Published in *Proceedings of the 18th International Conference on the European Energy Market (EEM)*, Ljubljana, Slovenia, 13-15 September 2022, which should be cited to refer to this work.
DOI: 10.1109/EEM54602.2022.9921095

Pricing Differentially Private Smart Meter Data in Distribution Networks

Mohammad Rayati, Mokhtar Bozorg
School of Engineering and Management Vaud (HEIG-VD)
Yverdon-les-Bains, Switzerland
{mohammad.rayati, mokhtar.bozorg}@heig-vd.ch

***Abstract*— More electrification in the mobility and building sectors, as well as increased electricity generation from distributed renewable energy sources such as household photovoltaic systems, are two of the most promising paths toward a more environmentally sustainable energy system. Electric power distribution system operators (DSOs) must improve the network's observability in this context to address a variety of technical and market-related concerns, including local network congestion, flexibility exchanges, and resource allocation. To achieve this goal, DSOs are installing smart meters at end-users' locations, as well as measuring devices and monitoring systems on low and medium-voltage networks. Despite the fact that smart meters are an important part of this transformation, privacy laws prevent data from being used for anything other than normal operation and billing without the consent of end-users. We present a model for dealing with differentially private data from smart meters. After that, we present an optimization problem for pricing such differentially private smart meters data, taking into account the value generated for the DSO through state estimation. Using real-anonymous smart meter data from a DSO in Switzerland, we evaluate the effectiveness of our suggested mechanism for buying such differentially private data.**

***Index Terms*— Data pricing, distribution network, smart meter, privacy.**

I. INTRODUCTION

In recent decades, smart meters have gradually replaced conventional meters. The smart meters were designed with the purpose of automatically reading and billing end-users' consumption [1]. However, thanks to the large number of time-series collected and the advancement of data-analytics tools, a broader range of applications are now envisaged [2]. They enable distribution system operators (DSOs) to efficiently operate the network for accommodating increasing renewable energy penetration and significant growth in the electric mobility sector. These new potential applications are consistent with the digitalization goals in distribution networks outlined by the European network of transmission system operators for electricity (ENTSO) for collaboration between transmission system operators (TSOs) and DSOs [3].

Some of these applications cannot be executed on the smart meter's edge. To apply a centralized algorithm, we must transfer the data to a remote server. One such application is state estimation. DSOs can employ state estimation to use the network's unused flexibility and, as a result, engage in the flexibility markets [4]. It is worth mentioning that involvement of DSOs in flexibility markets is restricted by legislation in some networks, whilst other entities known as aggregators only have the option of selling flexibility in distribution network [5].

A review of distribution system state estimation may be found in [6] and [7]. A suitable state estimation technique has been proposed in [8] to maximize the accuracy of the estimation based on data from smart meters. In [9], a cloud-based architecture has been proposed for centralizing smart meter data, allowing DSOs to combine various services based on a distributed state estimate algorithm. Other in-field measurement devices, such as smart meters, can be included to improve the estimation result. A near-optimal placement of several in-field measuring devices has been found in [10] and [11], improving the conventional state estimation results.

The studies stated above do not take into account the fact that smart meter data contains sensitive information about end-users, including as occupancy and consumption patterns [12]. There are various approaches for forecasting such information from historical data, such as those outlined in [13], [14], and [15]. To overcome this issue, data privacy must be addressed from both a regulatory and a technical standpoint [16] and [17]. In Switzerland, article 8 of the power supply regulation [18] is designed to protect the privacy of end-users with relation to measurement systems and information processing. A directive for the security of data from measurement and smart systems was also released in 2018 [19]. As a result, in each distribution network company, there are few trusted people who has access to historical measurement of smart meters data and they are obliged not to use that data for purposes other than billing and normal operation of the network [20].

There are numerous approaches to resolve the conflict of the end-users and DSO. The first approach legitimate applications (like those outlined in [21]) that helps the entire network and not just the DSO or a third party. The second approach is based on anonymization of smart meter data, which prohibits the DSO from anticipating the behavior of each end-user individually. In [22], an anonymization mechanism has been developed for sending sensitive smart meter data to a third-party, who does a network simulation and analysis for the DSO. However, each end-user assessed by a smart meter has a distinct assessment of the cost of privacy loss, which the anonymization techniques do not address. The third approach for dealing with the aforementioned issue is based on a differential privacy framework that may be used to model the privacy valuation functions of different end-users. The value of sharing differentially private smart meter data has been assessed in [23]. A differential privacy compliant algorithm has been created in [24] to ensure that the smart meters data privacy is preserved.

