Impact Assessment of Net Metering on Smart Home Cyberattack Detection

Invited

Yang Liu and Shiyan Hu
Michigan Technological University
1400 Townsend Drive
Houghton, MI, USA, 49931
{yliu18, shiyan}@mtu.edu

Jie Wu and Yiyu Shi
Missouri University of Science and Technology
1870 Miner Cir.
Rolla, MO, USA 65409
{wujie, yshi}@mst.edu

Yier Jin
University of Central Florida
4000 Central Florida Blvd
Orlando, FL, USA 32816
yier.jin@eecs.ucf.edu

Yu Hu and Xiaowei Li
State Key Laboratory of Computer Architecture
ICT of CAS
Beijing, China, 100190
{huyu, lxw}@ict.ac.cn

ABSTRACT

Despite the increasing popularity of the smart home concept, such a technology is vulnerable to various security threats such as pricing cyberattacks. There are some technical advances in developing detection and defense frameworks against those pricing cyberattacks. However, none of them considers the impact of net metering, which allows the customers to sell the excessively generated renewable energy back to the grid. At a superficial glance, net metering seems to be irrelevant to the cybersecurity, while this paper demonstrates that its implication is actually profound.

In this paper, we propose to analyze the impact of the net metering technology on the smart home pricing cyberattack detection. Net metering changes the grid energy demand, which is considered by the utility when designing the guideline price. Thus, cyberattack detection is compromised if this impact is not considered. It motivates us to develop a new smart home pricing cyberattack detection framework which judiciously integrates the net metering technology with the short/long term detection. The simulation results demonstrate that our new framework can significantly improve the detection accuracy from 65.95% to 95.14% compared to the state-of-art detection technique.

Keywords

Net Metering, Smart Home, Cyberattack, Renewable Energy, Stochastic Optimization

1. INTRODUCTION

Smart home has gained popularity in recent years due to the automatic control of household activities, energy efficiency and low economical cost. Taking advantage of the advanced metering infrastructure (AMI), the smart home system receives the utility pricing information using smart meters. Subsequently, smart home scheduling techniques are applied to schedule operations of home appliances for shifting the heavy energy load off the peak pricing hours [6]. There are two pricing schemes in this process. That is, *real time pricing* is used to bill the customers based on the energy usage during the past time window, and *guideline pricing*, in which the utility predicts the future electricity price, is used to facilitate the smart home scheduling [8]. This helps balance the energy load in the power grid.

In addition to smart home scheduling, home level distributed generation (DG) such as PV panels plays an important role in the smart home system. It supplies energy to customers directly using the local resource, mitigating the burden of power generation and transmission. In addition, when excessive renewable energy is generated, customers are encouraged to sell it back to the power grid to be rewarded, which is known as *net metering*. In fact, net metering has already been implemented in 27 states in U.S. [1, 2]. The reward for selling energy depends on the real time electricity price as well as the electricity market regulations that vary in different states. Furthermore, with a rechargeable battery, a customer can keep the energy for future use [5]. It is clear that the above mechanisms impact the energy demand from grid, which makes its prediction difficult.

On the other hand, the smart home system is vulnerable to cyberattacks. For example, a malicious hacker can attack smart meters through manipulating the received guideline prices. This can mislead the smart home scheduling solutions and further impact the energy load of a community. For this, two closely related pricing cyberattacks are proposed in [8] and [7], which increase the customer electricity bill and the peak energy usage. The single event and long term defense techniques are then developed based on support vector regression (SVR) and partially observable Markov decision process (POMDP). However, none of the previous works consider the impact of net metering which changes the energy demand from grid and thus the utility pricing. Since the detection techniques rely on the prediction of utility pricing, ignoring net metering impact can signifi-

DAC'15 June 7-11, 2015, San Francisco, California, USA

http://dx.doi.org/10.1145/2744769.2747930 .

cantly compromise the detection. This paper first analyzes such impact and then develops a net metering aware energy load prediction which is further integrated into the cyberattack detection. Our contributions are listed as follows.

- A net metering aware energy load prediction technique is proposed based on the cross entropy optimization.
- A smart home pricing cyberattack detection technique considering the net metering impact is proposed, which is the first such work in the problem context. This technique is constructed based on the partially observable Markov decision process smart home cyberattack detection framework developed in [7].
- The simulation results demonstrate that our new framework can significantly improve the detection accuracy from 65.95% to 95.14% compared to the state of art detection technique.

