Time Aggregation for Privacy-Protecting EMU based on Model-Distribution Predictive Control

Jun-Xing Chin, Tomas Tinoco De Rubira and Gabriela Hug
Power Systems Laboratory, ETH Zurich, Switzerland
{chin | tomast | hug}@eeh.ee.ethz.ch

***Abstract*—Smart meter adoption in electricity networks introduces privacy risks for consumers due to the increased measurement frequency and granularity. In particular, consumer behaviour and lifestyle choices may be inferred from their metering data using various Non-Intrusive Load Monitoring techniques. To protect consumer privacy, energy storage controlled by a Model-Distribution Predictive Control scheme can be utilised to mask the actual energy consumption by measuring privacy loss through the mutual information between actual and grid-visible energy consumption. However, the poor scalability of this approach limits the size of the prediction horizon, which is important for both energy cost and privacy loss reduction. In this paper, we propose using time aggregation to increase the reach of the controller's prediction horizon, and describe how to correctly model the statistics in this setting. Results show that with the proposed time aggregation, information leakage and energy costs can be further reduced without increasing the controller's computational requirements.**

***Index Terms*—consumer privacy, model-distribution predictive control, mutual information, smart meter**

I. Introduction

As part of grid modernisation efforts, Smart Meters (SMs) are being deployed globally to replace traditional electromechanical meters. In Europe, large scale roll-outs of SMs in European Union member states are mandated by the European Commission [1]. It is envisioned that real-time measurement of consumption data and two-way communications made possible by SMs would allow for more efficient management of the electrical grid. However, there are concerns that high frequency consumption data measurements would lead to consumer privacy loss [2], [3]. Individual appliance usage, lifestyle patterns, and even preferences may be inferred from consumer load profiles generated from SM data through the use of Non-Intrusive Load Monitoring (NILM) techniques such as those described in [4]–[6]. Even if Utility Providers were to be considered trustworthy, these load profiles may still be accessible by third parties due to the susceptibility of the metering infrastructure to attacks [7].

Various works have looked at methods to protect consumer privacy, enabled either by changing physical energy flow profiles or by information management techniques. One approach of the first category uses energy storage, typically batteries and hence broadly termed Battery Load Hiding (BLH), to change the consumer load profile visible to the grid. The authors in [8] propose the use of Non-Intrusive Load Leveling to hide changes in energy consumption, ideally resulting in a flat load profile. However, this is unsustainable with a finite battery size given the varying nature of consumer load. Another approach, which is described in [9], improves upon this by limiting the energy supplied by the grid to a few levels. Nonetheless, these techniques do not account for the actual information leakage in their control policies, nor consider the potential of energy storage devices to reduce energy costs. Also, heuristics-driven BLH techniques are forced to change their grid-visible consumption due to the battery's state of charge or inverter ratings being unable to cope with the consumer demand. This makes it possible for adversaries to infer information about the actual consumption from such changes [9].

Mutual information, or equivalently information leakage, has been used by prior works such as [10], [11] in the field of information theory as a measure of privacy loss, and to evaluate results in [9]. In our prior work [12], an Energy Management Unit (EMU) based on Model Predictive Control (MPC) that accounts for the mutual information between the consumer load and the nett grid-visible load (grid load) by predicting the effects of its actions on the statistics between these quantities has been proposed. This Model-Distribution Predictive Control (MDPC) scheme attempts to obtain a desired balance between energy cost and privacy by utilising energy storage for energy cost minimisation as well as for consumer load profile masking in a varying-price environment. It involves the introduction of binary variables for counting predicted observations and solving Mixed-Integer Quadratic Programs (MIQPs) whenever new meter readings are available. While the results shown in [12] indicate that privacy loss can be reduced at the expense of energy costs, the scheme is limited to short prediction horizons due to the poor scalability of MIQP solvers. However, longer prediction horizons allow a controller to better account for changes such as load and energy price, which are critical for minimising energy costs and privacy loss.

In this paper, we propose using time aggregations in the prediction horizon of the MDPC scheme proposed in [12], as is done in [13] for power system simulations. This allows time steps further into the future to represent larger time intervals,

This work was supported in part by the *Swiss National Science Foundation* for the COPES project under the CHIST-ERA Resilient Trustworthy Cyber-Physical Systems (RTCPS) initiative, and in part by the *ETH Zurich Postdoctoral Fellowship FEL-11 15-1*.

making it possible for the MDPC-based controller to optimise for events further into the horizon, *e.g.*, load and price changes, thereby further improving privacy protection and minimising energy costs without increasing the computational requirements. The counting scheme used to estimate the statistics of consumer and grid loads is modified to properly model the statistics under time aggregation in the prediction horizon.

