P2DR: Privacy-Preserving Demand Response System in Smart Grids

Depeng Li and Zeyar Aung
Masdar Institute Science and Technology
Abu Dhabi, UAE,
depenglee@gmail.com, zaung@masdar.ac.ae

John Williams and Abel Sanchez
Massachusetts Institute of Technology (MIT)
Cambridge, Massachusetts, USA
{jrw, doval}@mit.edu

Abstract— **Demand response programs are widely used to balance the supply and the demand in smart grids. They result in a reliable electric power system. Unfortunately, the privacy violation is a pressing challenge and increasingly affects the demand response programs because of the fact that power usage and operational data can be misused to infer personal information of customers. Without a consistent privacy preservation mechanism, adversaries can capture, model and divulge customers' behavior and activities at almost every level of society. This paper investigates a set of new privacy threat models focusing on financial rationality verse inconvenience. Furthermore, we design and implement a privacy protection protocol based on attributed-based encryptions. To demonstrate its feasibility, the protocol is adopted in several kinds of demand response programs. Real-world experiments show that our scheme merely incurs a substantially light overhead, but can address the formidable privacy challenges that customers are facing in demand response systems.**

Index terms- Consumer privacy, Demand Response, Privacy Preservation, Smart Grids;

I. INTRODUCTION

Smart grids facilitate smart energy management through active deployments of smart metering infrastructure in our society as part of a global initiative. An important feature in smart grid systems is the Demand Response (DR) program. In DR, customers alter their consumption patterns reacting to electricity price changes or utilities turn off customers' appliance when the system in jeopardy is sensed [25]. Through shaving power consumption peaks DR reliefs cost: even a light power consumption decrease, for example 5% introduces significant, say 50% price curtailment. The reason is because electricity generation cost raises sizably when the power generation capacity is near its maximum limit [2].

Despite aforementioned benefits, privacy leakages in DR have been widely discovered. DR together with smart metering technologies generates high-resolution data leaving customers' digital trails that others can monitor and exploit for their advantages. Without proper controls that eliminate privacy violation, customers participating in DR face unpleasant experiences: loss of personal information and disclosure of activity patterns [15], [19]. Privacy issues are of prime importance as long as a guarded DR is neglected.

Pioneer studies [13], [27] realize privacy violation can happen due to the free access to power consumption data. To safeguard privacy, recent researches deploy cryptographic tools [22], batteries [15], etc. to hide/encrypt metering data at the smart meter end.

However, privacy can be disclosed from other sources beyond power consumption data. In detail, DR systems contain several kinds of data: power consumption data, control commands, events, alarms, etc. [19]. The existing countermeasures mainly focus on the protection of electricity usages data. It is possible that the protection mechanisms could be bypassed while the adversary aims at other kinds of data. Messages sent from the utility to customers, for example, may trigger certain customers' reactions and in turn influence their power usage patterns. With the free access of those messages and contextual clues, scientific, curious or malicious users can not only infer customers' activity but deeply mine their habits such as their financial rationality. For example, at peak times, the electricity price is expensive. During that peak time, if a customer choose to turn off the air conditioner or raise the thermostat settings even though the outside temperature is baking hot, this particular behavior can be mined to deduce that the customer prefer financial savings to the comfortably cool living temperature.

Contributions:

Privacy Leakages: From an adversary's perspective, we practically illustrate privacy threats with the aid of corresponding examples. We further formalize two privacy leakage models, the Benefit Inconvenience Evaluation (BIE) and the Rationality Inconvenience Ratio (RIR). In BIE, the financial benefit resulting from rescheduling power consumption tasks is compared with the inconvenience that customers suffer. RIR compares customers' rationality with their discomfort experiences at every time instance.

P2DR Protocol: we focus on privacy preservation in the DR program's communication system rather than only at the smart meter end. We develop a new fine-grained protocol named the Privacy-Preserving Demand Response (P2DR) protocol through the usage of the Ciphertext-based Attribute-Based Encryption (CP-ABE, in short, ABE) system [4]. This protocol is compatible with the existing DR model, which is managed and operated by the easily-combined policy system based on residence addresses. It also offers high performance, and gives DR program a chance to fully take advantage of ABE's flexibility. We further demonstrate how P2DR is utilized in a few popular DR programs as examples.

Experimental Validation on Emulated Smart Grid Platform: Finally, we implement our approach which is executed on the commodity control server and emulated

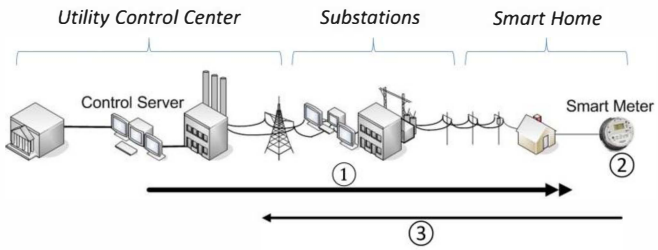

Figure 1. Demand Response Model. ① A DR control server multicasts initial DR signals and subsequent DR events: $M = \{\{C_1\} \ldots \{C_x\}\}$ $where$ $|M| = x$; ② After receiving M, each smart meter sm_i decides if C_i is designated to itself. If so, DR events are incorporated into residences' energy plan or the command C_i is executed on its appliance; ③ After the execution of C_i, smart meters sm_i estimate and validate actual load shedding, confirm actual results and unicast them back to the DR control server if necessary.

smart meters. The experimental results demonstrate that our solution merely incurs a low delay (≤ 500ms for number of attributes less than 5) which is acceptable to DR systems. Computational cost of P2DR is lightweight so that even emulated smart meters which are configured with low-end CPU and limited memory in our experiment, exhibit efficient performance.