2. PRELIMINARIES

Consider a community consisting of N customers. Refer to Figure 1. Each customer is supplied by energy from both the grid and the home level PV panel. Smart home technique is deployed such that each customer $n \in \mathcal{N}$ has a set of home appliances $\mathcal{A}_n$ to be scheduled by a smart controller. The customers keep receiving the guideline price from the utility, and each customer schedules the energy consumption in the next 24 hours which is divided into H time slots.

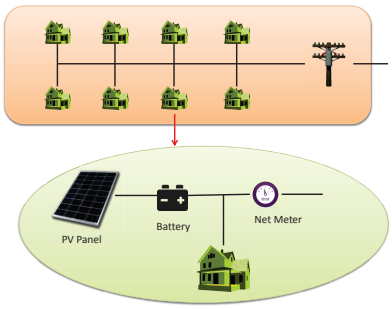

Figure 1: The system model.

2.1 Energy Consumption

Each customer uses smart home scheduling technique to schedule the home appliances. For home appliance $m \in \mathcal{A}_n$, denoted by $\mathcal{X}_m$ the set of power levels. At each time slot, the customer n chooses a power level $x_m^h \in \mathcal{X}_m$ for the home appliance m subject to the following constraints. (1) The total energy consumption of home appliance m over the time horizon is equal to the required energy consumption of the specified task E_m such that $\sum_{h=1}^{H} x_m^h e_m^h = E_m$, where e_m^h is the actual execution time period of home appliance m at time slot h. (2) The home appliance m starts to work no earlier than the required start time α_m and completes the task no later than the deadline β_m such that $x_m^h = 0, \forall h < \alpha_m \quad or \quad h > \beta_m$. Denote by l_n^h the energy consumption of customer n at time slot h. Thus, the community energy load L_h is calculated as $L_h = \sum_{n=1}^{N} l_n^h$. At time slot h, the total energy consumption of customer n is equal to the total energy consumption of all the home appliances such that $\sum_{m \in \mathcal{A}_n} x_m^h e_m^h = l_n^h$.

2.2 Net Metering

Each customer is installed with a home level PV panel and a rechargeable battery. The PV panel serves as a DG unit to the customer. The battery can store the residual energy for future use. Denote by θ_n^h the renewable energy generated by the PV panel of the customer n at time slot h, which is assumed to be approximately known in advance through prediction. The renewable energy generated in the whole community is calculated as $\Theta_h = \sum_{n=1}^{N} \theta_n^h$. The energy storage of customer n at time slot h is denoted by b_n^h, which is upper bounded by B_n such that $0 \leq b_n^h \leq B_n$.

Net metering says that each customer can sell the energy generated by the PV panel and stored in the battery back to the grid. Thus, at each time slot, the customer could purchase energy from the grid or sell energy to the grid. Denote by y_n^h the energy trading amount of customer n at time slot h. The customer purchases energy from the grid if $y_n^h > 0$ and sell energy to the grid if $y_n^h < 0$. The energy sold by a customer could be consumed by some neighbors in the same community. Thus, the total amount of energy purchased from the utility is $\sum_{n=1}^{N} y_n^h$. For each customer, the battery storage at each time slot is constrained by

$$b_n^{h+1} = b_n^h + \theta_n^h + y_n^h - l_n^h. \tag{1}$$

2.3 Monetary Cost

The popular quadratic pricing model is used to compute the monetary cost for purchasing energy from the utility. Thus, the total monetary cost of the community at time slot h is $p_h(\sum_{n=1}^{N} y_n^h)^2$ [9], where p_h is the guideline price.

