Hindawi
Mobile Information Systems
Volume 2017, Article ID 1325698, 9 pages
https://doi.org/10.1155/2017/1325698

Research Article

Privacy-Preserving Billing Scheme against Free-Riders for Wireless Charging Electric Vehicles

Xingwen Zhao,[1,2] Jiaping Lin,[1,2] and Hui Li[1,2]

[1]*State Key Laboratory of Integrated Service Networks, Xidian University, Xi'an 710071, China*
[2]*School of Cyber Engineering, Xidian University, Xi'an 710071, China*

Correspondence should be addressed to Xingwen Zhao; sevenzhao@hotmail.com

Received 25 October 2016; Revised 24 March 2017; Accepted 30 March 2017; Published 10 April 2017

Academic Editor: Jing Zhao

Recently, scientists in South Korea developed on-line electric vehicle (OLEV), which is a kind of electric vehicle that can be charged wirelessly while it is moving on the road. The battery in the vehicle can absorb electric energy from the power transmitters buried under the road without any contact with them. Several billing schemes have been presented to offer privacy-preserving billing for OLEV owners. However, they did not consider the existence of free-riders. When some vehicles are being charged after showing the tokens, vehicles that are running ahead or behind can switch on their systems and drive closely for a free charging. We describe a billing scheme against free-riders by using several cryptographic tools. Each vehicle should authenticate with a compensation-prepaid token before it can drive on the wireless-charging-enabled road. The service provider can obtain compensation if it can prove that certain vehicle is a free-rider. Our scheme is privacy-preserving so the charging will not disclose the locations and routine routes of each vehicle. In fact, our scheme is a fast authentication scheme that anonymously authenticates each user on accessing a sequence of services. Thus, it can be applied to sequential data delivering services in future 5G systems.

1. Introduction

As more and more people concern about air pollution and the exhaustion of fossil energy, the increasing use of combustion engines will receive more criticisms than before. In order to alleviate these problems, electric vehicles (EVs) were introduced as a good replacement for combustion engines. The engines in EVs can use electrical power much more efficiently than the combustion engines [1]. However, the battery price is high and its size is limited. Moreover, plug-in EVs have to stop periodically for a period of time to recharge the battery.

In order to handle the above problems of PEVs, wireless charging vehicle called the on-line electric vehicle (OLEV) was introduced and tested in South Korea [2]. The technology of charging the vehicle while it is moving along the road will greatly reduce the number of times that a driver needs to stop for recharging. Such a convenient method makes battery-powered vehicle more favorable. By this way, the industry can decrease the size of the battery and then the price of EVs [3]. In the OLEV system, power transmitters (PTs) are installed underneath the road and electric vehicles can be charged wirelessly when users drive them along the road. With enough segments of PTs, it is not necessary to stop the vehicle to recharge. When the OLEV is put to use, it needs to be charged frequently when it is on the road. Therefore, there should be a suitable billing scheme to control the authenticating and charging interactions between the vehicles and the PTs under the road. And the scheme should protect the location privacy of the vehicle users. If not, an adversary can collect the user location information along the road during the authenticating and charging processes. Collections of charging locations can be used to deduce a driver's residential address, working office, and places of interest, which can be misused for crimes such as robberies or automobile thefts.

However, it is not desirable to provide unconditional location privacy to vehicles' owners because the vehicles need to be traceable in some situations, for example, when the vehicle is stolen or the vehicle is occupied by some criminals. In that case, the police would like to trace the vehicle. Moreover, there should be a trusted party who can trace a user if he/she has violated traffic regulations. In these conditions,

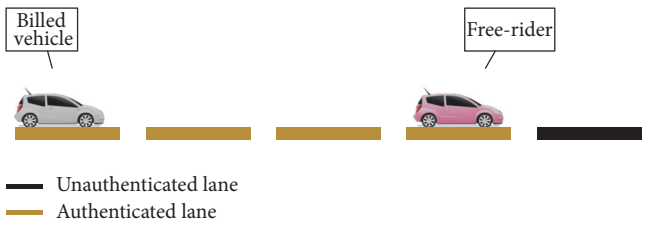

Figure 1: Free-rider in front of a billed vehicle on short lanes.

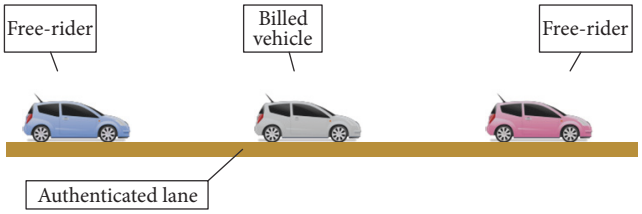

Figure 2: Free-riders near a billed vehicle on a long lane.

providing unconditional privacy is not suitable. Therefore, it is necessary to design a location privacy-preserving billing scheme for OLEV system in which the vehicles can only be traceable by a trusted party. The billing scheme should be efficient and can be carried out via vehicular ad hoc network (VANET) over 4G/5G when the vehicles are moving.

Currently, there exist several anonymous payment methods [6, 8, 9] that are suitable for wireless charging on the move. However, their scheme did not consider the cases of free-riders, and free-riders do exist since the charging is wireless and the charging segment is long enough for several closely moving vehicles (50 m in [10] and longer than one mile in [11]).

There will be several cases of free-riders. If the charging lane is short, each vehicle should authenticate itself with several charging lanes in front of it, in order to keep a moving speed. Then the vehicle driving ahead can slow down to get free charging from behind vehicle that is billed for wireless charging, as shown in Figure 1. If the charging lane is long, the vehicle driving ahead can slow down and the vehicle driving behind can speed up to get free charging, as shown in Figure 2. If the power supply is not constant for each charging lane, several vehicles can move together in a clustered group to get charging with only one vehicle paying for it. Or some vehicles can pay less money to get more supply by moving near other vehicles. These circumstances should have proper solutions before OLEV is put into wide application.