II. BACKGROUND

A. Demand Response Model

In smart grids, multicast is extensively deployed due to its scalability, its efficiency and its functionality across network segments [26], [28]. DR also takes advantage of it for sake of efficiency. As depicted in Fig. 1, the control server cooperates with smart meters to achieve DR protocol.

Note that, in DR systems, a set of policies is established to manage the power curtailment. In this paper, we use *streets*, *ZIP*, *cities*, etc. as examples; some utilities may use '*district #*', '*sub-district #*', '*substation #*', '*feeder #*', etc. They are interchangeable in this paper since policies have to be translated into command messages before they are sent out to smart devices via multicast technologies

B. Demand Response Program

The DR program aims to balance the supply and the load in real time. It can be classified into two categories [20]: 1) the time-based program such as *Day Ahead Pricing* (DAP) and 2) the incentive-based program such as *Direct Load Control* (DLC) and *Emergence Demand Response Program* (EDRP). For the former, customers can adapt their power usage based on electricity price changes over times. The latter enables utilities to offer an incentive price encouraging customers reduce their power consumption.

1) Direct Load Control Program (DLC)

While the stress status in supply, the DLC program enables the utility to remotely curtail customers' load in a short notice based on customers' prior consent [2]. The utility controls residents' smart appliances for example, turning off air conditioners, water heaters, etc. or changing their thermostat settings.

2) Emergency Demand Response Program (EDRP)

To mitigate peak demand of power consumption, utilities execute EDRP [2], one example of which is to solicit the customer enrolling for pre-defined promotion packages. Each package corresponds to a timeslot and a specific incentive price. After subscribing a package, participants allow utilities control their appliances in the particular time slot in return for financial incentive.

3) Day-Ahead Pricing (DAP)

The day is usually divided into a number of time slots, for instance 24 one-hour slots, each of which is associated with a particular price. DAP program [2] will inform the customers the set of slots and prices in one-day ahead.

III. PRIVACY LEAKAGES

In this paper, we realize that the direct access to utility control messages and metering data in DR offers a substantial potential for adversaries to easily infer customers' behavior model, daily activities, habits, etc. [13]. We further present 1) general privacy leakage, 2) BIE model based on task rescheduling, and 3) RIR model based on price changes.

Utilizing the BIE and RIR models, an adversary is able to quantify customers' financial rationality against discomfort and then launch the following privacy violations: 1) Targeted Advertisement: customers can be classified into *spendthrift, moderates* and *saver* types. Spendthrifts prefer to big ticket items or even luxuries. Savers favor economical-and-applicable issues. Moderates are in between. Plus, based on habits to postpone tasks or bring tasks forward, customers are labeled as *early bird* or *latecomer* types. The former prefers to flyers beforehand and the latter enjoys a last-minute deal. Targeted advertisements could be customized for each one of them. 2) Alteration of customer types: when customers' type is altered, it may infer something new: there maybe new tenants or the resident may confront economic status changes.

In this section, based on the two models, we analyze two real-world scenarios: rescheduling cloth washing tasks and turning up/down the air conditioner. According to the result, the adversary could evaluate the level of inconvenience customers can tolerate for sake of financial gain.

A. General Privacy Leakages in DR system

Privacy threats occur when an adversary associates customers' fine-granular power usage data to daily activities e.g. breakfast, laundry, wakeup cycles, etc. [13], [21], [23]. Unlike previous researches, we further observe that privacy violations can also happen by inferring utility messages sent to customers together with other context:

Privacy leakage for appliance malfunctions: In DLC program, utilities send control commands C_i to appliances A_i which then execute C_i. When the execution fails and the appliance status S is sent back in clear text, *Eve* is powerful sufficient to identify appliance malfunctions via analyzing the status S. Advertisement companies can send customers targeted advertisement for repair or purchase purpose.

Privacy leakage for customers' presence*:* A customer who enrolls at an EDRP program selects a specific package

corresponding to a time slot, for example, 13:00 to 15:00 to curtail the power usage.

Example: the utility sends a remote control command to a participant ('$address\ A$') whose package corresponds to the time slot from 13:00 to 15:00. The command shuts down the air conditioner though the temperature is high (e.g. >104°F/ 40°C). The resident maybe inferred to be absence at the time window. Based on the command, *Eve* can take the risk to break in from 13:00 to 15:00 in future.

Privacy leakage for customers' financial benefits: Assume that a customer enrolls a DAP program. *Eve* can deduce the following habits of a customer: 1) Though being informed the varied prices over times, no task is rescheduled by customers. It reflects customers' financial rationality. 2) If the customer reschedules the cloth-washing task to midnight in a building, it may infer that the customer pay little attention to neighbors' reaction if the washing machine is noisy. 3) When electricity prices turn to be higher, the customer turns down the air conditioner even the weather is sultry (e.g. >104°F/40°C). It means that the customer may tolerate to discomfort for sake of financial gain.

