SECURITY AND COMMUNICATION NETWORKS
Security Comm. Networks (2013)
Published online in Wiley Online Library (wileyonlinelibrary.com). DOI: 10.1002/sec.895

SPECIAL ISSUE PAPER

CIT: A credit-based incentive tariff scheme with fraud-traceability for smart grid

Mi Wen[1,2]*, Kuan Zhang[2], Jingsheng Lei[1], Xiaohui Liang[2], Ruilong Deng[3,2] and Xuemin (Sherman) Shen[2]

[1] School of Computer Engineering, Shanghai University of Electric Power, Shanghai 200090, China
[2] Department of Electrical and Computer Engineering, University of Waterloo, Waterloo, ON N2L 3G1, Canada
[3] State Key Laboratory of Industrial Control Technology, Zhejiang University, Hangzhou 310027, China

ABSTRACT

The growing peak-hour power demand has invoked an urgency to increase the peak-hour supply. Although smart grid has been envisioned as the next generation power system due to its two-way communication of information and power, the peak-hour power shortage problem still exists. In this paper, we propose a credit-based incentive tariff (CIT) scheme with fraud-traceability for smart grid. Specifically, the CIT encourages retail customers to sell the power generated by their renewable resources back to the grid during peak hours via giving additional incentive rate to them based on their credits. If a fraud is detected during the power transaction, the malicious customer's identity can be traced out and his or her credit can be correspondingly reduced. The security analysis shows that the CIT resists various security threats and makes the incentive tariff fair and more secure. The performance evaluation demonstrates that the CIT can dramatically increase the peak-hour supply and reduce the peak-to-average power demand ratio by up to 7%. Copyright © 2013 John Wiley & Sons, Ltd.

KEYWORDS
smart grid; incentive; tariff; peak-hour demand; traceability

***Correspondence**
Mi Wen, School of Computer Engineering, Shanghai University of Electric Power, Shanghai 200090, China
E-mail: miwen@shiep.edu.cn

1. INTRODUCTION

The July 2012 India blackout, known as the largest power outage in history, affected over 620 million people, about 9% of the world population [1]. Investigations revealed that in Indian, 27% of generated power was lost in transmission [2], while peak-hour supply fell short of demand by an average of 9%. Thus, it is necessary to increase peak-hour supply. Generally, there are three kinds of approaches to solve this problem. Firstly, the utility companies can generate more power to meet the peak-hour power demand, but, it may cause many additional generation costs. Second, as most existing studies [3] suggested, the peak-hour power demand can be handled by giving incentives to customers and motivating them to turn off their high-voltage appliances during peak hours [4]. However, this kind of passive methods for power consumption of reducing is not effective to solve the power shortage problem because some customers may have non-shiftable power demand in peak hours [4]. Thus, actively encouraging retail customers via incentive tariff to sell the power generated by their renewable resources back to the grid during peak hours is promising.

Recently, residential photovoltaic, methane generators, solar panels, and microcoupled heat-power systems can be used to produce power at the customer site. When the consumer's local generation exceeds his or her consumption, the excess power can be fed into the utility company's grid again [5]. The utility company can advertise an incentive rate to retail customers when it needs more power supply in peak hours. Accordingly, the customers can obtain additional financial rewards from the utility company when they sell power back during those time intervals. By this approach, the relationship between a utility company and retail customers can be changed into a more cooperative one for mutual benefits. The utility company benefits from reducing its costs for the energy generation, as less expensive peak generators need to be run and a cheaper base load can be generated. Customers entering such a power transaction benefit from maximizing profits and

other incentives provided by the utility company [6]. Thus, the power shortage problem could be better solved.

However, there exist various security and privacy vulnerabilities and threats as communications are deeply involved in smart grid [7]. If the security of the tariff is not achieved, the incentive tariff cannot play his or her original role. For example, a malicious customer may forge or modify his or other customers' tariff tickets, seeking to obtain more financial rewards [8]. This type of misbehavior degrades the fairness of the incentive tariff and is harmful to the power grid reliability. Consequently, achieving tariff confidentiality, integrity, and malicious customer's misbehavior traceability are significant for smart grid.

In this paper, we propose a credit-based incentive tariff (CIT) scheme with fraud-traceability for smart grid. Specifically, the utility company generates an incentive tariff ticket for retail customers to increase the peak-hour supply. Meanwhile, the customers can maximize their profits if they sell power back to the grid during peak hours. Additionally, the user's security can be achieved, and malicious user's misbehavior can be traced out. The contributions of this paper are twofold:

(1) We propose a CIT scheme with fraud-traceability for smart grid to encourage customers to sell power back to the grid during peak hours. Specifically, the incentive rate varies according to the customer's credit, and the incentive tariff ticket is generated by using an ID-based restrictive partially blind signature.
(2) The security analysis demonstrates that the CIT can achieve tariff ticket confidentiality and integrity and the traceability of malicious customer misbehavior. Thus, the CIT makes the incentive tariff fair and more secure. Furthermore, the performance analysis shows that the CIT can dramatically reduce customers' peak-hour power demand.

The remainder of this paper is organized as follows. The related works and some preliminary knowledge are presented in Sections 2 and 3, respectively. Then, we describe the system model in Section 4 and the proposed CIT scheme in Section 5, followed by its security analysis and performance evaluation in Sections 6 and 7, respectively. Finally, we conclude the paper in Section 8.

2. RELATED WORK

Recently, different time-variant tariff schemes have been studied for smart grid. Basically, three categories of solutions have been developed: time-of-use pricing (ToU) [9], real-time pricing (RTP)[10], and critical peak pricing (CPP) [11].

Time-of-use pricing: in ToU tariffs, one day is divided into a fixed number of time slots, for which different power prices apply. Such price structure reflects higher marginal production costs during peak production into the consumer tariffs. Price differences between slots are the incentives for customers to shift some consumption to cheaper slots. An example is the Ontario electricity ToU price established in May 2011 [12]. In case that ToU tariffs are implemented, new tariff schemes need to be distributed to all retail customers' meters periodically.

Real-time pricing: in RTP tariffs, the price of power varies at different hours of the day. The prices are usually higher during the afternoon, on hot days in the summer, and on cold days in the winter. While it is usually difficult and confusing for the users to manually respond to prices that are changing every hour. Another problem that RTP may face is load synchronization, where a large portion of load is shifted from a typical peak hour to a typical off-peak hour, without significantly reducing the peak-to-average ratio. In case RTP is implemented, a daily update of tariffs is required.