1.1. Our Contributions. In this paper, we present an efficient privacy-preserving billing scheme against free-riders for wireless charging electric vehicles by using several cryptographic tools including encryption scheme, signature scheme, and hash function. The proposed scheme achieves the following features:

(i) The scheme can fight against free-riders. Free-riders can be detected by checking their power levels and their authentication state. Proof of free-riding can be shown to the bank, so that the service provider can receive compensation from the free-riders. The compensation is much more than the fee of a full charging so the punishment can help to restrain free-riders.

(ii) The scheme is privacy-preserving because the billed user receives an anonymous token from bank. When the billed user charges his/her vehicle from any service provider, he/she shows only the anonymous token. His/her identity is not revealed so the location privacy of the user is enhanced.

(iii) The scheme can prevent double spending by employing online double spending checking. Banks only check the double spending of certificates but not the whole transactions, so that the efficiency of transactions is not affected. Banks can also cooperate to setup several distributed servers to alleviate the burdens.

(iv) The scheme is presented as a framework which can adopt the latest efficient public key encryption scheme, digital signature scheme, and hash function, so it can be implemented with the recent advances of modern technologies.

(v) The scheme is a fast authenticating framework which enables the vehicle to access one segment after another sequentially and securely. It uses hash chain receiving-and-acknowledging method to achieve fast authentication, which can be applied to sequential data delivering services in future 5G systems such as high-definition video streaming service.

1.2. Organization. The remainder of this paper is organized as follows. In Section 2 we describe the related works of billing schemes for wireless charging electric vehicles. In Section 3 we describe the system model and security requirements. In Section 4, we describe the proposed privacy-preserving billing scheme. The security of the proposed scheme is analyzed and features are compared in Section 5. Section 6 concludes the paper.

2. Related Works

Though we can obtain many benefits from OLEV, a privacy-preserving billing system is needed before OLEV is widely adopted. Recently, there are several contributions [6–9] that design privacy-preserving authentication and payment methods for OLEV.

Hussain et al. [6, 7] introduce a secure and privacy-aware fair billing framework for OLEV on the move through the charging plates installed under the road. They first propose two extreme lightweight mutual authentication mechanisms, namely, a direct mutual authentication method and a pure hash chain based authentication method. These methods can be used for different vehicular speeds on the road. Then they propose two power transfer and billing schemes separately based on the above two methods.

Zhao et al. [8] propose a secure and privacy-preserving billing scheme for OLEV. Users can buy electric energy

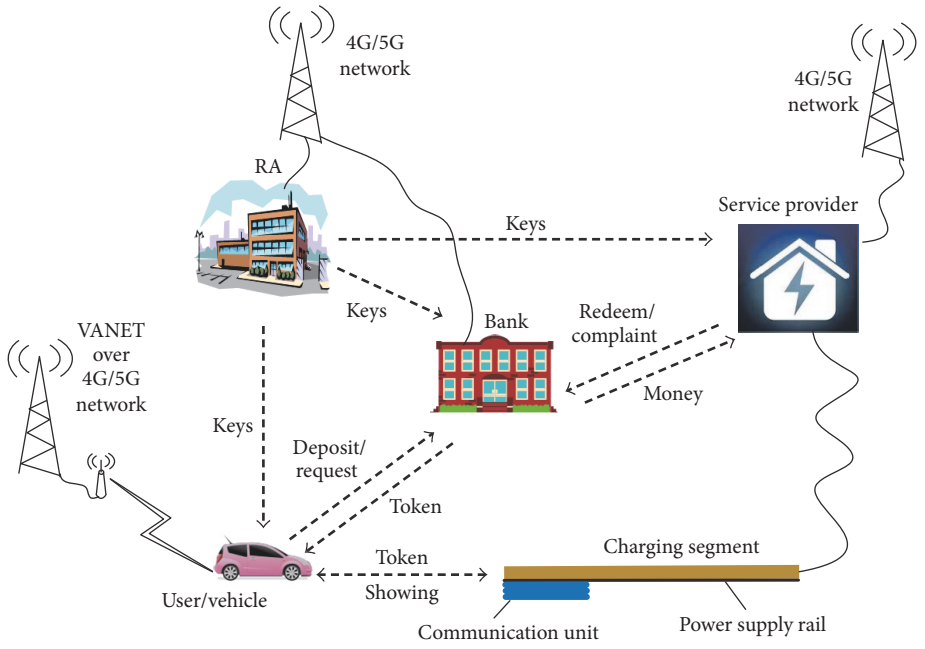

Figure 3: Network model used in the proposed scheme.

from power provider and charge their EVs anonymously and unlinkably. They assume that each PT transmits a fixed amount of energy to the EV and the energy supply company bills the EV the same amount of money for the electric energy from every PT. EVs can buy the energy according to the levels of their batteries.

Rezaeifar et al. [9] propose an efficient payment method based on "tokens" for wireless charging on the move, which minimizes the communications between service providers and users during the charging process. The proposed scheme prevents a user and the service provider from cheating each other, and it is robust to support different values for the price. However, their scheme cannot prevent double spending. A malicious user (e.g., a criminal) can obtain a token with small sum of deposit and distribute it to his/her colleagues. They can charge their vehicles from different service providers or the same service provider without a central certificates management server.

The above schemes cannot fight against free-riders, which may cause insufficient charging to billed user or electric energy lost to service providers.

3. System Model and Security Requirements

3.1. System Participants and Network Model. In summary, our proposed method consists of the following four main parties. First, there is a trusted registration authority (RA) that will generate system parameters for the system and public/private keys and signing/verifying keys for other parties. The second party is the bank, which is responsible for issuing authentication tokens to the users. There can be many banks and all the banks are also trustful that they will not disclose users' privacy and can help to track illegal users if needed. The third is the user who interacts with a bank to obtain his/her tokens and then connects to the power charging service provider to receive an electric charge for his/her EV by using the tokens. The fourth is the power charging service provider who owns the billing server and electrical power delivery service. The electrical power delivery service is to provide vehicles with an electric charge through a charging plate under the road.