B. Benefit Inconvenience Evaluation (BIE) Model

The Non-Intrusive Load Monitoring (NILM) technology can be used to break the electricitical demand profiles into different appliance usage tasks [7]. Through analyzing those tasks, we propose a *Benefit Inconvenience Evaluation* (BIE) model to evaluate the level of which a customer prefers financial gains while suffering conveniences in a DR program.

We assume that the adversary collect two sets of DR messages, one is before participating DR program and the other after. If the former is defined as m, the latter is m'. Assume the adversary capture the load profile in a time window with size x. To simplify, we assume the time window is one day. We define our privacy invasion method as the following: $N = \{\alpha_1, \dots, \alpha_n\}$ is a set of appliances where $|N| = n$; $\Psi = \{\psi_1, \dots, \psi_m\}$ is a set of tasks where $|\Psi| = m$; $P: N \times \Psi \to 0$ or 1 is a map between an appliance and a task; $D = \{d_1, \dots, d_x\}$ where $|D| = x$ is a set of power demand/consumption; $P = \{p_1, \dots, p_x\}$ where $|P| = x$, is a set of prices. Not loss the generality, we assume that the time step of each monitored time window is one hour. Therefore, $x = 24$. Based on the nature of demand response program, we also assume that $\forall\ d_i \in D$, there is one and only one corresponding $p_i \in P$.

Each task ψ_j where $1 \le j \le m$ occurred in the residence is corresponding to its host, namely, appliance α_i where $1 \le i \le n$. It can be a washing machine, an air conditioner, and so on. A task ψ_i is defined as follows:

$$\psi_j = \left(S_j, F_j, L_j = F_j - S_j, \left\{d_{s_j}, \dots d_{F_j}\right\}, \left\{p_{s_j}, \dots p_{F_j}\right\}\right) \quad (1)$$

$where\ L_j > 0$; Note that the schedule of a task ψ_j starts at S_j, ends at F_j and takes $L_j = F_j - S_j$ time units. For each time unit from S_j to $S_j + L_j$, a task ψ_j demands d_x electricity and its corresponding price is p_x.

To demonstrate BIE, two appliances, *washing machine* and *air conditioner*, are taken as examples:

Benefit vs. Inconvenience: Cloth Washing Task

For washing machines, BIE dedicates the scenario that how much inconveniences the customer bear to get the financial benefit in return. Regarding task rescheduling, assume the discomfort is the number of time slot difference that the cloth washing task ψ_j will be rescheduled, namely, $|S_j' - S_j|$. BIE for washing machines is defined as:

$$BIE_{wash} = \frac{\Delta C_{\psi_j}}{\Delta S_j} = \frac{\left(\sum_{t=S_j'}^{F_j'} d_t' \times p_t' - \sum_{t=S_j}^{F_j} d_t \times p_t\right)}{|(S_j' - S_j)|} \quad (2)$$

Benefit vs. Inconvenience: Air Conditioner

Assume that $\mathbb{C} = \{C_{S_j}, \dots, C_{F_j}\}$ is the corresponding temperature that the customer set for the air conditioner before the DR and $\mathbb{C}' = \{C_{S_j}', \dots, C_{F_j}'\}$ the counterpart thereafter for different time slots. BIE for air conditioners is defined as:

$$BIE_{AC} = \frac{\Delta C_{\psi_j}}{\mathbb{C}' - \mathbb{C}} = \frac{\left(\sum_{t=S_j'}^{F_j'} d_t' \times p_t' - \sum_{t=S_j}^{F_j} d_t \times p_t\right)}{\sum_{t=S_j}^{F_j} (C_t' - C_t)} \quad (3)$$

C. Rationality vs. Inconvenience Ratio (RIR) model

The Price Elasticity Matrix (PEM) [6] is defined to assess customers' financial rationality when they participate in DR programs. Unlike previous researches on PEM, we focus on inconvenience a customer has to suffer in exchange for financial gain and then further describe quantified evaluation for *Rationality vs. Inconvenience Ratio* (RIR).

The notion of *inconvenience* means the discomfort a customer experiences. It varies for difference appliances. Here, we use an air conditioner's temperature as examples. *Inconvenience* and *RIR for the air conditioner* are defined as in formula (4) and (5), respectively:

$$ic_{t_i} = \frac{\partial c_{t_i}/c_0}{\partial p_{t_i}/p_0} \quad (4)$$

$$RIR_{AC} = \frac{\sum_{i=1}^{24}\sum_{j=1}^{24} e_{i,j}}{\sum_{i=1}^{24} ic_{t_i}} = \frac{\sum_{i=1}^{24}\sum_{j=1}^{24} e_{i,j}}{\sum_{i=1}^{24} \frac{\partial c_{t_i}/c_0}{\partial p_{t_i}/p_0}} \quad (5)$$

where c_0 : initial temperature and p_0 : initial price. $e_{t,t'} = \partial d_t / \partial p_{t'}\ \ \forall t, t'$; t and t' are defined as different time instance; ∂d_t and ∂p_t are named as changes in demand and price at t and t' respectively. $e_{t,t}$ is referred as cross self-elasticity. It indicates the change in demand at a time instance t due to the price change at the same time instance t. $e_{t,t'}$ is cross elasticity. It is the change in demand at a time instance t due to the price change at the time instance t'. For $E = [e_{i,j}]_{24\times24}$, $e_{i,x} = \partial d(t_i)/\partial p(t_x)$, where $x \in \{i, j\}$.

