On the Impact of Side Information on Smart Meter Privacy-Preserving Methods

Mohammadhadi Shateri
McGill University
Montreal, Canada

Francisco Messina
McGill University
Montreal, Canada

Pablo Piantanida
CentraleSupélec-CNRS-Université Paris-Saclay
Gif-sur-Yvette, France

Fabrice Labeau
McGill University
Montreal, Canada

Abstract—Smart meters (SMs) can pose privacy threats for consumers, an issue that has received significant attention in recent years. This paper studies the impact of Side Information (SI) on the performance of possible attacks to real-time privacy-preserving algorithms for SMs. In particular, we consider a deep adversarial learning framework, in which the desired releaser, which is a Recurrent Neural Network (RNN), is trained by fighting against an adversary network until convergence. To define the objective for training, two different approaches are considered: the Causal Adversarial Learning (CAL) and the Directed Information (DI)-based learning. The main difference between these approaches relies on how the privacy term is measured during the training process. The releaser in the CAL method, disposing of supervision from the actual values of the private variables and feedback from the adversary performance, tries to minimize the adversary log-likelihood. On the other hand, the releaser in the DI approach completely relies on the feedback received from the adversary and is optimized to maximize its uncertainty. The performance of these two algorithms is evaluated empirically using real-world SMs data, considering an attacker with access to SI (e.g., the day of the week) that tries to infer the occupancy status from the released SMs data. The results show that, although they perform similarly when the attacker does not exploit the SI, in general, the CAL method is less sensitive to the inclusion of SI. However, in both cases, privacy levels are significantly affected, particularly when multiple sources of SI are included.

I. INTRODUCTION

Smart meters (SMs) provide advanced monitoring features for power grids by collecting the user's power consumption and reporting them to the utility providers almost in real time. Although this enables several important applications for smart grids (e.g., energy theft prevention, power quality monitoring, demand response, among others [1]), it also violates the user's privacy, which is a major concern for its wide deployment and adoption [2]. Actually, it has been shown that a potential attacker with access to the SMs data can infer sensitive information about the users such as the occupancy status [3] or the types of appliances being used by consumers [4].

In recent years, several studies on privacy-preserving approaches for SMs data sharing were conducted, which can be classified into two main families. On the one hand, the methods in the first family [5]–[16] use physical resources such as rechargeable batteries, electric vehicles, heating, ventilation, and air conditioning units, etc., to shape the consumed power so that the SMs measurements reveal minimum information about the user's actual power consumption pattern. The methods in the second family [17]–[24] manipulate the SMs data, to be reported to the utility provider, by distorting it in order to prevent the inference of sensitive information by potential attackers, while preserving the usefulness of the data. The study of this paper is focused around this latter family of privacy-preserving methods. We consider the real-time privacy problem, in which an attacker tries to infer sensitive information in an online fashion [23], [24], i.e., without accessing non-causally to SMs data.

Although many of these methods showed good performance on dealing with attackers that have access to the distorted or shaped SMs data, none of them studied the effect of side information (SI), which occurs when an attacker uses additional information to improve its performance. To the best of our knowledge, the only work where SI was considered is [25], in which it is used by the utility provider to predict if the consumers are shaping the power consumption or reporting the actual consumed power. The goal of our study is different. We study the impact of SI at the privacy level, as measured by the accuracy of an attacker trying to guess a sensitive attribute, that is obtained with two different privacy-preserving strategies. First, we consider a causal adversarial learning (CAL) algorithm, which is a generalized version of the privacy-preserving adversarial network (PPAN) approach introduced in [22], by including the temporal structure of SM data. The CAL algorithm is compared with a recently proposed state-of-the-art method, referred to as the directed information (DI) based learning [23], [24], considering attackers with and without SI and using a real world SMs dataset.

The rest of the paper is organized as follows. In Section II, the problem formulation of the SMs privacy-utility considering SI is developed for both CAL and DI approaches. Using the proposed formulations, the loss functions for the releaser and adversary are given in Section III along with the general training algorithm. Empirical results for both methods are presented and discussed in Section IV. Finally, some concluding remarks close the paper in Section V.