The EVs can connect to the bank to receive tokens using vehicle ad hoc networks (VANETs) via a road side unit (RSU) over 4G/5G network when they move on the road, before reaching the charging lane. A certain length of power transmitter is installed under the road to form a charging segment. The charging segment also includes a hardware section for communication and computation purposes. There are many charging segments along the road so each vehicle can obtain enough charging. The communication channel between an EV and a charging segment is based on the 5.9 GHz Dedicated Short Range Communication (DSRC) standards. The charging segment is connected to both the electrical power delivery service and the billing server, and the service provider can communicate with the bank server. We assume that these communications can be done through a secure channel using 4G/5G network. Figure 3 shows the network model of our proposed method.

3.2. Security Requirements. As mentioned in [12], the general requirements for Internet payment systems include security, reliability, and scalability to support various users and service providers without losing efficiency, anonymity, and flexibility. However, we will only discuss some of them in brevity though we have achieved all of them. The focused requirements are listed as follows.

(1) Security against Double Spending. It is one of the main requirements for the payment system. Since the payment

system for wireless charging of EVs is on the networks which are open to the public, the payment method should be secured to avoid such attacks that may occur in an open environment where all interactions can be sniffed by others. And each user can also attempt to spend his/her token several times in order to get multiple charging by paying the money once. If a malicious user can double spend his/her token many times in different service providers, some service providers may not get back the money that they deserve to have.

(2) Fast Authentication. One of the most important features of wireless charging on the move is the fast operation, as vehicles are running with high speeds. Therefore, time-consuming payment methods such as Bitcoin and methods using iterative zero-knowledge proofs are not practical for wireless charging on the move. Therefore, to make our proposed payment system more efficient, it is important to minimize the verification time and the number of exchanged messages during the transactions.

(3) Location Privacy. Since an EV needs to charge frequently throughout the day, the location privacy of the EV can be abused to profile the owners of the EV. Therefore, providing anonymity and preserving location privacy against the service providers and the eavesdroppers are important requirements that we consider in our scheme. We assume that none of service providers and eavesdroppers use camera to record the physical identities of vehicles, since no one can provide anonymity in that case.

(4) Security against Free-Riders. The scheme should be secure against free-riders. As shown in previous section, the free-riders do exist if the OLEV systems are widely deployed. Billing scheme that is resistant against free-riders should be deployed together to avoid electricity loss and uncertain burden imbalance.

3.3. Assumption. The proposed scheme is based on the following assumptions.

Each bank is a trusted entity and only the bank can link the real identity of the user to the token number. Each bank has public and private keys to communicate with other entities, and all the entities can verify the bank's signature with its public key. Moreover, we assume that each bank has secure connections with all service providers.

Electric vehicle users should make an account for this purpose at certain bank. They can receive a defined number of prepaid tokens if they have enough money in the deposit. The bank can also allow users to book a number of tokens according to their credit scores (e.g., with their credit cards), so it does not matter whether there is money in the deposit. How much can be paid by credit cards and how the credit system is operated are out of scope of this paper.

Vehicles are equipped with sensors which can show the users how much charging they need. Each vehicle also uses an On-Board Unit (OBU) to communicate with the charging plate wirelessly. Electric vehicle has a switch for wireless charging. An honest user can switch off the charging circuit if he/she just wants to pass the route and take no charging. Then the OBU on the vehicle will authenticate itself with the charging plate setting the number of charging segments to zero.

The power charging service provider checks battery power level values of a vehicle periodically to decide whether it is actually in the state of charging. Since some user may report the values dishonestly in order to avoid being detected when his/her vehicle is getting a free-riding, we assume that each OBU is equipped with tamper-proof meter to carry out battery power level checking. The tamper-proof meter reports the value in a certified form [13]. Similar assumptions can be found in many smart metering schemes such as [14–16]. They assume that smart meters are fully trusted or the readings from meters are certified.

3.4. Thread Model. In our threat model, we assume that both the service provider and the EV (representing a user) can be malicious. We consider several kinds of attacks for malicious behavior, namely, free-rider, location privacy infringement, and double spending. Free-riding behaviors can be malicious in terms of bypassing the billing process such as refusing to give an authenticated hash value after receiving a charge, or driving in front of or following behind a charging vehicle closely to get a free charging. Besides, the service provider can abuse the users' privacy by tracking the EV and giving location information to a third party, such as advertising agencies, and so forth. Furthermore, the user can double spend his/her tokens or the adversaries can sniff the communication between charging plates and the EVs to collect information for double spending and user identification.

4. The Proposed Billing Schemes against Free-Riders

In this section, we describe the privacy-preserving billing schemes for wireless charging electric vehicles against free-riders.

4.1. Our Idea. In order to get rid of free-riders, we suggest that two methods be used together. One is prepaid anonymous token. Each vehicle should always obtain a token from bank by depositing money more than a maximum compensation fee of free-riders before using the route for OLEV. Or the token is paid by credit cards. The token can be a charging token which means the vehicle wants to choose the route to get to the destination at the same time charging for a number of segments. The token can be an entrance token which means the vehicle wants to take the route without charging for some reasons (e.g., the way is a shortcut or other ways are jammed). If one vehicle enters a route that is for OLEV, it should authenticate itself with one token. If this vehicle is detected for free-riders, the token is sent to bank together with proof of free-riding. The service provider will get money for compensation. Another required method is detecting the power level of each vehicle now and then. The detection is interaction taken between the charging plates (or the service provider) and tamper-proof meter inside OBU, so the vehicle cannot cheat on the power level of its battery. If the power

level of some vehicle is increased while the vehicle is not in an authenticated state of charging or has finished charging, this vehicle is blamed for free-riders.

4.2. Cryptographic Tools. We need several cryptographic tools to construct the proposed billing scheme, including a secure signature scheme supporting batch verification, a secure encryption scheme, and a secure hashing function. Some notations used in this paper are listed in Notations.

(i) Encryption Scheme. It can be any efficient secure public key encryption scheme which can be denoted as the tuple (ES-SETUP(1^λ), $\mathrm{ENC}_{\mathrm{PK}}(\cdot)$, $\mathrm{DEC}_{\mathrm{SK}}(\cdot)$). ES-SETUP($1^\lambda$) is used to generated parameters for the scheme given a secure parameter λ and then public/private key pair (PK, SK) for each participant. $\mathrm{ENC}_{\mathrm{PK}}(\cdot)$ means encrypt something with key PK. $\mathrm{DEC}_{\mathrm{SK}}(\cdot)$ means decrypt something with key SK. For instance, encryption schemes such as Elgamal [17] and elliptic curve cryptography [18] can be used.