Note that even if privacy is ensured and sharing such data could benefit everyone, data owners (i.e., the monitored end-users) may be unwilling to disclose their differentially private smart meter data. Furthermore, if we analyze the alternatives, such as installing extra in-filed measurement devices in the network rather than purchasing such private data, extra measurement devices will have impacts on end-users' privacy.

In this paper, we first present a model of differential private smart meter data. Then, an optimization problem is introduced for pricing private data of smart meters while taking into account the benefits for the DSO to have a better network state estimation. Furthermore, the cost suffered by end-users as a result of losing their privacy has been considered. Importantly, the proposed mechanism preserves the end-users' right to decide whether or not to share their data, even when their privacy is maintained at a predetermined level.

The rest of this paper is organized as follows: Section II presents the mathematical formulation of the models for network and end-users' privacy. Section III proposes problem and its solution by formulating the network's state estimation problem and the optimization problem for pricing private smart meter data. Section III also includes an algorithm for solving the described optimization problem. Section IV contains a case study, followed by a conclusion in Section V.

II. Mathematical Formulation of Model

Consider a distribution network with nodes and lines denoted by $l \in L$. The node below line l is denoted by l, while the node above line l is marked by $l^{(up)}$. Each end-user is identified by $d \in D$ and has active and reactive consumption p_{dt} and q_{dt} at time $t \in T$. It is worth mentioning that end-user d could be a prosumer, implying that p_{dt} could be negative during production hours.

Fig. 1 displays an example of distribution network. The network is assumed to be radial, and the series and shunt impedances of lines are assumed to be known and equal to $(r_l + \mathrm{j} \cdot x_l)$ and $(2 \cdot \mathrm{j} \cdot b_l)$ for each line l. The slack node, denoted by $l = 0$, is the point at which the distribution network connects to the transmission system.

The goal of DSO is to estimate the state of the network, including $(u_{lt}, p_{lt}, q_{lt})_{l\in L, t\in T}$, where u_{lt}, p_{lt}, and q_{lt} are the voltage of the node l and the active/reactive power of the line l at downstream, respectively. To that purpose, the DSO has two options for improving the network observability:

1. The DSO might install the potential measurement device $m \in M$ at a cost of c to measure the voltage, active, and reactive power of the associated branch and node with an error of $\delta_m^{(u)}$, $\delta_m^{(p)}$, and $\delta_m^{(q)}$. We employ the binary variable v_m, where $v_m = 1$ if the potential measurement device m is installed and $v_m = 0$ otherwise.
2. The DSO may request that end-users disclose their private data with the privacy-level $(1 - \epsilon)$, including their consumption p_{dt} and q_{dt}. Instead, the DSO must pay in order to compensate the privacy of end-user d. The concept of privacy-level $(1 - \epsilon)$ is defined in the next section, and the method of acquiring end-users' private data with privacy-level $(1 - \epsilon)$ is discussed. We employ the binary variable w_d, where $w_d = 1$ if the end-user accepts the DSO's offer and discloses his private data with privacy-level $(1 - \epsilon)$ and otherwise $w_d = 0$.

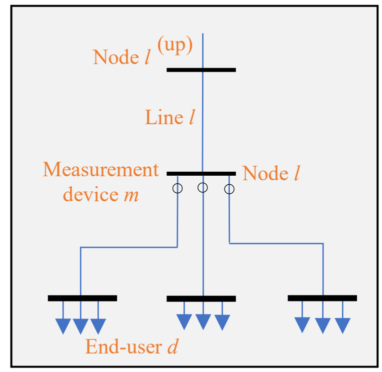

Figure 1. The example of distribution network.

A. Distflow Model

The Distflow model [22] is a load-flow model that does not rely on voltage angle and follows an iterative pattern that works well with radial networks. It is also compatible with the PI model of lines and may be used to any network topology [23] (Fig. 2). The investigated network is assumed radial, with a slack-bus at the transformation node.

