P^2: Privacy-Preserving Communication and Precise Reward Architecture for V2G Networks in Smart Grid

Zhenyu Yang, *Student Member, IEEE*, Shucheng Yu, *Member, IEEE*, Wenjing Lou, *Senior Member, IEEE*, and Cong Liu, *Member, IEEE*

***Abstract*—Vehicle-to-grid (V2G) networks are important components of the smart grid (SG) for their capability of providing better ancillary services and facilitating the adoption of renewable resources. The operation of the V2G networks is based on continuously monitoring the status of individual battery vehicle (BV) as well as a carefully designed incentive scheme to attract sufficient participating BVs. However, the close monitoring tends to raise privacy concerns from the BV owners about identity and location information leakage, which have not been considered in previous works. In this paper, we make the first attempt to identify the privacy-preserving issues and propose a precise reward scheme in V2G networks, both of which are important towards bringing the concept of V2G network into practice. In V2G networks, it is the service providers (individual BVs) who need privacy protection rather than the service consumer (power grid). This unique characteristic renders privacy protection solutions proposed for conventional network systems not directly applicable. To protect privacy of BVs in V2G networks, we present P^2, a secure communication architecture which achieves privacy-preserving for both BVs' monitoring and rewarding processes. Extensive performance analysis shows that P^2 only incurs moderate communication and computational overheads.**

***Index Terms*—Secure communication, smart grid, V2G networks.**

I. Introduction

THE transforming of the traditional power grid to the smart grid (SG) has drawn great attentions in both industry and academia. Vehicle-to-grid (V2G) networks are emerging as an important part of SG due to their capability of providing better ancillary services than traditional approaches [1], [2] as well as the rapidly increasing penetration rate of battery vehicles (BVs).[1] Specifically, a V2G network is a system where parked BVs communicate with the power grid to consume electricity. In addition, these BVs also sell their electricity storage capability by delivering electricity to or from the power grid as required. By letting BVs charge during off-peak hours (storing surplus electricity generated during that time) and discharge during peak hours (returning the stored electricity back into the grid to meet the current high demand), V2G networks bring lots of benefits to power grid, including 1) enabling new ways of providing ancillary services (regulation and spinning reserve); 2) faster response time (start charging/discharging within milliseconds [3]) and no running cost of the unit commitment schedules; 3) smoothing variable generations from renewable sources like solar, wind, etc. [4], [5]; 4) providing distributed grid-connected storage for unexpected outages. Many trial projects for V2G network have already been deployed around the world [6], [7].

In order to provide services to the power grid, operators of the V2G networks need to monitor the up-to-date status of each BV to evaluate the total electricity storage capability currently available. The status information includes the BV's location,[2] battery's capacity, battery's state-of-charge (s.o.c., which is defined as the ratio of the energy stored in a battery to its full capacity), expected time to leave, etc. This monitoring process has to be continuous due to two reasons. Firstly, individual BV joins and leaves the V2G network in a dynamic way. Secondly, providing these ancillary services requested by power grid needs BV to do lots of charging/discharging operations, which may harm the battery's life (also referred as battery degradation) and the effect of battery degradation is closely related to the battery's current s.o.c. [8]. For example, s.o.c. higher than some level makes the discharging operation less harmful to the battery. Since the s.o.c. of a parked BV is variable due to charging or discharging operations, the continuous monitoring is necessary for operators of the V2G networks to reduce the harm imposed on individual BV's battery caused by providing services.

The capacity of individual BV's battery is usually tens of KWh. To satisfy the service requirement of power grid which is in tens of MWh level, a V2G network needs a large amount of BVs' participation to ensure the availability of sufficient electricity storage at any given time. For instance, it is estimated that about 200 000 BVs are needed to meet the requirement of regulation services and an additional 273 000 BVs for the spinning reserves of California's power grid [2]. To ensure the adequate participation of the BVs into the V2G network, a well-designed

Manuscript received October 15, 2010; accepted February 14, 2011. Date of publication May 19, 2011; date of current version November 23, 2011. This work was supported in part by the U.S. National Science Foundation under Grants CNS-0746977 and CNS-0831628. Paper no. TSG-00176-2010.

Z. Yang and W. Lou are with the Department of Electrical and Computer Engineering, Worcester Polytechnic Institute, Worcester, MA 01609 USA (e-mail: zyyang@wpi.edu; wjlou@wpi.edu).

S. Yu is with the Department of Computer Science, University of Arkansas at Little Rock, AR 72204 USA (e-mail: sxyu1@ualr.edu).

C. Liu is with the Decision and Information Sciences Division, Argonne National Laboratory, Argonne, IL 60439 USA (e-mail: liuc@anl.gov).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2011.2140343

[1] In this paper, BV refers to various vehicles that have a battery as part of (or all) the energy sources required for propulsion, including battery electric vehicles, fuel cell vehicles, plug-in hybrid electric vehicles, etc.

[2] The purpose of operators of the V2G networks to monitor BVs' locations is to avoid making improper charging schedule that causes grid congestion for some specific area.

incentive scheme is a necessity. One type of incentive scheme is based on long-term agreement [9], [10]. Specifically, operators of the V2G networks provide BV owners battery maintenance service and discounts in the rates for the BV charging and parking if they signed a long-term participation agreement. In return, the BV owners are obligated to connect their BVs with the power grid at designated time periods specified in the agreement. BV owners who fail to meet the obligations will be penalized by stopping the battery maintenance service, canceling discount on charging rate, etc.

However, the fixed connection requirement contained in the long-term agreement will cause inconvenience to the BV owners. For instance, there could be occasions when BV owners need to drive BVs away during the connection times specified in the agreement, either due to an unexpected early leaving from the office or some other accidental events. In these cases, the long-term agreement-based incentive schemes enforce BV owners to give up one of the benefits, either the services provided by operators of the V2G networks or the freedom to use their own BVs. In another word, this type of incentive schemes do not possess good usability. Besides this, considering that different BVs may possess different types of batteries with different capacities and may contribute to different services, the long-term agreement-based incentive schemes that does not take these differences into consideration fail to achieve equitable incentive. This may also reduce BV owners' interest in joining the V2G networks. In this paper, we propose another type of precise and equitable incentive scheme with better usability, where operator of a V2G network rewards each participating BV for each service that it made contribution to. This incentive scheme does not require BV owners to sign a long-term contract and obey restricted connection times, thus giving the BV owners total freedom to user their own BVs. The reward is in the form of E-cash [11] and BV owners could redeem it later at the operator of the V2G network for battery maintenance, cheaper charging/parking, etc.

The continuous monitoring and rewarding tend to raise privacy concerns from BV owners about identity and location information leakage. For instance, survey data shows that most vehicles are in parked status 95% of a day on average [12]. Thus, by analyzing the monitoring data of specific BV, such as the parking lots it visited and how long it stayed there, the operator of a V2G network can easily deduce the personal activities of this BV's owner. Secondly, since ancillary services will be requested by power grid quite frequently (e.g., regulation services could be requested 400 times per day and each of them typically lasts just a few minutes [1]), the detailed service record for specific BV could result in privacy leakage too. For example, based on those service records, battery sellers could find BVs that likely need to replace their batteries due to heavy service load and make targeted advertising, which maybe not wanted by all the people. Finally, due to the direct interaction with the power grid, a secure communication architecture is required to protect the V2G networks against various cyber attacks, like impersonation attack, replay attack, data modification, and injection. For reasons presented above, an effective secure and privacy-preserving communication architecture is fundamental towards implementation of V2G networks.