(ii) Signature Scheme. It can be any efficient secure digital signature scheme, and it will be better if batch verification is supported. The scheme can be denoted as the tuple (DS-SETUP(1^λ), $\mathrm{SIG}_{\mathrm{CK}}(\cdot)$,$\mathrm{VER}_{\mathrm{VK}}(\cdot)$). DS-SETUP($1^\lambda$) is used to generate parameters for the scheme given a secure parameter λ and then signing/verifying key pair (CK, VK) for each participant. $\mathrm{SIG}_{\mathrm{CK}}(\cdot)$ means signing something with key CK. $\mathrm{VER}_{\mathrm{VK}}(\cdot)$ means verify some signature with key VK. Schemes with batch verification ability [19, 20] will be better because the service provider can verify multiple signatures in one round and detect bogus signatures quickly.

(iii) Hash Function. We require the hash function (denoted as $H(\cdot)$) to be an efficient collusion secure one-way hash function with input and output values in the same domain. In other words, the output value can be fed as input. We need this feature to generate hash chains like $h_1 = H(h_0)$, $h_2 = H(h_1)$, $h_3 = H(h_2)$, and so on, if given an initial value h_0.

4.3. The Schemes

4.3.1. Setup. In this phase, the trusted registration authority (RA) selects a large number λ according to the security requirement of the application and generates the system parameters *Params* by running ES-SETUP(1^λ) and DS-SETUP(1^λ). We assume that all entities are properly authenticated with RA and receive the required system parameters. RA generates their permanent private and public keys and transmits to each entity securely. A bank with identity B_i ($i = 1, 2, \ldots$) will receive a pair of public/private keys ($\mathrm{PK}_{B_i}, \mathrm{SK}_{B_i}$) and a pair of signing/verifying key ($\mathrm{CK}_{B_i}, \mathrm{VK}_{B_i}$). A service provider with identity S_i ($i = 1, 2, \ldots$) will receive a pair of public/private keys ($\mathrm{PK}_{S_i}, \mathrm{SK}_{S_i}$) and a pair of signing/verifying key ($\mathrm{CK}_{S_i}, \mathrm{VK}_{S_i}$). A user with identity U_i ($i = 1, 2, \ldots$) will receive a smart card embedded with a pair of public/private keys ($\mathrm{PK}_{U_i}, \mathrm{SK}_{U_i}$) and a pair of signing/verifying key ($\mathrm{CK}_{U_i}, \mathrm{VK}_{U_i}$). Moreover, electric vehicles are equipped with a tamper-proof meter (part of the OBU) to carry out battery power level checking. And each user should insert his/her smart card into the OBU before operating. We assume that all parties are consistent with the standard time so they do not have any dispute on timestamps.

4.3.2. Token Obtaining. When a user U_i wants to charge his/her vehicle along the way to a destination, he/she can use the On-Board Unit (OBU) to obtain a token by connecting to his/her bank B_j via RSU or VANET over a cellular network. The token is prepaid with two parts of money by deposit or by credit cards. One is for free-riders compensation; the other is the cost for the wireless charging from a number of charging plate segments. The token is retrieved in three steps as follows.

(1) U_i obtains a random pair of temporary signing/verifying keys ($\mathrm{TCK}_{U_i}, \mathrm{TVK}_{U_i}$) and a hash chain h_0, $h_1 = H(h_0), \ldots, h_n = H(h_{n-1})$. The key pair should be qualified for the selected signature scheme, and h_0 should be selected randomly. The key pair and the hash chain can be generated in leisured time. U_i sends a request message to the bank. The message contains the temporary verifying key TVK_{U_i}, user's identity U_i, an expected expiration time T, the end value of hash chain h_n, and the number n for the requested token. n is the expected number of the charging plate segments that the vehicle needs. If the user wants to drive along the way to a destination without charging for some reason (e.g., the way is a shortcut or other ways are jammed), he/she should set $n = 0$. T should be bounded according to the application, for instance 4 hours later from now. The request message is signed with user's signing key CK_{U_i} and then encrypted with bank's public key PK_{B_j}. The request message may be sent through a protected channel such as a transport layer security protocol (TLS) link. Let $M_1 = (\mathrm{TVK}_{U_i}, U_i, T, h_n, n)$. The request message is denoted as

$$U_i \longrightarrow B_j : C_1 = \mathrm{ENC}_{\mathrm{PK}_{B_j}}\left(M_1, \mathrm{SIG}_{\mathrm{CK}_{U_i}}(M_1)\right). \quad (1)$$

(2) When receiving the request, the bank B_j decrypts the message with its secret key SK_{B_j}. The process can be denoted as $(M_1, \mathrm{SIG}_{\mathrm{CK}_{U_i}}(M_1)) = \mathrm{DEC}_{\mathrm{SK}_{B_j}}(C_1)$ and M_1 is parsed as $(\mathrm{TVK}_{U_i}, U_i, T, h_n, n)$. It verifies the signature of user and the expected expiration time T. It also checks whether the user has enough money in the deposit or enough credit score for the tokens. If all are qualified, the bank generates the token for user and the corresponding amount of money is frozen. The token is the bank's signature to $(\mathrm{TVK}_{U_i}, T, h_n, n)$. The user should refresh to obtain a new token if the token is not spent before the expiration time. Let $M_2 = (\mathrm{TVK}_{U_i}, T, h_n, n)$. The returned message is denoted as

$$B_j \longrightarrow U_i : C_2 = \mathrm{ENC}_{\mathrm{PK}_{U_i}}\left(\mathrm{SIG}_{\mathrm{CK}_{B_j}}(M_2)\right). \quad (2)$$

(3) After receiving the returned message, U_i decrypts with the secret key SK_{U_i} and does the verification with the verifying key VK_{B_j}. If the signature is correct, $\mathrm{SIG}_{\mathrm{CK}_{B_j}}(\mathrm{TVK}_{U_i}, T, h_0, n)$ is stored as the token. As we notice, the token is the bank's signature on the temporary verifying key TVK_{U_i}, which is a randomly generated value and does not cause any privacy leakage of the user. At the same time, the bank knows the connection between U_i and TVK_{U_i}, so it can take method to punish the user if there is any malicious behavior.