Each customer is paid with a partial price when selling energy to the grid, which is denote by $\frac{p_h}{W}$ where $W \geq 1$ is a constant. Thus, the total monetary cost of customer n at time slot h is given as

$$C_n^h = \begin{cases} p_h(\sum_{i=1}^{N} y_i^h) y_n^h, & if \quad y_n^h \geq 0 \\ -\frac{p_h}{W}(\sum_{i=1}^{N} y_i^h) y_n^h, & if \quad y_n^h < 0 \end{cases}. \tag{2}$$

Note that the utility pays the customer with the rate $\frac{p_h}{W}$ for selling energy back to the grid and sells it to other customers with price p_h. The difference between those two prices is cost of the utility due to supporting net metering. Plugging Eqn. (1) into Eqn. (2), the monetary cost of customer n at time slot h can be rewritten in terms of energy consumption, renewable energy generation and battery storage as

$$C_n^h = \begin{cases} p_h[\sum_{i=1, i\neq n}^{N}(y_i^h) + l_n^h + b_n^{h+1} - \theta_n^h - b_n^h](l_n^h \\ -\theta_n^h - b_n^h + b_n^{h+1}), \quad if \quad l_n^h - \theta_n^h - b_n^h + b_n^{h+1} \geq 0 \\ -\frac{p_h}{W}[\sum_{i=1, i\neq n}^{N}(y_i^h) + l_n^h + b_n^{h+1} - \theta_n^h - b_n^h](l_n^h \\ -\theta_n^h - b_n^h + b_n^{h+1}), \quad if \quad l_n^h - \theta_n^h - b_n^h + b_n^{h+1} < 0 \end{cases}. \tag{3}$$

3. ENERGY LOAD PREDICTION CONSIDERING NET METERING

3.1 Game Formulation Considering Net Metering

Given the above model of smart home technique, each customer n aims to minimize his/her monetary cost within the next 24 hours, which depends on the energy scheduling and net metering/energy trading. Each customer aims to assign the power level of each home appliance x_m^h and determine the battery storage b_n^h. This naturally leads to a game among customers as follows.

Net Metering Aware Energy Consumption Scheduling Game

- Players: Customers $\{1, 2, \ldots, N\}$
- Shared Information: y_n^h
- Optimization Problem:

$$\textbf{P1} \quad \textbf{minimize} \quad \sum_{h=1}^{H} C_n^h$$

$$\textbf{subject to} \quad \sum_{h=1}^{H} x_m^h e_m^h = E_m$$

$$\sum_{m \in \mathcal{A}_n} x_m^h e_m^h = l_n^h$$

$$b_n^{h+1} = b_n^h + \theta_n^h + y_n^h - l_n^h$$

$$x_m^h = 0, \forall h < \alpha_m \quad or \quad h > \beta_m$$

$$C_n^h = \begin{cases} p_h[\sum_{i=1, i\neq n}^{N}(y_i^h) + l_n^h + b_n^{h+1} - \theta_n^h - b_n^h] \\ (l_n^h - \theta_n^h - b_n^h + b_n^{h+1}), \\ if \quad l_n^h - \theta_n^h - b_n^h + b_n^{h+1} \geq 0 \\ -\frac{p_h}{W}[\sum_{i=1, i\neq n}^{N}(y_i^h) + l_n^h + b_n^{h+1} - \theta_n^h - b_n^h] \\ (l_n^h - \theta_n^h - b_n^h + b_n^{h+1}), \\ if \quad l_n^h - \theta_n^h - b_n^h + b_n^{h+1} < 0 \end{cases}$$

- Decision Variables: x_m^h and b_n^h.

Each customer tends to follow the above game to minimize the monetary cost, which means that solving it can predict the energy load in the future given the guideline price.

3.2 Problem Solving

The iterative approach is a standard way to solve the energy consumption scheduling game in which each customer solves Problem **P1** assuming the total energy trading of other customers is fixed in each iteration. After the new solution is obtained, each customer updates the energy trading to solve Problem **P1**. This is repeated until convergence. The complete procedure is described in Algorithm 1. In line 4, the customer determines x_m^h while assuming b_n^h is fixed using the dynamic programming based method proposed in [6]. In line 5, the customer determines the optimal battery storage b_n^h using the stochastic optimization algorithm proposed. Problem **P1** is non-convex in terms of the battery storage. To circumvent this difficulty, we propose a stochastic optimization algorithm based on cross entropy optimization to compute the battery storage that minimizes the monetary cost.