Critical peak pricing: in CPP tariffs, the electricity prices of several time slots on a day or in a year, where consumption is very high, become significantly more expensive. It is often combined with the flat rate or ToU pricing. Such CPP-slots can vary and customers are informed late, and the customers can save much by avoiding these slots. For CPP, even sub-daily data need to be downloaded to the meters.

However, all these tariff schemes have not considered the security issues related to the tariff information. If there exist malicious customers or adversaries, the tariff can be modified. It is not fair for those honest retail customers. Thus, the retail customer's enthusiasm will be discouraged. Recently, various security vulnerabilities and threats have been studied in the research literatures [7,8]. Lu *et al.* used a super-increasing sequence to structure multidimensional data and encrypt the structured data by the homomorphic paillier cryptosystem technique [13]. Wen *et al.* proposed a searchable encryption scheme to achieve query on encrypted data for smart grid [14]. Yang *et al.*[15] proposed a privacy-preserving communication and precise reward architecture for vehicle-to-grid networks. Liang *et al.*[16] presented a usage-based dynamic pricing with privacy preservation for smart grid, which enables the electricity price to correspond to the electricity usage in real-time. However, these encryption and privacy preservation schemes cannot be directly applied into the tariff schemes to increase customers' peak-hour supply.

3. SYSTEM MODEL

In this section, we formalize the system model, identify the security requirements, and design our goals.

3.1. System model

In this paper, we consider a typical residential area, as shown in Figure 1, which comprises a control center (CC), local gateways (GA), and some retail customers $\mathbb{U} = \{U_1, U_2, \ldots, U_n\}$. U_i sells or purchases power through

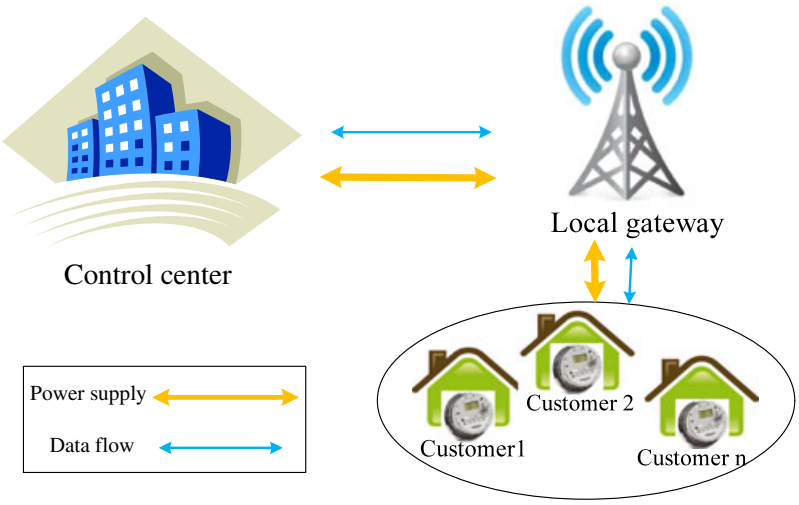

Figure 1. System model for smart grid.

the smart meters installed at his or her premise. Smart meters are usually equipped with network interfaces (e.g., wireless sensors) reporting power consumption data to the *GA* via advanced metering infrastructure. The GA controls the power delivery and communicates with the CC for reporting information or obtaining feedback. The GA is a proxy to relieve the burden of the CC for checking the validity of customers' incentive tariff tickets. The GA reports power transaction information to the CC at a later time. The CC is a trusted authority (TA), which can generate secret keys for the customers and acts as an arbitrator when misbehavior occurs.

Every customer has a credit V_i associated with his/her real identity U_i. Each V_i is initially set to the same value. For example, $V_i = 20$. Usually, U_i can obtain financial rewards from the TA if it sells the power back to the utility company. Moreover, if U_i sells the power during the peak hours, it can obtain the additional incentive rate from the TA. On the contrary, if a malicious customer's fraud is detected during the ticket deposit phase, his/her credit V_i will be decreased accordingly. The customer's credit V_i has several merits. One possible merit is to punish customers with misbehavior history by higher network access latency. Moreover, if $V_i \leq 0$, the TA will refuse to issue a ticket to the customer.

3.2. Security requirements

Security is crucial for the success of secure smart grid communications, especially for the incentive tariff distribution. In our security model, we consider the CC is trustable, the GA is honest but curious, and the retail customers $\mathbb{U} = \{U_1, U_2, \ldots, U_v\}$ might be malicious. For example, a malicious customer $\mathcal{A}$ in the system may pry into other customer's incentive tariff information. $\mathcal{A}$ also can launch some active attacks to threaten other customer's tariff confidentiality and integrity. Therefore, to secure the customer's incentive tariff and to detect $\mathcal{A}$'s malicious behaviors, the following security requirements should be satisfied in our incentive tariff scheme.

- *Incentive rate's confidentiality and Tariff ticket's unforgeability*: To preserve incentive rate's privacy such as how much power the customer sold to the grid and how much tariff the customer got from the utility company, cannot be exposed to the $\mathcal{A}$. Otherwise, $\mathcal{A}$ can replay the tariff ticket to obtain illegal rewards from the utility company. Additionally, $\mathcal{A}$ cannot forge a tariff ticket to obtain benefits. All these misbehaviors should be detected.
- *Tariff ticket's integrity*: The incentive tariff ticket should not be changed by the malicious customers or the illegal competitors. For example, if the price or other information in the tariff ticket are maliciously modified, the operations of the incentive tariff scheme and the tariff rules will be disordered or broken in the long run.
- *Malicious customer's traceability*: After receiving the tariff from the utility company, U_i can use it at the target time slot or date. However, the incentive tariff ticket can be used only once. If the tariff ticket is used for twice or more, this kind of fraud should be detected, and the user's identity should be traced by the GA. Otherwise, the GA cannot know the real identity of the honest customers. In other words, the GA cannot link a power transaction with honest customers' real identity, and customers' privacy can be achieved.

3.3. Design goals

To stimulate customers to increase the peak-hour supply and reduce the demand during peak hours under the aforementioned model, our design goal is to develop a secure tariff mechanism achieving traceability for smart grid.