4.3.3. Token Using. Before any vehicle enters the wireless charging road, it should be authenticated with a token. There are two cases for the authentication: normal charging and passing by without charging. No matter which case, when an EV reaches the entrance of the charging road, the EV should connect and show its token to the service provider. After that, the EV should periodically answer the service provider's query on battery power level. We explain these separate interactions in detail as follows.

(1) Entering. Each vehicle should finish this interaction at the entrance of charging road, or it will be rejected. The user U_i sends a message $(\mathrm{TVK}_{U_i}, T, h_n, n, \mathrm{SIG}_{\mathrm{CK}_{B_j}}(\mathrm{TVK}_{U_i}, T, h_n, n))$ to the service provider S_k together with the number of segments m ($m \leq n$) that it needs for charging. The user sets $m = 0$ indicating that this vehicle is taking the road without charging. Then, the service provider S_k checks the validity of the signature and the expiration time T and then forwards the message to bank B_j. If the signature is valid, T is not expired and bank B_j shows the token is spent for the first time; the service provider replies with a message (co, S_k, T_e, $\mathrm{SIG}_{\mathrm{CK}_{S_k}}(\mathrm{co}, S_k, T_e, h_n)$) that contains the cost of each segment of the charging plate co, its identity S_k, and a timestamp T_e. The timestamp is served as entering time of this vehicle and also used to prevent reply attacks. co can be varied according to m so as to attract customers by using price strategy. The user computes $\mathrm{SIG}_{\mathrm{TCK}_{U_i}}(m, \mathrm{co}, S_k, T_e)$ as message and sends it to the service provider. With this message, the service provider checks the validity of this message with TVK_{U_i}. If the signature is valid, the service provider now assures the authentication of this vehicle and lets it enter the charging road. This interaction can be denoted as

$$\begin{aligned} &U_i \longrightarrow S_k : \mathrm{TVK}_{U_i}, T, h_n, n, \mathrm{SIG}_{\mathrm{CK}_{B_j}}\left(\mathrm{TVK}_{U_i}, T, h_n, n\right), m; \\ &S_k \longrightarrow U_i : \mathrm{co}, S_k, T_e, \mathrm{SIG}_{\mathrm{CK}_{S_k}}\left(\mathrm{co}, S_k, T_e, h_n\right); \\ &U_i \longrightarrow S_k : \mathrm{SIG}_{\mathrm{TCK}_{U_i}}\left(m, \mathrm{co}, S_k, T_e\right). \end{aligned} \tag{3}$$

(2) Charging. This interaction should be taken between the service provider and the vehicles that need wireless charging. If the token is valid and $m > 0$, the service provider switches on the first charging segment to this vehicle. After receiving a charge from each segment, the vehicle should report the value of the hash chain to the service provider sequentially. The message after the first charge should be $(T_{m-1}, h_{m-1}, \mathrm{TVK}_{U_i})$, where T_{m-1} is current time and the sequential hashing of h_{m-1} should lead to h_n. It means the service provider can verify the following equations $h_m = H(h_{m-1})$, $h_{m+1} = H(h_m), \ldots, h_n = H(h_{n-1})$. If the hash chain is valid, the service provider switches on the next charging segment to this vehicle and sends a confirming message to the vehicle $\mathrm{SIG}_{\mathrm{CK}_{S_k}}(T_{m-1}, h_{m-1}, \mathrm{TVK}_{U_i})$. Then the vehicle sends the second message $(T_{m-2}, h_{m-2}, \mathrm{TVK}_{U_i})$, where the service provider can validate it as $h_{m-1} = H(h_{m-2})$ and switches on the third charging segment. The service provider also returns a signature $\mathrm{SIG}_{\mathrm{CK}_{S_k}}(T_{m-2}, h_{m-2}, \mathrm{TVK}_{U_i})$ on the message containing the new time T_{m-2}. We should remark that the user should reject releasing the next value of the hash chain if the vehicle did not receive a charge from current segment or did not receive the confirming message, where the messages can be used to prove its innocence. Since $H(\cdot)$ is a secure one-way hash function, the service provider cannot figure out the input value from the given sequence of output values. Thus, in order to redeem the money from the bank, the service provider should treat the vehicle fairly to obtain a full hash value chain. This interaction will continue until the user sends $(T_0, h_0, \mathrm{TVK}_{U_i})$ to the service provider and receives a charging and a confirming message from the mth segment. This interaction can be denoted as

$$\begin{aligned} &U_i \text{ gets the first charging} \\ &U_i \longrightarrow S_k : T_{m-1}, h_{m-1}, \mathrm{TVK}_{U_i}; \\ &S_k \longrightarrow U_i : \mathrm{SIG}_{\mathrm{CK}_{S_k}}\left(T_{m-1}, h_{m-1}, \mathrm{TVK}_{U_i}\right); \\ &U_i \text{ gets the second charging} \\ &U_i \longrightarrow S_k : T_{m-2}, h_{m-2}, \mathrm{TVK}_{U_i}; \\ &S_k \longrightarrow U_i : \mathrm{SIG}_{\mathrm{CK}_{S_k}}\left(T_{m-2}, h_{m-2}, \mathrm{TVK}_{U_i}\right); \\ &\vdots \\ &U_i \text{ gets the } m\text{th charging} \\ &U_i \longrightarrow S_k : T_0, h_0, \mathrm{TVK}_{U_i}; \\ &S_k \longrightarrow U_i : \mathrm{SIG}_{\mathrm{CK}_{S_k}}\left(T_0, h_0, \mathrm{TVK}_{U_i}\right). \end{aligned} \tag{4}$$

We notice that it is possible that the user refuses to offer a sequent hash value after receiving the ith ($0 \leq i \leq m-1$) charging from the service provider. In this case, the service provider will treat it as a free-rider. The service provider saves the interactions and the periodical power reporting and reports them to the bank to obtain the compensation. The processing is described in the following *Power Reporting* and *Redeeming* phases.