Although security and privacy issues have been extensively studied in various networks, such as wireless mesh networks (WMNs) [13], [14], cellular networks [15], and indoor location networks [16], solutions proposed for these network systems are not directly applicable due to the unique characteristic of V2G networks. In V2G networks, it is the individual BVs who provide ancillary services to the power grid, thus the service paradigm is that multiple service providers (individual BVs) provide services to a single[3] user (power grid).[4] This is in sharp contrast with the common service paradigm in conventional network systems where single or few service provider provide services to a large amount of users. In addition, in V2G networks, it is the service providers who need privacy protection during the monitoring and rewarding processes rather than users. However, as the research in V2G networks is still in its early stage, most existing works [1], [9], [17]–[20] are mainly focused on the design of conceptual structures or the impact of V2G networks on the current power grid. To the best of our knowledge, no previous work clearly identified the privacy issues in V2G networks.

In this paper, we make the following main contributions. 1) We make the first attempt to identify the privacy protection issues in V2G networks based on their unique characteristic. 2) We propose a precise and equitable reward scheme for V2G networks where individual BV is rewarded according to its contribution to each service. This reward scheme allows participants to enjoy both the total freedom of using their BVs and full benefits provided by operators of the V2G networks. 3) To protect privacy of BVs in V2G networks, we propose a secure communication architecture which achieves privacy-preserving for both BV's monitoring and rewarding processes. P^2 also pursues important objectives for secure communication, including mutual authentication, confidentiality, data integrity, and so forth.

The rest of the paper is organized as follows. Section II introduces preliminaries and Section III describes the system models used in this work. Section IV will present the design of P^2 in detail, which is followed by security and performance analysis in Section V. Finally, Section VI makes a conclusion.

II. Preliminaries

A. Background of V2G Networks

One of the fundamental properties of current power grid is lacking of cost-effective storage (only 2.2% capacity in pumped storage) [1], so the operator of the power grid has to continuously manage the generation and transmission of the electricity to match fluctuating customer load. This is now primarily accomplished by ancillary services provided by large generators, where they are tuned on a minute-by-minute basis and tend to be underutilized. The situation could be worse in the future smart grid where large amount of intermitting renewable resources, like solar and wind, are expected to be adopted. One promising solution for this problem is BV-based V2G networks [21]. Although batteries installed on BVs have limited energy storage, short battery lifetime and high energy cost per KWh, which

[3] Due to the natural monopoly of the power grid in a specific area.

[4] In this paper, we focus on the process of providing ancillary services rather than the charging process that BVs are considered as normal loads.

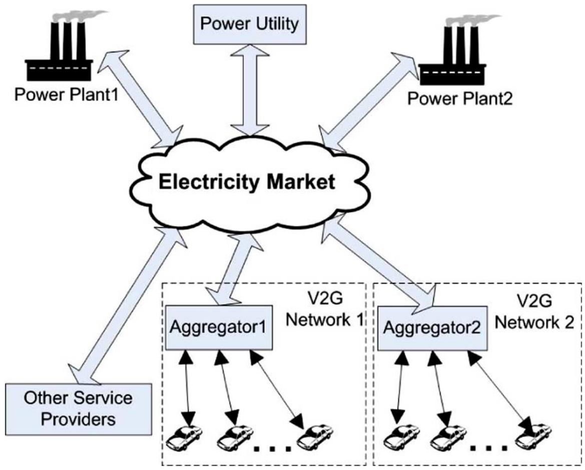


Fig. 1. Aggregators in the V2G networks.

make them not suitable for providing baseload services [1], they are perfectly fit for providing high-value, short-duration ancillary services due to their quicker response time, lower standby cost and lower capital cost per KWh.

However, individual battery's capacity is too small, usually tens of KWh. This is far below the base requirement for making transaction in electricity market, which is at least in MWh level. In addition, the charging/discharging operations of individual BV alone can not provide any meaningful service to the power grid if they are not synchronized with many other BVs' operations. These problems could be addressed by introducing the concept of aggregator in the system architecture for V2G networks [9], [18], which collects large amount of BVs as a group and makes transaction with the power grid on behalf of them, as illustrated in Fig. 1. Another function of the aggregator is to avoid the V2G network's reliance on individual BV's behavior during providing services. For instance, although individual BVs may leave the parking lot earlier than expected, thus interrupting the service providing process, the rate of early departure would be quite stable and predictable for a group consisting of a large amount of BVs [17].

B. Basic of Blind Signature Techniques

Blind signature technique is introduced by David Chaum in 1982 [22], which enables a recipient to get signature on a message without revealing this message to the signer. Since then it has been widely used in applications like E-voting [23], E-cash [11], etc., where user anonymity is required. Brands developed the first restrictive blind signature scheme [24], which restricts the signed message to conform certain rules rather than being totally random. Abe and Fujisaki developed the first partially blind signature scheme [25], where the signed message could explicitly include some common agreed information that is visible during the blind signature process.

Maitland *et al.* and Chen *et al.* combined these two blind signature techniques and proposed provably secure restrictive partially blind signatures, based on public key infrastructure (PKI) and ID-based encryption (IBE) systems, respectively [26], [27]. The concept of IBE system is firstly proposed by Shamir [28]. Compared with certificate-based PKI system, IBE allows an entity to use his identity as its public key, which greatly simplifies the key management. The first implementation of a practical IBE system is presented by Boneh *et al.* [29] in 2001, which is based on Weil pairing. We adopt the ID-based restrictive partially blind signature technique as the cryptographic building block of P^2's design and readers could refer to [27] for detailed description.

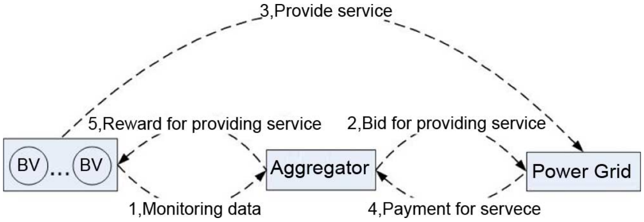


Fig. 2. Network model of the V2G networks.

III. System Models

A. System Model

The system model considered in this paper is illustrated in Fig. 2. Each participating BV connected with the power grid periodically reports its current status to the aggregator. The power grid publishes the service requests for the near future in the electricity market. Through the reports collected from BVs, the aggregator evaluates the current total electricity storage capacity of all the BVs in the V2G network. Based on the total capacity and service requests from the power grid, the aggregator makes bids in the electricity market for providing some of the services. If a bid is successful, the aggregator selects a subset of BVs that could provide the requested service with minimum cost and then commands them to do the corresponding operations. For example, charging in the following 5 minutes or discharging until the s.o.c. reaches 60%. After confirming the service is fulfilled, power grid makes payment to aggregator and then aggregator rewards each BV that is selected to provide this service. Due to the fast response requirement of regulation services, the reporting period of BV is usually a few seconds [9].

Since the interaction between aggregator and power grid just follows routine in the electricity market, in this paper, we only focus on the interaction between BVs and the aggregator. Specifically, how to report monitoring data to the aggregator and how to reward individual BV for providing services. Both processes need to achieve security and privacy objectives which will be identified in Section III-C.