Cross entropy optimization method is a stochastic optimization technique based on importance sampling [3]. For completeness, some theoretic foundation of the cross entropy optimization method is included as follows. Consider the following optimization problem as a generalization of **P1**.

$$\begin{aligned} \textbf{minimize} \quad & f(\mathbf{b}_n) \\ \textbf{subject to} \quad & \mathbf{b}_n \in \mathcal{B} \\ & \mathbf{b}_n = \{b_n^1, b_n^2, \ldots, b_n^H\} \end{aligned}, \tag{4}$$

where $\mathbf{b}_n = \{b_n^1, b_n^2, \ldots, b_n^H\}$ is the battery storage over the time horizon and $\mathcal{B}$ is the feasible set of $\mathbf{b}_n$. In the cross entropy optimization method, a probability density function (PDF) in $\mathcal{B}$ is employed, which is denoted by $\rho(\mathbf{b}, p)$ while p characterizes the PDF. The cross entropy optimization method aims to find the maximum value of ϵ such that

Algorithm 1 Net Metering Aware Energy Load Prediction Algorithm

Require: E_m, θ_n^h, α_m, β_m, $\mathcal{X}_m$ and p_h

```
1: while Not converge do
2:   for Each customer n do
3:     while Not converge do
4:       Solve Problem P1 using dynamic programming based method to compute x_m^h assuming b_n^h is fixed.
5:       Solve Problem P1 using cross entropy optimization based method to compute b_n^h assuming x_m^h is fixed.
6:     end while
7:   end for
8: end while
9: return x_m^h and b_n^h
```

$P[f(\mathbf{b}_n) \leq \epsilon] \rightarrow 0$. Since $P[f(\mathbf{b}_n) \leq \epsilon]$ cannot be known analytically, the cross entropy optimization method evaluates it using Monte-Carlo simulations. Denote by $\delta(\epsilon) = P[f(\mathbf{b}_n) \leq \epsilon]$ an indicator function and $[\mathbf{B}_1, \mathbf{B}_2, \ldots, \mathbf{B}_K]$ a set of samples generated from the PDF $\rho(\mathbf{b})$. Thus, the indicator function is evaluated by $\delta(\epsilon) = \frac{1}{K}\sum_{k=1}^{K} P[f(\mathbf{B}_k) \leq \epsilon]$.

However, $P[f(\mathbf{b}_n) \leq \epsilon]$ is a rare event since it approaches zero eventually. Thus, a large amount of samples are needed to compute the maximum value of ϵ. To circumvent this difficulty, the cross entropy optimization method utilizes the idea of importance sampling. It updates the PDF $\rho(\mathbf{b}, p)$ to improve the generated samples such that they will locate in an area with better objective values. Denote by $\theta(\mathbf{b}, p)$ the optimal PDF. The estimation of $\delta(\epsilon)$ can be presented by $\hat{\delta}(\epsilon) = \frac{1}{K}\sum_{k=0}^{K} P[f(\mathbf{B}_k) \leq \epsilon] \frac{\rho(\mathbf{B}_k)}{\theta(\mathbf{B}_k)}$.

Define by $\theta^*(\mathbf{b}) = \frac{P[f(\mathbf{B}_k) \leq \epsilon]\rho(\mathbf{b}, p)}{\delta(\epsilon)}$ the optimal PDF. Thus, $\hat{\delta}(\epsilon)$ can approach the optimal value of $\delta(\epsilon)$. The cross entropy method finds the optimal PDF by minimizing the Kullback-Leibler distance, which is equivalent to solving the optimization problem

$$\max_{p} \int \theta^*(\mathbf{b}) \ln \rho(\mathbf{b}, p) d\mathbf{b}, \tag{5}$$

Thus, the optimal PDF in $\rho(\mathbf{b}, p)$, p^* can be estimated as $\hat{p}^* = \arg\max_{p} \frac{1}{K}\sum_{k=1}^{K} P[f(\mathbf{B}_k) \leq \epsilon] \frac{f(\mathbf{B}_k, u)}{f(\mathbf{B}_k, w)} \ln \rho(\mathbf{B}_k, p)$. In the optimization of battery storage, we repeatedly generate samples using the PDF $\rho(\mathbf{b}, p)$ and update it through solving Eqn. (5) until convergence.