To get the financial gain, a customer can postpone tasks or schedule tasks in advance. The former is defined by adding up elements below diagonal and the latter by adding up elements above diagonal in $E = [e_{i,j}]_{24\times24}$. They are described in formula (6) and (7), respectively.

$$R_{post} = \sum_{i=1}^{24} \sum_{j=1}^{i-1} e_{i,j} \quad (6)$$

$$R_{prior} = \sum_{i=1}^{24} \sum_{j=i+1}^{24} e_{i,j} \quad (7)$$

IV. System Overview and Protocol

A. Adversary Model and Security Assumption

Adversary Model: like other researches in areas of privacy preservations [9], [11], [22], we follow the semi-honest adversary model in which smart devices (e.g. smart meters, etc.) obey DR. Meanwhile, they are also curious about messages they learn (or share) and have the intension to combine these information if possible. Therefore, any participating smart devices should relay packets and also intend to uncover others' privacy by studying sensitive messages received.

Security Assumption: we assume that smart devices such as smart meters, etc. are tamper-resistant. Furthermore, we also assume the availability of PKI deployed in utilities [17]. Likewise, we assume that the control server hides its own private key and publishes its public key (e.g. RSA [16]). Moreover, we assume that device attestations are deployed to validate smart meters, etc. Besides, our protocol mainly focuses on the confidentiality service to protect privacy. The authentication and integrity services guaranteed by digital signatures [16] and one-way hash functions [16] are also important but beyond the scope of our paper. Hence, we will not describe them due to page limits.

B. System Overview

There are three participants in P2DR system: smart meters installed in customer residences as well as control servers and the trusted Key Distribution Center (KDC) deployed in utility control centers. To protect multicast communication which sends crucial DR messages from the control server to multiple smart meters, we adopt an ABE encryption system [4]. To secure unicast communication which feedbacks results from the smart meter to the control server, we deploy the RSA public key encryption [16] which is faster as compared with others e.g. El Gamal [16] in terms of encryption operations. It is of importance for smart meters which are resource-limited in terms of processors. The KDC's responsibility is to issue ABE keys and RSA private/public key pairs to smart meters and the control server.

C. Protocol

The essential goal of P2DR protocol is to realize an efficient privacy preservation mechanism satisfying scalability and time-critical requirements of DR program without any privacy exposures. P2DR protocol takes advantage of the multicast encryption functionality and fine-grained attributes of ABE scheme for sake of efficiency. It is also in conformance with regulations in DR system [10]. The basic components and their correlation of P2DR protocol are depicted in Fig. 2. We describe them in details as follows:

System Settings:

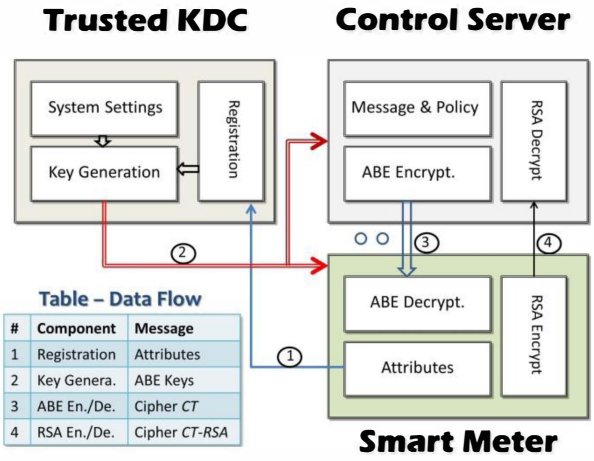

Figure 2. Architecture of P2DR protocol

Step 1: during the setup phase of the ABE scheme, a trusted KDC first creates the public key (PK) and master secret key (MSK). Thereafter, it publishes PK and hides MSK.

Step 2: the trusted KDC generates the RSA public and private key pair ($PB_{RSA}^{CS}, Pr_{RSA}^{CS}$) for the control server. After that, PB_{RSA}^{CS} is published and Pr_{RSA}^{CS} is issued to the control server via secure channels. For every smart meter, repeat this procedure since the RSA public key encryption algorithm plays the secure channel role to encrypt & deliver ABE Secret Key (SK) to its corresponding smart meter.

Registration: according to the regulation of a particular DR program, the trusted KDC first assigns each smart meter an attribute set. Second, the set is parsed into standard attribute $\mathbb{S}$ which is used to create the smart meter's secret key (SK).