B. Network Architecture

We describe the network architecture of a V2G network in this section, which is shown in Fig. 3. In our architecture, there are 4 parties, including central aggregator (CAG), local aggregators (LAGs), individual BV, and trusted authority (TA). CAG and LAGs usually belong to the operator of the V2G network, individual BV belongs to its owner, and TA belongs to some independent organizations like Regional Transmission Organizations (RTO)/Independent System Operators (ISO). In the following we will introduce them in detail.

CAG is the only entity that could directly communicate with the electricity market on behalf of those geographically dispersed BVs. To reduce the communication burden on CAG

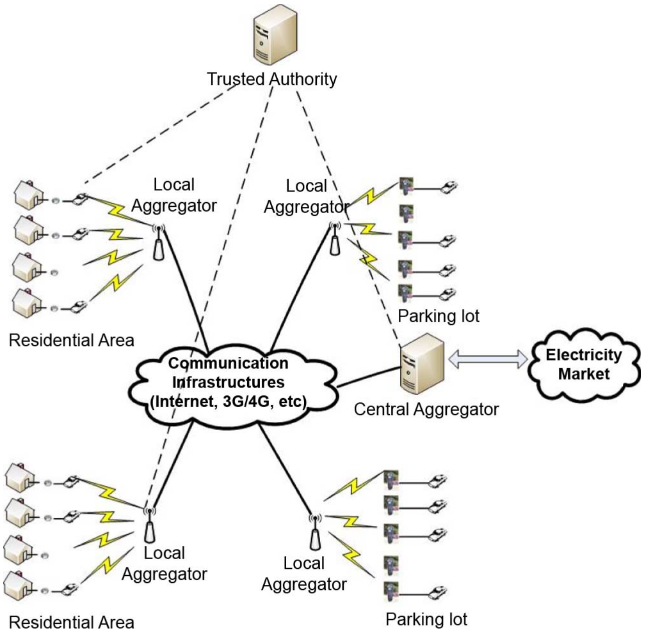


Fig. 3. Network architecture of a V2G network.

caused by directly communicating with each BV, a hierarchical aggregation scheme is adopted. Specifically, a LAG will be deployed for each local area. This LAG will directly monitor every BV within this local area and send the collected monitoring data to CAG in batch mode. For each BV parking position, either it belongs to a commercial parking lot or a private residence, a charging device should be deployed, through which the parked BV could connect to the power grid. The TA could be shared by multiple V2G networks, which does the system initialization, like generating public system parameters, assigning private key for each entity and so forth. Now we describe an imaginary V2G network. Assume there is a V2G network focused on the New England area. It has one CAG located in Boston and multiple LAGs dispersed in Massachusetts, New Hampshire, Rhode Island, and other states, and the ISO-New England plays the role of TA. The system initialization is represented by dotted lines in Fig. 3, where each BV, LAG, and CAG get a public/private key pair from TA. The communication between smart meters and LAG in the local area, which is represented by lighting marks in Fig. 3, could be implemented with various technologies, including Zigbee networks, WMNs, power line networks, or a combination of them. The communication between LAGs and CAG could go through broadband infrastructures like Internet, 3G/4G, etc., which is represented by bold solid lines in Fig. 3. Note that we do not consider the communication between different BVs in this paper.

We assume the deployment of charging device for each parking position for two reasons if the V2G networks are going to be widely deployed: 1) the charging speed of the battery is too slow (usually needs 3–5 h for a fully charging) for the BV owner to wait during the charging process, which makes it not enough to just build designated charging stations for BVs, as was done for gasoline vehicles; 2) vehicles stay in parked status the most time of a day, during which the batteries could be charged without affecting BV owners' daily lives. For instance, the owners do not need to purposely change their time schedules to wait for charging the BVs. This charging device deployment is also assumed by many other works [9], [17], [18], either explicitly or implicitly and is suggested as the most suitable infrastructure deployment strategy for V2G networks according to the current industrial conditions by [30].

C. Security Model

1) Trust Model: The trust relationships between the 5 parities in a V2G network are defined as follows. TA is trusted by all the other parties. There is no direct trust relationship between individual BV and CAG or LAGs since they belong to different organizations. In general, the operator of the V2G network (CAG and LAGs) is honest but curious, which means it will basically follow our proposed protocols, but will try to figure out as much private information of each BV as possible during the execution of these protocols. More specifically, the private information here means the location and identity of each BV during its participation in the V2G network.

2) Security Goals: To protect the privacy of each BV as well as the communications between different parties within the V2G network against various cyber attacks, we recognize the following security goals needed to be achieved which are not necessarily a complete list.

1) Mutual authentication between BV and aggregator (CAG or LAG): a BV should authenticate an aggregator for preventing impersonation attack and the aggregator also should authenticate the BV to prevent illegitimated BV from joining the V2G network.
2) Confidentiality and integrity of the communication: the communicated messages between different parties should be kept confidential and integrated to prevent eavesdropping and data modification from malicious attackers or commercial opponents.
3) Location and identity privacy of BV: no entity other than the BV itself could link the real identity with each parking location of the BV.
4) Incontestable and anonymous reward: a BV should get exact amount of rewards from aggregators according to its contribution of providing services and does not need to reveal its real identity during the rewarding process. When the BV owner redeems a reward at any aggregator, the aggregator should not able to link it with any reward assigned previously. However, if the BV owner redeemed the same reward twice, which is called double redeeming, the aggregator should be able to trace the real identity of this BV owner with the help of CAG.
5) Efficient revocation of BVs: since P^2 does not impose long-term contract on the BVs, It should provide mechanism to allow BVs to join or quit the V2G network efficiently.

Assumptions: We make the following assumptions in the design of P^2.

1) The CAG and LAGs will not be compromised since they are powerful and could be carefully placed in physical secure locations.
2) Each BV is uniquely identified by its battery. The same assumption is also made in [9].

3) Each BV is equipped with 3 necessary devices for participating V2G network, as stated in [2], [9]. The first one is a precise, tamper-resistant metering device, which measures exactly how much electricity or electricity storage capacity a BV did provide. The second one is a set of control devices, which allow the driver to set parameters like willingness of participating the V2G network,[5] minimum allowed s.o.c. during parking period, expected leaving time, etc. The third one is a communication module. The total cost of all devices is moderate according to [2], [9].