This paper is organized as follows: Section II describes the general problem. Section III provides a review of the MDPC scheme proposed in [12]. Section IV introduces the proposed time aggregation technique for the MDPC scheme. Section V analyses the effects of linearising the log terms in MDPC, and Section VI presents the results from numerical experiments. Lastly, Section VII summarizes this work and provides an outlook on further research.

II. Problem Description

In [12], we considered the problem of minimising energy costs and reducing consumer privacy loss in a varying-price environment. The system setup is shown in Fig. 1, where an energy storage device and local generation supplement the grid energy supply at the consumer.

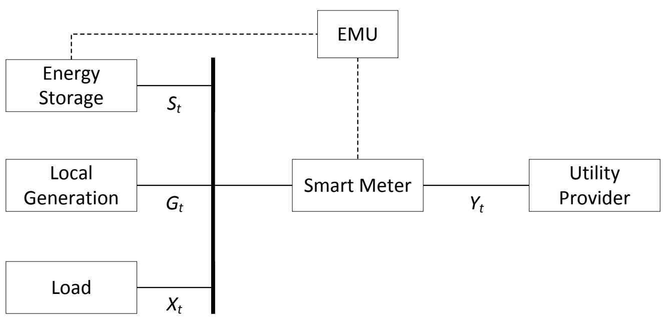


Fig. 1. Energy System Model

The evolution of the considered system is represented by the discrete-time random process $\{(S_t, G_t, X_t, Y_t) \mid t \in \mathbb{Z}_+\}$, where S_t is the energy supplied to the energy storage, G_t is the energy supplied by the local generator (*e.g.*, rooftop solar), X_t is the consumer load, and Y_t is the grid load at time t, *i.e.*,

$$Y_t = X_t + S_t - G_t. \tag{1}$$

The quantities s_t, g_t, x_t, and y_t denote the realisations of these random variables at each time t.

The problem considered may be posed as finding a control policy U^* that determines the charge and discharge of the energy storage over the horizon based on the observed system history such that the expected time-average energy cost and information leakage (privacy loss) is minimised.

The system is subject to the following constraints:

$$S^{\min} \le S_t \le S^{\max} \tag{2}$$

$$0 \le E_t \le E^{\max} \tag{3}$$

$$0 \le G_t \le G^{\max} \tag{4}$$

$$0 \le Y_t \le Y^{\max} \tag{5}$$

$$E_{t+1} = E_t + \alpha S_t, \tag{6}$$

where $-S^{\min} \ge 0$ and $S^{\max} \ge 0$ are the maximum discharging and charging energy over a single time interval, respectively, $G^{\max}$ is the maximum energy output of the generation device, $Y^{\max}$ is the grid supply limit, $E^{\max}$ is the maximum energy storage capacity, and

$$\alpha := \begin{cases} \eta_c, & S_t \ge 0 \\ 1/\eta_d, & S_t < 0 \end{cases}$$

models the charging and discharging losses. Moreover, it is assumed that the energy storage has equal charging and discharging efficiencies, *i.e.*, $\eta_c = \eta_d$.

III. Review of MDPC

In [12], an EMU based on MPC that controls the charge and discharge of energy storage to strike a balance between energy costs and consumer privacy is presented. It uses mutual information between consumer and grid loads as a measure for privacy loss. Assuming time independence, stationarity, and finite support for the statistics of both consumer load X_t and grid load Y_t during a time period spanning the recent past and near future, mutual information is given by

$$I(X;Y) = \sum_{i=1}^{m} \sum_{j=1}^{n} p_{X,Y}(x^i, y^j) \log \frac{p_{X,Y}(x^i, y^j)}{p_X(x^i) p_Y(y^j)},$$

where $\{x^1, ..., x^m\}$ are the possible values for X, $\{y^1, ...y^n\}$ are the possible values for Y, $p_A(a)$ denotes the probability that a random variable A takes on the value a, and log denotes the base-2 logarithm. Introducing binary variables z_τ^{ij} to count predicted observations of $(X_\tau, Y_\tau) = (x^i, y^j)$ in a time window containing the present, it can be shown that the mutual information between X and Y can be estimated using[1]