The variables are computed in two steps: first, the power flow in the lines is computed from the bottom-up using the backward-Distflow equation (1), and then the square voltage magnitude of the nodes from the slack bus to the end-nodes is computed using the forward-Distflow equation (2). These calculations are carried out in loop until the convergence is achieved.

$$p_{lt}^{(up)} = r_l \cdot \frac{(p_{lt})^2 + (q_{lt})^2}{(u_l)^2} + \sum_{d\in D_l} p_{dt} + \sum_{l'\in L_l} p_{l't}^{(up)}, \forall l \tag{1.a}$$

$$\begin{aligned} q_{lt}^{(up)} = x_l \cdot \frac{(p_{lt})^2 + (q_{lt})^2}{(u_l)^2} + \sum_{d\in D_l} q_{dt} + \sum_{l'\in L_l} q_{l't}^{(up)} \\ -2 \cdot (u_{lt})^2 \cdot \sum_{l'\in L_l \cup \{l\}} b_{l'}, \forall l \end{aligned} \tag{1.b}$$

$$\begin{aligned} (u_{lt})^2 = \left(u_{lt}^{(up)}\right)^2 - 2 \cdot (r_l \cdot p_{lt} + x_l \cdot q_{lt}) + (r_l^2 + x_l^2) \\ \cdot \frac{(p_{lt})^2 + (q_{lt})^2}{(u_l)^2}, \forall l \end{aligned} \tag{2}$$

where D_l is the set of end-users connected to node l, and L_l is the set of lines downstream of line l.

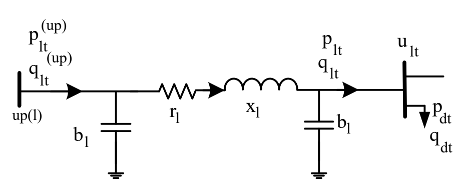

Figure 2. Pi model of a line and notations used in the Distflow.

B. Privacy-Level of End-Users

We must evaluate and define end-user's privacy since historical consumption data of end-users can give considerable amounts of personal information about an individual. When defining privacy for smart meter data, we must consider what specific information an end-user want to keep private, which in this case is $(p_{dt})_{t\in T}$ and $(q_{dt})_{t\in T}$. Although data aggregation and anonymization give some additional privacy protection, they do not guarantee that an end-user cannot be recognized or that information will not be disclosed. Differential privacy, on the other hand, is defined as a set of techniques by which we assure that an end-user d cannot be individually recognized. While the advantages of sharing such private data will be realized in differential privacy setting, the data will not be shared explicitly. Even by utilizing data analytics and machine-learning approaches, one cannot determine an end-user's consumption [27].

Differential privacy presents a mathematical framework to define the likelihood of being identified when looking at the entire announced dataset. Given a set of $d \in D$ end-users, a randomized mechanism M is $(1-\epsilon)$-differentially private if, for all conceivable situations of reported $\vec{p} = (p_{dt})_{d\in D, t\in T}$, $\vec{q} = (q_{dt})_{d\in D, t\in T}$, $\vec{p}' = (p'_{dt})_{d\in D, t\in T}$, and $\vec{q}' = (q'_{dt})_{d\in D, t\in T}$, $\vec{p}$ and $\vec{p}'$ differ only in one element and $\vec{q}$ and $\vec{q}'$ also differ in one element, we get:

$$\text{Prob}\big(\,\vec{p}|M(\,\vec{p})\big) \leq \exp(\epsilon)\cdot \text{Prob}\big(\vec{p}'\,|M(\,\vec{p})\big), \tag{3.a}$$

$$\text{Prob}\big(\,\vec{q}|M(\,\vec{q})\big) \leq \exp(\epsilon)\cdot \text{Prob}\big(\vec{q}'\,|M(\,\vec{q})\big), \tag{3.b}$$

where $1-\epsilon$ denotes the differential privacy-level of end-users if the mechanism M is used, i.e., the smaller ϵ, the more private M [23].

One mechanism for achieving $(1-\epsilon)$-privacy is to introduce a Laplacian noise to each end-user load profile separately. For active and reactive power, the injected Laplacian noise is $n_{dt}^{(p)} \sim L\left(0, b_t^{(p)}\right)$ and $n_{dt}^{(q)} \sim L\left(0, b_t^{(q)}\right)$, where $b_t^{(p)}$ and $b_t^{(q)}$ are scaling factors. It should be noted that the noises must be mutually independent for all $d \in D$, time $t \in T$, and active/reactive power profiles. The Laplacian noise $n_{dt}^{(p)}$ and $n_{dt}^{(q)}$ injections can ensure $(1-\epsilon)$ differential privacy if the relationship between ϵ and $b_t^{(p)}, b_t^{(q)}$ is satisfied as shown below.

$$b_t^{(p)} = \frac{\max\limits_{\forall d\in D}(p_{dt}) - \min\limits_{\forall d\in D}(p_{dt})}{\epsilon \cdot |I|}, \tag{4.a}$$

$$b_t^{(q)} = \frac{\max\limits_{\forall d\in D}(q_{dt}) - \min\limits_{\forall d\in D}(q_{dt})}{\epsilon \cdot |I|}, \tag{4.b}$$

where $|I|$ is the number of end-users in the network.