Notation and conventions

In this paper, a sequence of random variables, or a time series, of length T is shown by $X^T = (X_1, \ldots, X_T)$ while $x^T = (x_1, x_2, \ldots, x_T)$ is used as a realization of X^T. The ith sample in a minibatch used for training of the model is shown by $x^{(i)T} = (x_1^{(i)}, x_2^{(i)}, \ldots, x_T^{(i)})$. p_X is used to denote the probability distribution function of random variable X and its expectation is shown as $\mathbb{E}[X]$. The Shannon entropy of random variable X is represented by $H(X)$ and $\mathrm{KL}(p_X \| q_X)$ is used to denote the Kullback-Leibler divergence between two probability

distributions p_X and q_X. In addition, the mutual information (MI) between random variables X and Y is represented as $I(X;Y)$ and $X \multimap Y \multimap Z$ denotes a Markov chain among random variables X, Y and Z.

II. PROBLEM FORMULATION

Consider a user's power consumption or demand load measured by the SM over T time slots, represented as the time series $Y^T = \{Y_t\}_{t=1}^T$. In addition, let $X^T = \{X_t\}_{t=1}^T$ represent sensitive user information, which could represent power profile details, the presence of individuals at home, the appliances' state (either on or off), etc. As shown in Fig. 1, the power consumption measurements need to be sanitized before being communicated with the utility provider or shared with a third-party for different data analysis tasks. Concretely, the goal of a privacy-preserving system is to generate a masked load Z^T (referred to as the released time-series), based on knowledge of Y^T and X^T, which is similar to Y^T but provides minimum information about the sensitive attribute X^T. Note that a potential attacker will try to infer the sensitive information based on the released data. We also assume that the attacker has access to SI (e.g., the day of the week), represented as S, which can be used as auxiliary data to improve its inference performance.

In the following subsections, we present two possible formulations of the privacy-preserving problem in this context.
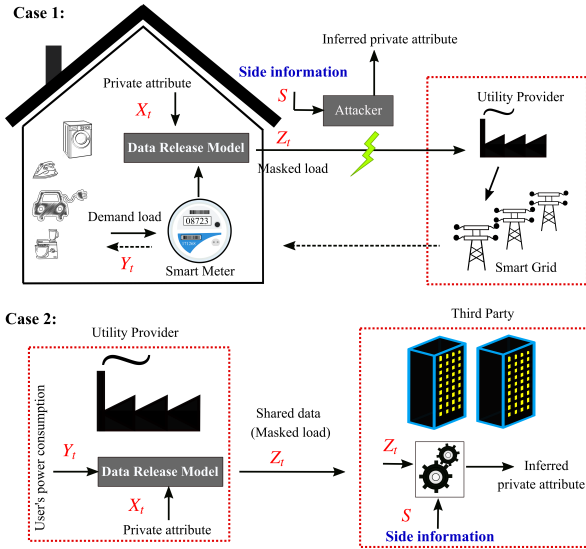

Fig. 1. Privacy-preserving SM framework. Case 1: SMs data are communicated with the utility provider. Case 2: Utility provider is sharing the SMs data with a third-party.

A. Causal adversarial learning (CAL) approach

The first approach considered in this study for formulating the privacy-preserving problem is referred to as the CAL method. This approach is a generalized version of the PPAN model introduced in [22] but, in addition, includes the temporal correlation and causality involved in the time series data processing. In this setting, the privacy measure is defined as the conditional MI between the released time-series Z^T and sensitive attribute X^T, conditioned on the SI S. The conditional

MI $I(X^T; Z^T|S)$ quantifies the amount of information shared between the released Z^T and sensitive attribute X^T when the side information S is revealed (the reader is referred to [26] for details on information-theoretic concepts and properties). The releaser aims to minimize this privacy measure by adding a controlled amount of distortion, say $\varepsilon > 0$, to the useful data Y^T so as to keep a desired utility level. Therefore, the problem of finding the optimal releaser can be cast as follows:

$$\min_{p_{Z^T|X^T,Y^T}} \frac{1}{T} I\left(X^T; Z^T|S\right) \quad \text{s.t.} \quad D(Z^T, Y^T) \leq \varepsilon. \quad (1)$$

where $D(Z^T, Y^T)$ is the normalized expected distortion between Z^T and Y^T, defined as

$$D(Z^T, Y^T) := \frac{\mathbb{E}[d(Z^T, Y^T)]}{T}, \quad (2)$$

with $d : \mathbb{R}^T \times \mathbb{R}^T \to \mathbb{R}$ any distortion function.