$$\begin{aligned} I(X;Y) \approx & \sum_{i=1}^{m} \sum_{j=1}^{n} \left(a_t^{ij} + \frac{1}{N} \sum_{\tau=t}^{t+T} z_\tau^{ij} \right) \times \\ & \left\{ \log \left(a_t^{ij} + \frac{1}{N} \sum_{\tau=t}^{t+T} z_\tau^{ij} \right) - \right. \\ & \left. \log \left(b_t^j + \frac{1}{N} \sum_{\tau=t}^{t+T} \sum_{k=1}^{m} z_\tau^{kj} \right) - \log c_t^i \right\}, \end{aligned} \tag{7}$$

where a_t^{ij}, b_t^j, and c_t^i are constants that are computed at time t based on observations up to t, T is the prediction horizon, and N is the size of the counting window. At each time τ, there should be precisely one z_τ^{ij} that equals one, *i.e.*,

$$\sum_{j=1}^{n} z_\tau^{ij} = 1 \tag{8}$$

for each $\tau \in \{t, \ldots, t+T\}$, where

$$i = \underset{k \in \{1,\ldots,m\}}{\arg\min} \|x_\tau - x^k\|_2,$$

[1]Details of this derivation are given in [12].

where x^k is the k-th possible value of the discrete random variable X. Moreover, the constraint

$$z_\tau^{ij} = 1 \iff j = \underset{k\in\{1,\ldots,n\}}{\arg\min} \|y_\tau - y^k\|_2, \tag{9}$$

where y^k is the k-th possible value of the discrete random variable Y, is used to make the binary variables correspond to the appropriate discretised values of Y.

The controller then solves at each time t an optimisation problem with an approximation of the right-hand side of (7) denoted by $\tilde{I}(X;Y)$ obtained by linearising the $\log$ functions:

$$\underset{(y,s,z)\in\mathcal{F}}{\text{minimise}} \ \frac{1}{T+1}\sum_{\tau=t}^{t+T} c_\tau y_\tau + \mu\big[\tilde{I}(X;Y)\big], \tag{10}$$

and implements s_t to achieve the desired y_t that balances energy costs and privacy loss. Parameters c_τ and μ are the costs of energy and privacy loss, respectively, and $\mathcal{F}$ denotes the system and discretisation constraints. Problem (10) is an MIQP, which does not scale well. In [12], we use additive smoothing to prevent linearising the $\log$ functions near zero, and also introduce an l_1-norm regularisation term $r(y)$ in the objective of (10) to reduce the number of candidate MIQP solutions. This regularisation term is given by

$$r(y) = \frac{\rho T^{-1}\|Py - \bar{y}\|_1}{\gamma(\|Px - \bar{x}\|_1 + \|Pg - \bar{g}\|_1) + 1}, \tag{11}$$

where ρ and γ are positive constants, $y,\ x$, and g are grid load, consumer load and local generation vectors used in problem (10) for time t, the matrix P extracts components that correspond to times $t, \ldots, t+T-1$, and $\bar{y},\ \bar{x}$, and $\bar{g}$ denote values of $Y_\tau,\ X_\tau$, and G_τ for $\tau = t, \ldots, t+T-1$ predicted during the solution of problem (10) for time $t-1$.

While this method is computationally tractable for small instances of problem (10) and balances privacy loss with energy costs, it does not scale with large prediction horizons T and number of possible Y values. This limits the controller's prediction time reach, which is important for anticipating events further into the future that are critical for further reduction of energy costs and privacy loss, *e.g.* price and load changes.

IV. MDPC WITH TIME AGGREGATION

In order to extend the time reach of the MDPC scheme, we propose the use of prediction time horizons with varying step sizes (denoted as time aggregation in [13]), terming the approach Model-Distribution Predictive Control with Time Aggregation (MDPC-TA). Fig. 2 illustrates this concept, where M is the observation history considered by the controller, and N_{HS} is the counting window for the MDPC-TA scheme.