4. IMPACT OF NET METERING TO PRICING CYBERATTACK DETECTION

The smart home system is vulnerable to cyberattacks. The malicious hacker can attack the smart meter and manipulate the received guideline price. This can mislead the smart home scheduling of the customers and impact the energy load. As demonstrated by [8], the cyberattacks can significantly increase the peak to average ratio (PAR) of the energy load, which can impact the stability of the power grid. In terms of detection, [7] proposes to predict the future guideline price from the historical data using support vector regression (SVR) and compares it with the received guideline price. Since this technique works only for single event detection, subsequently a partially observable Markov decision process based detection is developed for long term

monitoring and detection. However, net metering changes the grid energy demand which also changes the guideline pricing. Since the detection framework in [7] involves the guideline pricing prediction, it could be compromised if the net metering impact is not considered. It motivates us to integrate the above cross entropy optimization based grid energy prediction (and thus the guideline price prediction) into the pricing cyberattack detection to improve detection accuracy.

4.1 SVR Based Single Event Detection

At each single time slot, the cyberattack is detected based on the comparison between the received guideline price and historical data. Since the electricity price tends to be similar in short term, support vector regression (SVR) is deployed to predict the guideline price using only the historical data [10]. However, such a prediction is not accuracy since the energy demand prediction also needs to consider the net metering impact.

As is known, the energy demand depends on the current guideline price as well as the renewable energy generation. Thus, we consider both the impact of the historical guideline price and the renewable energy in our SVR model. Denote by $\mathbf{p} = \{p_1, p_2, p_3, \ldots, p_T\}$ the vector of guideline price from time slot 1 to T. Denote by $\mathbf{V} = \{\Theta_1, \Theta_2, \Theta_3, \ldots, \Theta_T\}$ the vector of renewable energy generation from time slot 1 to T. Denote by $\mathbf{D} = \{L_1, L_2, \ldots, L_T\}$ the energy demand from time slot 1 to T. We define a function $\mathbf{G}(\mathbf{p}, \mathbf{V}, \mathbf{D})$, which models the predicted guideline price $\mathbf{p}_v$ using the difference between the total energy demand and renewable energy. Thus, the single event defense technique originally proposed in [7] is modified as follows.

- Predict the guideline price $\mathbf{p}_v$ using SVR from the time series $\mathbf{G}(\mathbf{p}, \mathbf{V}, \mathbf{D})$.
- The customers conduct smart home scheduling simulation with predicted and received guideline prices, respectively.
- Compare the peak to average ratio (PAR) with predicted and received guideline prices, defined by P_p and P_r, respectively.
- Cyberattack is reported if $P_r - P_p > \delta_P$, where δ_P is a predefined threshold.

4.2 POMDP Based Long Term Detection

The single event detection technique is based on the PAR increase in a single time slot, which cannot address the cumulative impact [7]. Furthermore, the transient variation of the electricity price can reduce the detection accuracy. Thus, a partially observable Markov decision process (POMDP) based long term detection technique is proposed in [7]. For completeness, some details of this technique are included as follows.

The POMDP technique [4] takes the real world state $s \in \mathcal{S}$ as the input and generates actions $a \in \mathcal{A}$ as the output [4]. Since the real world state cannot always be perfectly known, the decision maker needs to estimate the state from the observation $o \in \mathcal{O}$. Thus, state, observation and action are the three key components of POMDP. A general POMDP problem is denoted by $\langle \mathcal{S}, \mathcal{O}, \mathcal{A}, T, R, \Omega \rangle$. In this problem, the state is defined as the number of hacked smart meters such that $\mathcal{S} = \{s_0, s_1, \ldots, s_N\}$, where s_i means that there are totally i smart meters hacked. Similarly, $\mathcal{O} = \{o_0, o_1, \ldots, o_N\}$, where o_i means that there are i smart meters hacked according to the observation. In our long term detection technique, the SVR based single event detection technique is used to obtain the observation. Given the current state and observation, the decision maker has two available actions in the set $\mathcal{A} = \{a_0, a_1\}$. a_0 means ignoring the cyberattack and continue monitoring the system. a_1 means checking and fixing the hacked smart meters.