C. Privacy Cost of End-Users

Prospect theory better depicts the end-user's behavior under uncertainty settings than expected utility theory, which is a commonly used modeling approach in economics. According to prospect theory, a person judges an outcome based on subjective impression due to psychological loss and risk preference [28].

In our problem, privacy is likewise seen as an unpredictable metric for end-users. In [28], the following cost function has been suggested.

$$\text{PrivacyCost}(\epsilon) = \lambda \cdot \epsilon^{\beta}, \tag{5}$$

where λ captures the loss aversion level, and $0 \leq \beta \leq 1$ describes for convexity of the cost function to the risk aversion level. We can investigate different levels of risk aversion in end-users by varying the parameters λ and β. A statistical study would be helpful to determine these parameters for a specific population.

D. Acceptance Rate of End-Users

The DSO attempts to estimate the network's state at each time instant. To accomplish this purpose, he may pay each end-user $comp\,(\epsilon)$ for releasing his private information with a privacy-level of $1-\epsilon$. In fact, the DSO will only get the noisy version of smart meter data, i.e., $p_{dt} + n_{dt}^{(p)}$ and $q_{dt} + n_{dt}^{(q)}$, to undertake state estimation. The DSO needed this information in order to participate in the flexibility markets.

The proposed mechanism is as follows. Each end-user has the choice to accept or reject the offer after it is presented to him. If end-user d rejects the offer, his net payoff is equal to $x_d = 0$; otherwise, if he accepts the offer, his net payoff is:

$$x_d = \text{comp}(\epsilon) - \text{PrivacyCost}(\epsilon). \tag{6}$$

We do not know how much privacy loss each end-user costs, thus neither DSO nor end-user can anticipate x_d exactly. When we obtain an estimate of each end-user's cost based on statistical analysis of the parameters λ and β in (5), we need a probabilistic function to estimate how probable it is that end-user d will accept the offer, i.e., $w_d = 1$. We will use the Sigmoid function (shown in Fig. 3) to demonstrate this aspect of end-user's behavior.

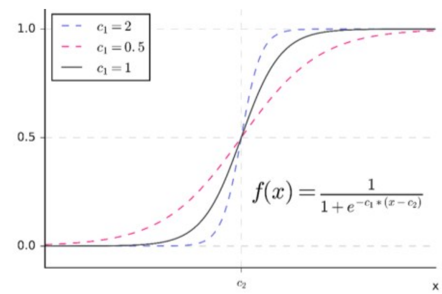

Figure 3. Basic Sigmoid function.

$$\text{Prob}\{w_d = 1\} = \frac{1}{1 + e^{-c_1\cdot(x_d - c_2)}}, \tag{7}$$

where c_1 and c_2 are parameters that can be estimated statistically.

In brief, we can change the parameters β, δ, c_1 and c_2 to simulate various end-users' reactions to the DSO's suggested offer for collecting smart meter data.

III. Private Smart Meter Data Princing Problem and Proposed Solution Algorithm

Using acquired smart meter data and in-field measurements, the DSO will determine the state of the distribution network.

Here, we first describe a state estimation algorithm. However, the DSO requires private smart meter data in order to perform this algorithm. In the following part, we will provide an optimization problem for pricing smart meter data. Because the proposed optimization problem cannot be solved using standard solvers, we describe a heuristic iterative algorithm in the final part of this section for finding an accurate solution to the proposed optimization problem.

A. State Estimation Algorithm

In this section, we describe a state estimation algorithm based on the Distflow model presented in Section II.A. The shunt capacitance of the lines is taken into account in the Distflow model under consideration.

The goal of the state estimation algorithm is to calculate the flowing power of all lines and voltage magnitudes of all nodes, namely $\vec{s} = (p_{lt}, q_{lt}, u_{lt})_{l\in L, t\in T}$. To reach this aim, we define the vector $\vec{x} = \left((u_{0t})^2, (p_{dt}, q_{dt})_{d\in D, t\in T}\right)$. Using the weighted-least-square (WLS) estimation method and a set of measurements $\vec{z} = (p_{mt}, q_{mt}, (u_{mt})^2)_{m\in M, t\in T}$, we have:

$$\vec{z} = h(\vec{x}) + \text{error}, \tag{7}$$

where $m \in M$ is the measuring device's index, p_{mt}, $q_m t$, and $(u_{mt})^2$ are the active power, reactive power, and square of voltage magnitude measured by the measurement device m, $h(\vec{x})$ is a function between $\vec{x}$ and $\vec{z}$ based on the Distflow distribution network model, and error is measurement noise. It should be noted that the vector $\vec{z}$ contains both real measurements from measuring devices $m \in M$ and pseudo-measurements acquired by DSO offers specified in Section II.C.

