Wireless Pers Commun (2017) 92:1011–1028
DOI 10.1007/s11277-016-3589-x

A New Privacy Aware Payment Scheme for Wireless Charging of Electric Vehicles

Zeinab Rezaeifar[1] · Rasheed Hussain[2] · Sangjin Kim[3] · Heekuck Oh[1]

Published online: 11 August 2016

Abstract Electric vehicles (EVs) can be considered as a revolution in the combustion industry with significant improvement in fuel utilization and decrease in pollution compared to combustion engines. However, by decreasing the size of the battery to reduce the cost, the frequency of charging EVs in a day increases. Therefore, to reduce the downtime required for charging EVs, wireless charging on the move can be an effective solution. In such a situation, paying for wireless charging on the move is an important issue. However, it can endanger the location privacy of users, since the EVs need to charge frequently in a day. In this paper, we first explain different methods of payment and problems with such payment methods in the case of wireless charging on the move. Then, we 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 users and service providers from cheating, and it is robust to support different values for the price. Finally, we compare it with other payment methods that have been proposed for plug-in electric vehicles.

Keywords Electric vehicles (EVs) · Wireless charging · Payment · Location privacy

✉ Heekuck Oh
hkoh@hanyang.ac.kr

Zeinab Rezaeifar
rezaeifar@hanyang.ac.kr

Rasheed Hussain
r.hussain@innopolis.ru

Sangjin Kim
sangjin@koreatech.ac.kr

[1] Department of Computer Science and Engineering, Hanyang University, ERICA Campus, Sa 3-dong, Sangnok-gu, Ansan, Gyeonggi 426-791, South Korea

[2] Institute of Information Sciences, Innopolis University, Innopolis, Tatarstan, Russia

[3] Department of Computer Science and Engineering, Korea University of Technology and Education, Cheonan, South Korea

1 Introduction

The air pollution and limitation of fossil energy with the rapidly increasing use of combustion engines are more critical than before. Electric vehicles (EVs) are a good replacement for combustion engines to alleviate these problems. Moreover, electric vehicles are cost effective given the increasing price of gasoline every day [1]. However, the most significant reason for replacing electric vehicles with combustion engines is the efficiency of its engine in using electrical power. While the combustion engine can only utilize about 30 % of its fuel tank, where most of its energy is wasted in heating, the efficiency of the electrical engine is more than 80 % [2]. Therefore, the plug-in electric vehicle (PEV) has been introduced. However, the price and the size of the battery are the main reasons preventing the use of electrical power as the main source of energy for vehicles. Combustion engine vehicles can travel more than 310 miles without refueling, but a battery has an average driving distance of 75 miles per charge [3]. Also, this limitation of driving is accompanied by the lack of charging stations. Moreover, by increasing the size of the batteries to achieve the longest duration of power usage, the price of the batteries will raise significantly.

To counter the above problems of PEVs, wireless charging technology has been introduced [3]. By charging on the move, the number of times that a driver needs to stop for recharging will decrease, which makes it more comfortable for the users. In this case, the industry can decrease the size of the battery which reduces the price of EVs and makes them more commercial [4]. The On-Line Electric Vehicle (OLEV) project, which has been recently carried out by the Korea Advanced Institute of Science and Technology (KAIST), was selected as one of the best innovations of 2010 [5]. In this project, electric vehicles can be charged remotely from power transmitters that are installed under the road, so EVs can be charged when they move on the road, and the re-charging downtime is significantly reduced. Also, this project has achieved the power transfer efficiency of 80 % with an air gap of 10 cm between an underground coil and a power receiving unit in the vehicle [4]. However, as the battery capacity of the fully charged electric vehicle is much smaller than that of combustion engines, by decreasing the size of the battery, this capacity will further decrease. Thus, the electric vehicles need to be charged frequently throughout the day, which can have an adverse effect on the location privacy of the vehicle users. In other words, the adversary can collect the user location information during the payment process for wireless charging on the move. Location history of the electric vehicle can be accumulated over time and can be associated with places of interest of the users, which can be misused for crimes such as kidnapping or automobile thefts.