We now consider an arbitrary conditional distribution $q_{X^T|Z^T,S}$ and note that the conditional MI in (1) satisfies the following relation:

$$
\begin{aligned}
I\left(X^T; Z^T|S\right) &= H(X^T|S) - H(X^T|Z^T, S) \\
&\overset{(i)}{=} H(X^T|S) - \sum_{t=1}^T H\left(X_t|X^{t-1}, Z^T, S\right) \\
&\overset{(ii)}{=} H(X^T|S) + \sum_{t=1}^T \Big[\mathbb{E}[\log q_{X_t|X^{t-1}, Z^T, S}] \\
&\quad + \text{KL}\left(p_{X_t|X^{t-1}, Z^T, S} \| q_{X_t|X^{t-1}, Z^T, S}\right) \Big] \\
&\overset{(iii)}{\geq} H(X^T|S) + \sum_{t=1}^T \mathbb{E}[\log q_{X_t|X^{t-1}, Z^T, S}],
\end{aligned}
$$
$$(3)$$

where (i) is due to the chain rule of entropy, (ii) is a consequence of the definition of the Kullback-Leibler (KL) divergence, and (iii) is due to the fact that $\text{KL}(\cdot\|\cdot)$ is non-negative. In addition, the expectations are taken with respect to the distribution $p_{X_t|X^{t-1}, Z^T, S}$ at each time slot t. The equality in (3) happens when $\text{KL}(p_{X^T|Z^T,S} \| q_{X^T|Z^T,S}) = 0$, i.e., when $q_{X^T|Z^T,S} = p_{X^T|Z^T,S}$ (almost surely). Therefore,

$$I(X^T; Z^T|S) = H(X^T|S) \quad + \quad (4)$$
$$\max_{q_{X^T|Z^T,S}} \sum_{t=1}^T \mathbb{E}[\log q_{X_t|X^{t-1}, Z^T, S}].$$

Substituting equation (4) in (1), dropping the constant term $H(X^T|S)$, and imposing causality constraints, the privacy-preserving optimization (1) can be written as follows:

$$\min_{p_{Z^T|X^T,Y^T}} \max_{q_{X^T|Z^T,S}} \frac{1}{T} \sum_{t=1}^T \mathbb{E}[\log q_{X_t|X^{t-1}, Z^t, S}] \quad (5)$$
$$\text{s.t.} \quad D(Z^T, Y^T) \leq \varepsilon.$$

The minmax problem (5) can be interpreted in an adversarial learning context in which the adversary network uses the released data Z^T and S to estimate the posterior $q_{X^T|Z^T,S}$ by

maximizing the log-likelihood $\mathbb{E}[\log q_{X_t|X^{t-1},Z^t,S}]$ at time slot t, while the releaser attempts to prevent that by minimizing the same quantity. Details for implementing this approach will be presented in Section III.

B. Directed information (DI) based approach

The second methodology considered in this study is the DI-based learning approach, which was introduced in [23]. In the DI method, by considering the SI, the privacy measure is defined by $I(X^T \to \hat{X}^T|S)$, the conditional DI between the sensitive attribute X^T and the approximated sensitive attribute $\hat{X}^T$, conditioned on the SI S. In [24], it was shown that such a privacy measure can effectively be used to limit the performance of any potential attacker. In this case, the problem of finding the optimal releaser is formulated as the following optimization problem:

$$\min_{p_{Z^T|X^T,Y^T}} \frac{1}{T} I\left(X^T \to \hat{X}^T \Big| S \right) \quad \text{s.t.} \quad D(Z^T, Y^T) \le \varepsilon. \tag{6}$$

Proceeding similarly as in [24], the conditional DI privacy measure can be upper bounded as follows:

$$I\left(X^T \to \hat{X}^T \Big| S \right) \le T\log|\mathcal{X}| - \sum_{t=1}^{T} H(\hat{X}_t|Z^t, S). \tag{7}$$

The main advantage of the upper bound (7), as discussed in [23], is its computational tractability for the learning process. By substituting (7) in (6), and dropping the constant term $T\log|\mathcal{X}|$, we obtain the following relaxation of the optimization problem:

$$\min_{p_{Z^T|X^T,Y^T}} -\frac{1}{T} \sum_{t=1}^{T} H(\hat{X}_t|Z^t, S) \quad \text{s.t.} \quad D(Z^T, Y^T) \le \varepsilon. \tag{8}$$

Finally, to complete the specification of this problem, we need to define the (optimal) adversary, which is given by the solution to the following optimization problem:

$$\min_{p_{\hat{X}^T|Z^T,S}} \mathrm{KL}(p_{X^T|Z^T,S} \| p_{\hat{X}^T|Z^T,S}), \quad \text{i.e.,}$$

$$\min_{p_{\hat{X}^T|Z^T,S}} -\sum_{t=1}^{T} \mathbb{E}[\log p_{\hat{X}_t|\hat{X}^{t-1},Z^t,S}], \tag{9}$$

where the expectation is taken with respect to $p_{X^t,Z^t,S}$ for each t. It should be noted that this is in fact equivalent to the max part in the CAL optimization problem (5) by considering the correspondence $p_{\hat{X}^T|Z^T,S} \sim q_{X^T|Z^T,S}$.