We can use an iterative method with update (8) to tackle the state estimation problem.

$$\vec{x}_{(k+1)} = \vec{x}_{(k)} + (H^{\mathrm{T}} \cdot W \cdot H)^{-1} \cdot H^{\mathrm{T}} \cdot W \cdot r_{(k)}, \tag{8}$$

where k is the iteration index, $r_{(k)}$ is the difference between the measurement and the results of applying the measurement function to the computed state vector at each iteration, i.e., $r_{(k)} = \vec{z} - h(\vec{x})$, H is the Jacobian matrix of $h(\vec{x})$ as defined in (9), and W is the inverse of the variance matrix formulated in (10) for all measurements, where $\left(\sigma_{z_m}\right)^2$ is the respected measurement standard deviation.

$$H = \left[\frac{\partial h(\vec{x})_{z_m}}{x_i}\right]_{z_m i} \tag{10}$$

$$W = \begin{bmatrix} \left(\sigma_{z_1}\right)^2 & 0 & 0 \\ 0 & \ddots & 0 \\ 0 & 0 & \left(\sigma_{z_m}\right)^2 \end{bmatrix} \tag{11}$$

Following the convergence of (8), the DSO will calculate the state vector $\vec{s}$ using its relationship to vector $\vec{x}$ based on the Distflow model.

B. Pricing Private Smart Meter Data

The DSO tries to estimate the state vector $\vec{s}$ with maximum error then $\delta^{(\max)}$. He will need private information from end-users and in-field measurements to do so. To collect smart meter data, he proposes (ϵ, comp) offers to each end-user $d \in D$, with each one is free to accept or reject the offer. If someone declines the offer, the DSO will get that end-data user's data with a privacy-level of 1. Another option for DSO is to install an in-field measurement device $m \in M$, which costs c.

The DSO must solve the following optimization problem to determine optimal (ϵ, comp) and which measurement device $m \in M$ is worthy of installation $\{m | v_m = 1\}$.

$$\min_{\Gamma} \mathbf{Obj} = \mathbb{E}\left\{\sum_{m\in M} \mathrm{c} \cdot v_m + \sum_{d\in D} \text{comp} \cdot w_d\right\} \tag{12.a}$$

subject to:

$$\left\|(\tilde{p}_{lt}, \tilde{q}_{lt}, \tilde{u}_{lt})_{l\in L, t\in T} - (p_{lt}, q_{lt}, u_{lt})_{l\in L, t\in T}\right\|_{\infty} \le \delta^{(\max)}, \tag{12.b}$$

$$\text{Prob}\{w_d = 1\} = \frac{1}{1 + e^{-c_1\cdot(x_d - c_2)}}, \quad \forall d \in D, \tag{12.c}$$

$$\text{Prob}\{w_d = 0\} = 1 - \text{Prob}\{w_d = 1\}, \quad \forall d \in D, \tag{12.d}$$

$$v_m = \{0,1\}, \quad \forall m \in M, \tag{12.e}$$

where $(\tilde{p}_{lt}, \tilde{q}_{lt}, \tilde{u}_{lt})_{l\in L, t\in T}$ is the estimated state of the network, $(p_{lt}, q_{lt}, u_{lt})_{l\in L, t\in T}$ is the actual state of network the set Γ of decision variables for this problem includes comp, ϵ, $(v_m)_{m\in M}$.

The proposed optimization problem (12.a)–(12.e) is a non-convex mixed-integer programming problem that cannot be solved precisely. In the section that follows, we offer an algorithm for solving this problem.