(3) Power Reporting. This interaction should be taken between the service provider and the vehicles entering the charging road. The service provider periodically (e.g., once per segment or every 20 seconds) queries these vehicles with a message as $(\mathrm{TVK}_{U_i}, T_q)$. Each vehicle should answer its battery power level Pow_q to the query with a form as $(\mathrm{Pow}_q, \mathrm{SIG}_{\mathrm{TCK}_{U_i}}(\mathrm{Pow}_q, \mathrm{TVK}_{U_i}, T_q))$, where Pow_q is generated in a certified form [13] by the tamper-proof module embedded in vehicle's OBU. If Pow_q is detected increasing during the interactions while the vehicle is not in the authenticated state of charging, the service provider decides the vehicle is acting as a free-rider. It can alert this vehicle and save the report as the proof for later use. This interaction can be denoted as

$$\begin{aligned} &S_k \longrightarrow U_i : \mathrm{TVK}_{U_i}, T_q; \\ &U_i \longrightarrow S_k : \mathrm{Pow}_q, \mathrm{SIG}_{\mathrm{TCK}_{U_i}}\left(\mathrm{Pow}_q, \mathrm{TVK}_{U_i}, T_q\right). \end{aligned} \tag{5}$$

4.3.4. Redeeming. In normal circumstances, the service provider builds a message from those received in Entering and Charging interactions of the Token Using phase to the bank B_j to redeem the token. The message is of the form $(M_{E_1}, M_{E_2}, M_{\text{hash}}, M_{\text{sig}})$, where $M_{E_1} = (\text{TVK}_{U_i}, T, h_n, n, \text{SIG}_{\text{CK}_{B_j}}(\text{TVK}_{U_i}, T, h_n, n))$, $M_{E_2} = (m, \text{co}, S_k, T_e, \text{SIG}_{\text{TCK}_{U_i}}(m, \text{co}, S_k, T_e))$, $M_{\text{hash}} = (h_0, h_1, \ldots, h_n)$, and $M_{\text{sig}} = \text{SIG}_{\text{CK}_{S_k}}(M_{E_1}, M_{E_2}, M_{\text{hash}})$. The bank can verify whether all the above signatures are valid and whether it is a transaction between a normal user and the specified service provider. The service provider redeems the money for that charging and the rest will be returned the user's deposit. If the M_{hash} is incomplete (such as $M_{\text{hash}} = h_l, \ldots, h_m, \ldots, h_n$), the service provider can only redeem the money for $m - l$ segments. This interaction can be denoted as

$$\begin{aligned} M_{E_1} &= \text{TVK}_{U_i}, T, h_n, n, \text{SIG}_{\text{CK}_{B_j}}\left(\text{TVK}_{U_i}, T, h_n, n\right); \\ M_{E_2} &= m, \text{co}, S_k, T_e, \text{SIG}_{\text{TCK}_{U_i}}\left(m, \text{co}, S_k, T_e\right); \\ M_{\text{hash}} &= h_0, h_1, \ldots, h_n; \\ M_{\text{sig}} &= \text{SIG}_{\text{CK}_{S_k}}\left(M_{E_1}, M_{E_2}, M_{\text{hash}}\right); \\ S_k &\longrightarrow B_j : M_{E_1}, M_{E_2}, M_{\text{hash}}, M_{\text{sig}}. \end{aligned} \tag{6}$$

In a circumstance where at least one suspected free-rider exists, the service provider builds a message from those received in all interactions of the Token Using phase to the bank. The message is of the form $(M_{E_1}, M_{E_2}, M_{\text{hash}}, M_{\text{rep}}, M_{\text{sig}})$, where $M_{E_1} = (\text{TVK}_{U_i}, T, h_n, n, \text{SIG}_{\text{CK}_{B_j}}(\text{TVK}_{U_i}, T, h_n, n))$, $M_{E_2} = (m, \text{co}, S_k, T_e, \text{SIG}_{\text{TCK}_{U_i}}(m, \text{co}, S_k, T_e))$, M_{hash} is set to $(h_l, \ldots, h_n)$ where h_l $(l \leq n)$ is the last valid hash value received from the vehicle or a null value indicating that the vehicle claims no charging, $M_{\text{rep}} = (\ldots, \text{Pow}_q, \text{SIG}_{\text{TCK}_{U_i}}(\text{Pow}_q, \text{TVK}_{U_i}, T_q), \ldots)$, and $M_{\text{sig}} = \text{SIG}_{\text{CK}_{S_k}}(M_{E_1}, M_{E_2}, M_{\text{hash}}, M_{\text{rep}})$. They are listed as follows.

$$\begin{aligned} M_{E_1} &= \text{TVK}_{U_i}, T, h_n, n, \text{SIG}_{\text{CK}_{B_j}}\left(\text{TVK}_{U_i}, T, h_n, n\right); \\ M_{E_2} &= m, \text{co}, S_k, T_e, \text{SIG}_{\text{TCK}_{U_i}}\left(m, \text{co}, S_k, T_e\right); \\ M_{\text{hash}} &= h_l, \ldots, h_n; \\ M_{\text{rep}} &= \ldots, \text{Pow}_q, \text{SIG}_{\text{TCK}_{U_i}}\left(\text{Pow}_q, \text{TVK}_{U_i}, T_q\right), \ldots; \\ M_{\text{sig}} &= \text{SIG}_{\text{CK}_{S_k}}\left(M_{E_1}, M_{E_2}, M_{\text{hash}}, M_{\text{rep}}\right); \\ S_k &\longrightarrow B_j : M_{E_1}, M_{E_2}, M_{\text{hash}}, M_{\text{sig}}. \end{aligned} \tag{7}$$

The bank can verify whether all the above signatures are valid and whether there is a valid proof of some vehicle being free-rider. If so, the bank accepts the complaint and calls the suspected user to show the proof for its innocence. If the user cannot show the confirming messages holding a sequence of timestamps that cover the complained time period, the user will be blamed for being a free-rider and compensation fee is given to the service provider. If the user can show the confirming messages, the bank decides the service provider is wrong and the user is innocent. How to punish the service provider is out of scope of this paper.