- *The security requirements should be guaranteed in the proposed CIT*. As stated earlier, if smart grid does not

consider the tariff tickets' security, the tariff tickets might be modified or forged by malicious customers or adversaries. As a result, the security and fairness of the incentive tariff scheme are broken. Therefore, the proposed CIT scheme should achieve the tariff confidentiality, integrity, and malicious customer's misbehavior traceability.

- *The peak-to-average power demand ratio should be reduced in the proposed CIT.* To stimulate the retail customers to sell power back to the utility company during the peak hours, the incentive tariff is calculated in the basis of the general ToU pricing and the customer's credit. The CIT should be more effective than the general ToU approach in raising the retail customers enthusiasm to increase the peak supply and thus reduce the peak-to-average power demand ratio.

4. PRELIMINARIES

In this section, we will briefly describe the basic definition and properties of bilinear pairings and ID-based signature with restrictive and partially blind properties.

4.1. Bilinear pairing

Bilinear pairing is an important cryptographic primitive. Let $(G_1, +)$ and $(G_2, *)$ be two cyclic groups of prime order q. Let $a, b \in Z_q^*$. We assume that the discrete logarithm problem in both G_1 and G_2 are hard. A bilinear pairing is a map $e : G_1 * G_1 \rightarrow G_2$ with the following properties. We note that the bilinear parings can be derived from the Weil or Tate pairing [17].

(1) Bilinear: $e(aP, bQ) = e(P, Q)^{ab}$.
(2) Non-degenerate: There exists P and $Q \in G_1$ such that $e(P, Q) \neq 1$.
(3) Computable: There is an efficient algorithm to compute $e(P, Q)$ for all $P,Q \in G_1$.

Definition 1. *A bilinear parameter generator $\mathcal{G}en(\kappa)$ is a probabilistic algorithm that takes a security parameter κ as input and outputs a 5-tuple (q, P, G_1, G_2, e).*

4.2. ID-based partially blind signature

An ID-based partially blind signature [18] is made of four algorithms that are depicted as follows.

Setup: The TA first generates (q, P, G_1, G_2, e) by running $\mathcal{G}en(\kappa)$. Then, the TA chooses a random number $s \in Z_q^*$ as the master key and computes the associated public key as $P_{pub} = sP$. It also picks two cryptographic hash functions $H:\{0,1\}^* \rightarrow G_1$, $H_1:G_1^3 * G_2^4 \rightarrow z_q^*$. The system's public parameters are $\{G_1, G_2, e, q, P, P_{pub}, H, H_1\}$.

Keygen: Given a customer's identity, the TA computes the customer's public key as $Q_{ID} = H(ID)$ and returns $S_{ID} = sQ_{ID}$ to the customer as his or her private key.

Sign: customer randomly chooses $r \in z_q^*$ and sends $U = rP_1$, $Y = rQ_{ID}$ to TA. Given a negotiated common information Δ and a plaintext m, TA randomly selects $\alpha, \beta, \gamma \in z_q^*$, then computes $Y' = \alpha Y + \alpha\beta Q_{ID} - \gamma H(\Delta)$, $U' = \alpha U + \gamma P_{pub}$, $h = \alpha^{-1} H_1(m, Y') + \beta$. TA sends h to the customer. The customer responds TA with $S = (r + h)S_{ID} + rH(\Delta)$. The customer computes $S' = \alpha S$. Therefore, the signature on m and Δ is (Y', U', S').

Verify: To verify the signature, the verifier checks if $e(S', P) = e(Y' + H_1(m, Y')Q_{ID}, P_{pub})\ e(H(\Delta), U')$. If it holds, the verifier accepts, otherwise, it rejects it.

5. PROPOSED CREDIT-BASED INCENTIVE TARIFF SCHEME

In this section, we propose a CIT scheme with fraud-traceability for smart grid. Firstly, we will introduce the main idea of the CIT and the incentive tariff rule. Then, three phases of the CIT, registration and advertising phase, incentive tariff ticket generation, and incentive tariff ticket deposit phases, will be introduced.

5.1. Overview of the credit-based incentive tariff

5.1.1. Intuition of credit-based incentive tariff.

Every customer U_i has a billing account number I_{U_i}, which is linked to his or her real identity U_i. When U_i sells the power back to the utility company, he or she should register an account and negotiate a common agreed incentive tariff Ψ_i with the TA. Then, the TA can generate an incentive tariff ticket (i.e., a common agreed incentive tariff) $tick_i$=$\{Seq_i$,B,Ψ_i,$\sigma_i\}$ to U_i by using a restrictive partially blind signature scheme [19]. Seq_i is the unique serial number of the ticket that can be computed from the customer's account number I_{U_i}. σ_i is the signature on common agreed information (Seq_i,B,Ψ_i), where B is necessary for verifying the validity of the signature in the tariff ticket deposit phase. When U_i begins selling power to the *GA*, it deposits $tick_i$ to the GA. The *GA* verifies the validity of $tick_i$. If this is the first time $tick_i$ is deposited, the *GA* creates a record for $tick_i$ and keeps a record of how much power it has sold. Then, the GA reports U_i's amount of sold power to the TA at a later time. If there already exists a record of $tick_i$, the *GA* detects a fraud. The TA recovers the real identity of the customer and reports it to the TA. The TA can decrease the customer's credit according to some policy.

5.1.2. The incentive tariff rule.

In this paper, the utility company determines the market power price $p(t)$ for the smart grid. We add an additionally incentive rate in the commonly used ToU pricing approach, aiming to motivate the customer to sell power back to the utility company during peak hours. Essentially, a day can be divided into several time segments: on-peak hours (P), mid-peak hours (MP), and off-peak hours (NP),

each of which corresponds to a certain price as shown in Equation (1).

$$p(t) = \begin{cases} p_h & t \in P \\ p_m & t \in MP \\ p_o & t \in NP \end{cases} \quad (1)$$

where $t \in K$ and K are the set of all time slots.

When U_i launchs a power transaction (sell or purchase) from the TA (i.e., CC), it should offer an application $\Lambda_i = (ts_i, V_i, r_t^i)$ in advance, where ts_i denotes the target time slot and r_t^i is U_i's target consumption in the time slot t. Note that, r_t^i facilitates the utility company to predicate U_i's power consumption in the time slot t. V_i refers to U_i's credit based on his or her previous contributions to the peak-hour power demand and his or her misbehavior history.