Notations

- $\rightarrow\rightarrow$ and $||$: denote multihop communication and concatenation, respectively.
- ID_x: the real identity of an entity x in V2G network.
- PS_x: the pseudonym generated by a BV x based on ID_x.
- $\mathcal{Q}_x/\Gamma_x$: the public/private key pair of BV x corresponding to its real identity ID_x.
- $\mathcal{Q}_{\mathrm{PS}_x}/\tilde{\Gamma}_x$: the public/private key pair of BV x corresponding to its pseudonym PS_x.
- $\mathcal{SIG}_{\Gamma_x}(M)$: the ID-based signature on a message M using signer x's private key Γ_x.
- $\mathcal{SKE}_k(M)$: the symmetric key encryption on message M using the shared secret key k.
- $\mathcal{HMAC}_k(M)$: a hash-based message authentication code on message M using the shared secret key k.
- $\mathcal{ST}_x$: the current status of the BV x, which consists of BV's parking location, battery's type, battery's capacity, battery's s.o.c., minimum allowed s.o.c. during the parking period, expected leaving time, expected s.o.c. when leaving and charging/discharging rates.[6]

IV. Design of P^2

We firstly present the main idea of P^2. In order to achieve secure and privacy preserving communication and precise reward for individual BVs in a V2G network, we novelly utilize the ID-based restrictive partially blind signature technique in the design of P^2. Specifically, each participating BV firstly makes a registration at the CAG, during which the CAG will generate a *permit* using ID-based restrictive partially blind signature technique and assign it to the BV. This *permit* has to be presented to the LAG to ensure only the eligible BV could access the V2G network. The blindness property of the *permit* protects the BV's real identity from the LAG. We modify the original ID-based restrictive partially blind signature technique to make it suitable for LAG to generate precise *reward* for individual BV while the BV's real identity is unknown to the LAG. Due to the restrictiveness property of the blind signature technique, the *reward* contains encoded information related to the real identity which enables the traceability of its double redeeming. To reduce the potential computational overhead on LAGs incurred by generating large amount of *reward* s, we propose a lazy reward scheme which postpones and aggregates the generation of *rewards* for all the services provided by a BV during its current parking period to the time when the BV is going to leave. In this way, LAGs only need to generate a single aggregated *reward* for each BV during one of its parking periods.

Generally, P^2 consists of initialization, *permit*-based access control and BV's monitoring, anonymous service providing and rewarding, and BV's revocation protocols. In what follows, we will describe these protocols in detail.

A. Initialization

TA initializes the V2G network by performing the following algorithm [27]:[7] Assume $\mathcal{PG}$ is an arbitrary Bilinear Diffie-Hellman (BDH) parameter generator which satisfies the BDH assumption.

1) Select a security parameter $k \in \mathbb{Z}^+$ and then run $\mathcal{PG}$ on k to generate a prime q, two groups $\mathbb{G}_1, \mathbb{G}_2$ of order q and an admissible bilinear map $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$. Then TA chooses 3 random generators $P, P_1, P_2 \in \mathbb{G}_1$ and 4 cryptographic hash functions: $H_1 : \{0,1\}^* \rightarrow \mathbb{G}_1$, $H_2 : \mathbb{G}_1^3 \times \mathbb{G}_2^5 \rightarrow \mathbb{Z}_q$, $H_3 : \mathbb{G}_1^3 \times \mathbb{G}_2^4 \rightarrow \mathbb{Z}_q$, and $H_4 : \mathbb{G}_2 \times \mathbb{G}_2 \times \mathrm{ID}_x \times \{0,1\}^* \rightarrow \mathbb{Z}_q$.
2) Pick a random $s \in \mathbb{Z}_q^*$ and set $P_{pub} = sP$.
3) The system parameters are $\mathbf{params} =< q, \mathbb{G}_1, \mathbb{G}_2, e, P, P_{\mathrm{sub}}, P_1, P_2, H_1, H_2, H_3, H_4 >$, which will be published by TA and the $\mathbf{master-key}$, $s \in \mathbb{Z}_q^*$, will be kept as secret.

Each entity x, including all the BVs, LAGs, and CAG, submits its ID information, which could be represented by a unique string $\mathrm{ID}_x \in \{0,1\}^*$, to TA to get its public/private key pair $\mathcal{Q}_x/\Gamma_x$, where $\mathcal{Q}_x = H_1(\mathrm{ID}_x) \in \mathbb{G}_1^*$ and $\Gamma_x = sH_1(\mathrm{ID}_x)$.

Each BV participating the V2G network has to register its ID information at CAG, during which BV randomly generates a number $u \in Z_q^*$ and computes an unique account number $A_{\mathrm{BV}} = u_s P_1 + P_2$. Both $\mathrm{ID}_{\mathrm{BV}}$ and A_{BV} will be stored on CAG and u_s will be kept as BV's secret number. We note that although the participants of the V2G network in P^2 do not need to sign a long-term contract with the operator of the V2G network, BVs still have to do a simple registration at CAG. Those failed to do so will be denied from accessing the V2G network.

B. *permit*-Based Access Control and BV's Monitoring

To ensure only the eligible BVs could access the V2G network, operator of the V2G network asks each BV to present a *permit* before its participation, where the *permit* is generated by CAG and assigned to eligible BV in advance. In the following we will introduce the *permit* generation, *permit* verification and BV monitoring schemes in detail.

1) permit Generation: Since the BV has to reveal its real identity for obtaining the *permit*, restrictive partially blind signature technique is applied for generating *permit* to ensure that verifier can not link BV's real identity with this *permit* when it sees the *permit* later. The ID-based restrictive partially blind

[5] A BV owner may choose not to join the V2G. If this is the case, the BV will not periodically report its battery's current status and thus is invisible in the V2G network. However, it still could execute normal charging operation.

[6] According to [17], once BV has to do charging/discharging operations, the maximum rates should be adopted.

[7] We adopt standard IBE scheme in this paper due to its simplicity which could facilitate readers to understand P^2, we note that more advanced hierarchical ID-based encryption (HIDE) scheme could also be used by P^2 for higher key management efficiency.

TABLE I
permit GENERATION ALGORITHM

BV		**CAG**
let $M = A_{BV}$, $g = e(P, \mathcal{Q}_{CAG})$, $g_1 = e(P_1, \mathcal{Q}_{CAG})$, $g_2 = e(P_2, \mathcal{Q}_{CAG})$, $y = e(P_{pub}, \mathcal{Q}_{CAG})$.	$\xrightarrow{Step\ \ 1:\ ID_{BV}, M, t_1, \mathcal{SIG}_{\Gamma_{BV}}(H_1(ID_{BV}\|\|M\|\|t_1))}$	randomly chooses $Q \in_R \mathbb{G}_1$ and $r \in_R \mathbb{Z}_q^*$, then computes $z = e(M, \Gamma_{CAG})$, $a = e(P, Q)$, $b = e(M, Q), U = rP$ and $Y = r\mathcal{Q}_{CAG}$.
	$\xleftarrow{Step\ \ 2:\ z, a, b, U, Y, t_2, \mathcal{HMAC}_{k_1}(z\|\|a\|\|b\|\|U\|\|Y\|\|t_2)}$	the symmetric key $k_1 = e(\Gamma_{CAG}, \mathcal{Q}_{BV})$.
randomly chooses $\alpha, \beta, \gamma, \lambda, \mu, \sigma, u, v \in_R \mathbb{Z}_q^*$, and computes $M' = \alpha M, A = e(M', \mathcal{Q}_{CAG})$, $B = g_1^{\beta} g_2^{\sigma}, z' = z^{\alpha}, a' = a^u g^v, b' = b^{u\alpha} A^v$, $Y' = \lambda Y + \lambda\mu\mathcal{Q}_{CAG} - \gamma H_1(c)$, $U' = \lambda U + \gamma P_{pub}$, $h = \lambda^{-1} H_2(M', Y', U', A, B, z', a', b') + \mu$, $c' = hu$ and $k_1 = e(\Gamma_{BV}, \mathcal{Q}_{CAG})$.	$\xrightarrow{Step\ \ 3:\ h, t_3, \mathcal{HMAC}_{k_1}(h\|\|t_3)}$	
	$\xleftarrow{Step\ \ 4:\ S_1, S_2, t_4, \mathcal{HMAC}_{k_1}(S_1\|\|S_2\|\|t_4)}$	computes $S_1 = Q + h\Gamma_{CAG}$, $S_2 = (r + h)\Gamma_{CAG} + rH_1(c)$.
If $e(P, S_1) = ay^h, e(M, S_1) = bz^h$ hold. computes $S_1' = uS_1 + v\mathcal{Q}_{CAG}, S_2' = \alpha S_2$. The restrictive partially blind signature on (M', c) is $(Y', U', z', c', S_1', S_2')$ and the requested *permit* is $\{(M', c), (Y', U', z', c', S_1', S_2'), B\}$, where B will be used in the verification of the *permit*.		

signature scheme proposed in [27] is adopted by P^2. Specifically, the *permit* generation algorithm is presented in Table I. Suppose M is the original message sent from BV to CAG for signing, c is the agreed common information and t_i is a precise timestamp. We define c to be the expiration time of this *permit* for BV's efficient revocation, which is set to be 24 h after the current time. The purpose of timestamp t_i is to prevent replay attack.