5. Security Analysis and Comparisons

We first discuss the security of our proposed scheme. Then, we compare our method with several schemes proposed for plug-in electric vehicles and wireless charging electric vehicles.

5.1. Security Analysis. According to the security requirements presented in Section 3, we will discuss the double spending avoidance, location privacy infringement, and free-riders resistance. For each of them, we discuss how our method can achieve them.

(1) Security against Double Spending. Double spending may occur when an adversary replays a sniffed token or certain user shows the already-spent token again. We will discuss them in the following two cases, respectively, as follows.

Case 1. The adversary can access the messages exchanged between the owner of the tokens and the service provider. Since the adversary does not possess the secret signing key of that token, he/she cannot show its validly to any service provider.

Case 2. Each user as the owner of a token may spend the token several times through different service providers since he/she holds the token's private key. However, double spending of the same token will be detected when the token is forwarded to local certificate management server setup by the bank. Token matching is fast in local server since each token has a limited validation time period and the server does not need to store large amount of tokens.

(2) Location Privacy. A secure channel is established between EVs and the bank by using signature and encryption schemes, so the adversary cannot obtain any information about token received by the specific EV. The temporary verification key and the hash value in each token are generated randomly by its owner, so the adversary cannot link one to another and the privacy of each EV is enhanced. Even the service provider cannot track the vehicles by analyzing all messages in the interactions unless they use a camera in charging places to record the physical identities of vehicles.

(3) Security against Free-Riders. The battery power level of each vehicle is checked periodically when it is moving. If power level is increasing while the vehicle is not in the authenticated state of being charged, it will be treated as a free-rider. The battery power level is reported by a tamper-proof module embedded in vehicle's OBU, so the user cannot cheat on it. The service provider can complain to the bank to obtain the compensation. If the compensation is confirmed by the bank, the free-rider will have to pay certain amount of money that is more than the battery charging it received. The money was prepaid by the deposit or by credit cards, so the

Table 1: Comparison with previous works.

	Feature	Location privacy	Price flexibility	Detect double spending	Prevent double spending	Avoid fraudulence in charging	Track illegal user	Avoid free-rider
[4]	Plug-in EV	√	not specified	√	√	×	√	Not concern†
[5]	Plug-in EV	√	√	√	√	√	×#	Not concern†
[6, 7]	OLEV	√‡	√	√	√	√	√	×
[8]	OLEV	√	√	×	√	√	×	×
[9]	OLEV	√	√	√	×	√	√	×
Proposed scheme	OLEV	√	√	√	√	√	√	√

†: the schemes for plug-in EV do not care about free-rider.
#: the scheme can track a stolen vehicle with consent from its owner but cannot track illegal user.
‡: weak protection that CP can link all authentications of the same vehicle.

free-rider should pay the compensation or get his/her credit score decreased.

5.2. Comparisons. In this section, we compare different features of our method with the proposed methods of two billing schemes for plug-in electric vehicles [4, 5] and four schemes for wireless charging electric vehicles [6–9]. The comparison is shown in Table 1, which focuses on several capabilities including location privacy, flexibility of charging price, detecting double spending, preventing double spending, avoiding fraudulence in charging, tracking illegal user, and avoiding free-rider.

The scheme [4] is for plug-in electric vehicles. It uses hash function and online authentication to achieve its designing goal. But it cannot avoid fraudulence in charging since the charging station can refuse to charge the vehicle after receiving the pseudonymous public key and the signed request. The scheme [5] cannot track illegal users since each user will be totally anonymous without consent value from the user. In the scheme by Hussain et al. [6, 7], the department of mobile vehicle (DMV) selects a set of pseudonyms for each vehicle and the vehicle authenticates itself to the charging plate (CP) using the hash value X_{OBU} of this set. However, all authentications of the same vehicle use the same hash value X_{OBU}, so CP can link all the charging locations of this vehicle together though it does not know who owns this vehicle. Thus, their scheme achieves a weak privacy protection. In the scheme of [8], zero-knowledge proof is used in all phases so the user is unconditional privacy-preserving. Thus, their scheme cannot track illegal users. In their scheme, the authenticating values sent to CP will be used once and then discarded, so the action of double spending will cause authentication failure in CP but CP cannot know whether the voucher has been spent or not. As a result, their scheme cannot detect double spending though it is very easy to achieve. In the scheme of [9], the service provider authenticates each user in an offline form, so the user can double spend his/her token elsewhere with different service providers. All the above schemes cannot fight against free-riders, which is the main focus of this paper.

6. Conclusion

We present an efficient privacy-preserving billing scheme for wireless charging electric vehicles against free-riders by using compensation-prepaid tokens and detecting battery power levels periodically when the vehicles are moving on the road. We need a tamper-proof device inside OBU, so the vehicle will report the power level of its battery honestly. How to get rid of the tamper-proof device will be an interesting topic for future research in smart grid and vehicle to grid (V2G) network.

Notations

λ:	A security parameter that measures the input size of the computational problem in cryptography
U_i:	The identity of a user with index i
B_j:	The identity of a bank with index j
S_k:	The identity of a service provider with index k
PK:	A public key used in the encryption scheme, for example, PK_{U_i} is the public key of U_i
SK:	A private key used in the encryption scheme, for example, SK_{B_j} is the private key of B_j
CK:	A signing key used in the signature scheme
VK:	A verifying key used in the signature scheme
ES-SETUP(1^λ):	The algorithm to setup the system parameters for the encryption scheme
$\mathrm{ENC}_{\mathrm{PK}}(m)$:	The algorithm that encrypts a message m with a public key PK to generate a ciphertext
$\mathrm{DEC}_{\mathrm{SK}}(c)$:	The algorithm that decrypts a ciphertext c with a private key SK to recover a message
DS-SETUP(1^λ):	The algorithm to setup the system parameters for the signature scheme

$\mathrm{SIG}_{\mathrm{CK}}(m)$:	The algorithm that signs a message m with a signing key CK to generate a digital signature
$\mathrm{VER}_{\mathrm{VK}}(\sigma)$:	The algorithm that verifies a signature σ with a verifying key VK
$H(m)$:	The algorithm that maps data m of arbitrary size to a hash value of fixed size
TCK:	A temporary signing key used in the signature scheme
TVK:	A temporary verifying key used in the signature scheme
$B_j \rightarrow U_i : m$:	An entity B_j sends another entity U_i a message m
h_i:	A hash value with index i
T, T_c, T_e, T_q:	Some timestamps used in different phases
OBU:	On-Board Unit equipped in a vehicle
VANET:	Vehicular ad hoc network
RSU:	Road Side Units deployed along the roadside to help to construct VANET.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work is supported by the Research Fund for the Doctoral Program of Higher Education of China (no. 20130203120003), the National Natural Science Foundation of China (no. U1401251), Major Basic Research Program of Shaanxi Province Natural Science Foundation Research Project (no. 2016ZDJC-04), and the China 111 Project (no. B16037).