However, providing unconditional location privacy is not desirable in practice because we need to track the vehicles in some conditions. Consider the case when the vehicle is stolen; in such a condition, the owner would definitely want to trace the vehicle. Also, illegal vehicle users should be traceable by a trusted party. In these conditions, providing unconditional privacy is not suitable. Therefore, the goal of this paper is to find an anonymous payment method to provide location privacy which is applicable to wireless charging of electric vehicles on the move and which is only traceable by a trusted party.

There are many methods of anonymous electronic payment such as [6] and [7], in which the authors use complicated cryptographic methods that need many messages to be exchanged between users and service providers. On the other hand, the timing needed for these protocols will not be appropriate for charging electric vehicles on the move.

Moreover, some other payment methods such as [7] try to use a hash chain to improve the efficiency during the payment process, but these methods do not provide anonymity.

In this paper, we first discuss different payment methods and the problems with applying them to wireless charging on the move. Then, we propose an efficient suitable payment method based on 'tokens' for wireless charging on the move. 'Tokens' are the signature of the bank on the root of the hash chain, and the public key of the token and timestamp are generated by the bank. Moreover, our proposed payment method not only provides anonymity for users against the service provider but can also be traceable by the trusted party.

The rest of the paper is organized as follows. Related works are presented in Sect. 2, followed by the system model and problem statement in Sect. 3. In Sect. 4, we present our proposed method followed by analysis in Sect. 5. Finally, we provide our concluding remarks in Sect. 6.

2 Related Works

There are different payment methods and all of them have specific features. In general, we can classify them into three groups as below:

Paper cash The main feature of paper cash is that it can provide anonymity because it does not include any information about users. On the other hand, for charging on the move we cannot use paper cash to transfer money, so we should search for another payment method.

Credit card Although it is a widely adopted payment method that supports transactions of large amounts of money, it does not provide anonymity. Due to the frequent charging in a day for EV, location privacy can easily be abused by tracking the credit card payment.

E-payment There are many different kinds of existing electronic payments such as micropayment [8], Paypal [9] and prepaid cash cards [10]. All of these methods have different features, but in general, we can say that most of these methods can detect double spending but cannot prevent it. These methods are suitable for small amounts of money and do not provide lost protection. Moreover, we can classify electronic payments into two groups: online and offline methods. In online methods, for each transaction, the service provider or the merchant must interact with the bank or the server. When the merchants receive verification from the bank, they will let users start a transaction. Moreover, the bank is responsible for identifying double spenders. In offline methods, the merchant accepts a payment anonymously and later deposits the payment to the bank. This requires the merchant to verify the transactions. Therefore, with respect to communication overhead, offline methods are more efficient than online methods. There are different offline methods that can be divided into two groups, i.e., anonymous and nonanonymous methods. In the following, we first explain these two kinds of methods and then discuss various schemes that have been suggested for PEVs.

2.1 Offline Electronic Payment

Nonanonymous methods such as Payword [7] are based on credit cards and use hash chains verified with a trusted party (broker). For each vendor, they can receive different hash chains, and users employ each hash for every purchase from this vendor. The advantages of this method are that it decreases the number of public key operations, becoming more

efficient and minimizing communication with a broker, but it does not provide anonymity. The main feature of anonymous methods to provide privacy is untraceability of the honest users, but if the users perform double spending they should be detectable by the trusted party. Untraceable offline cash in a wallet with an observer is one of the anonymous methods [7]. In this method, authors use a blind signature to preserve privacy. The identity of the account holder must be encoded in the withdrawn information, and the authors use the wallet with observer to stop double spending. In this method, the number of coins in circulation can never exceed the number of executions of the withdrawal protocol. However, the drawback of this method is its poor efficiency compared to previous methods that use a hash, and we also cannot consider it as a robust method as it does not implement variable values.