To raise the retail customers' enthusiasm, the utility company posts different incentive rates q_t^i to them at different time slots. q_t^i varies according to the power demand and supply in that month or week. Usually, if U_i sells power back to the utility company, he or she can obtain financial rewards. Especially, when U_i sells power back to the utility company during peak hours, he or she can obtain an additional incentive rate q_t^i based on his or her credit. If U_i's credit V_i is higher than a threshold λ, he or she can obtain a higher additional incentive rate, as shown in Equation (2). For those customers who sell power back to the utility company during MP and NP, they obtain less additional incentive rates. Essentially, $\theta_1 > \theta_2 \geq \theta_3 > \theta_4 \geq \theta_5 > \theta_6$.

$$q_t^i = \begin{cases} \theta_1 & V_i \geq \lambda, t \in P \\ \theta_2 & V_i < \lambda, t \in P \\ \theta_3 & V_i \geq \lambda, t \in MP \\ \theta_4 & V_i < \lambda, t \in MP \\ \theta_5 & V_i \geq \lambda, t \in NP \\ \theta_6 & V_i \geq \lambda, t \in NP \end{cases} \quad (2)$$

Finally, an incentive tariff for U_i includes $\Psi_i = \{p(t), q_t^i, E_d, V_i\}$, where E_d is the target power transaction date.

To model the welfare that U_i can obtain if he or she sells power back to the grid, we consider a utility function $\mathcal{U}(x)$ representing the level of satisfaction obtained by the user, which is non-decreasing and concave as in [10]. Let x_t^i denote the power consumption of U_i in the time slot t. Let y_t^i be the power sold by U_i in time slot t. x_t^i and y_t^i have to satisfy $x_t^i \geq b_t^i$ and $x_t^i + y_t^i = z_t^i$, where b_t^i denotes U_i's non-shiftable power requirements of in time slot t; z_t^i denotes the generation of U_i in the time slot t. r_t^i is U_i's target consumption in the time slot t. Specifically, the utility function is set as follows [20], where α ($\alpha < 0$) is a system parameter. It means that the more U_i's actual consumption deviates from the target, the less his or her utility is

$$\mathcal{U}\left(x_t^i\right) = \begin{cases} \alpha\left(x_t^i - r_t^i\right)^2 & x_t^i \leq r_t^i \\ 0 & x_t^i > r_t^i \end{cases} \quad (3)$$

Next, the U_i's welfare can be simply represented as

$$\mathcal{W}\left(x_t^i, y_t^i\right) = \mathcal{U}\left(x_t^i\right) + p(t)\left(1 + q_t^i\right) y_t^i \quad (4)$$

The more power he or she sells back, the more his or her welfare is. Therefore, U_i decides his or her power transaction (purchase or sell power) to optimize the expected welfare before power delivery as Equation (5).

$$Max:\ \mathcal{U}\left(x_t^i\right) + p(t)\left(1 + q_t^i\right) y_t^i \quad (5)$$

Subject to

$$x_t^i + y_t^i = z_t^i,$$
$$x_t^i \geq b_t^i \geq 0,$$
$$y_t^i < z_t^i$$

At delivery time, U_i sells or purchases additional power on the real-time market. During the renewable generation, such as methane generators are used, z_t^i can be predicated. r_t^i can be modeled by users' pattern learning [20]. Hence, the optimal value of x_t^i and y_t^i can be estimated. If $y_t^i > 0$, U_i can sell excess power back to the utility company; otherwise, if $y_t^i \leq 0$, U_i needs to purchase power from the utility company.

5.2. Registration and advertising phase

At the beginning, the TA selects some random elements $p, P_1, P_2 \in G_1$. The TA also selects a master key $s \in \mathbb{Z}_q^*$ and computes $P_{pub} = sP$. Then, the TA computes U_i's public key as $Q_{U_i} = H(U_i)$ and returns $S_{U_i} = sQ_{U_i}$ to the customer as his or her private key. Similarly, the TA has a pair of public/private keys (Q_{TA}, S_{TA}). H, H_1, H_2 are three cryptographic hash functions $H: \{0,1\}^* \rightarrow G_1, H_1: G_1^3 * G_2^5 \rightarrow z_q^*$ and $H_2: G_2 * G_2 * ID_s * T_d \rightarrow z_q^*$. For the sake of simplicity, we define $g = e(P, Q_{TA})$, $g_1 = e(P_1, Q_{TA})$, $g_2 = e(P_2, Q_{TA})$, $y = e(P_{pub}, Q_{TA})$.

Every customer U_i should register an account at the TA as follows: U_i randomly selects a number $\mu_i \in \mathbb{Z}_q^*$ and computes a unique account number $I_{U_i} = \mu_i P_1$. Then, it computes a message $m = \mu_i P_1 + P_2$. If $m \neq 0$, U_i transmits m to the TA and keeps μ_i secret. Then, the TA keeps a record (I_{U_i}, V_i) in his or her database. If $V_i \leq 0$, the TA refuses to issue a ticket to him.

$$U_i \rightarrow TA: \{U_i, I_{U_i}, m, V_i\}$$

When U_i needs to apply a power transaction with the utility company, he or she should offer an application $\Lambda_i = (ts_i, V_i, r_t^i)$ one week or one day in advance. For efficiency, U_i also can apply a power transaction for a continuous time slots, for example, $\Lambda_i = (ts_i, V_i, r_{t1}^i, r_{t2}^i, \ldots)$, where ts_i is the starting time of the transaction. For simplicity, we just consider a power transaction in one time slot. Therefore, the parameters for incentive tariff ticket generation, except incentive rate, will not be attached with parameter t.

$$U_i \rightarrow TA: \{t_1, \Lambda_i, H_k(\Lambda_i \| t_1)\}$$

where, k is a symmetric key. U_i and the TA can locally derive $k = e(S_{TA}, Q_{U_i})$ and $k = e(Q_{TA}, S_{U_i})$ [21].