In the MDPC-TA scheme, time steps further into the future represent larger time intervals, thus allowing for the controller to reach further in time without increasing the computational requirements. However, the counts used for estimating the statistics in the computation of mutual information are based on a fixed time interval denoted by Δ. For statistical consistency, (7) needs to be modified to account for the heterogeneous time intervals. For example, a time step that represents an interval twice the length of Δ should also have twice the statistical count. As such, the statistical counts of time steps representing time intervals different from Δ are multiplied by a scaling factor $w_\tau \in \mathcal{W}$ that defines their size in units of Δ. The counting window $N = M + T$ also needs to be modified to $N_{HS} = M + \sum_{\tau=t}^{t+T} w_\tau$ to ensure that the probabilities sum to one. The approximation (7) is reformulated as

$$\begin{aligned} I(X;Y) \approx &\sum_{i=1}^{m}\sum_{j=1}^{n}\left(\bar{a}_t^{ij} + \frac{1}{N_{HS}}\sum_{\tau=t}^{t+T} z_\tau^{ij} w_\tau\right)\times \\ &\left\{\log\left(\bar{a}_t^{ij} + \frac{1}{N_{HS}}\sum_{\tau=t}^{t+T} z_\tau^{ij} w_\tau\right) - \right. \\ &\left.\log\left(\bar{b}_t^{j} + \frac{1}{N_{HS}}\sum_{\tau=t}^{t+T}\sum_{k=1}^{m} z_\tau^{kj} w_\tau\right) - \log \bar{c}_t^{i}\right\}, \end{aligned} \tag{12}$$

where $\bar{a}_t^{ij}$, $\bar{b}_t^{j}$, and $\bar{c}_t^{i}$ are now constants at time t computed with N_{HS} instead of N. Furthermore, it is assumed that $N_{HS} \geq N \gg T$ so that the $\log$ terms can be linearised, giving

$$\begin{aligned} \tilde{I}_w(X;Y) = &\sum_{i=1}^{m}\sum_{j=1}^{n}\left(\bar{a}_t^{ij} + \frac{1}{N_{HS}}\sum_{\tau=t}^{t+T} z_\tau^{ij} w_\tau\right)\times \\ &\left\{\log\frac{\bar{a}_t^{ij}}{\bar{b}_t^{j}\bar{c}_t^{i}} + \frac{\nu}{\bar{a}_t^{ij} N_{HS}}\sum_{\tau=t}^{t+T} z_\tau^{ij} w_\tau - \right. \\ &\left.\frac{\nu}{\bar{b}_t^{j} N_{HS}}\sum_{\tau=t}^{t+T}\sum_{k=1}^{m} z_\tau^{kj} w_\tau\right\}, \end{aligned}$$

where $\nu := 1/\log_e 2$.

The controller now solves

$$\underset{(y,s,z)\in\mathcal{F}}{\text{minimise}} \ \frac{1}{T+1}\sum_{\tau=t}^{t+T} c_\tau y_\tau w_\tau + \mu\big[\tilde{I}_w(X;Y)\big]. \tag{13}$$

The objective function (13) and constraints (1) - (6), (8), and (9) result in a formulation that allows for consideration of events further in the future without increasing the problem size. It also shifts the weights of the controller actions, making predicted actions of time steps representing larger intervals carry more weight in reducing information leakage. We hypothesize that this would cause the controller to allocate more valuable control actions, *i.e.*, less energy costs (due to w_τ in (13)) or lower privacy loss, to the time steps further in the prediction horizon.

V. ANALYSIS OF $\log$ LINEARISATION

Due to the linearisation of the $\log$ function in the optimisation problem, there are instances where the controller may perceive that its actions reduce information leakage, when in fact they increase it instead. We illustrate this by an example shown in Fig. 3 and Table I, where $\hat{I}(X;Y)$ denotes the right hand side of (12). Given are two feasible control actions,

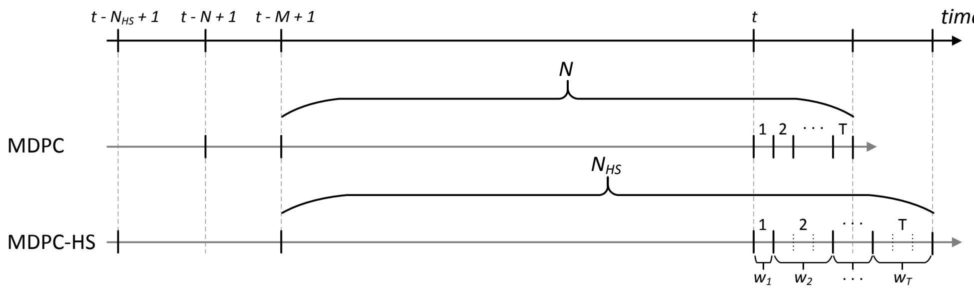
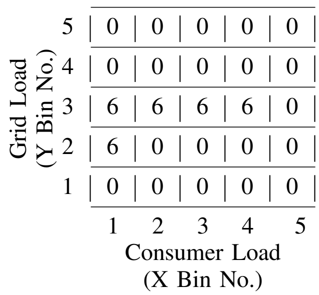
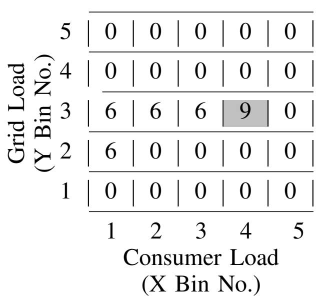