III. PRIVACY-PRESERVING MODEL

In this section, the releaser design problem formulations are tackled by using an adversarial learning framework, as shown in Fig. 2. In order to exploit the time structure of the data, both the releaser and adversary are modeled using recurrent neural networks (RNNs). RNNs are a class of artificial neural networks specialized for processing sequential data. However, conventional RNNs suffer from the so-called vanishing gradient issue, which leads to difficulties in the training process [27]. To address this problem, the gated RNNs based on long short-term memory (LSTM) cells were introduced in [28], [29], which are widely used in practice currently. For more details on RNNs and LSTMs, the reader is referred to [30].
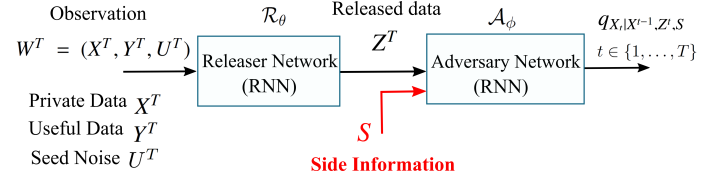

Fig. 2. Privacy-preserving framework based on adversarial learning. The observed data W^T is defined as the combination of private and useful data and the seed noise. The seed noise U^T is generated from independent and identically distributed (i.i.d.) samples according to a uniform distribution: $U_t \sim U[0,1]$.

The loss functions required for the training of the releaser and adversary networks can be readily defined based on the problem formulations (5), (8) and (9). On the one hand, for both the CAL and DI models, the adversary network loss function can be written as follows:

$$\mathcal{L}_{\mathcal{A}}(\phi) := \frac{1}{T} \sum_{t=1}^{T} \mathbb{E}\left[-\log q_{X_t|X^{t-1},Z^t,S} \right], \tag{10}$$

where ϕ are the parameters of the adversary network and we consider again the correspondence $p_{\hat{X}^T|Z^T,S} \sim q_{X^T|Z^T,S}$. On the other hand, the loss functions for training the releasers are

$$\mathcal{L}_{\mathcal{R}}^{\mathrm{CAL}}(\theta, \phi, \lambda) := D(Z^T, Y^T) + \frac{\lambda}{T} \sum_{t=1}^{T} \mathbb{E}\left[\log q_{X_t|X^{t-1},Z^t,S} \right], \tag{11}$$

$$\mathcal{L}_{\mathcal{R}}^{\mathrm{DI}}(\theta, \phi, \lambda) := D(Z^T, Y^T) - \frac{\lambda}{T} \sum_{t=1}^{T} H(\hat{X}_t|Z^t, S), \tag{12}$$

where θ are the parameters of the releaser network and λ controls the privacy-utility trade-off.

The training process for both cases is presented in detail in Algorithm 1.

Algorithm 1: Privacy-preserving data release with side information. Batch size B, number of steps to apply to the Adversary k, seed noise dimension m, and ℓ_2 regularization parameter β are hyperparameters.