Then, the TA checks his or her predicted peak-hour power demand in the time slot t. If there needs some peak-hour power supplies in the time slot t, the TA randomly chooses $Q \in G_1$, $r \in z_q^*$ and computes $z{=}e(m, S_{TA})$, $a = e(P, Q)$, $b = e(m, Q)$, $U = rP$, $Y = rQ_{TA}$. Then, the TA sends these parameters and an incentive tariff $\Psi_i = \{p(t), q_t^i, E_d, V_i\}$ to U_i. Let $\Psi_{Ct}^i = Enc_k(\Psi_t^i)$. $\mathsf{Enc}(\cdot)$ can be any symmetric encryption algorithm, for example, Advanced Encryption Standard.

$$TA \rightarrow U_i : \left\{\Psi_{Ct}^i, z, a, b, U, Y, t_2, MAC_k(z||a||b||U||Y||t_2)\right\}$$

5.3. Incentive tariff ticket generation phase

If U_i does not sell his or her power, he or she just neglects this information. If U_i accepts the incentive tariff Ψ_i when he or she decrypts Ψ_{Ct}^i, he or she should generate some parameters for TA to sign a ticket on the commonly agreed incentive tariff. Then, he or she chooses $x_1, x_2, \alpha, u, v, \mu, \gamma \in Z_q$ and computes $m' = \alpha m$, $B = g_1^{x_1} g_2^{x_2}$, $z' = z^{\alpha}$, $A = e(m', Q_{TA})$, $Y' = \lambda Y + \lambda\mu Q_{TA} - \gamma H(\Psi_i)$, $U' = \lambda U + \gamma P_{pub}$, $a' = a^u g^v$, $b' = b^{ua} A^v$, $c' = H_1(m', Y', U', A, B, z', a', b')$, $h_1 = c'/u$, $h_2 = \lambda^{-1} c' + \mu$. U_i sends them to the TA as

$$U_i \rightarrow TA : \{h_1, h_2, t_3, MAC_k(h_1||h_2||t_3)\}$$

The TA records (I_{U_i}, Ψ_{Ct}^i) in his or her database. Then, the TA computes $S_1 = Q + h_1 S_{TA}$, $S_2 = (r + h_2)S_{TA} + rH(\Psi_i)$ and responds as

$$TA \rightarrow U_i : \{S_1, S_2, t_4, MAC_k(S_1||S_2||t_4)\}$$

Finally, U_i checks if the following equalities hold: $e(P, S_1) = ay^{h_1}$ and $e(m', S_1) = bz^{h_1}$. If so, U_i calculates $S_1' = uS_1 + vQ_{TA}$ and $S_2' = \alpha S_2$. t_i in each message is used to guarantee the freshness of the message.

Thus, $\sigma_i = (Y', U', z', c', S_1', S_2')$ is the valid signature on message (Seq_i, B, Ψ_t^i), and the tariff ticket for U_i is $tick_i = \{Seq_i, B, \Psi_{Ct}^i, \sigma_i\}$.

5.4. Incentive tariff ticket deposit phase

After obtaining an incentive tariff ticket, U_i may deposit it when he or she sells the power back to the utility company through the GA. The GA (i.e., local home power manager) controls power delivery of the retail area. For privacy concern, U_i does not want the GA to know his or her real identity, he or she can employ some tricking technique to transform his or her real identity to a pseudonym. U_i generates his or her own pseudonym by selecting a secret number $\tau \in z_q^*$ and computing the pseudonym $PA_i = \tau H(U_i)$. The corresponding private key can be derived as $SA_i = \tau S_{U_i} = \tau\, sH(U_i) = sPA_i$. U_i generates a signature for his or her tariff ticket deposit $\sigma_{di} = Sig_{SA_i}(m'||B||Seq_i||\sigma_i||t_5)$

$$U_i \rightarrow GA : \{PA_i, m', tick_i, t_5, \sigma_{di}\}$$

If $A = e(m', Q) \neq O$, the GA sends a challenge $d = H_2(A, B, GA, T_d)$ to U_i.

$$GA \rightarrow U_i : \{d, t_6, MAC_{k_1}(d||t_6)\}$$

U_i then computes $r_1 = d(\mu_1\alpha) + x_1$, $r_2 = d\alpha + x_2$ and sends them to the GA.

$$U_i \rightarrow GA : \{r_1, r_2, t_7, MAC_{k_1}(r_1||r_2||t_7)\}$$

The GA accepts this incentive tariff ticket if the equality $g_1^{r_1} g_2^{r_2} = A^d B$ holds and σ_i is a valid signature on (m', B, Ψ_t^i).

If it is the first time that U_i deposits ticket Seq_i to the GA, the GA then creates a record for it as $rec = (tick_i, m', r_1, r_2, log, T_d)$, where log is the logged data of the U_i's behavior. Here, k_1 in the earlier also can be established between U_i and the GA by using his or her pseudonym PA_i as $k_1 = e(S_{GA}, PA_i) = e(Q_{GA}, SA_i)$.

Next, the GA sends this transaction transcript and the amount of power U_i supplies y_t^i to TA.

$$GA \rightarrow TA : \left\{m', tick_i, r_1, r_2, y_t^i, T_d, t_9, MAC_{k2}(m'||B||\sigma_i||r_1||r_2||T_d||y_t^i||t_9)\right\}$$

where $k_2 = e(Q_{TA}, S_{GA})$.

Finally, the TA verifies the signature. If it can be successfully verified, the TA checks if $tick_i$ has been stored. If Seq_i is not stored, the TA stores the following information: $(tick_i, m', T_d, GA)$ for the fraud detection. The TA decrypts Ψ_{Ct}^i and checks if $(E_d - T_d)$ is within a tolerable time difference. If so, the TA computes a financial reward F_t^i for U_i and saves it in U_i's financial account I_{U_i}; if not, the TA publishes U_i by reducing his or her financial rewards. If Seq_i has been stored and from the same GA, the TA can revoke the GA.

6. SECURITY ANALYSIS

In this section, we analyze the security properties of the proposed CIT. In particular, following the security requirements discussed earlier, our analysis will focus on how the proposed CIT can achieve the goals.

• *The confidentiality of the incentive rate and the unforgeability of the tariff ticket are achieved in the proposed CIT*: In the CIT, U_i's incentive rate is encrypted by a symmetric key k as $\Psi_{Ci} = Enc_k(\Psi_i)$. Anyone, except the TA, cannot know the content of the incentive rate for U_i. When TA generates the incentive tariff ticket $tick_i = \{Seq_i, B, \Psi_{Ci}, \sigma_i\}$ to U_i, the ticket includes signature

σ_i and parameter B, which are related to secret numbers r, x_1, x_2. Anyone who does not know these secret numbers cannot forge a valid incentive tariff ticket. Thus, in the CIT, the confidentiality of the incentive rate and the unforgeability of the tariff ticket are achieved.