2) permit Verification: When accessing the V2G network, each BV presents a *permit* and a pseudonym $\mathrm{PS}_{\mathrm{BV}}$ to the LAG located in the local area. BV generates the pseudonym by randomly selecting a number $\tilde{u} \in_R \mathbb{Z}_q^*$ and computes the corresponding public/private key pair as $\mathcal{Q}_{\mathrm{PS}_{\mathrm{BV}}} = \tilde{u}H_1(\mathrm{ID}_{\mathrm{BV}})$ and $\tilde{\Gamma}_{\mathrm{BV}} = \tilde{u}\Gamma_{\mathrm{BV}} = s\mathcal{Q}_{\mathrm{PS}_{\mathrm{BV}}}$. The purpose of the pseudonym $\mathrm{PS}_{\mathrm{BV}}$ is for easily constructing session keys for the frequent communication during the BV's monitoring process. A general description of the *permit* verification process is like below.

(1) $\mathbf{BV} \rightarrow\rightarrow \mathbf{LAG}$: $\mathcal{Q}_{\mathrm{PS}_{\mathrm{BV}}}$, $permit$, t_5, $\mathcal{HMAC}_{k_2}(\mathcal{Q}_{\mathrm{PS}_{\mathrm{BV}}}\|permit\|t_5)$, where $k_2 = e(\tilde{\Gamma}_{\mathrm{BV}}, \mathcal{Q}_{\mathrm{LAG}}) = e(\Gamma_{\mathrm{LAG}}, \mathcal{Q}_{\mathrm{PS}_{\mathrm{BV}}})$. The LAG firstly checks if the *permit* is expired and then verifies its validity. If this *permit* is valid and not expired, it continues to check the validity of the $\mathcal{Q}_{\mathrm{PS}_{\mathrm{BV}}}$ by computing the $\mathcal{HMAC}$ value and compares it with the received one. If both *permit* and $\mathcal{Q}_{\mathrm{PS}_{\mathrm{BV}}}$ are valid, the verification is successful and the LAG stores them together. The *permit* verification algorithm is presented in Table II. For each accepted *permit*, LAG also records the following items: $M', c, r_1, r_2, time$ and sends them to CAG through the encrypted channel created by shared symmetric key $k_3 = e(\mathcal{Q}_{\mathrm{CAG}}, \Gamma_{\mathrm{LAG}}) = e(\mathcal{Q}_{\mathrm{LAG}}, \Gamma_{\mathrm{CAG}})$.

3) BV's Monitoring: After confirming the validity of the presented *permit* and $\mathcal{Q}_{\mathrm{PS}_{\mathrm{BV}}}$, a session key k_2' generated based on the shared symmetric key k_2, will be used in the following communication between this BV and LAG. k_2' could be updated periodically. When the next monitoring cycle comes, this BV reports its current status $\mathrm{ST}_{\mathrm{BV}}$ to the LAG. After collecting $\mathrm{ST}_{\mathrm{BV}}$s for this monitoring period from all the BVs in the local area, LAG forwards them to the CAG in batch mode. Since each $\mathrm{ST}_{\mathrm{BV}}$ is identified by pseudonym $\mathrm{PS}_{\mathrm{BV}}$, both the LAG and CAG could not link the monitoring data with the real identity of the BV.

1) $\mathbf{BV} \rightarrow\rightarrow \mathbf{LAG}$: $\mathcal{SKE}_{k_2'}(\mathcal{Q}_{\mathrm{PS}_{\mathrm{BV}}}, \mathcal{ST}_{\mathrm{BV}}, t_7)$, $\mathcal{HMAC}_{k_2'}(\mathcal{Q}_{\mathrm{PS}_{\mathrm{BV}}}\|\mathcal{ST}_{\mathrm{BV}}\|t_7)$.
2) $\mathbf{LAG} \rightarrow\rightarrow \mathbf{CAG}$: $\mathcal{SKE}_{k_3}(\mathrm{ST}_{\mathrm{BV}}s, t_8)$, $\mathcal{HMAC}_{k_3}(\mathrm{ST}_{\mathrm{BV}}s\|t_8)$.

C. Anonymous Service Providing and Rewarding

After receiving those monitoring data from LAGs, the CAG computes the current available electricity storage capacity resides in the V2G network and makes bids for providing some services which are publicly requested by power grid in the electricity market. How to do such computation is a complicated problem which attracts lots of research efforts [31]. Here we just assume there is one computation algorithm exists, since this is out of the range of this paper and does not affect the usability of P^2. If a bid is successful, CAG will ask LAGs to select a subset of BVs to provide the requested service [9]. How to choose a proper subset is another complicated problem which needs to consider many factors, including the battery status, electricity price, BV owner's specific schedule, the restriction of power lines, etc. This also attracts many research efforts [32], [33]. we assume there is an algorithm exists to select the BVs, since this is out of the range of this paper and does not affect the usability of P^2. LAGs then send each selected BV a service command cmd_{service} separately, which is encrypted by already built shared secret key k_2'.

1) $\mathbf{LAG} \rightarrow\rightarrow \mathbf{BV}$: $\mathcal{SKE}_{k_2'}(cmd_{\text{service}}, t_9, \mathcal{SIG}_{\Gamma_{\text{LAG}}}$ $(H_1(cmd_{\text{service}} \| t_9))$

During the following monitoring cycles, LAGs keep checking if the selected BV is executing cmd_{service} indeed by observing its ST_{BV}, for instance, whether the s.o.c. has increased from 80% to 90% or not. If the LAG observed that some BV left unexpectedly during the service providing process, it will immediately find new BV to join the subset. After confirming the accomplishment of the service, the LAG has to give corresponding $reward$ to each selected BV. To achieve anonymous reward and the traceability of its double redeeming, we also adopt restrictive partially blind signature technique for the generation of the $reward$. Compared with generation of $permit$, generation of $reward$ faces a challenge which is the anonymity of the BV (only PS_{BV} is known to LAG now). In the generation of $permit$ during the registration process where the BV has to present its real identity to CAG, the CAG could restrict the original message M to contain identity related information. However, directly imposing such a restriction during the generation of a $reward$, which is the key step for achieving traceability of the possible double redeeming, is impossible since LAG does not know BV's real identity now. Fortunately we observe that LAG has a copy of $permit$ of each participating BV, one component of which is the blind message M' that contains information related to the real identity of the BV. By letting M' to be the original message during the generation of $reward$, real identity-related information is naturally contained in the original message.