1: **for** number of training iterations **do**
2:   **for** k steps **do**
3:     Sample minibatch of B examples $\{w^{(b)T} = (x^{(b)T}, y^{(b)T}, u^{(b)T})\}_{b=1}^{B}$ and generate releases $\{z^{(b)T}\}_{b=1}^{B}$.
4:     Compute the gradient of $\mathcal{L}_{\mathcal{A}}(\phi)$ with respect to ϕ, empirically approximated with the minibatch data.
5:     Update ϕ by applying the RMSprop optimizer [31].
6:   **end for**
7:   Sample minibatch of B examples $\{w^{(b)T} = (x^{(b)T}, y^{(b)T}, u^{(b)T})\}_{b=1}^{B}$ and generate releases $\{z^{(b)T}\}_{b=1}^{B}$.
8:   Compute the gradient of $\mathcal{L}_{\mathcal{R}}(\theta, \phi, \lambda)$ with respect to θ, empirically approximated with the minibatch data.
9:   Use Ridge(L_2) regularization [32] with value β and update θ by applying RMSprop optimizer.
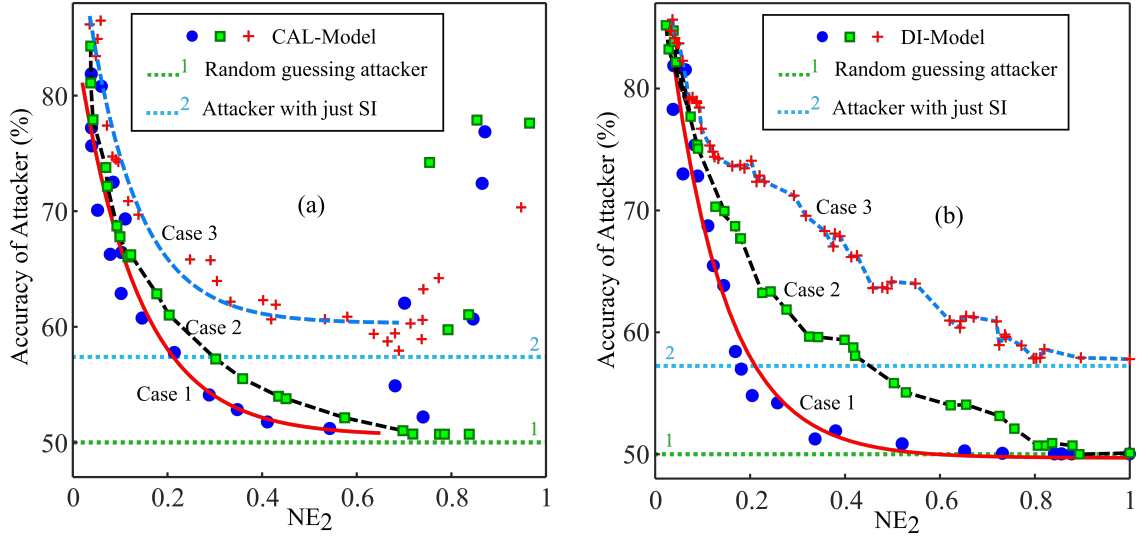10: **end for**

Fig. 3. (a) CAL model, (b) DI model, Privacy-utility trade-off for house occupancy inference. Case 1: no side information; Case 2: day of the week as side information; Case 3: day of the week joined with month of the year as side information.

IV. RESULTS AND DISCUSSION

A. Dataset and model parameters

In this work, we use the electricity consumption and occupancy (ECO) dataset published by [33], which includes 1 Hz electricity usage measured by SMs along with the occupancy labels of five houses in Switzerland. For the sake of simplicity, the dataset is re-sampled every one hour and samples over one day ($T = 24$) are considered. The dataset is split into training and test sets with a ratio of 85:15, while 10% of training data is considered as the validation dataset. Using the validation dataset, the values of the hyperparameters (including batch size B, number of adversary training step k, seed noise dimension m, and regularization value β) were tuned to achieve the best privacy-utility trade-off. Both the CAL and DI models are trained to hide the occupancy labels by distorting the electricity consumption. The performance of these models are evaluated based on the performance of an attacker, trained in a supervised manner, which attempts to infer the occupancy labels. Three different cases are considered:

- Case 1: No SI is considered for training the privacy-preserving model nor for training the attacker.
- Case 2: The day of the week associated to the SMs samples is used as SI for both training the privacy-preserving model and the attacker.
- Case 3: The day of the week and the month of the year are used as SI for both training the privacy-preserving model and the attacker.

The structures of the releaser, adversary, and attacker are similar for both the CAL and DI methods. The releaser is composed of 4 LSTM layers (each including 64 cells) with $\beta = 1.5$, $k = 4$, $m = 8$, and $B = 128$, while the attacker is made of 3 LSTM layers (each including 32 cells). For the second and third cases, the adversary network consists of 3 LSTM layers (each including 32 cells), while for the first case it is composed by 2 LSTM layers (each including 32 cells).