• *The integrity of the individual customer's application and incentive tariff ticket are achieved in the proposed CIT*: In the CIT, during the registration and advertising phase, U_i's application Λ_i and all of the communication messages are attached with hash MACs and time stamps. In this way, the integrity of Λ_i and the incentive tariff ticket is achieved. During the incentive tariff ticket generation phase, the communications between the TA and U_i are all attached with MACs and time stamps. If any message is modified by other malicious customers or adversaries, both TA and U_i can detect this kind of attack by verifying the MACs. Therefore, the integrity of the individual customer's application and incentive tariff ticket is achieved in the CIT.

• *The customer's privacy and malicious customer's fraud-traceability are achieved in the proposed CIT*: due to the use of pseudonyms in tariff ticket deposit phase, the GA learns nothing about the identity of the customer. The reason is that the pseudonym is generated by using the customer's secret number, the hardness of revealing the real identity from the pseudonym equals that of solving the discrete logarithm problem. As long as U_i operates honestly, the GA does not know U_i's identity. Otherwise, U_i can be punished, and his or her fraud will be reported to the TA. In the next power transaction, U_i should change another secret $\mu_i \in Z_q^*$ and register another account. If his or her credit is too low, he or she may be refused in the registration. Therefore, it can be easily shown that the GA cannot link a customers ticket to his or her real identity if he or she operates honestly. Hence, the customer's privacy is achieved in the CIT.

In the CIT, when U_i sends the incentive tariff ticket to the GA, the GA first searches his or her database to find out whether the ticket has been stored before. If the ticket has not been stored before, the GA stores a record in his or her database; else, the GA detects a duplicate ticket. The GA can conclude that misbehavior has occurred and reveals the identity of the malicious customer by constructing the following two sets of equations from two different ticket records received from U_i:

$$r_1 = d\mu_1\alpha + x_2, r_2 = d\alpha + x_2,$$

$$r_1' = d'\mu_1\alpha + x_2, r_2' = d'\alpha + x_2$$

The GA can resolve for $\mu_1 = \frac{r_1 - r_1'}{r_2 - r_2'}$ and obtain the billing account number I_{U_i}=$\mu_1 P_1$ to reveal the associated identity U_i. At the same time, the GA reports U_i's misbehavior to the TA, and the TA may decrease the credit based on the misbehavior level indicated in *log*. By far, it is clear that the customer-chosen secret $\mu_1 \in z_q^*$ in incentive tariff ticket serves as the embedded clue for tracing misbehaving customers.

7. PERFORMANCE ANALYSIS

In this section, we evaluate the performance of the proposed CIT in terms of the computation complexity, communication overhead, and the peak-hour power demand reduction.

7.1. Computation complexity

In the CIT, the computation tasks include pairing and exponentiation operations. Because the hash operation and number multiplication are too fast compared with the pairing operations, we will not take them into consideration in this subsection. For simplicity of description, the pairing and exponentiation operations can be denoted as C_p and C_e, respectively. In the registration phase, the TA computes 3 pairing operations to generate parameters for the user's power transaction application. In the ticket issuance phase, the user needs to compute 3 pairings, 4 exponentiation operations, that is, $3C_p + 4C_e$, to generate a valid signature $\sigma_i = (Y', U', z', c', S_1', S_2')$ on message (Seq_i, B, Ψ_t^i) to construct a tariff ticket. In the ticket deposit phase, the GA should compute 2 exponentiation operations to verify the ticket. Then, the GA and TA need 1 pairing operation to generate a symmetric key.

7.2. Communication overhead

Most pairing-based cryptosystems need to work in a subgroup of the elliptic curve $E(F_q)$. By representing elliptic curve points using point compression [22], the length of the elements in G_1 and G_2 are roughly 161 bits (using point compression) and 1024 bits, respectively. If SHA-1 is used to compute the hash function, which yields a 160-bit output. If needed, a ticket can be issued to the user for multiple time slots; the average communication cost can be reduced because some parameters need only be transmitted once. In a single time slot ticket issuance, firstly, the user applies a power transaction and sends 1 hash value and other little data to the TA, that is, 160 bits. Then, the TA sends some important parameters and an incentive tariff to the user, which include 3 G_2 elements, 2 G_1 elements, and 1 hash value, that is, $3 * 10242 * 161 + 160 = 3554$ bits.

In the ticket generation phase, the user needs to send 2 G_1 elements and 1 hash value to the TA to help issue a tariff ticket, that is, $2 * 161 + 160 = 482$ bits. The TA also sends 2 G_1 elements and 1 hash value to the user to help the user generate a tariff ticket. Finally, in the ticket deposit phase, the user sends roughly 12 G_1 elements, 1 G_2 elements, 1 hash value, and 1 256-bits long ciphertext (if Advanced Encryption Standard is used to encrypt the data) to the GA, that is, $12 * 161 + 1024 + 160 + 256 = 3372$ bits. The GA sends to the user approximately 11 G_1 elements, 1 G_2 elements, 3 hash value, and 1 256-bits long ciphertext to the GA, that is, $11 * 161 + 1024 + 160 + 256 = 3211$ bits.

7.3. Peak-hour power demand reduction

In our simulation model, the intended time cycle for the operation of U_i is divided into 24 time slots, where $|K| = 24$, and K is the set of all time slots. The Ontario electricity TOU price [12], as shown in Table I, is used in our simulation. Thus, $p_h = 11.8$ ¢/kWh, $p_m = 9.9$ ¢/kWh, $p_o = 6$ ¢/kWh.

$$\mathcal{U}(x_t^i) = \begin{cases} (-3/2)\left(x_t^i - r_t^i\right)^2 & x_t^i \le r_t^i \\ 0 & x_t^i > r_t^i \end{cases} \quad (6)$$

With the utility function ($\alpha = -3/2$) in Equation (5), retail customer U_i's objective is to maximize his or her welfare.

$$Max: \mathcal{W}\left(x_t^i, y_t^i\right) = (-3/2)\left(x_t^i - r_t^i\right)^2 + p(t)\left(1 + q_t^i\right) y_t^i \quad (7)$$