Example I (DLC): In DLC, we assume that there is a smart meter sm_i installed at a residence. The residential address is selected as an attribute set to represent the smart meter sm_i. For example, the following attributes are used in our application, DLC-P2DR: $\mathbb{S}$ ={$attr1$= "*street number*"; $attr2$ = "*street name*"; $attr3$ = "*ZIP value*"; $attr4$ = "*city name*"}. For a particular smart meter sm, let $\mathbb{S}_{sm}$ be {$attr1$= "*12345*"; $attr2$ = "*main street*"; $attr3$ = "*XYZ*"; $attr4$ = "*noname*"}. In DLC-P2DR, the trusted KDC's registration component parses the attributes, $\mathbb{S}$ and informs the corresponding smart meter.

Example II (EDRP): In EDRP, let us assume that a customer selects the promotion package corresponding to a time slot, for example from 13:00 to 15:00. In this time window, the control server can reduce the customer's power consumption through controlling customers' appliances. The following attributes are used in our application, EDRP-P2DR: $\mathbb{S}$ ={$attr1 \geq$ *start of time slot*; $attr2 \leq$ end of time slot}. For a particular smart meter sm, let $\mathbb{S}_{sm}$ = {$attr1 \geq$ *13:00*; $attr2 \leq$ 15:00}. In EDRP-P2DR, the trusted KDC's registration component parses the attributes, $\mathbb{S}$ and informs the corresponding smart meter.

Example III (DAP): in DAP, the control server will only broadcast the price for 24-hour time slots of the next day. The information is plaintext which can be accessed by

everyone. Therefore, we do not need to encrypt them via ABE system. So, our scheme does not prepare any attributes for any smart meters in DAP-P2DR.

ABE Key Generation: In the P2DR system, the trusted KDC first generates the secret key, SK for each smart meter. with the input as smart meter's attributes $\mathbb{S}$ and ABE scheme's Master Secret Key (MSK). Then, the trusted KDC uses smart meter's RSA public key to encrypt SK. The ciphertext is delivered to the corresponding smart meter which is the only one that can decrypt it.

ABE Encryption: In DR program, DR messages such as prices, remote control commands, events, alarms, etc. should be broadcasted in such a way that each smart meter can be informed of the real-time information. In P2DR, the control server assigns a proper policy, $\mathbb{P}$ to reflect each message.

The control server then encrypts each message M with M's policy, $\mathbb{P}$ and ABE scheme's public key PK. After that, the ciphertext CT and $\mathbb{P}$ are delivered to corresponding smart meters via multicast / broadcast channels.

Example I (DLC): In DLC, to achieve the demand and supply balance, one *scenario* is to deliver a message M to a specific area to control these air conditioners. For example, the control server multicasts a control command to an area with the attributes "*main street; noname city; zip XYZ*". Then, let message M's policy $\mathbb{P}$ be $\{attr2$ = "*main street*"; $attr3$ = "*XYZ*"; $attr4$ = "*noname*"$\}$. Our DLC-P2DR will encrypt a message M with ABE public key, PK and M's policy, $\mathbb{P}$. At last, the control server multicasts the ciphertext CT together with policy $\mathbb{P}$ to smart meters in this area.

Example II (EDRP): In EDRP, during emergence status at a time slot, t, one *scenario* is to send a message M to smart meters which enroll EDRP. If subscribing a package which reflects the same time slot t, smart meters execute appliance control commands indicated by M. For example, the command will control air conditioners from *14:00* to *15:00.* Then, let message M 's policy $\mathbb{P}$ = $\{ attr1 \geq 14{:}00;\ attr2 \leq 15{:}00\}$. Our EDRP-P2DR encrypts message M with ABE public key, PK and policy, $\mathbb{P}$. At last, the control server multicasts the ciphertext CT together with its policy $\mathbb{P}$ to smart meters. Only the ones enrolling for a particular package reflecting time slot [14:00, 15:00] execute the command to get the incentive prices in return.

ABE Decryption: After successfully receiving ciphertext CT and $\mathbb{P}$, each smart meter sm first matches its own attributes $\mathbb{S}_{sm}$ with $\mathbb{P}$ to decide if the ciphertext CT is designated to itself. If so, smart meter sm decrypts the ciphertext CT by using its own secret ABE key SK_{sm}. After decryption operation, sm can read message C_i. Then, sm associates C_i into its energy use plan or executes C_i directly. The control server waits for smart meter sm's result which is encrypted and sent back in such a way that outsiders cannot peek.

Example I (DLC): In DLC, let smart meter sm 's attributes $\mathbb{S}_{sm}$ ={$attr1$= "*12345*"; $attr2$ = "*main street*"; $attr3$ = "*XYZ*"; $attr4$ = "*noname*"$\}$. Since ciphertext CT 's police $\mathbb{P}$ is $\{attr2$ = "*main street*"; $attr3$ = "*XYZ*"; $attr4$ = "*noname*"$\}$, $\mathbb{S}_{sm}$ matches with $\mathbb{P}$. Therefore, the smart meter decrypts the ciphertext CT and gets the message M.

Example II (EDRP): In EDRP, let smart meter sm's attributes $\mathbb{S}_{sm}$ ={ $attr \geq$ *13:00*; $attr2 \leq$ 15:00$\}$. Since ciphertext CT's police $\mathbb{P}$ is $\{attr1 \geq$ *14:00*; $attr2 \leq$ 15:00$\}$, $\mathbb{P}$ matches with $\mathbb{S}_{sm}$. Therefore, the smart meter decrypts the ciphertext CT and gets the message M.