C. Algorithm of Finding Solution

We build an iterative algorithm inspired by [26] to solve the aforementioned optimization problem. Consider $\vec{\zeta}_{(i)} = \left(\left(v_m^{(i)}\right)_{m\in M}, \text{comp}, \epsilon\right)$, which is the solution at iteration i. In each iteration, we have the budget c, which can be associated to installing a measurement device or increasing payment to the end-users. The problem of each iteration is as below:

$$\min_{\zeta_{(i)}} \mathbf{J}\left(\vec{\zeta}_{(i)}\right) \tag{13.a}$$

subject to:

$$\vec{\zeta}_{(i)} \gg \vec{\zeta}_{(i-1)} \tag{13.b}$$

$$\mathbf{Obj}\left(\vec{\zeta}_{(i)}\right) - \mathbf{Obj}\left(\vec{\zeta}_{(i-1)}\right) \le c \tag{13.c}$$

where $\gg$ is used for element-wise vector comparison, $\mathbf{J}\left(\vec{\zeta}_{(i)}\right) = \min\left(\delta^{(max)}, \|(\tilde{p}_l, \tilde{q}_l, \tilde{u}_l)_{l\in L} - (p_l, q_l, u_l)_{l\in L}\|_{\infty}\right)$, $(\tilde{p}_l, \tilde{q}_l, \tilde{u}_l)_{l\in L}$ is estimated based on $\vec{\zeta}_{(i)}$.

The above algorithm continues until it converges or (13.c) is not feasible. The final solution includes the offers of DSO for pricing private smart meter data.

IV. Case Study

The performance of the suggested approach for collecting private smart meter data is discussed in the following using a medium voltage and low voltage distribution network. The network includes 52 nodes connected by two main transformers

(Fig. 4). The link between nodes 2 to 0 and 2 to 5 are medium-voltage/low-voltage transformers, whereas the others are cables.

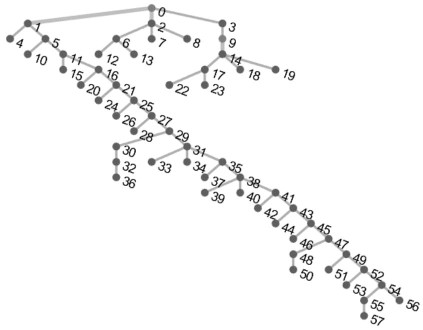

Figure 4. The distribution network under consideration.

This case study network is located in a residential area of the city Geneva and possesses:

- 52 nodes, 49 lines, and 2 MV/LV transformer,
- 58 smart-meters installed (over 89 meters, so 65% of the consumer are covered): Active and reactive power are available with an average over period of 15 minutes,
- 31 conventional meters, in which the annual active power data of these meters is available, and
- 43200 kWh active power consumption monthly.

The 15-minute data of end-users with smart meters is collected here during a period of 79 days, from 17/01/2020 to 04/04/2020. Because of privacy concerns, the data is anonymized from the beginning and is randomly assigned to different end-users. As a result, we do not have access to each end-user's actual data.

The cost of installing one in-field measurement instrument is estimated to be \$10,000. The parameters λ, β, c_1, and c_2 are considered equal to 500, 0.5, 0.1, and 10, respectively. Fig. 5 depicts the privacy cost for various lambda values.

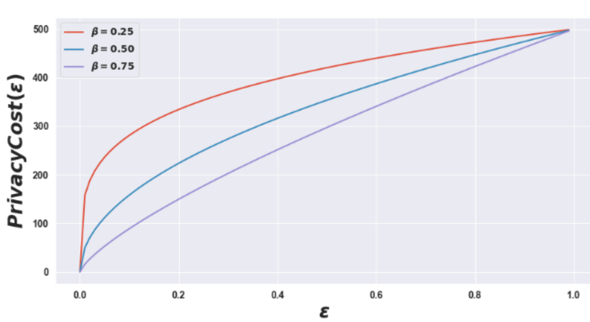

Figure 5. Sensitivity of privacy cost to the value of β.

We determine the final solution of the proposed algorithm after only three iterations with a budget of \$30,000 to have a maximum error of state estimation, $\delta^{(\max)}$, of less than 2%. The final solution is privacy-level $(1-\epsilon) = 0.7788$, $\text{comp} = 420.37\$$, and just one measuring device installed at node 9. Figs. 6.a and 6.b show the sensitivity of the resulted ϵ and comp to the parameters of privacy cost, i.e., λ and β.

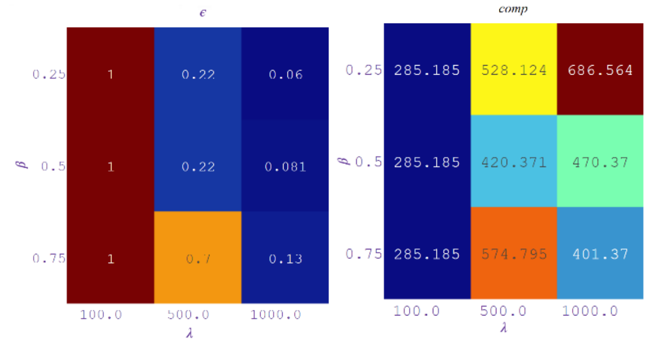

Figure 6. Sensitivity of resulted (a) ϵ and (b) compensation to the selected parameters for privacy cost.