Subject to

$$x_t^i + y_t^i = z_t^i,$$
$$r_t^i \ge x_t^i \ge b_t^i,$$
$$y_t^i < z_t^i$$

By solving $\frac{\partial \mathcal{W}}{\partial x} = 0$, we can obtain $x_t^{i*} = [r_t^i - \frac{p_t^i(1+q_t^i)}{2}]_{b_t^i}$ and $y_t^{i*} = z_t^i - x_t^{i*}$. Here, $[\cdot]_{b_t^i} = max(\cdot, b_t^i)$. Since different customer has different non-shiftable power consumption in each time slot, it is hard to model it. For simplicity, in our simulation, we set $b_t^i = 0$ kWh for $\forall t \in K$. We use the average value of customer's target power consumption as suggested in [20]. Thus, in a time cycle customer's target power consumption value $(r_t^i, \forall t \in K) = (2.3, 2.5, 3.4, 4.4, 5, 6.25, 5, 5.75, 4.3, 3.6, 5, 7.8, 9, 10.85, 11.25, 10, 6.85, 4.35, 4.05, 2.25, 2.35, 2.2, 1.95, 0.6)$, unit = kWh. Then, we let $\lambda = 15$ in Figures 2, 4, and 5. $\theta_1 = 20\%, \theta_2 = \theta_3 = 10\%, \theta_4 = 5\%, \theta_5 = 0\%, \theta_6 = -10\%$.

Table I. Ontario electricity time-of-use price (¢/kWh) [12].

Time slots	Summer	Weekend/holiday	Winter
7 AM–7 PM	6.3	6.3	6.3
11 AM–5 PM	11.8	6.3	9.9
7 AM–11 AM, 5 PM–7 PM	9.9	6.3	11.8

(1) If methane generators are used, z_t^i is a constant value, for example, $z_t^i = 5$ kWh. Figure 2 depicts that the proposed CIT can encourage the customer to sell more power back to the utility company than the general ToU pricing approach. However, if the customer maximizes his or her profit, he or she needs to stock the excess power during the off-peak hours and sell them back during peak hours. The cost for energy stock is not considered in our paper.

(2) Consider a building area with customer numbers of $n = 20$, and the power demand in each time slot is $x_t = \sum_{i=1}^{10} U_i(x_t^i)$. If the retail customers' credits are randomly set as $(V_1, \ldots V_{20}) = (15, 7, 16, 19, 8, 10, 4, 5, 1, \quad 16, 12, 6, 14, 18, 2, 10, 9, 11, 3, 17)$, Figure 3 shows their power demand with different λ. We can see that, if there are more retail customers whose credits are above the threshold λ, the power consumption becomes lower, and the power demand can be reduced.

(3) If solar panels are used as the small-scale renewable energy sources to produce power at the customers' sites. NREL Solar Radiation Research Laboratory (BMS) provides a solar access at the South Table Mountain location. Based on their collected solar power generation in October 2012 [23], from 7:25 AM to 16:55 PM, the sampled real-time power generation corresponds to the time slots 7-16 is $(z_t^i, \forall t \in K) = (1.6, 10.4, 20.4, 27.4, 31.4, 31.7, 28.4, 21.6, 11.9, 2.2)$. Here, unit = kWh/m^2. Figure 4 shows that if the customer maximizes his or her welfare, how much power he or she can sell back to the utility company. It can also be seen from Figure 4 that the proposed CIT can encourage the customer to sell more power back to the utility company than the general ToU pricing approach.

(4) Figure 5 shows the customer's power consumption under the objective of maximizing his or her welfare. We can see that, with the CIT, the customer's power consumption is reduced in the CIT. Taking the peak-to-average power demand ratio into consideration, the customer with higher credit, for example, $V_i = 20$, in the CIT can reduce the peak-to-average

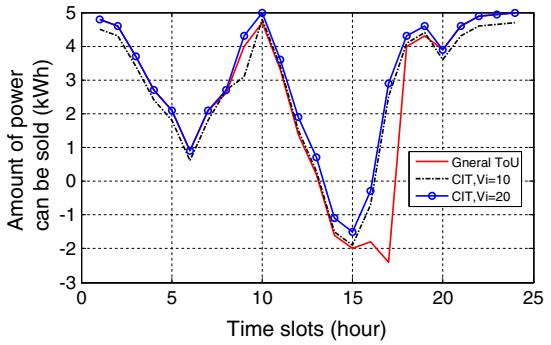

Figure 2. The amount of power can be sold with constant generation.

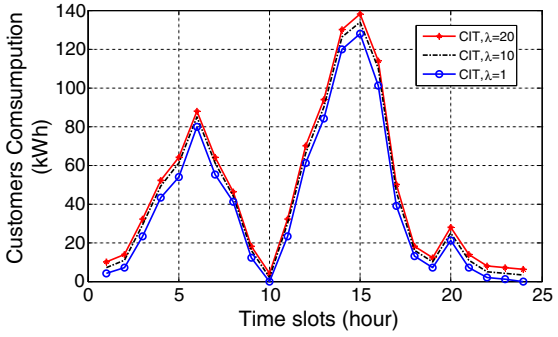

Figure 3. The customers' consumption with different thresholds.

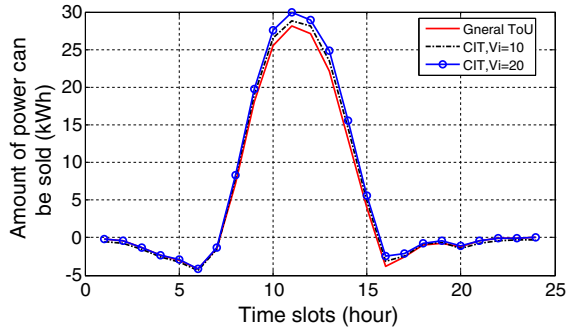

Figure 4. The amount of power can be sold with solar generation.

