanism (DPNCT), where in addition to adding Laplacian noise $n_{\Delta t}$ in time period Δt, each user subtracts the noise nc added in $\Delta t - 1$. As a demand response scheme, aggregator checks if the total energy consumption of a single user is more then $maximumAllowedUnits$ set by grid utility, then instead of base unit price, aggregator charges surcharge price for the extra units. However, if the user gets surcharged price due to added noise then the error is corrected in the next bill.

B. Differential Privacy

As proposed by Dwork et al. [3] differential private noise gives ϵ privacy for a mechanism, M, if for any two neighbouring data-sets $D1$ and $D2$ which differ in at most one record

Algorithm 1: Calculation of Bill and Aggregated Load at Aggregator

```
Function AggregatedLoadCalculation();
begin
    Input: mIDs
    while Billing Period T do
        for all smart meters i in N do
            X_i = getMaskedData(i);
        end
        for masterID in mIDs do
            N_K = getNoiseData(masterID);
        end
        totalLoad_t = Σ_{i=1}^{N} X_i − Σ_{i=1}^{K} N_i ;
    end
end
Function BillCalculation();
begin
    Input:
          maxUnits, SurchargePrice, UnitPrice, Er_{T−1}
    for all smart meters i in N do
        if Σ_i^T X_i ≥ maxAllaowedUnits then
            surchargeUnits =
              Σ X_i − maxAllaowedUnits;
            BaseBill = maxAllaowedUnits * UnitPrice;
            SurchargeBill =
              surchargeUnits * SurchargePrice;
            TotalBill_i
              =BaseBill + SurchargeBill − Er_{T−1};
            Notify TotalBill_i and surchargeUnits to
              smart meter i;
        else
            TotalBill_i = Σ X_i * UnitPrice;
            Notify TotalBill_i to smart meter i ;
        end
    end
end
```

TABLE III: Comparison of DPNCT with DRDP

Feature	DRDP [6]	DPNCT
Aggregator-to-grid anonymity	Yes	Yes
Dynamic Billing	Yes	Yes
User-to-Aggregator anonymity	No	Yes

Algorithm 2: Differential Privacy With Noise Cancellation at Smart Meter

```
Function DPNCT();
begin
    Input: x_t, ID, Δt, masterID_t, totalBill, surchargeUnits
    N_{t-1} = N_t;
    N_t = 0;
    while Time Period Δt do
        n_t = G(N,λ) - G'(N,λ);
        N_t = Push(n_t);
        nc_{t-1} = Pop(N_{t-1});
        X_t = x_t + n_t - nc_{t-1};
        Send X_t to aggregator ;
        if masterID_t = ID then
            for all k smart meters in group do
                get noise n_{k,t} from member smart meter;
            end
            Report aggregated group noise Σ_k n_{k,t} to
              aggregator
        else
            Send n_t to master smart meter with masterID_t
        end
    end
    if surcharge Reported By Aggrgator then
        if SurchargeUnits ≥ TotalNoisein Δt then
            Error = TotalNoise
        else
            Error = SurchargeUnits ;
        end
        Notify Error To Aggregator ;
    else
        Error = 0;
    end
end
```

and for all possible answers $S \subseteq Range(M)$, the following equation holds true.

$$Pr(M(D1) \in S) \leq e^{\epsilon} * Pr(M(D2) \in S) \tag{1}$$

In simpler terms, it is unlikely that an adversary finds out anything meaningful from smart meters data-set that is differentially private where ϵ is the privacy parameter controlled by user ranges from 0 to 1. The lesser the value of ϵ the more private the data would be but, with less utility.