To evaluate the amount of distortion added by the releaser network, we use the Normalized Error (NE) measure, defined as follows:

$$\text{NE}_2 := \frac{\mathbb{E}\left[\|Y^T - Z^T\|_2\right]}{\mathbb{E}\left[\|Y^T\|_2\right]}. \quad (13)$$

In addition, the performance of the attacker in inferring the sensitive data is measured using the balanced accuracy [34], presented below:

$$\text{Balanced Accuracy} := \frac{1}{2}\left(\frac{c_{11}}{c_{11} + c_{12}} + \frac{c_{22}}{c_{22} + c_{21}}\right), \quad (14)$$

where c_{ij} represent the fraction of examples of class i classified as class j. Using these metrics, the privacy-utility trade-off for the CAL and DI models are presented in Figs. 3.

Considering the first case, in which no SI is taken into account, it can be seen that both models have very similar performances. However, the CAL model behaves erratically for large values of distortion, in the sense that the accuracy of the attacker does not monotonically decrease as the distortion increases. From a practical perspective, however, the high distortion region for which this happens is not particularly interesting, since the utility of the distorted data is very low in such cases. To understand this issue, we studied the evolution of the releaser loss function during training for both models, considering different values of λ. As can be seen in Fig.4, for small values of λ, the releaser loss functions behave very similarly with a clean convergence pattern. However, as λ increases and more distortion is allowed, the convergence of the loss for the CAL model becomes noisier than for the DI model. In other words, for large values of λ (i.e., the full privacy regime) the DI model, by maximizing the conditional entropy, can push the adversary towards a random guessing classifier, while the CAL model, by maximizing the cross-entropy, does not seem to work well. However, in the area where there is a balance between privacy and distortion, the cross-entropy seems to be effective in controlling the privacy-utility trade-off.

For the other cases, where SI is included in the models, it is clearly seen that the privacy performance is degraded, which is expected since the attacker has more information about the sensitive attribute to perform the inference task. It should be noted that the baseline for full privacy changes for the different cases. Indeed, an attacker trained and tested with just SI for estimating the sensitive attribute suggests a balanced accuracy of 50.7% and 57.8% as the baseline for Cases 2 and 3, respectively. In particular, for the Case 3 in which both the day of the week and month of the year are considered, the attacker performance is improved in a very significant way. In fact, the models can not completely fool the attacker even when arbitrarily large distortion is allowed. This phenomenon can be understood because the SI provides some prior information for the attacker, which can be exploited independently from the amount of noise added to the power measurements by the releaser (see attacker performance with just SI in Fig. 3. On the other hand, the CAL model seems to be less sensitive (in the low distortion range) to SI than the DI model. This can be justified by revising the loss functions for each model (see (11) and (12)). The releaser in the DI method completely relies on the adversary uncertainty and therefore is unsupervised, while the CAL releaser gets supervision from the actual sensitive labels, which can make it more effective.
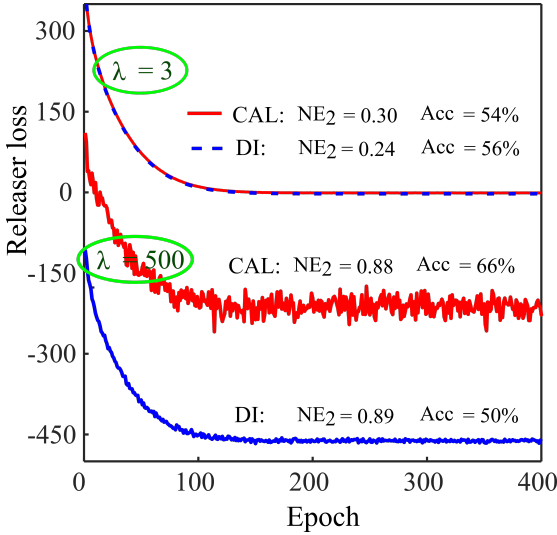

Fig. 4. Examples of the releaser network loss function versus training epochs for both DI and CAL models.

A final experiment that we conducted was including the SI at the input of the releaser network for Case 2, which means that the privacy-preserving mechanism can change its behavior according to the day of the week. As can be seen in Fig.5, however, this is not helpful in reducing the gap between Case 2 and Case 1 in Fig. 3. This might be due to the fact that the SI S can be readily inferred from X^T and Y^T. For example, for the data set in our study the day of the week can be predicted from the X^T and Y^T with balanced accuracy of more than 85%. This suggests that SI is in some sense a redundant input for the releaser network.
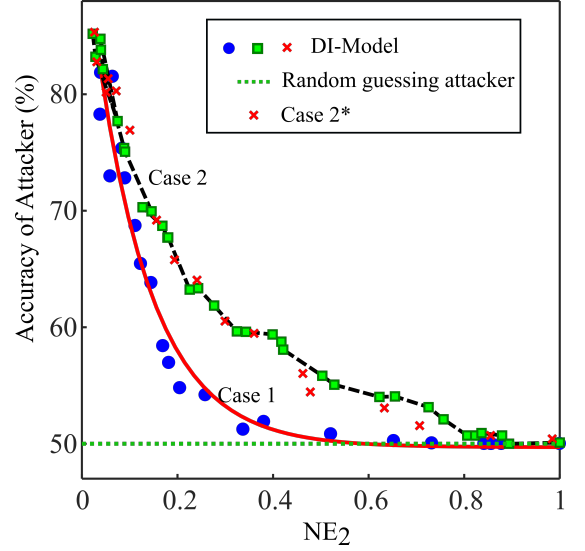