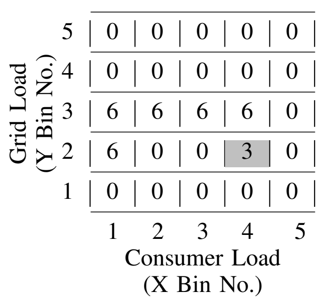
Fig. 2. The concept of heterogenous time-steps in MDPC



(a) Observed history



(b) Alternative A



(c) Alternative B

Fig. 3. Statistics illustrating two alternative control actions

TABLE I
FEASIBLE CONTROL ACTIONS FOR GIVEN EXAMPLE

	$\hat{I}(X;Y)$	$\tilde{I}(X;Y)$
Current privacy loss	0.287	0.287
Alternative A	0.289	0.315
Alternative B	0.217	3.532

highlighted in grey in Fig. 3(b) and 3(c), based on the observed history and privacy loss shown in Fig 3(a). As seen in Table I, the controller would choose control action A, which it perceives to result in a lower privacy loss. However, this increases the actual privacy loss from 0.287 bits to 0.289 bits. Had it chosen control action B instead, it would have reduced privacy loss to 0.217 bits.

Due to time steps farther into the horizon having greater statistical count from the larger step sizes, actions that seem more valuable in reducing privacy loss but actually result in its increase may be allocated to these later time steps, potentially avoiding their implementation, resulting in a more monotonic evolution of privacy loss over time.

TABLE II
GENERAL SIMULATION PARAMETERS

MDPC		MDPC-TA	
T	12	T	12
M	120	M	120
N	132	N_{HS}	144
ρ	0.11	ρ	0.11
γ	0	γ	0
Battery Size	6.4kWh	Battery Size	6.4kWh
Battery Power	3.3kW	Battery Power	3.3kW
Battery Eff. η_c, η_d	96%	Battery Eff. η_c, η_d	96%

VI. NUMERICAL EXPERIMENTS

We implemented both the MDPC and MDPC-TA schemes in YALMIP [14], and simulated them in MATLAB with the IBM CPLEX 12.6.3 solver. The load profiles were generated using tools developed in [15] over the period of one month (30 days) with hourly resolution in a two-tier pricing environment (c_t = {24.6 , 13.15} Rp/kWh). Simulations were run on a computer with an Intel Core i7-2600 CPU at 3.40 GHz and 16.0 GB of RAM, running 64-bit Windows 10 Enterprise.

Both schemes were applied for varying prices of privacy loss, μ, with local generation set to zero, using battery parameters from the Tesla Powerwall and $\mathcal{W} = \{1, 1, 1, 1, 2, 2, 2, 2, 2, 2, 4, 4\}$ for the MDPC-TA scheme. Unless stated otherwise, the general simulation parameters shown in Table II are used for the simulations.

The regularisation term $r(y)$, (11), is modified to $r'(y)$ to account for the varying step sizes. The additive smoothing parameter is chosen to be 0.1 in order to ensure that the logarithms are sufficiently expanded away from zero [12].

A. Visualisation of Load Profiles

Fig. 4 shows the consumer and grid loads for the MDPC and MDPC-TA schemes over the course of seven days with $\mu = 16$. Both schemes result in a grid load profile that differs from the original consumer load profile by a random pattern, preventing malicious third parties from inferring the original consumer load profile. Both curves also take on a step-like behaviour similar to that in [9]. However, the MDPC-TA scheme has more periods of levelled grid load, exhibiting a behaviour closer to that of [8], but with an adaptive stepping to cater for battery state, energy cost and consumer load changes.