RSA Encryption: Each smart meter needs to report its status, execution result, etc. to the control server so that DR program can verify whether the real-time power usage comply with the balance principle. Therefore, in P2DR, the smart meter encrypts its result or its status via RSA encryption Alg. with the control server's RSA public key PB_{RSA}^{CS}. Then, the ciphertext $CT\text{-}RSA$ is sent back to the control server. The control server is the only one which can decrypt it since it retains its own RSA secret key Pr_{RSA}^{CS}. All results for each smart meter should be reported in the RSA-encrypted format.

RSA Decryption: After receiving ciphertext $CT\text{-}RSA$ sent from the smart meter, sm, the control server invokes RSA decryption Alg. with its RSA public key as input to decrypt it. The outputted plaintext M will be used by the control server to evaluate the accomplishment of the mission designated to the smart meter, sm. It will also be used to assess the power curtailment and to generate customer bills.

V. Experiments and Performance Evaluation

The performance for P2DR protocol depends on two critical parts: 1) *ABE Encryption* and *RSA Decryption* components at the control server end as well as 2) the *ABE Decryption* and *RSA Encryption* components at the smart meter end. As depicted in Fig. 2, they correspond to messages transmission ③ and ④, respectively. Note that signal propagation delays are negligible. Times used to parse the *Message & Policy* component are trivial. We will not discuss their performance due to page limits. Thus, our emphasis specifically focuses on *ABE* and *RSA* components. We implement ABE based on Pairing-Based Crypto-graphy (PBC) library [14] built on the GNU Multiple Precision (GMP) arithmetic library [1]: GMP library provides arbitrary precision arithmetic APIs which are invoked by PBC to support pairing-based cryptosystem. In our application, we use the pairing-friendly elliptic curves $E(\mathbb{F}_{2^{379}})\colon y^2 + y = x^3 + x + 1$ and $E(\mathbb{F}_p)\colon y^2 = x^3 + Ax + B$ with a 512-bit prime. Furthermore, to satisfy the performance requirement, we deploy MNT elliptic curve to implement the ABE scheme. Table I evaluates the number of operations to accomplish each ABE component.

In Fig. 3, we demonstrate these functions' performance when executing them on a control server, a KDC and a smart meter, respectively. We notice that ABE encryption at a control server and ABE decryption at a smart meter executes less than 80 *ms* and 300 *ms* respectively when the number of attributes is 5 or less. The roundtrip execution time for P2DR takes less than 400 ms when the number of attributes is 5. In words, P2DR system can satisfy the DR program because DR program accepts up to a few seconds' delay [18].

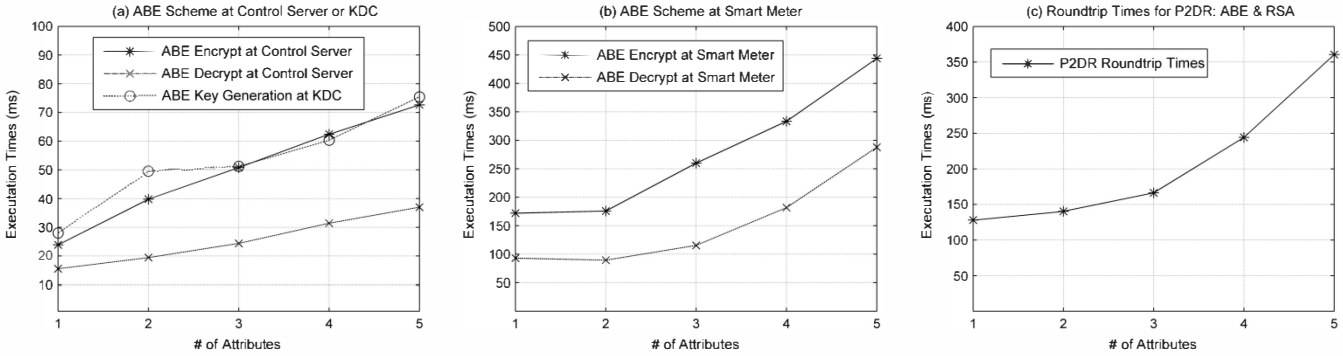

Figure 3. Test Results of Execution Times. MNT elliptic curve of embedding degree 6 with order 160 bits length and base field order 512 bits length were utilized in P2DR. We collected ten times' (randomly selected number) executions of ABE operations, the average values of which are illustrated at (a) – (c), including (a) ABE key generation, ABE De/Encryption on a KDC / Control Server, (b) ABE De/Encryption on a smart meter and (c) the roundtrip time to process a utility task from the control server to smart meters and vice versa (the propagation delay is too trivial to be included). The number of attributes were ranging from 1 to 5 (randomly selected number). As executing unauthorized 3rd party system software upon real-world smart meters is prohibited (according to GE Company), the control server/KDC and the smart meter in the experiment were both virtual machines hosted by Oracle's VirtualBox installing Ubuntu 11.10. The detailed configuration of KDC/server: Memory-496MB; CPU-2.67GHz; Disk-7.9 GB. That of the smart meter is Memory-64MB; CPU-33MHz which is the same configuration as an ARM Cortex 926EJS processor. It, generally, serves as a real-world smart meter CPU.