For specific BV, the frequency of providing services, thus the frequency of requesting for $reward$ from LAG, is much higher than the frequency of requesting for $permit$. Thus generating reward immediately after each accomplished service will put heavy computational burden on the LAG. To solve this problem, we propose a lazy reward scheme which postpones the generation of the $reward$s for all the services provided during the current parking period to the time when the BV is going to leave. Specifically, LAG gives a simple signature sig_{service} to BV immediately after it accomplished an service, which indicates the reward value $reward_{\text{value}}$ of this service. When the BV is going to disconnect from the power grid, it requests a single $reward$ from LAG based on the sum of the reward values of all the sig_{service}s it received during this parking period. Since generating a sig_{service} just involves one normal signature and one hash operation that is far efficient than generating a $reward$ which needs 3 pairing operations and several hash operations, the computational burden of the reward scheme on LAG is greatly alleviated.

The precise reward scheme is described below.

1) $\mathbf{LAG} \rightarrow\rightarrow \mathbf{BV}$: $\mathcal{SKE}_{k_2'}$ (PS_{BV}, ID_{LAG}, cmd_{service}, $reward_{\text{value}}$, t_9 and sig_{service}), where sig_{service} consists of $\mathcal{SIG}_{\Gamma_{\text{LAG}}}(H_1(\text{PS}_{\text{BV}} \| \text{ID}_{\text{LAG}}$, $service_{\text{service}} \| reward_{\text{value}} \| t_9))$.
2) $\mathbf{BV} \rightarrow\rightarrow \mathbf{LAG}$: when BV is about to leave, it sends $\mathcal{SKE}_{k_2'}(\sum reward_{\text{value}}, t_{10})$, $\mathcal{HMAC}_{k_2'}(\sum reward_{\text{value}} \| t_{10})$.
3) $\mathbf{LAG} \rightarrow\rightarrow \mathbf{BV}$: LAG and BV execute the restrictive partially blind signature scheme presented in Table I. However, now we let $M_r = M'$ represent the original message sent from BV to CAG for signing and $c_r = \sum reward_{\text{value}}$ represent the agreed common information. $M_r' = \alpha_r M_r$ is the blinded message, where the α_r is the random number that BV selected in step 2 which corresponds to α in Table I. The $reward$ consists of $\{(M_r', c_r), (Y_r', U_r', z_r', c_r', S_{1_r}', S_{2_r}'), B_r\}$.

When BV owner wants to redeem the $reward$ at CAG (or other LAGs), she presents the $reward$ and the identity of the LAG where this $reward$ is generated to CAG. CAG does the verification by generally following algorithm shown in Table II. The difference is that the BV owner calculates responses as $r_{1_r} = d_r(u_s \alpha \alpha_r) + \beta_r$ and $r_{2_r} = d_r \alpha \alpha_r + \sigma_r$. If the verification is successful, CAG accepts and stores this $reward$.

D. BV's Revocation

We need to consider two types of revocations. In the first case, if the operator of the V2G network wants to revoke a BV's right to access the V2G network, what it needs to do is just deny this BV's new requests for $permit$, since the $permit$s already possessed by this BV will be expired in the next day automatically. In another case, the BV is compromised, which means its secret number u_s and private key Γ_{BV} are both revealed to the attacker. The BV needs to report all its $permit$s which are still not expired to the operator of the V2G network and the operator will immediately notify all LAGs to deny all attempts to access the V2G network by using those $permit$s to prevent attackers from gaining invalid accesses to the V2G network. The BV also has to ask for a new private key from TA, select another secret number and make another registration on the CAG.

V. Security and Performance Analysis

In this section, we give a comprehensive security and performance analysis of P^2. Through the analysis, we will show how the security goals listed in Section III-C are achieved with moderate communication overhead, which also demonstrates P^2's usability for large V2G networks.

A. Security Analysis

Location and identity privacy of BV. Due to the adoption of restrictive partially blind signature technique in the generation of $permit$, the LAG which verified the $permit$ can not deduce the BV's real identity from the $permit$ and the related pseudonym, even with the help of CAG. Further, for each pair of $permit$ and pseudonym, a BV only uses it within single parking

TABLE II
permit VERIFICATION ALGORITHM

BV		**LAG**
	$\xrightarrow{\mathit{Step}\ \ 1:\ \ \mathit{permit}, t_6, \mathcal{HMAC}_{k_2}(\mathit{permit} \Vert t_6)}$	
	$\xleftarrow{\mathit{Step}\ \ 2:\ \ \mathit{challenge}\ \ d}$	computes $A = e(M', \mathcal{Q}_{CAG})$. If $A \neq 0$, computes $d = H_4(A, B, \mathcal{Q}_{LAG}, time)$, where $time$ is the binary representation of the current time.
computes $r_1 = d(u_s\alpha) + \beta$ and $r_2 = d\alpha + \sigma$.	$\xrightarrow{\mathit{Step}\ \ 3:\ \ \mathit{responses}\ \ r_1, r_2}$	computes $a' = e(P, S_1')y^{-c'}$ and $b' = e(M', S_1')z'^{-c'}$. The signature is valid if $e(S_2', P) = e(Y' + H_3(M', Y', U', A, z', a', b')\mathcal{Q}_{CAG}, P_{pub}) \times e(H_1(c), U')$ holds. LAG accepts this *permit* if and only if $g_1^{r1} g_2^{r2} = A^d B$ holds, and the signature is valid and not expired.

period, thus LAGs can not link a specific BV's multiple parking activities with the same BV. In this way, the location and identity privacy of individual BV owner during the monitoring process is well protected. An additional advantage of adopting restrictive partially blind signature is its capability of tracing *permit*'s double using, either caused by illegal sharing or caused by compromisation. In detail, if a *permit* has been used twice, during its two verification processes, the CAG could get two pairs of responses from the corresponding LAG, respectively

$$r_1 = d(u_s\alpha) + \beta, r_2 = d\alpha + \sigma \quad (1)$$

$$r_1' = d'(u_s\alpha) + \beta, r_2' = d'\alpha + \sigma \quad (2)$$

from which the CAG could deduce the secret number $u_s = (r_1 - r_1')/(r_2 - r_2')$ of the BV that applied this *permit* and obtain its unique account number $A_{\mathrm{BV}} = u_s P_1$ to reveal the real identity of this BV. We note that simply obtaining a valid *permit* and use it twice does not enable the identity disclosure presented above, since the generations of both responses r_1 and r_2 during the verification process involve the secret number u_s, which is only known to the BV itself if it is not compromised or shared with other BVs.

Anonymity and incontestability of the reward. In order to protect the identity privacy of the well-behaved BVs and at the same time keep the capability of tracing BVs which commit double redeeming, the generation of *reward*, similar as that of the *permit*, also adopts the restrictive partially blind signature technique. The difference is that when generating the *permit*, the real identity and the associated unique account number A_{BV} is revealed to the CAG, thus by letting A_{BV} be the original signing message, CAG could easily impose the restriction on the generation of the blinded messages which must contain encoded identity information. However, when generating *reward*, the LAG does not know the real identity of the BV. P^2 addresses this problem by letting M' to be the original signing message and modifying the calculation of responses r_1 and r_2 to r_{1_r} and r_{2_r}. The traceability of the double redeeming BVs could be deduced similarly as that of *permit*. Finally, although LAGs in P^2 apply a lazy reward scheme when assigning *reward*s to a specific BV, rather than reward it immediately after each accomplished service, the signatures made by the LAG for every service the BV provided during this parking period make it unable to deny the *reward* request from BV, the value of which is the sum of all the $reward_{\mathrm{value}}$s contained in the signatures. This ensures the incontestability of the reward scheme.