B. Performance of the MDPC-TA Scheme

The proposed scheme was evaluated using the right-hand side of (12) with a static window length $N = 718$, which

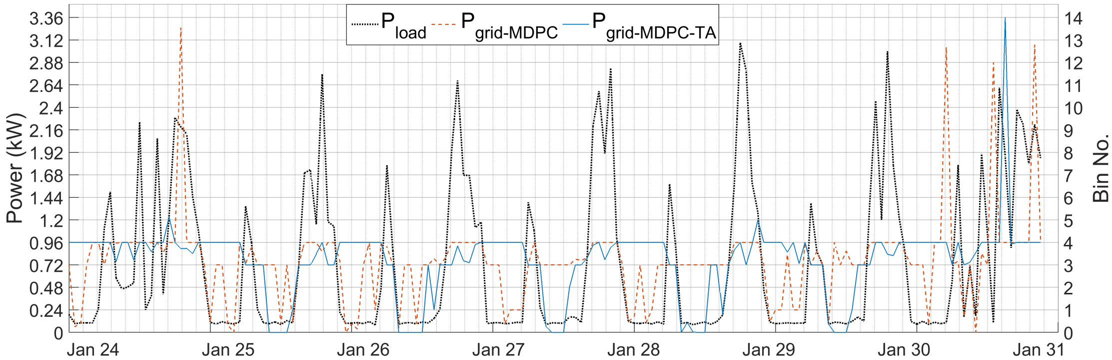


Fig. 4. Consumer and grid loads over 7 days

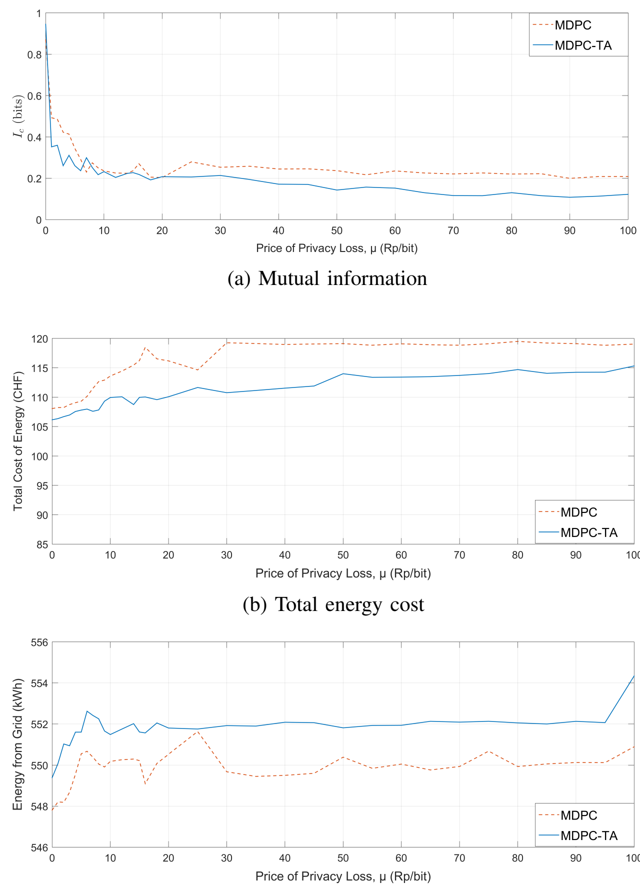
TABLE III
COMPUTATIONAL TIME AND RESULTS OF COMPARED SCHEMES AT $\mu = 15$

	MDPC	MDPC-Ext	MDPC-TA
Average Solver Time (s)	0.161	9.26	0.221
Median Solver Time (s)	0.126	5.64	0.206
Min. Solver Time (s)	0.053	1.59	0.122
Max. Solver Time (s)	1.14	152	0.776
I_c (bits)	0.236	0.209	0.227
Total Grid Energy (kWh)	550	552	552
Total Energy Costs (CHF)	116	109	110

is approximately the entire 30 day simulation period. This "cumulative" mutual information, which we denote by I_c, measures the privacy loss using statistics gathered over the entire simulation period. In Fig. 5, the mutual information I_c, total energy cost, and total grid energy consumption are shown as a function of the price of privacy loss, μ. As seen in Fig. 5(a) and 5(b), the MDPC-TA scheme is able to further reduce both the privacy loss and total cost of energy by using a prediction horizon that reaches further into the future. It does this without increasing the computational requirements of the controller since the size of the problem is the same as for the MDPC scheme. As shown in Fig. 5(c), the total energy consumed with the MDPC-TA scheme is greater than with the MDPC scheme. This is evidence of the the fact that the MDPC-TA scheme utilises the full capacity of the battery to cover more consumer load during high-price periods, and further illustrated in Fig. 6(a) that shows the change in the battery's state of charge. This difference in effectiveness of utilising the full battery capacity is more pronounced for a larger 12.8 kWh battery, as seen in Fig. 6(b). The sections highlighted in Fig. 6 indicate periods of lower energy prices.