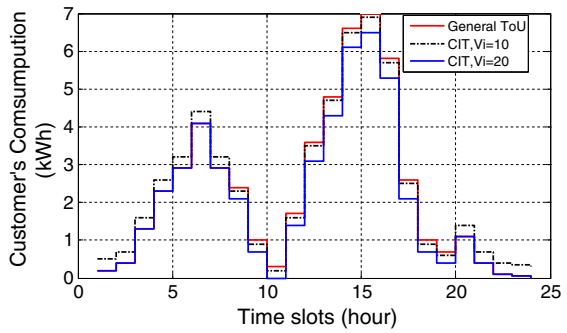

Figure 5. The customer's consumption in summer.

power demand ratio by 7%, as shown in Figure 5. The customer with lower credit, for example, V_i = 10, in the CIT can also reduce the peak-to-average power demand ratio by 3%.

8. CONCLUSION

We have proposed a CIT scheme with fraud-traceability for smart grid by using an ID-based restrictive partially blind signature. The scheme can improve security, fairness, and increase the peak-hour supply. In addition, malicious customer's fraud during the power transaction can be detected, and their credits can be reduced. The performance evaluation results show that the CIT achieves incentive tariff ticket confidentiality and integrity and malicious customers' fraud-traceability. For our future work, we will consider retail customers with power storage capacity and how they contribute to increasing the peak-hour supply.

ACKNOWLEDGEMENTS

This work is supported by the National Natural Science Foundation of China under Grant Nos. 60903188, 61073189, 61103207, and 61272437 and NSERC, Canada.

The authors really appreciate Dr Rongxing Lu from School of Electrical and Electronics Engineering at the Nanyang Technological University for his helpful discussions.

REFERENCES

1. 2012 India blackouts. http://en.wikipedia.org/wiki/2012_India_blackouts.
2. Singh R K, Katakey R. *"Worst India Outage Highlights 60 Years of Missed Targets."* Bloomberg News, August 1, 2012. Web. http://www.bloomberg.com/news/2012-08-01/worst-india-outage-highlights-60-years-of-missed-targets-energy.html.
3. Nunna H, Kumar V, Doolla S. Demand response in smart distribution system with multiple microgrids. *IEEE Transactions on Smart Grid* 2012; **4**(3): 1641–1649.
4. Kankar B, Math H, Jaap E. Real time optimal interruptible tariff mechanism incorporating utility-customer interactions. *IEEE Transactions on Power Systems* 2000; **15**(2): 700–706.
5. Deconinck G, Decroix B. Smart metering tariff schemes combined with distributed energy resources, *Proc. Fourth International Conference on Critical Infrastructures (CRIS 2009)*, Linkoping, Sweden, 2009; 1–8.
6. Rahimi F, Ipakchi A. Demand response as a market resource under the smart grid paradigm. *IEEE Transactions on Smart Grid* 2010; **1**(1): 82–88.
7. Wang Y, Gu D, Wen M, Xu J, Li H. Denial of service detection with hybrid fuzzy set based feed forward neural network, *Proc. Advances in Neural Networks (ISNN 2010), LNCS 6064*, Shanghai, China, 2010; 576–585.
8. Wang Y, Ruan D, Xu J, Wen M, Deng L. Computational intelligence algorithms analysis for smart grid cyber security, *Proc. Advances in Swarm Intelligence (ASI 2010)*, Brussels, Belgium, 2010; 77–84.
9. Liang H, Choi B, Zhuang W, Shen X. Towards optimal energy store-carry-and-deliver for PHEVs via V2G system, *Proc. The 31st IEEE International Conference on Computer Communications (INFOCOM'12)*, Orlando, Florida, USA, 2012; 1674–1682.
10. Deng R, Chen J, Cao X, Zhang Y, Maharjan S, Gjessing S. Sensing-performance tradeoff in cognitive radio enabled smart grid. *IEEE Transactions on Smart Grid* 2013; **4**(1): 302–310.
11. Mohsenian A, Wong V, Jatskevich J, Schober R, LeonGarcia A. Autonomous demand-side management based on game-theoretic energy consumption scheduling for the future smart grid. *IEEE Transactions on Smart Grid* 2010; **3** (1): 320–331.

12. *Ontario electricity time-of-use price*. http://www.ontarioenergyboard.ca/OEB/_Documents/For+Consumers/TOU_prices_Winter.pdf.
13. Lu R, Liang X, Li X, Lin X, Shen X. EPPA: an efficient and privacy-preserving aggregation scheme for secure smart grid communications. *IEEE Transactions on Parallel and Distributed Systems* 2012; **23**(9): 1621–1632.
14. Wen M, Lu R, Lei J, Li H, Liang X, Shen X. SESA: an efficient searchable encryption scheme for auction in emerging smart grid marketing. *Security and Communication Networks* 18 January 2013, DOI: 10.1002/sec.699.
15. Yang Z, Yu S, Lou W, Liu C. *P^2: Secure and privacy-preserving communication and precise reward architecture for V2G networks in smart grid*. *IEEE Transactions on Smart Grid*; **2**(4): 697–706.
16. Liang X, Li X, Lu R, Lin X, Shen X. UDP: usage-based dynamic pricing with privacy preservation for smart grid. *IEEE Transactions on Smart Grid* 2013; **4** (1): 141–150.
17. Boneh D, Franklin M. Identity-based encryption from the Weil pairing, *Proc. Advances in Cryptology(Crypto 2001), LNCS 2139*, Santa Barbara, California, USA, 2001; 213–229.
18. Chow SM, Hui CK, Yiu SM, Chow KP. Two improved partially blind signature schemes from bilinear pairin, *Proc. The 8th Australasian Conference Information Security and Privacy (ACISP 2005)* LNCS 3574, Brisbane, Australia, 2005; 316–328.
19. Chen X, Zhang F, Liu S. *ID-based restrictive partially blind signatures and applications*. http://eprint.iacr.org/2005/319/.
20. Jiang L, Low S. Multi-period optimal energy procurement and demand response in smart grid with uncertain supply, *50th IEEE Conference on Proc. Decision and Control and European Control Conference (CDC-ECC 2011)*, Orlando, FL, USA, 2011; 4348–4353.
21. Sakai R, Ohgishi K, Kasahara M. Cryptosystems based on pairing, *Proc. Symposium on Cryptography and Information Security*, Okinawa, Japan, 2000.
22. Galbraith S. Pairings. In *Advances in Elliptic Curve Cryptography, Chapter 9*. Cambridge University Press: New York, NY, USA, 2005; 183–213.
23. NREL Solar Radiation Research Laboratory (BMS), October 2012. Solar Calendar, http://www.nrel.gov/midc/apps/calendar.pl?site=BMS;year=2012;month=10.