Basic security requirements. P^2 can also achieve security objectives, including mutual authenticaiton between BV and aggregators, confidentiality of the communications, validation of the communicating messages, through the adoption of the standard cryptographic primitives: namely, symmetric key-based encryption, secure hashed message authentication, digital signature. The use of timestamp in all the communicating messages could effectively prevent replay attack.

B. Performance Analysis

In this section, we analyze the performance of P^2 in terms of computational and communication overheads.

1) Computation: For each *permit* generation process, the BV needs to do 8 pairings, 9 exponentiations on G_2, and 9 scalar multiplications on G_1. However, 5 pairings could be precomputed and shared by multiple generation processes, including the computing of g, g_1, g_2, y, and k_1. Other operations like hashing and message authentication code are omitted since they just contribute negligible computation cost. Based on the test presented in [34]–[36], a Tate pairing operation consumes about 10 ms on a platform with PIII 3.0 GHz, 30 ms on a platform with Pentium D 3.0 GHz and 170 ms on an iMote2 sensor working at 416 MHz. The underlying based field of the elliptic curve is over F_p with a 512-bit prime p which could achieve similar security level as 1024-bit RSA. The exponentiation and scalar multiplication operations are more efficient than pairing and usually consume much less time [37]. We note that although there is no clear standard about the computational capability of BV, it is supposed to be more powerful than iMote2 sensor used in [34], [35] due to unlimited power supply. Thus these testing results can be used for a meaningful evaluation. During the *permit* verification, BV only needs to generate two responses r_1 and r_2 by doing several normal multiplications and additions on Z_q. The computational cost for generating and redeeming *reward* is similar as that of the *permit*.

Although the generation of the *permit* and *reward* involve several complex computations, especially those pairing operations, they will not be executed often. During each parking period (from the time the BV enters the parking position and connects to the power grid to the time when the BV disconnects from the power grid and leaves the parking position), the BV only needs to present one $permit$ for accessing the V2G network and request for single $reward$ from corresponding LAG. Since any specific BV would experience quite few number of parking periods during a day, for example, less than 10, it only needs a few number of $permit$s[8] and $reward$s within a day.

During the monitoring process, each BV needs to periodically report its current status to LAG. Those reports will be encrypted with standard symmetric encryption method like DES. Since the reporting period is usually several or even tens of seconds, this will incur negligible computational cost for BV.

On the aggregator side, the CAG needs to do 4 pairings and 5 scalar multiplications for the generation of single $permit$ and $reward$, respectively. In the verification process of $permit$ and the redeeming process of $reward$, aggregators need to do 6 pairings, 5 exponentiations, and 1 scalar multiplication. For a large-scaled V2G network with hundreds of thousands of BVs, the computational burden on the aggregators could be millions of pairings and other operations for each day. However, we note that these operations will be scattered throughout the whole day. In addition, considering that those aggregators are dedicated equipment and could be built with advanced computing techniques including cluster or even delegated to cloud computing service providers [38], [39], they are supposed to be much more powerful and could afford these computational cost easily.

2) Communication: The communication overhead incurred by P^2 mostly comes from the periodical monitoring, where each BV needs to report its current status $\mathrm{ST}_{\mathrm{BV}}$ to LAG. Since the information contained in the $\mathrm{ST}_{\mathrm{BV}}$ only occupies very short message (no larger than 100 bytes) and the period of reporting is usually several or even tens of seconds, this communication overhead is totally tolerable for current communication techniques [9].

VI. Conclusion

In this paper, we make the first attempt to identify and formulate the privacy protection and precise reward problems in V2G networks, both of which are important for bring the V2G concept into practice. We give our solution P^2, a secure and privacy-preserving communication and precise reward architecture for V2G networks, which could not only provide satisfiable privacy protection and precise reward to the BVs, but also achieves other important security objectives including mutual authentication, confidential communication, data integrity, etc.

References

[1] W. Kempton and J. Tomic, "Vehicle-to-grid power fundamentals: Calculating capacity and net revenue," *J. Power Sources*, vol. 144, no. 1, pp. 268–279, Jun. 2005.

[2] S. E. Letendre and W. Kempton, "The V2G concept: A new model for power?," *Public Utilities Fortnightly*, pp. 16–26, Feb. 2002.

[3] C. K. Chan and C. C. Chan, *Modern Electric Vehicle Technology*. New York: Oxford Univ. Press, 2001.

[4] W. Kempton and A. Dhanju, *Windtech International*, vol. 2, no. 2, pp. 18–21, Mar. 2006.

[5] W. Kempton and J. Tomic, "Vehicle-to-grid power implementation: From stabilizing the grid to supporting large-scale renewable energy," *J. Power Sources*, vol. 144, no. 1, pp. 280–294, Jun. 2005.

[6] Smartgrid city [Online]. Available: http://smartgridcity.xcelenergy.com/

[7] Center for Carbon-Free Power Integration [Online]. Available: http://www.carbonfree.udel.edu/

[8] Y. Hisayuki, S. Motoharu, S. Mitsuru, F. Miho, S. Makoto, T. Masaki, N. Fiji, and T. Nobuo, "Cycle performance in each state-of-charge in $limn_2o_4$," *J. Electrochem. Soc.*, 2002.

[9] C. Guille and G. Gross, "A conceptual framework for the vehicle-to-grid (V2G) implementation," *Energy Policy*, vol. 37, no. 11, pp. 4379–4390, Jun. 2009.

[10] T. B. Gage, "Final report: Development and evaluation of a plug-in HEV with vehicle-to-grid power flow," AC Propulsion, Inc., Dec. 2003.

[11] A. Karygiannis, A. Kiayias, and Y. Tsiounis, "A solution for wireless privacy and payments based on e-cash," in *Proc. 1st Int. Conf. Security Privacy Emerging Areas Commun. Netw. (SecureComm)*, Sep. 2005, pp. 206–218.

[12] Car prototype generates electricity and cash, Dec. 2007 [Online]. Available: http://www.sciencedaily.com/releases/2007/12/071203133532.htm

[13] K. Ren and W. Lou, "A sophisticated privacy-enhanced yet accountable security framework for metropolitan wireless mesh networks," in *Proc. 28th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Jun. 2008, pp. 286–294.

[14] J. Sun, C. Zhang, Y. Zhang, and Y. Fang, "SAT: A security architecture achieving anonymity and traceability in wireless mesh networks," *IEEE Trans. Dependable Secure Comput.*, vol. 8, no. 2, pp. 295–307, Mar.–Apr. 2008.

[15] R. Cheng, Y. Zhang, E. Bertino, and S. Prabhakar, "Preserving user location privacy in mobile data management infrastructures," in *Proc. 6th Workshop Privacy Enhancing Technol.*, 2006, pp. 393–412.