1) Sensitivity: Sensitivity of a function f is defined as maximum difference in output of any two neighbouring datasets. In our case, we can make use of pointwise sensitivity, explained in detail by Eibl and Engel [5], where each data smart meter i at time t generates noise $n_{i,t}$ independently irrespective of the data of other smart meters.

$$S_{pw} = max_{D1,D2}|f(D1) - f(D2)| = max_{i,t}|x_{i,t}| \tag{2}$$

So the query at time t is $\epsilon_t = \epsilon/t$ private such that $\sum \epsilon_t = \epsilon$ where sensitivity for the data would be maximum consumption by any smart meter at all time. Selection and analysis of different sensitivity strategies is out of scope of this paper's work.

2) Infinite divisibility of Laplace distribution: For the privacy of individual consumer we need to add noise at each smart meter before reporting the data to the aggregator. We use Laplacian noise due to its property of infinite divisibility as each smart meter will add noise on their own independently without any prior knowledge of other smart meters. Infinite divisibility of Laplace distribution states that if a random variable is sampled from the probability distribution function of Laplace distribution that is: $f(x, \lambda) = 1/2(e^{|x|/\lambda})$, then the distribution is infinitely distributed for $N \geq 1$,

$$Lap(\lambda) = \sum_{i=1}^{N}(G(N, \lambda) - G'(N, \lambda)) \tag{3}$$

Where G and G' are independent and identical distributed gamma density functions with same parameters. N is the number of smart meters at network level and λ is drawn on the basis of ϵ and point wise sensitivity. Equation 3 implies that at an instant t the aggregated noise of all smart meters would be equal to $Lap(\lambda)$ when using gamma density function.

C. Differentially Private Noise Cancellation Mechanism

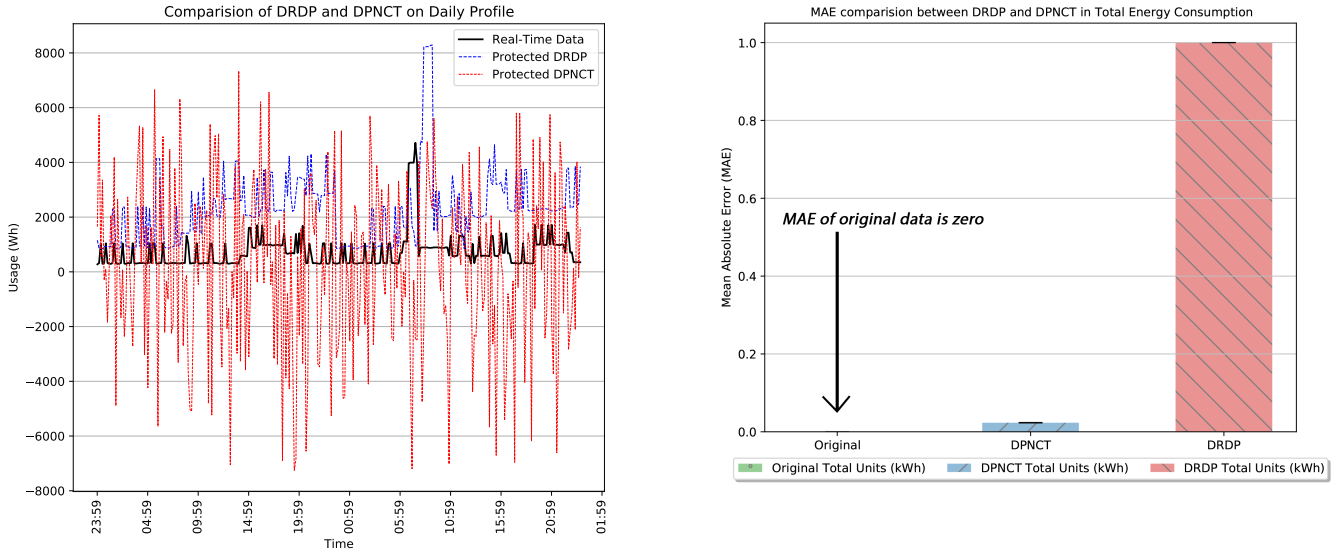
We assume that our smart grid model has N smart meters and one aggregator. Each smart meter i records its power consumption reading $x_{i,t}$ in kWh at an instant t. Since, aggregator does not need to know the individual consumption of users, each smart meter i adds gamma noise to its original energy consumption data at time t i.e. $x_{i,t} + (G(N, \lambda) - G'(N, \lambda))$ and sends this masked data to the aggregator. Using 3, the masked data $X_{i,t}$ of N smart meters gives differential privacy of ϵ when aggregated as follows.