Fig. 5. DI model: Privacy-utility trade-off for house occupancy inference. Case 2* refers to Case 2 but including side information also at the input of the releaser.

V. Concluding Remarks

In this work, we took into account the effect of SI (correlated with sensitive information) on the formulation of SMs privacy-preserving mechanisms. Concretely, two distortion-based real-time privacy-preserving models were presented and implemented using a deep adversarial learning framework. The privacy-utility trade-offs associated with both models were then investigated and compared. For the case in which SI is not considered, both models perform very similarly, except for large distortion values, where the CAL model showed instability issues. For the other cases, in which the attacker had access to SI, the privacy levels are significantly affected, but the CAL model was shown to be more robust than the DI model to the inclusion of SI. The privacy degradation was particularly noticeable when multiple sources of SI were considered jointly. This result clearly shows how it is possible to overestimate the privacy level attained by a privacy-preserving mechanism ignoring sources of SI, a particularly serious hurdle for offering actual privacy guarantees. This observation raises several questions for future research: How should privacy be evaluated when not all possible sources of SI can be taken into account? How can we effectively model the attacker prior information in general?

REFERENCES

[1] Y. Wang, Q. Chen, T. Hong, and C. Kang, "Review of smart meter data analytics: Applications, methodologies, and challenges," *IEEE Transactions on Smart Grid*, vol. 10, pp. 3125–3148, May 2019.

[2] G. Giaconi, D. Gunduz, and H. V. Poor, "Privacy-aware smart metering: Progress and challenges," *IEEE Signal Processing Magazine*, vol. 35, no. 6, pp. 59–78, 2018.

[3] C. Feng, A. Mehmani, and J. Zhang, "Deep learning-based real-time building occupancy detection using ami data," *IEEE Transactions on Smart Grid*, 2020.

[4] 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*, BuildSys '10, (New York, NY, USA), pp. 61–66, ACM, 2010.

[5] G. Kalogridis, C. Efthymiou, S. Z. Denic, T. A. Lewis, and R. Cepeda, "Privacy for smart meters: Towards undetectable appliance load signatures," in *2010 First IEEE International Conference on Smart Grid Communications*, pp. 232–237, IEEE, 2010.

[6] J. Yao and P. Venkitasubramaniam, "On the privacy-cost tradeoff of an in-home power storage mechanism," in *2013 51st Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pp. 115–122, IEEE, 2013.

[7] O. Tan, D. Gunduz, and H. V. Poor, "Increasing smart meter privacy through energy harvesting and storage devices," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1331–1341, 2013.

[8] J. Gomez-Vilardebo and D. Gündüz, "Smart meter privacy for multiple users in the presence of an alternative energy source," *IEEE Transactions on Information Forensics and Security*, vol. 10, no. 1, pp. 132–141, 2014.

[9] 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, 2016.

[10] G. Giaconi, D. Gündüz, and H. V. Poor, "Smart meter privacy with renewable energy and an energy storage device," *IEEE Transactions on Information Forensics and Security*, vol. 13, no. 1, pp. 129–142, 2017.

[11] S. Li, A. Khisti, and A. Mahajan, "Information-theoretic privacy for smart metering systems with a rechargeable battery," *IEEE Transactions on Information Theory*, vol. 64, no. 5, pp. 3679–3695, 2018.

[12] E. Erdemir, P. L. Dragotti, and D. Gündüz, "Privacy-cost trade-off in a smart meter system with a renewable energy source and a rechargeable battery," in *ICASSP 2019-2019 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, IEEE, 2019.

[13] G. Giaconi, D. Gündüz, and H. V. Poor, "Optimal demand-side management for joint privacy-cost optimization with energy storage," in *2017 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, pp. 265–270, IEEE, 2017.