References

[1] E. Valsera-Naranjo, A. Sumper, P. Lloret-Gallego, R. Villafáfila-Robles, and A. Sudria-Andreu, "Electrical vehicles: state of art and issues for their connection to the network," in *Proceedings of the 10th International Conference on Electrical Power Quality and Utilisation (EPQU '09)*, pp. 1–3, Łódź, Poland, September 2009.

[2] P. Dutta, "Coordinating rendezvous points for inductive power transfer between electric vehicles to increase effective driving distance," in *Proceedings of the 2nd IEEE International Conference on Connected Vehicles and Expo (ICCVE '13)*, pp. 649–653, December 2013.

[3] N. P. Suh, D. H. Cho, and C. T. Rim, *Design of On-Line Electric Vehicle (OLEV)*, Springer, Berlin, Germany, 2011.

[4] H. Nicanfar, S. Hosseininezhad, P. Talebifard, and V. C. M. Leung, "Robust privacy-preserving authentication scheme for communication between electric vehicle as power energy storage and power stations," in *Proceedings of the 32nd IEEE Conference on Computer Communications (IEEE INFOCOM '13)*, pp. 3429–3434, Turin, Italy, April 2013.

[5] M. H. Au, J. K. Liu, J. Fang, Z. L. Jiang, W. Susilo, and J. Zhou, "A new payment system for enhancing location privacy of electric vehicles," *IEEE Transactions on Vehicular Technology*, vol. 63, no. 1, pp. 3–18, 2014.

[6] R. Hussain, D. Kim, M. Nogueira, J. Son, A. O. Tokuta, and H. Oh, "PBF: a new privacy-aware billing framework for online electric vehicles with bidirectional auditability," https://arxiv.org/abs/1504.05276.

[7] R. Hussain, D. Kim, M. Nogueira, J. Son, A. Tokuta, and H. Oh, "A new privacy-aware mutual authentication mechanism for charging-on-the-move in online electric vehicles," in *Proceedings of the 11th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN '15)*, pp. 108–115, Shenzhen, China, December 2015.

[8] T. Zhao, L. Wei, and C. Zhang, "A secure and privacy-preserving billing scheme for online electric vehicles," in *Proceedings of the IEEE 83rd Vehicular Technology Conference (VTC '16)*, pp. 1–5, IEEE, Nanjing, China, May 2016.

[9] Z. Rezaeifar, R. Hussain, S. Kim, and H. Oh, "A new privacy aware payment scheme for wireless charging of electric vehicles," *Wireless Personal Communications*, pp. 1–18, 2016.

[10] Y. D. Ko, Y. J. Jang, and S. Jeong, "Mathematical modeling and optimization of the automated wireless charging electric transportation system," in *Proceedings of the IEEE International Conference on Automation Science and Engineering: Green Automation Toward a Sustainable Society (CASE '12)*, pp. 250–255, Seoul, Korea, August 2012.

[11] Z. Chen, F. He, and Y. Yin, "Optimal deployment of charging lanes for electric vehicles in transportation networks," *Transportation Research Part B: Methodological*, vol. 91, pp. 344–365, 2016.

[12] B. Neuman and G. Medvinsky, "Requirements for network payment: the NetCheque perspective," in *Proceedings of the Digest of Papers. Technologies for the Information Superhighway (COMPCON '95)*, pp. 32–36, San Francisco, Calif, USA, 1995.

[13] A. Rial and G. Danezis, "Privacy-preserving smart metering," in *Proceedings of the 10th Annual ACM Workshop on Privacy in the Electronic Society (WPES '11)*, Y. Chen and J. Vaidya, Eds., pp. 49–60, Chicago, Ill, USA, October 2011.

[14] C. Rottondi, G. Verticale, and C. Krauss, "Distributed privacy-preserving aggregation of metering data in smart grids," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1342–1354, 2013.

[15] F. Diao, F. Zhang, and X. Cheng, "A privacy-preserving smart metering scheme using linkable anonymous credential," *IEEE Transactions on Smart Grid*, vol. 6, no. 1, pp. 461–467, 2015.

[16] H. J. Jo, I. S. Kim, and D. H. Lee, "Efficient and privacy-preserving metering protocols for smart grid systems," *IEEE Transactions on Smart Grid*, vol. 7, no. 3, pp. 1732–1742, 2016.

[17] T. E. Gamal, "A public key cryptosystem and a signature scheme based on discrete logarithms," in *Advances in Cryptology, Proceedings of CRYPTO '84, Santa Barbara, California, USA, August 19-22, 1984, Proceedings*, pp. 10–18, 1984.

[18] H. Cohen, G. Frey, R. Avanzi et al., Eds., *Handbook of Elliptic and Hyperelliptic Curve Cryptography*, Chapman and Hall/CRC, 2005.

[19] Y. Jiang, M. Shi, X. Shen, and C. Lin, "BAT: a robust signature scheme for vehicular networks using binary authentication tree," *IEEE Transactions on Wireless Communications*, vol. 8, no. 4, pp. 1974–1983, 2009.

[20] M. Bayat, M. Barmshoory, M. Rahimi, and M. R. Aref, "A secure authentication scheme for VANETs with batch verification," *Wireless Networks*, vol. 21, no. 5, pp. 1733–1743, 2015.