Figs. 7.a and 7.b show the actual and state estimation results for voltage level and line loading at time "2020-01-28 18:45:00", which is the maximum network loading. As we can see, the biggest inaccuracy will occur during the estimation of voltage levels of nodes adjacent to loads.

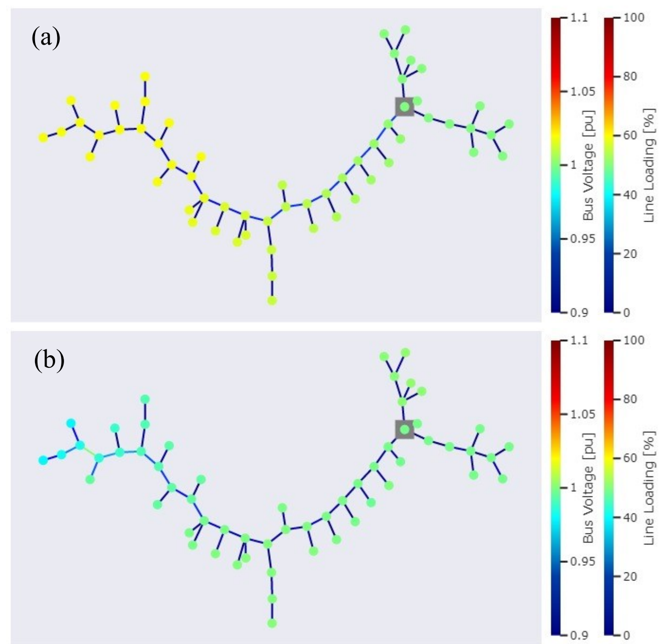

Figure 7. The (a) actual and (b) estimated voltage level and line loading for maximum network loading.

V. Conclusion

In this paper, we present an algorithm for valuing private data from smart meters. Smart meter data is used in differentially private format with artificial added noise for reasons other than normal network operation. We propose an optimization problem that prices smart meter data, optimizes privacy-level, and places measurement devices based on estimated privacy cost for end-users and measurement device installation cost. Because the proposed optimization problem is non-convex, an algorithm to find an estimated result is proposed. The proposed algorithm is evaluated on an exemplary distribution network in Geneva, Switzerland.

References

[1] Office fédéral de l'énergie, ""Bases pour l'introduction de systèmes de mesure intelligents auprès du consommateur final en Suisse Exigences techniques minimales et modalités d'introduction," Département fédéral de l'environnement, des transports, de l'énergie et de la communication (DETEC), OFEN, Division Economie, Section Réseaux, Bern, 2014.

[2] D. B. Arnold, C. Roberts, O. Ardakanian and E. M. Stewart., "Synchrophasor data analytics in distribution grids," in *IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2017.

[3] M. Radi, G. Taylor, J. Cantenot, E. Lambert and N. Suljanovic, "Developing Enhanced TSO-DSO Information and Data Exchange Based on a Novel Use Case Methodology," *Frontiers in Energy Research 9,* p. 259, 2021.

[4] O. Valarezo, T. Gómez, J. P. Chaves-Avila, L. Lind, M. Correa, D. U. Ziegler and R. Escobar, "Analysis of new flexibility market models in Europe," *Energies ,* vol. 14, no. 12, p. 3521, 2021.

[5] G. Tsaousoglou, J. S. Giraldo, P. Pinson and N. G. Paterakis, "Mechanism design for fair and efficient dso flexibility markets."," *IEEE transactions on smart grid,* vol. 12, no. 3, pp. 2249-2260, 2021.

[6] A. Primadianto and C.-N. Lu, "A review on distribution system state estimation," *IEEE Transactions on Power Systems ,* vol. 32, no. 5, pp. 3875-3883, 2016.

[7] M. Majdoub, J. Boukherouaa, B. Cheddadi, A. Belfqih, O. Sabri and T. Haidi, "A review on distribution system state estimation techniques," in *6th International Renewable and Sustainable Energy Conference (IRSEC)*, 2018.