Note that the curves in Fig. 5(a) to 5(c) do not evolve monotonically with increasing price of privacy due to the inherent randomness in choosing from multiple non-unique optimal points of the MIQP problems, which was also presented in [12]. These different candidate solutions are equivalent from the perspective of the MIQP solver but result in different trajectories of the controller during the evaluation period. We hypothesize that this "range" of fluctuations goes down as the length of the evaluation period of the controller increases.

In order to compare the proposed MDPC-TA scheme's performance to the MDPC scheme with similar time reach,



(a) Mutual information

(b) Total energy cost

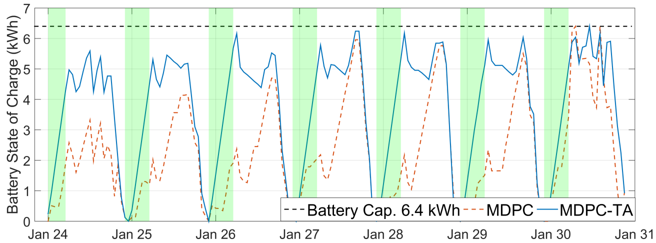
(c) Total grid energy consumption

Fig. 5. Comparison between the MDPC and MDPC-TA schemes with 6.4kWh batteries

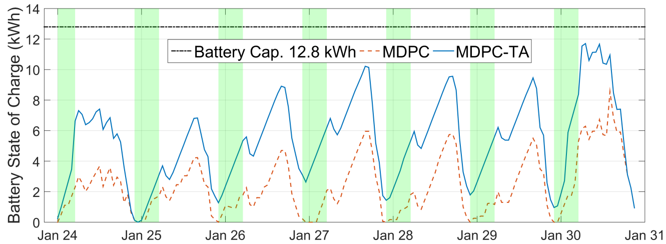
we simulated an instance of the MDPC scheme with $T = 24$ and $\mu = 15$, denoted by MDPC-Ext. As seen in Table III, the MDPC-TA scheme is able to achieve lower energy costs similar to that of MDPC-Ext and better privacy protection, whilst maintaining the computational tractability similar to that of the MDPC scheme with $T = 12$.

C. Rolling Window Mutual Information Time Series

In order to study the evolution of mutual information with time, we evaluated both controllers' performance with $\mu =$



(a) 6.4 kWh battery



(b) 12.8 kWh battery

Fig. 6. Battery SoC for two battery sizes

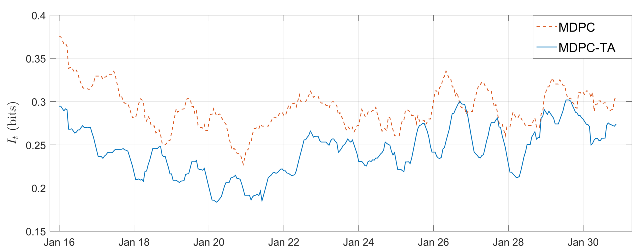


Fig. 7. I_t over 16 days for the MDPC and MDPC-TA schemes

16 using the right-hand-side of (12) with a moving window of $N = 132$, denoting this by I_t. More specifically, I_t is associated with the observation history from time $t - N + 1$ to time t.

In Fig. 7, the mutual information rolling window time series, I_t, for the MDPC-TA scheme is seen to be visibly lower than that for the MDPC scheme, consistent with findings from Fig. 5(a). Additionally, both I_t curves exhibit a pattern consistent with the daily consumer load cycles. Further analysing the curves, it can be seen that the MDPC-TA scheme also has less "noise-like" variability, which we quantify using total variation (sum of absolute changes), and summarise in Table IV. As discussed in Section IV, this is due to seemingly "more private" control actions that actually increase information leakage being less likely to be implemented. Moreover, the battery is more likely to have sufficient charge to maintain a certain privacy level due to its further prediction reach.