POMDP models the mappings between the states when an action is taken. When taking action a, the state transits from s to s' with probability $T(s', a, s)$, which is called transition probability. Meanwhile, the decision maker receives a reward $R(s', a, s)$. The mapping between states and observations is defined as $\Omega(o, a, s) = P(o|a, s)$, which is the probability of observation o conditioned on state s and action a. In this problem, the state transition probability $T(s', a, s)$ and observation function $\Omega(o, a, s) = P(o|a, s)$ are trained based on the historical data. The reward function $R(s', a, s)$ is defined based on the losses taken by each hacked smart meter and the labor cost for checking and repairing the hacked smart meters. Given the model, the POMDP technique aims to optimize the discounted expected reward through picking the optimal action, which is formulated as a Bellman equation. Refer to [4, 7] for more details of POMDP technique.

Our detection technique is illustrated in Figure 2. Given the predicted and received guideline prices, the net metering aware energy load prediction technique is involved in computing the PAR increase.

5. SIMULATION RESULTS

In this section, simulations are conducted to analyze the impact of cyberattacks and the impact of net metering to our defense techniques. In the simulation, we consider a community consisting of 500 customers. The setup of the energy consumptions of the customers is similar to the previous works [8, 7].

From Figure 3, Figure 4, Figure 5, Figure 6 and Table 1, we make the following observations.

- Refer to Figure 3 for the prediction technique without considering the impact of net metering even if it is actually deployed. Shown in Figure 3(a) is the received guideline price without cyberattack and the predicted guideline price using the SVR based method in [8], respectively. The predicted guideline price does not match the received guideline price well such that it forms a peak from 12:00 to 14:00 while it is a gap in the received guideline price. Shown in Figure 3(b) is the predicted energy load using this predicted guideline price. The PAR is 1.4700.
- Refer to Figure 4 for the prediction technique considering net metering. Shown in Figure 4(a) is the received guideline price without cyberattack and the predicted guideline price considering net metering, respectively. The predicted guideline price matches the received one better than the SVR based method in [8]. Shown in Figure 4(b) is the predicted energy load using the predicted guideline price in Figure 4(a). The PAR is 1.3986. Comparing with this result, the PAR corresponding to the predicted energy load in Figure 3(b) is $\frac{1.4700-1.3986}{1.3986} = 5.11\%$ higher.
- Refer to Figure 5 for the impact of cyberattack. Shown in Figure 5(a) is the manipulated guideline price. The price is manipulated to be zero between 16:00 and 17:00. Shown in Figure 5(b) is the energy load under cyberattack. Corresponding to the manipulated guideline price, the energy load reaches a peak at 16:00 and 17:00. The PAR is 1.9037. This is $\frac{1.9037-1.4700}{1.4700} =$

Table 1: Simulation Results for Detection Techniques.

	No Detection	Detection without Considering Net Metering	Detection Considering Net Metering
PAR	1.6509	1.5422	1.4112
Normalized Labor Cost	-	1	1.0067

29.50% higher than the predicted energy load in Figure 3(b) and $\frac{1.9037-1.3986}{1.3986} = 36.11\%$ higher than the predicted energy load in Figure 4(b).

- The POMDP based long term detection technique is simulated in 48 hours and the results are shown in Figure 6 and Table 1, respectively. Refer to Figure 6. The detection technique considering net metering has an observation accuracy of 95.14% on average while it is 65.95% when the impact of net metering is not considered. The detection techniques with and without considering net metering are also compared in terms of the corresponding labor cost and PAR of the energy load. Refer to Table 1. Without any detection technique, the PAR of the energy load is 1.6509. Using the detection technique without considering net metering, the PAR is decreased to 1.5422. Using the defense technique considering net metering, the PAR is further reduced to 1.4112. The detection technique considering net metering can reduce the PAR by $\frac{1.5422-1.4112}{1.5422} = 8.49\%$ at the cost of increasing the labor cost by $\frac{1.0067-1}{1} = 0.67\%$ compared to that without considering net metering.

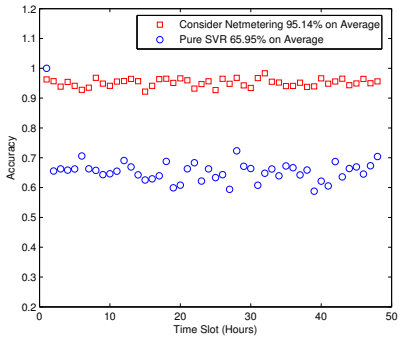

Figure 6: Observation accuracy.