[8] M. Pau, E. Patti, L. Barbierato, A. Estebsari, E. Pons, F. Ponci and A. Monti, "Low voltage system state estimation based on smart metering infrastructure.," in *IEEE international workshop on applied measurements for power systems (AMPS)*, 2016.

[9] M. Pau, E. Patt, L. Barbierato, A. Estebsari, E. Pons, F. Ponci and A. Monti, "Pau, Marco, Edoardo Patti, Luca Barbierato, Abouzar Estebsari, Enrico Pons, Ferdinanda Ponci, and Antonello Monti. "A cloud-based smart metering infrastructure for distribution grid services and automation," *Sustainable Energy, Grids and Networks,* vol. 15, pp. 14-25, 2018.

[10] B. Matthiss, J. Erb and J. Binder, "Using smart meters for distribution grid state estimation," in *International Conference on Smart Energy Systems and Technologies (SEST)*, 2019.

[11] P. Paruta, T. Pidancier, M. Bozorg and M. Carpita, "Greedy placement of measurement devices on distribution grids based on enhanced distflow state estimation," *Sustainable Energy, Grids and Networks,* vol. 26, p. 100433, 2021.

[12] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," *first IEEE international conference on smart grid communications,* pp. 238-243, 2010.

[13] G. Giaconi, D. Gunduz and H. V. Poor, "Smart meter data privacy," *arXiv preprint arXiv,* vol. 01364, 2020.

[14] B. Hayes, J. Gruber and M. Prodanovic, "Short-term load forecasting at the local level using smart meter data," in *IEEE Eindhoven PowerTech*, Eindhoven , 2015.

[15] C. Beckel, L. Sadamori, T. Staake and S. Santini, "Revealing household characteristics from smart meter data," *Energy ,* vol. 78, pp. 397-410, 2014.

[16] Y. Poullet, "EU data protection policy. The Directive 95/46/EC: Ten years after," *Computer Law & Security Review,* vol. 22, no. 3, pp. 206-217, 2006.

[17] PEAN UNION, "DIRECTIVE 2009/136/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL," *Official Journal of the European Union,* vol. 337, 2009.

[18] Le Conseil fédéral suisse, "Ordonnance sur l'approvisionnement en électricité (OApEl)," Bern, 2008.

[19] Association des entreprises électriques Suisse, "Directives pour la sécurité des données des systèmes de mesure intelligents," Aarau, 2018.

[20] M. R. Asghar, G. Dán, D. Miorandi and I. Chlamtac, "Smart meter data privacy: A survey," *IEEE Communications Surveys & Tutorials,* vol. 19, no. 4, pp. 2820-2835, 2017.

[21] E. McKenna, I. Richardson and M. Thomson, "Smart meter data: Balancing consumer privacy concerns with legitimate applications," *Energy Policy,* vol. 41, pp. 807-814, 2012.

[22] J. Holweger, L. Bloch, C. Ballif and N. Wyrsch, "Privacy-preserving methods for smart-meter-based network simulations."," *arXiv preprint arXiv:,* p. 2110.03491, 2021.

[23] S. Chhachhi and F. Teng, "Market Value of Differentially-Private Smart Meter Data," in *In Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)*, 2021.

[24] M. B. Gough, S. F. Santos, T. AlSkaif, M. S. Javadi, R. Castro and J. P. Catalão, "Preserving privacy of smart meter data in a smart grid environment," *IEEE Transactions on Industrial Informatics,* vol. 18, no. 1, pp. 707-718, 2021.

[25] M. E. Baran and F. F. Wu, "Network reconfiguration in distribution systems for loss reduction and load balancing," *IEEE Power Engineering Review,* vol. 9, no. 4, pp. 101-102, 1989.

[26] M. H. Haque, "A general load flow method for distribution systems," *Electric Power Systems Research,* vol. 54, no. 1, pp. 47-54, 2000.

[27] Z. Yang, P. Cheng and J. Chen, "Differential-privacy preserving optimal power flow in smart grid," *IET Generation, Transmission & Distribution,* vol. 11, no. 15, pp. 3853-3861, 2017.

[28] G. Liao, X. Chen and J. Huang, "Prospect theoretic analysis of privacy-preserving mechanism.," *IEEE/ACM Transactions on Networking,* vol. 28, no. 1, pp. 71-83, 2019.

[29] P. Paruta, T. Pidancier, M. Bozorg and M. Carpita, "Greedy placement of measurement devices on distribution grids based on enhanced distflow state estimation," *Sustainable Energy, Grids and Networks,* vol. 26, no. 100433, 2021.