$$\sum_{i=1}^{N} x_{i,t} + (G(N, \lambda) - G'(N, \lambda)) = \sum_{i=1}^{N} x_{i,t} + Lap(\lambda) = \sum_{i=1}^{N} X_{i,t} \tag{4}$$

However, to increase the accuracy of aggregated load at an instant t, we use aggregated noise cancellation protocol. In this protocol, each smart meter is assigned an ID by aggregator and in each round K groups are formed. Each group has k out of N smart meters randomly selected. A master k_i is selected randomly in each group and all members send their noise to the master which then send the aggregated group noise to the aggregator. The aggregator subtract the aggregated group noise i.e., $\sum_{i=1}^{k} n_{i,t}$ from total masked values ($X_{i,t}$) to get accurate load at time t as follows.

$$\sum_{i=1}^{n} X_{i,t} - \sum_{i=1}^{k} n_{i,t} = \sum_{i=1}^{n} x_{i,t} \tag{5}$$

In order to improve accuracy in billing, each smart meter records noise added to the smart meter data over a period of time Δt. Each smart meter generate gamma noise $n_{i,t}$ independently using 3 and adds it to the original data before reporting to the aggregator. The total noise added in Δt is



(a) (b)

Fig. 2: Evaluation of differential privacy and comparison of DRDP and DPNCT with real-time daily profile of a randomly selected house. Fig. 2(a) shows comparison of DRDP and DPNCT with real-time data. This graph shows that the daily usage is well masked by both DRDP and DPNCT schemes. But with DPNCT, the masking is much better. Fig. 2(b) shows comparison of MAE between Original Unprotected data, DRDP, and DPNCT in total energy consumption.

subtracted from the smart meter data in the next period of time Δt to cancel the overall effect of noise in billing. We will see the effect of selecting this time period Δt schemes in performance evaluation section. The protocol is further elaborated in Algorithm 2 with the help of Table II.

IV. Performance Analysis

In this section, we evaluate our algorithm for privacy and accuracy. The experiments are performed over the energy consumption data provided by [11] and results are compared with the benchmark set by DRDP [6]. In [11] residential energy profiles in watts of 200 households with the granularity of 10 minutes is provided which gives $T = 6{*}24{*}30 = 4,320$ data points per month for a single household. For implementation of DPNCT we used Numpy library of Python 3.0 (cf. https://numpy.org). For simplicity, we used $\epsilon = 1$ and point-wise sensitivity $max_{i,t}|x_{i,t}|$ with $mean = 0$ to calculate scale parameter λ for Laplacian noise generation. The complexity cost of generating a random number is $O(1)$ and our algorithm adds a random number i.e., noise n_t at each reading $x_{i,t}$ so the complexity of our Algorithm per smart meter is $O(N)$, N being the total number of data points in time period T. For noise cancellation, we keep track of the noise added in previous period Δt_{t-1} and the same noise is then subtracted in the next period Δt_t. We compare noise cancelling schemes with Δt as hourly, daily, and weekly. For dynamic billing we set $MaxAllowedUnits$ to be $5500kWh$ and $Unit$ and $SurchargePrice$ to be 10$ and 20$ respectively. All the experiments were performed 20 times and the average of them is taken as to normalise the nature of randomness in the noise cancellation and noise generation.