TABLE I
PERFORMANCE EVALUATION OF ABE COMPONENTS

Component	Computation	Communication
ABE Key Gen.	$2 \cdot E \times (\#\ of\ A.)$	$(\#\ of\ A.) \times \lvert g \rvert$
ABE Encryption	$2 \cdot E \times (\#\ of\ L.)$	$(\#\ of\ L.) \times \lvert g \rvert$
ABE Decryption	$2 \cdot \underset{\#\ of\ L.}{\mathrm{MAX}}(P \times (\#of\ L.)) + \underset{N\ on\ Path}{\mathrm{MAX}}(E \times (\#of\ N.))$	$\lvert M \rvert$

E-Exponentiation, P-Pairing; L.-Leaf, N-Node; A.-attributes; $g \in \mathbb{G}$;

TABLE II
EXECUTION TIMES OF CRYPTOGRAPHIC COMPONENTS

Items	Host	Times (ms)
ABE Setup	Trusted KDC	26.45
RSA Encrypt.	Smart Meter	8.096
RSA Decrypt.	Control Server	2.952

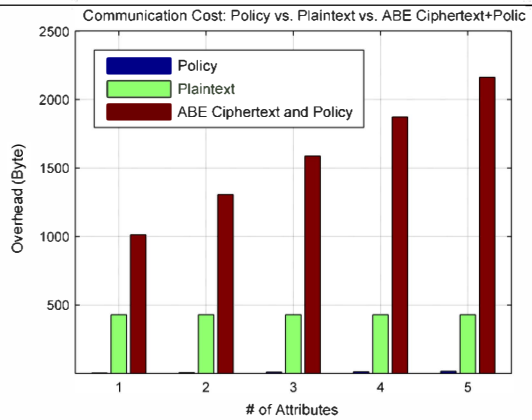

Figure 4. Communication overhead for the ABE component in P2DR (interchangeably, P2DR Ciphertext and Policy) *where* plaintext: 429 bytes. It includes packet sizes of ciphertext and that of policies (refer to $Alg.5$). The ratio between it and plaintext is 235.9%, 304.4%, 370.2%, 436.6% and 503.9% when the numbers of attributes are 1, 2, 3, 4, and 5 respectively.

The ABE communication overhead in real-world for P2DR is illustrated in Fig. 4. It shows the bytes transmitted for policies, for plaintext and for overall ABE ciphertext messages (in details, policies || ciphertext). Though communication overhead is still affordable in DR, its reduction is highly demanded. The execution times of ABE Setup at the trusted KDC, of the RSA encryption at the smart meter and of the RSA decryption at the control server are listed in Table II. We conclude that they are efficient sufficient to be utilized in DR system.

VI. RELATED WORKS

Several means extract privacy of power usage data in DR program. Lisovich *et al.* [13] conduct a live monitoring experiment in a student residence. Collected power usage data with a time resolution of 15 seconds is analyzed via NILM to extract appliance usage. They further design a behavior extraction algorithm to measure critical privacy parameters (presence, sleep cycle, number of residence, etc.). In [27], Wicker and Thomas propose a framework guided by privacy-aware design practice (HEW methodology). H. S. Cho, *et al*. [5] propose AERO to extract user's activities based on the Activities of Daily Living (ADL).

Researchers also study means to preserve privacy for smart metering technologies but they are not designed specifically for DR. **1)** ***Battery***: McLaughlin *et al.* [15] develop the Non-Intrusive Load Leveling (NILL) to mask the appliance's power usage signature via rechargeable battery. However, rechargeable batteries is costly ($1,000 [15]) and labor-intensive. **2)** ***Anonymity***: Efthymiou and Kalogridis [8] propose a trusted key escrow service to anonymize frequent readings with pseudonymmous IDs for metering data. **3)** ***Disturbance***: Li *et al.* [12] design an approach to compress meter reading. It enhances privacy. Tomosada *et al.* [24] propose a method to generate virtual demand data which can be distributed among institutes to protect customer's privacy. **4)** ***Cryptographic Schemes***: Li *et al.* [11] protect smart metering data aggregation via homomorphic encryption algorithm. Garcia and Jacobs [9] design a privacy-friendly protocol by using homomorphic

(Paillier) encryption and additive secret sharing. Rial and Danezis [22] use zero knowledge proofs and commitments to preserve smart meters' privacy.

VII. CONCLUSIONS AND FUTURE WORKS

DR is a critical service in smart grids. However, the privacy leakage also raises customers' concerns. DR data including utility messages and smart metering data can easily be mined to expose customers' privacy. We propose two privacy violation models to assess customers' financial rationality and their ability to tolerate inconvenience. Furthermore, we develop P2DR, a privacy preserving protocol to conceal customers' sensitive information with the use of ABE scheme. Our experiments show an acceptable result. At last, it is exceedingly required to revoke expired ABE keys in a more efficient way, remarkably reduce the size of ciphertext and reasonably hide policies of ciphertext. They all will serve as our future research.