[16] A. Beresford and F. Stajano, "Location privacy in pervasive computing," *Pervasive Comput.*, vol. 2, no. 1, pp. 46–55, Jan. 2003.

[17] S. Han, S. Han, and K. Sezaki, "Development of an optimal vehicle-togrid aggregator for frequency regulation," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 65–72, Jun. 2010.

[18] C. Quinn, D. Zimmerle, and T. H. Bradley, "The effect of communication architecture on the availability, reliability, and economics of plug-in hybrid electric vehicle-to-grid ancillary services," *J. Power Sources*, vol. 195, no. 5, pp. 1500–1509, 2009.

[19] K. Clement-Nyns, E. Haesen, and J. Driesen, "The impact of charging plug-in hybrid electric vehicles on a residential distribution grid," *IEEE Trans. Power Syst.*, vol. 25, no. 1, pp. 371–380, Feb. 2010.

[20] Smart grid cyber security strategy and requirements, NIST standard,, Feb. 2010.

[21] S. B. Peterson, J. Whitacre, and J. Apt, "The economics of using plug-in hybrid electric vehicle battery packs for grid storage," *J. Power Sources*, vol. 195, no. 8, pp. 2377–2384, 2010.

[22] "Blind signatures for untraceable payments," in *Proc. CRYPTO*, 1982, pp. 199–203.

[23] I. Ray and N. Narasimhamurthi, "An anonymous electronic voting protocol for voting over the Internet," in *Proc. 3rd Int. Workshop Adv. Issues E-Commerce Web-Based Inf. Syst. (WECWIS 2001)*, pp. 188–190.

[24] S. Brands, *Untraceable Off-Line Cash in Wallets With Observers*. New York: Springer-Verlag, 1993, pp. 302–318.

[25] M. Abe and E. Fujisaki, "How to date blind signatures," in *ASIACRYPT '96: Proc. Int. Conf. Theory Appl. Cryptol. Inf. Security*, London, U.K., 1996, pp. 244–251.

[26] G. Maitland and C. Boyd, "A provably secure restrictive partially blind signature scheme," in *Public Key Cryptography*, 2002, vol. 2274, Lecture Notes in Computer Science, pp. 351–354.

[27] X. Chen, F. Zhang, and S. Liu, "Id-based restrictive partially blind signatures and applications," *J. Syst. Softw*, vol. 80, no. 2, pp. 164–171, 2007.

[28] A. Shamir, "Identity-based cryptosystems and signature schemes," in *Proc. CRYPTO 84 Adv. Cryptol.*, New York, 1985, pp. 47–53.

[29] D. Boneh and M. K. Franklin, "Identity-based encryption from the weil pairing," in *CRYPTO '01: Proc. 21st Annu. Int. Cryptol. Conf. Adv. Cryptol.*, London, U.K., 2001, pp. 213–229.

[30] A. Senart, S. Kurth, and G. L. Roux, "Assessment framework of plug-in electric vehicles strategies," in *Proc. IEEE SmartGridComm 2010*, Oct. 2010, pp. 155–160.

[8] The BV could request those $permit$s any time before using them. One simple way is to request enough $permit$s to be used in the next day when it parks at home.

[31] S. Jang, S. Han, S. H. Han, and K. Sezaki, "Optimal decision on contract size for V2G aggregator regarding frequency regulation," in *Proc. 12th Int. Conf. Optim. Electr. Electron. Equip. (OPTIM)*, May 2010, pp. 54–62.

[32] G. Venayagamoorthy, P. Mitra, K. Corzine, and C. Huston, "Real-time modeling of distributed plug-in vehicles for v2g transactions," in *Proc. Energy Convers. Congr. Expo. (ECCE)*, Sep. 2009, pp. 3937–3941.

[33] O. Sundström and C. Binding, Planning electric-drive vehicle charging under constrained grid conditions, Aug. 2010 [Online]. Available: http://domino.research.ibm.com/library/cyberdig.nsf/papers/DF933AB3E9D615BC85257789002A4483/$File/rz3785.pdf

[34] S. Yu, K. Ren, and W. Lou, "FDAC: Toward fine-grained distributed data access control in wireless sensor networks," *IEEE Trans. Parallel Distrib. Syst.*, vol. 22, no. 4, pp. 673–686, Apr. 2011.

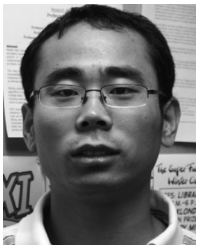
[35] S. Yu, K. Ren, and W. Lou, "Attribute-based on-demand multicast group setup with membership anonymity," *Comput. Netw.*, vol. 54, no. 3, pp. 377–386, 2010.

[36] P. S. L. M. Barreto, B. Lynn, and M. Scott, "Efficient implementation of pairing-based cryptosystems," *J. Cryptol.*, vol. 17, no. 4, pp. 321–334, 2004.

[37] H. W. Lim, "On the application of identity-based cryptography in grid security," Ph.D. dissertation, Univ. London, London, U.K., 2006.

[38] A.-H. Mohsenian-Rad and A. Leon-Garcia, "Coordination of cloud computing and smart power grids," in *Proc. IEEE SmartGridComm*, Oct. 2010, pp. 368–372.

[39] S. Yu, C. Wang, K. Ren, and W. Lou, "Achieving secure, scalable and fine-grained data access control in cloud computing," in *Proc. Infocom*, Mar. 2010, pp. 1–9.



Zhenyu Yang (S'08) received the B.E and M.E degrees in computer science both from Xi'an Jiaotong University, China, in 2004 and 2007, respectively. He is currently working toward the Ph.D. degree in the Electrical and Computer Engineering Department at Worcester Polytechnic Institute, Worcester, MA.

His current research interests are in the area of wireless networks and network security, with emphases on network coding and the smart grid.

Shucheng Yu (S'07-M'10) received the B.S. degree in computer science from Nanjing University of Post & Telecommunication, China, the M.S. degree in computer science from Tsinghua University, China, and the Ph.D degree in electrical and computer engineering from Worcester Polytechnic Institute, Worcester, MA.

He joined the Computer Science Department, University of Arkansas, Little Rock, as an Assistant Professor in 2010. His current research interests include data service security in cloud computing, attribute-based cryptography, and security and privacy protection in cyberphysical systems.

Wenjing Lou (S'01-M'03-SM'08) received the B.E. and M.E. degrees in computer science and engineering from Xi'an Jiaotong University, China, the M.A.Sc. degree in computer communications from the Nanyang Technological University, Singapore, and the Ph.D. degree in electrical and computer engineering from the University of Florida, Gainesville.

She joined the Electrical and Computer Engineering Department at Worcester Polytechnic Institute, Worcester, MA, as an Assistant Professor in 2003, where she is now an Associate Professor. Her current research interests are in the areas of ad hoc, sensor, and mesh networks, with emphases on network security and routing issues. She was a recipient of the U.S. National Science Foundation Faculty Early Career Development (CAREER) award in 2008.

Cong Liu (S'08-M'10) received the B.S. and M.S. degrees in electrical engineering from Xi'an Jiaotong University, China, in 2003 and 2006, respectively, and the Ph.D. degree from Illinois Institute of Technology, Chicago, in 2010.

Currently, he is working at Decision and Information Sciences Division of Argonne National Laboratory, Argonne, IL. His research interests include power systems and natural gas systems optimization and operation as well as smart grid.