[14] Y. Sun, L. Lampe, and V. W. Wong, "Smart meter privacy: Exploiting the potential of household energy storage units," *IEEE Internet of Things Journal*, vol. 5, no. 1, pp. 69–78, 2017.

[15] M. Shateri, F. Messina, P. Piantanida, and F. Labeau, "Privacy-cost management in smart meters using deep reinforcement learning," in *IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*, IEEE, 2020. Accepted.

[16] M. Shateri, F. Messina, P. Piantanida, and F. Labeau, "Privacy-cost management in smart meters: An information-theoretic deep reinforcement learning approach," *arXiv preprint arXiv:2006.06106*, 2020.

[17] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *2010 First IEEE International Conference on Smart Grid Communications*, pp. 238–243, IEEE, 2010.

[18] L. Sankar, S. R. Rajagopalan, S. Mohajer, and H. V. Poor, "Smart meter privacy: A theoretical framework," *IEEE Transactions on Smart Grid*, vol. 4, pp. 837–846, June 2013.

[19] H. Yang, L. Cheng, and M. C. Chuah, "Evaluation of utility-privacy trade-offs of data manipulation techniques for smart metering," in *2016 IEEE Conference on Communications and Network Security (CNS)*, pp. 396–400, IEEE, 2016.

[20] M. Shateri and F. Labeau, "Privacy-preserving adversarial network (PPAN) for continuous non-gaussian attributes," *arXiv preprint arXiv:2003.05362*, 2020.

[21] P. Barbosa, A. Brito, and H. Almeida, "A technique to provide differential privacy for appliance usage in smart metering," *Information Sciences*, vol. 370-371, pp. 355 – 367, 2016.

[22] A. Tripathy, Y. Wang, and P. Ishwar, "Privacy-preserving adversarial networks," in *2019 57th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, pp. 495–505, IEEE, 2019.

[23] M. Shateri, F. Messina, P. Piantanida, and F. Labeau, "Deep directed information-based learning for privacy-preserving smart meter data release," in *2019 IEEE International Conference on Communications, Control, and Computing Technologies for Smart Grids (SmartGridComm)*, pp. 1–7, IEEE, 2019.

[24] M. Shateri, F. Messina, P. Piantanida, and F. Labeau, "Real-time privacy-preserving data release for smart meters," *arXiv preprint arXiv:1906.06427*, 2020.

[25] S. Salehkalaibar, F. Aminifar, and M. Shahidehpour, "Hypothesis testing for privacy of smart meters with side information," *IEEE Transactions on Smart Grid*, vol. 10, no. 2, pp. 2059–2067, 2017.

[26] T. M. Cover and J. A. Thomas, "Elements of information theory, 2nd edition," *Willey-Interscience: NJ*, 2006.

[27] Y. Bengio, P. Simard, P. Frasconi, *et al.*, "Learning long-term dependencies with gradient descent is difficult," *IEEE transactions on neural networks*, vol. 5, no. 2, pp. 157–166, 1994.

[28] S. Hochreiter and J. Schmidhuber, "Long short-term memory," *Neural computation*, vol. 9, no. 8, pp. 1735–1780, 1997.

[29] F. A. Gers, J. Schmidhuber, and F. Cummins, "Learning to forget: continual prediction with lstm," in *1999 Ninth International Conference on Artificial Neural Networks ICANN 99. (Conf. Publ. No. 470)*, vol. 2, pp. 850–855 vol.2, Sep. 1999.

[30] I. Goodfellow, Y. Bengio, and A. Courville, *Deep Learning*. MIT Press, 2016.

[31] G. Hinton, N. Srivastava, and K. Swersky, "Neural networks for machine learning lecture 6a overview of mini-batch gradient descent," *Cited on*, vol. 14, p. 8, 2012.

[32] T. Hastie, R. Tibshirani, J. Friedman, and J. Franklin, "The elements of statistical learning: data mining, inference and prediction," *The Mathematical Intelligencer*, vol. 27, no. 2, pp. 83–85, 2005.

[33] C. Beckel, W. Kleiminger, R. Cicchetti, T. Staake, and S. Santini, "The eco data set and the performance of non-intrusive load monitoring algorithms," in *Proceedings of the 1st ACM Conference on Embedded Systems for Energy-Efficient Buildings*, pp. 80–89, ACM, 2014.

[34] L. Mosley, *A balanced approach to the multi-class imbalance problem*. PhD thesis, Iowa State University, 2013.