The net metering helps reduce the peak demand from the grid rather than increasing it. Thus, the PAR could be significantly reduced. On the other hand, the detection detection of cyberattacks depends on PAR. The predicted guideline price considering net metering leads to a lower PAR than that without considering net metering. The cyberattack induced PAR increase is smaller than the actual increase when net metering is not considered. This is why the detection technique without considering net metering cannot detect $95.14\% - 65.95\% = 29.19\%$ of the cyberattacks as demonstrated by our simulation results.

6. CONCLUSION

In this paper, the impact of net metering to the smart home cybersecurity is analyzed. Since net metering impacts the grid energy demand prediction and the guideline pricing prediction, cyberattack detection, purely based on the historical pricing detection, can be compromised without considering it. Thus, a cross entropy optimization based net metering aware energy prediction technique is developed in this paper, which is further integrated into a POMDP based smart home pricing cyberattack detection framework. Our simulation results demonstrate that the new net metering aware smart home pricing cyberattack detection framework can significantly improve the detection accuracy from 65.95% to 95.14% compared to a state-of-art detection technique.

7. REFERENCES

[1] [Online]. Available: `http://www.solarcity.com/learn/understanding-netmetering.aspx`

[2] Distributed generation and renewable energy current programs for businesses. [Online]. Available: `http://docs.cpuc.ca.gov/published/newsrelease/7408.htm`

[3] Z. I. Botev, D. P. Kroese, R. Y. Rubinstein, et al. The cross entropy method for optimization. *Machine Learning: Theory and Applications, V. Govindaraju and C. R. Rao, Eds, Chennai: Elsevier BV*, 31:35–59, 2013.

[4] L. P. Kaelbling, M. L. Littman, and A. Cassandra. Planning and acting in partially observable stochastic domains. *Artificial Intelligence*, pages 99-134, 1998.

[5] B. Li, S. Gangadhar, S. Cheng, and P. Verma. Maximize user rewards in distributed generation environments using reinforcement learning. In *Proceedings of IEEE Energytech*, pages 1–6, 2011.

[6] L. Liu, Y. Zhou, Y. Liu, and S. Hu. Dynamic programming based game theoretic algorithm for economical multi-user smart home scheduling. In *Proceedings of IEEE Midwest Symposium on Circuits and Systems*, pages 362–365, 2014.

[7] Y. Liu, S. Hu, and T.-Y. Ho. Leveraging strategic defense techniques for smart home pricing cyberattacks. *Accepted to IEEE Transactions on Dependable and Secure Computing.*

[8] Y. Liu, S. Hu, and T.-Y. Ho. Vulnerability assessment and defense technology for smart home cybersecurity considering pricing cyberattacks. In *Proceedings of IEEE/ACM International Conference on Computer-Aided Design*, pages 183–190, 2014.

[9] A. Mohsenian-Rad, V. Wong, J. Jatskevich, R. Schober, and A. Leon-Garcia. Autonomous demand-side management based on game-theoretic energy consumption scheduling for the future smart grid. *IEEE Transactions on Smart Grid*, 1(3):320–331, 2010.

[10] K. Tuomas, F. Rossi, and A. Lendasse. Ls-svm functional network for time series prediction. In *Proceedings of European Symposium on Artificial Neural Networks*, 2006.