TABLE IV
TOTAL VARIATION OF I_t

	MDPC	MDPC-TA
Total Variation	1.38	1.23
Reduction (%)	0%	-11.4%

VII. CONCLUSION

In this paper, we introduced time aggregations for the prediction horizon in the MDPC scheme, allowing it to account for events further into the future. The counts used in estimating the statistics of the consumer and grid loads were modified to model the increased time intervals using appropriate weights. This allowed the proposed MDPC-TA scheme to achieve better privacy protection and lower energy costs without increasing the computational requirements of the controller.

Future research will focus on studying time correlation of the statistics, and relaxation techniques for the MDPC scheme, as well as studying the impact of forecast errors.

REFERENCES

[1] European Union, "Directive of 2009/72/EC of the European Parliament and of the Council of 13 July 2009 Concerning Common Rules for the Internal Market in Electricity and Repealing Directive 2003/54/EC," *Official Journal of the European Union*, vol. L211, no. August, pp. L211/55-L 211/93, 2009.

[2] E. L. Quinn, "Privacy and the New Energy Infrastructure," in *Social Science Research Network*, 2009. [Online]. Available: http://dx.doi.org/10.2139/ssrn.1370731

[3] P. McDaniel and S. McLaughlin, "Security and Privacy Challenges in the Smart Grid," *IEEE Security & Privacy*, vol. 7, no. 3, pp. 75-77, 2009.

[4] Z. Guanchen, G. Wang, H. Farhangi, and A. Palizban, "Residential electric load disaggregation for low-frequency utility applications," in *Power & Energy Society General Meeting*, 2015 IEEE, 2015, pp. 1-5.

[5] M. A. Lisovich, D. K. Mulligan, and S. B. Wicker, "Inferring Personal Information from Demand-Response Systems," *IEEE Security & Privacy*, vol. 8, no. 1, pp. 11-20, 2010.

[6] U. Greveler, B. Justus, and D. Loehr, "Multimedia content identification through smart meter power usage profiles," *Computers, Privacy and Data Protection*, vol. 1, p. 10, 2012.

[7] S. McLaughlin, D. Podkuiko, S. Miadzvezhanka, A. Delozier, and P. McDaniel, "Multi-vendor penetration testing in the advanced metering infrastructure," in *Proc. 26th Annual Computer Security Applications Conference (ACSAC)*, Austin, Texas, USA, pp. 107-116, 2010.

[8] S. McLaughlin, P. McDaniel, and W. Aiello, "Protecting consumer privacy from electric load monitoring," in *Proceedings of the 18th ACM Conference on Computer and Communications Security*, Chicago, Illinois, USA, pp. 87-98, 2011.

[9] W. Yang, N. Li, Y. Qi, W. Qardaji, S. McLaughlin, and P. McDaniel, "Minimizing private data disclosures in the smart grid," in *Proceedings of the 2012 ACM Conference on Computer and Communications Security*, Raleigh, North Carolina, USA, pp. 415-427, 2012.

[10] G. Giaconi and D. Gunduz, "Smart meter privacy with renewable energy and a finite capacity battery," in *IEEE Workshop on Signal Processing Advances in Wireless Communications, SPAWC*, vol. 2016-August, Edinburgh, UK, 2016, pp. 1-5.

[11] S. Li, A. Khisti, and A. Mahajan, "Structure of optimal privacy preserving policies in smart-metered systems with a rechargeable battery," in *Signal Processing Advances in Wireless Communications (SPAWC)*, 2015 IEEE 16th International Workshop on, 2015, pp. 375-379.

[12] J. Chin, T. Tinoco De Rubira, and G. Hug, "Privacy-protecting energy management unit through model-distribution predictive control," unpublished, *IEEE Trans. Smart Grid*. [Online]. Available: https://arxiv.org/abs/1612.05120

[13] S. Deml, A. Ulbig, T. Borsche, and G. Andersson,"The role of aggregation in power system simulation," in *2015 IEEE Eindhoven PowerTech. IEEE*, 6 2015, pp. 1-6.

[14] J. Lofberg, "YALMIP : a toolbox for modeling and optimization in MATLAB," in *Computer Aided Control Systems Design, 2004 IEEE International Symposium on*, 2004, pp. 284-289.

[15] N. Pflugradt, J. Teuscher, B. Platzer, and W. Schufft, "Analysing low voltage grids using a behaviour based load profile generator," in *Renewable Energy and Power Quality Journal*, 2013.