In the Figure 2, we compare our DPNC Technique with the results of DRDP strategy used by [6] on the daily profile of a randomly chosen single user. In the given Figure 2a, the solid black line denotes original real-time data and the dotted blue line shows protected data by DRDP, the dotted red line depicts DPNCT protected data. The masking effect of noise added by DPNCT technique has close to none correlation (0.11, 1 being the highest correlation) with the real-time data profile. This low correlation depicted in 2a, means that an adversary cannot infer a users behaviour and life style patterns, ensuring the privacy of user data patterns generated without the underlying assumption of a trusted third party aggregator.

As demonstrated in the Table III, our proposed DPNCT, ensures user-to-aggregator anonymity as an additional feature over DRDP. We calculated Mean Absolute Error (MAE) in total energy consumption of a single household as follows:

$$MAE = \sum_{i=1}^{N} \frac{|x_i - X_i|}{x_i} \tag{6}$$

Where $|x_i - X_i|$ is the absolute error between sum of real values and total DPNC masked values of a household. In Figure 2b, we compare MAE in total energy consumption of a single household between DPNCT hourly scheme and DRDP. The impact of DPNCT schemes on the utility goals of smart metering data i.e., billing and load aggregation for load monitoring and dynamic pricing, is analysed in the following subsections.

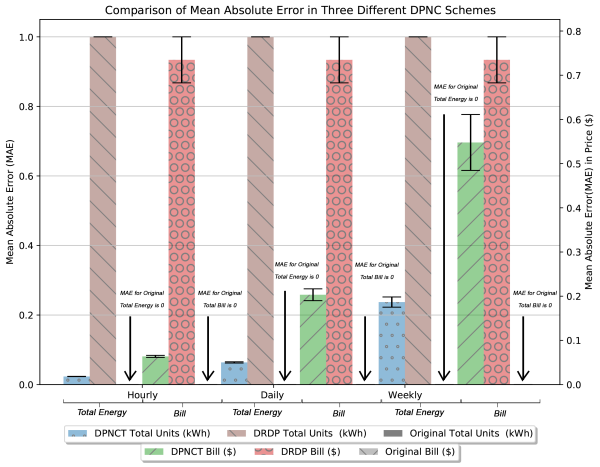


Fig. 3: Comparison of Mean Absolute Error in different schemes of DPNCT for total consumption and dynamic bill of a randomly selected household.

1) Billing: For billing period T, if a single meter i with energy consumption $x_{i,t}$ provides the ϵ_i differential privacy at an instant t then the total error in the bill would be noise $Lap(\lambda)_{\Delta t}$ added in the last Δt of the billing period T, where Δt can be an hour or a day or a week, according to the selected noise cancellation technique. In Figure 3, we compare different noise cancellation period schemes i.e., hourly, daily, and weekly. We calculated Mean Absolute Error (MAE) in total energy consumption (kWh) of a arbitrarily selected single household. In Figure 3, we also compared the effect of different schemes on our dynamic billing scheme. The MAE in hourly noise cancellation scheme for total energy consumption was the lowest (0.045) because of the least amount of noise left at the end of the billing period. For example, in hourly noise cancelling scheme, if a total noise n_{t1} of $7kWh$ is added in the hour $12:00-01:00$ then the cancelling noise of exact same amount i.e., $7kWh$ is subtracted in the next hour $01:00-02:00$. The MAE at the end of billing period for hourly noise cancellation scheme was the lowest (0.06) because the bill only has small error added due to the addition of noise in the last hour of last day of the billing period. The MAE in total energy consumption of daily and weekly schemes are 0.2 and 0.5 respectively. As the error in bill is reported to the aggregator and it gets corrected in the next billing period, the customer sees no impact in terms of billing given the operation of the DPNCT Algorithm 1.