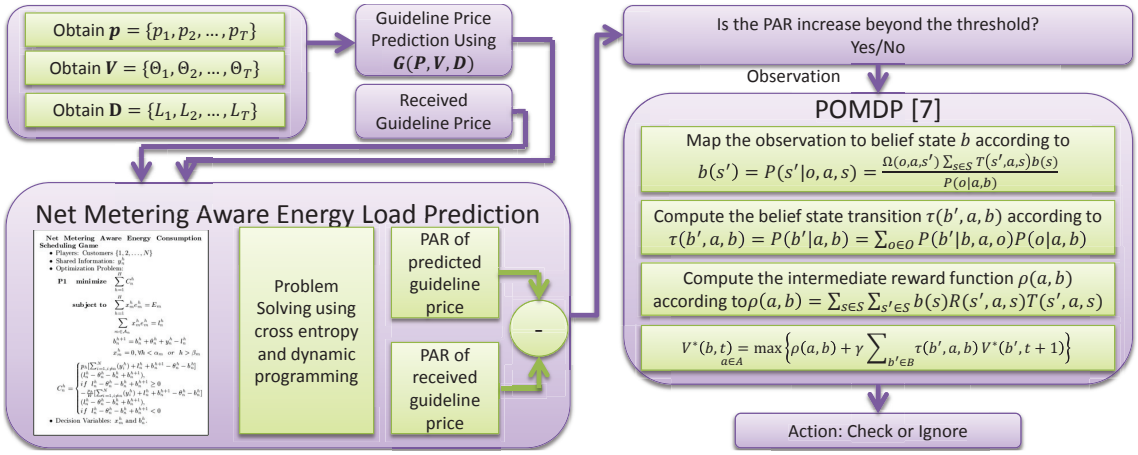

Figure 2: Algorithmic flow for the net metering aware energy load prediction and smart home pricing cyberattack detection technique.

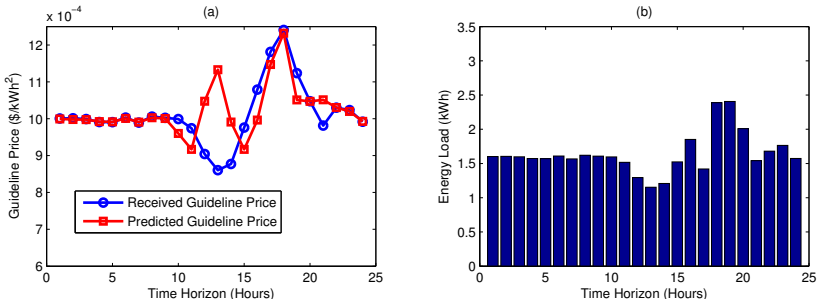

Figure 3: Without cyberattack, without considering the impact of net metering. (a) Received guideline price and predicted guideline price. (b) Predicted energy load according to the predicted guideline price in (a), PAR=1.4700.

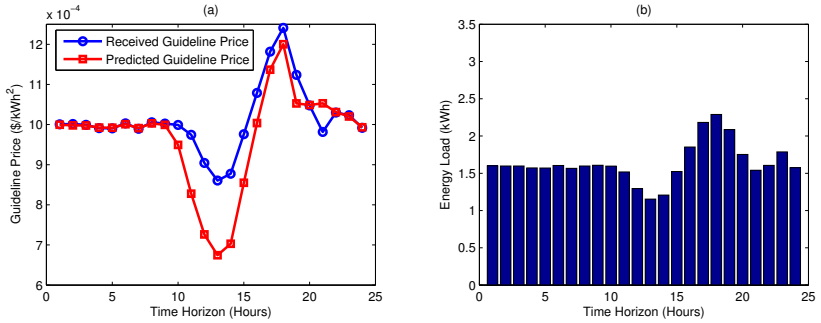

Figure 4: Without cyberattack, considering net metering. (a) Received guideline price without cyberattack and predicted guideline price. (b) Predicted energy load according to the predicted guideline price in (a), PAR=1.3986.

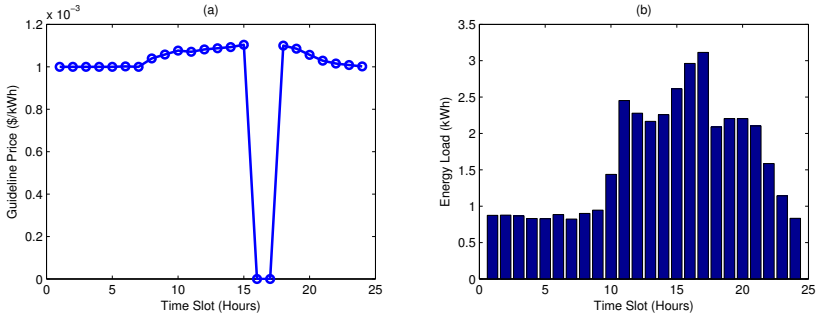

Figure 5: With cyberattack. (a) The manipulated received guideline price. (b) Energy load corresponding to the manipulated received guideline price, PAR=1.9037.