VIII. REFERENCES

[1] http://gmplib.org/

[2] M. H. Albadi, E. F. El-Saadany. Demand Response in Electricity Markets: An Overview, IEEE Power Engineering Society General Meeting, 2007. pp. 1-5

[3] P. Barreto, B. Lynn, and M. Scott, Efficient implementations for Pairing-based Cryptography. *Journal of Cryptology,* 17, pp.321-334, 2004.

[4] J. Bethencourt, A. Sahai, and B. Waters. Ciphertext-policy attribute-based encryption. In *IEEE Symposium on Security and Privacy*, pp. 321-334, 2007.

[5] H. S. Cho, T. Yamazaki, and M. Hahn. AERO: Extraction of user's activities from electric power consumption data. *IEEE Transactions on Consumer Electronics*, vol 56(3), pp. 2011-2018, 2010.

[6] A. K. David and Y. Z. Li. consumer rationality assumptions in the real time pricing of electricity. IEE Proceedings of Gene., Trans. and Distr. Vol 139(4) pp. 315-322. July 1992.

[7] S. Drenker, A. Kader. Nonintrusive Monitoring of Electric Loads. IEEE Computer Applications in Power, Vol. 12, pp.47-51, 1999.

[8] C. Efthymiou and G. Kalogridis. Smart Grid Privacy via anonymization of smart metering data. In *IEEE (SmartGridComm'10)*, pp. 238-243, 2010.

[9] F. D. Garcia and B. Jacobs. Privacy-friendly energy-metering via homomorphic encryption. *Security and Trust Management,* LNCS vol. 6710, pp. 226-238, 2011.

[10] D. Irwin, N. Sharma, and P. Shenoy. Towards Continuous Policy-drivenDemand Response in Data Centers. In Proceedings of the ACM SIGCOMM Workshop on Green Networking, pp. 19-24, 2011.

[11] F. Li, B. Luo, and P. Liu. Secure information aggregation for smart grids using homomorphic encryption. In *SmartGridComm'10*, pp. 327-332.

[12] H. Li, R. Mao, L. Lai, and R. C. Qiu. Compressed meter reading for delay-sensitive and secure load report in smart grid. In *SmartGridComm'10*, pp. 114-119.

[13] M. A. Lisovich, D. K. Mulligan, S. B. Wicker. Inferring personal information from demand-response systems, In *IEEE Security & Privacy*, vol 8(1), pp. 11-20, Jan.-Feb. 2010.

[14] B. Lynn. The Stanford Pairing Based Crypto Library. http://crypto.stanford.edu/pbc/

[15] S. McLaughlin, P. McDaniel and W. Aiello. Protecting consumer privacy from electric load monitoring. In *Proc. of the 18th ACM CCS'11,* 2011.

[16] A. Menezes, P. C. van Oorschot, and S. A. Vanstone, Handbook of Applied Cryptography, CRC Press, 1997.

[17] A. R. Metke and R. L. Ekl. Security Technology for smart grid networks. *IEEE Transactions on Smart Grid*, 1, pp. 99-107, 2010.

[18] NIST, Guidelines for Smart Grid Cyber Security: Vol. 1, Smart Grid Cyber Security Strategy, Architecture, and High-Level Requirements, NISTIR 7628. August, 2010.

[19] NIST, Guidelines for Smart Grid Cyber Security: Vol. 2, Privacy and the Smart Grid, NISTIR 7628. August, 2010.

[20] M. Parvania and M. F.-Firuzabad. Demand Response Scheduling by Stochastic SCUC. IEEE Trans. on Smart Grid. Vol 1(1), pp. 89-98. June 2010.

[21] S. R. Rajagopalan, L. Sankar, S. Mohajer, and H. V. Poor, Smart meter privacy: A utility-privacy framework, *In IEEE SmartGrid Comm'11*, pp. 190-195, Oct. 2011.

[22] A. Rial and G. Danezis. Privacy-preserving smart metering. In *Proc. of ACM CCS Workshop WPES'11*, pp.49-60, Oct. 2011.

[23] L. Sankar, S. Kar, R. Tandon, and H. V. Poor. Competitive privacy in the smart grid: An information-theoretic approach. In *SmartGrid Comm'11,* pp. 220-225, Oct. 2011.

[24] M. Tomosada, Y. Sinohara. Virtual energy demand data: Estimating energy load and protecting consumers' privacy. in *Proceedings of 2nd IEEE PES ISGT 2011*. pp. 1-8. Anaheim California, USA.

[25] U.S. Department of Energy. Assessment of Demand Response and Advanced Metering. Federal Energy Regulatory Commission report. Aug. 2006, www.FERC.gov.

[26] Q. Wang, H. Khurana, Y. Huang; K. Nahrstedt,Time Valid One-Time Signature for Time-Critical Multicast Data Authentication, *IEEE INFOCOM 2009*, pp. 1233 – 1241.

[27] S. Wicker and R. Thomas. A Privacy-Aware Architecture For Demand Response Systems. in *Proc. of the Hawaii International Conference on System Sciences (HICSS)*, 2011, pp. 1-9.

[28] J. Zhang and C. A. Gunter. Application-aware secure multicast for power grid communication. In *IEEE SmartGridComm'10*, pp. 339-344, 2010.