2) Load Monitoring: For Load Monitoring at an instant t, each $x_{i,t}$ provides the ϵ_t at instant t then the total privacy would be $\sum \epsilon_t$. In best case scenario, the average error in aggregated load would be zero due to aggregated noise cancellation as all the k groups send aggregated noise at an instant t. However, in worst case scenario where no accumulated noise would be reported by any group then the total noise at an instant t would be $Lap(\lambda)$. This means the worst case scenario can be improved by selecting robust value for sensitivity instead of overall maximum. Different statistical techniques are used by [8], [9] to increase the utility of aggregated load, which is one of our future goals.

V. Conclusion

In this paper, we proposed a privacy preserving solution for smart meters with maximum utility for bill calculation and aggregated load monitoring using noise cancellation technique. Further, we cancel the effect of noise on the surcharge billed to the customer due to the added noise. In this way, minimizing the financial impact of privacy on the costumer while preserving the privacy. DPNCT provides 5% MAE in total energy consumption and 6% in billing as compared to DRDP which provides 100% MAE in total load consumption and 70% in billing. Similarly, privacy at the individual level precludes the requirement of a trusted third party and ensures that adversary will not be able to deduce users' life style and sensitive behavioural information from collected data. In future, we will work on the selection of sensitivity and analysis of its impact on aggregated load monitoring.

Acknowledgement

This publication has emanated from research conducted with the financial support of Science Foundation Ireland (SFI) and is funded under the Grant Number 18/CRT/6222.

References

[1] M. A. Lisovich, D. K. Mulligan, and S. B. Wicker, "Inferring personal information from demand-response systems," *in IEEE Security Privacy*, vol. 8, no. 1, pp. 11–20, 2010.

[2] A. Molina-Markham, P. Shenoy, K. Fu, E. Cecchet, and D. Irwin, "Private memoirs of a smart meter," in *Proceedings of the 2nd ACM Workshop on Embedded Sensing Systems for Energy-Efficiency in Building*, ser. BuildSys '10, New York, NY, USA, 2010, p. 61–66.

[3] C. Dwork, A. Roth *et al.*, "The algorithmic foundations of differential privacy." *Foundations and Trends in Theoretical Computer Science*, vol. 9, no. 3-4, pp. 211–407, 2014.

[4] G. Ács and C. Castelluccia, "I have a dream! (differentially private smart metering)," vol. 6958 LNCS, 2011.

[5] G. Eibl and D. Engel, "Differential privacy for real smart metering data," *Computer Science - Research and Development*, vol. 32, p. 173–182, 2017.

[6] M. U. Hassan, M. H. Rehmani, and J. Chen, "Differentially private dynamic pricing for efficient demand response in smart grid," in *IEEE International Conference on Communications (ICC)*, 2020, pp. 1–6.

[7] P. Barbosa, A. Brito, and H. Almeida, "A technique to provide differential privacy for appliance usage in smart metering," *Information Sciences*, vol. 370-371, 2016.

[8] J. Won, C. Y. T. Ma, D. K. Y. Yau, and N. S. V. Rao, "Privacy-assured aggregation protocol for smart metering: A proactive fault-tolerant approach," *IEEE/ACM Transactions on Networking*, vol. 24, no. 3, pp. 1661–1674, June 2016.

[9] M. Hale, P. Barooah, K. Parker, and K. Yazdani, "Differentially private smart metering: Implementation, analytics, and billing," in *Proceedings of the 1st ACM International Workshop on Urban Building Energy Sensing, Controls, Big Data Analysis, and Visualization*, ser. UrbSys'19, New York, NY, USA, 2019, p. 33–42.

[10] H. Sandberg, G. Dán, and R. Thobaben, "Differentially private state estimation in distribution networks with smart meters," in *2015 54th IEEE conference on decision and control (CDC)*, 2015, pp. 4492–4498.

[11] M. Muratori, "Impact of uncoordinated plug-in electric vehicle charging on residential power demand-supplementary data." *National Renewable Energy Laboratory-Data (NREL DATA),Golden, CO (United States)*, 2017.