Bitcoin, which was introduced first by Nakamoto [11], is peer-to-peer electronic cash. The bitcoin transaction is completely public, and it is a decentralized method that does not need any central bank or authority to prevent double spending. To prevent double spending, it depends on a public history of transactions based on the block hash chain and using the proof-of-work system. Although the anonymity in Bitcoin is a complicated issue, there is a possibility of the linkability between different transactions, since all transactions are public, and user privacy is provided only with pseudonyms [12]. To break the link between different Bitcoin transactions, a Zerocoin scheme applied the cryptographic extension to the structure of Bitcoin. The cryptography of Zerocoin relies on zero-knowledge proofs converted into non-interactive-proofs and accumulators. It uses zero-knowledge proofs to reveal that the committed value is in an accumulator [13]. However, both of these methods require considerable computational effort that is not suitable for wireless charging on the move.

2.2 Payment Methods for PEV

In [6], the authors propose a new payment system for enhancing the location privacy in electric vehicles. In this method, the authors suppose that vehicles are equipped with an in-car-unit that consists of small read-only memory, which is initialized during the registration process. During this registration process, the user should contact the supplier for opening an account and paying a deposit of at least D dollars. In the charging process, the in-car-unit runs an interactive protocol to communicate with the charging plate, and it also communicates with the supplier to check the balance of the user anonymously. After decreasing users' balance to be less than D dollars, users should approach the supplier to increase their balance to make it D again. Moreover, with user consent, the judge can trace all transactions conducted by this user. However, in [6], the authors used bilinear pairing and zero-knowledge proofs for verifying users' accounts to the service provider, in which the charging process takes 10 s. Therefore, it will not be appropriate for wireless charging when vehicles move on the road.

In [14], the authors consider a smart grid as a trusted entity. As EVs need to authenticate themselves with the charging plate, they use pseudonyms that only the smart grid can map to the identity of the real vehicle. Moreover, vehicles should change pseudonyms after each charging session when connecting to the smart grid. However, if the service provider receives a pseudonym and does not give a charge, users cannot do anything.

Therefore, because of these drawbacks and in order to provide an efficient method, we propose a new payment scheme to minimize the communication overhead and complexity. Moreover, to provide anonymity and preserve location privacy, we use different tokens which are not linkable in our proposed payment method. Also, robustness is achieved, as

our method is based on user accounts, and given that the token does not have any specific value, users can spend as much as they need.

3 System Model and Problem Statement

3.1 System Participants and Network Model

In summary, our proposed method consists of the following three main parties. First, a bank is responsible for account opening and storing users' public keys. Each user should open an account in the bank and deposit some amount of money in this account. Then, the users can receive tokens that are at most equal to their deposit value. Later on, they can use these tokens to recharge the battery of an electric vehicle on the move. However, unless they use these tokens, the money will not be withdrawn from their accounts. Second is the user who connects to the service provider to receive an electric charge for his/her EV. Third is the service provider who owns the billing server and electrical power delivery service. The electrical power delivery service is exercised by the power station to provide vehicles with an electric charge through a charging plate.

The EVs can connect to the bank to receive tokens using Vehicle Ad-hoc Networks (VANETs) via a Road Side Unit (RSU) or Long-Term Evolution (LTE) through the cellular network when they move on the road, before reaching the charging plate. The charging plate is installed under the road, and a certain length of the road is covered with the charging plate. The charging plate includes a hardware section for communication and computation purposes and also contains different charging segments that can be turned on or off for each of the vehicles. These segments have a specific amount of the charge for transferring to EVs. The communication channel between an EV and a charging plate is based on the Dedicated Short Range Communication (DSRC) standard. The charging plate is connected to both the billing server and the electrical power delivery service, and the service provider can communicate with the bank server. We assume that these communications can be done through a secure channel using the LTE through the cellular network. Figure 1 shows the network model of our proposed method.

3.2 System Requirements

As mentioned in [15], the general requirements for Internet payment systems include security, reliability, and scalability to support various users and merchants without losing performance, anonymity, acceptability, customer base (i.e., a significant number of customers use this payment system), flexibility, convertibility, efficiency, ease of integration with an application, and ease of use. However, in some applications such as wireless charging on the move, some requirements, such as efficiency and anonymity, are more important. To consider these requirements for specific communication, we have to neglect the requirements that are less significant. In the following, we explain the suitable requirements that we consider in our payment system for wireless charging on the move.

1. Security 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 attacks that may accur in an open environment such as eavesdropping and replying attacks.

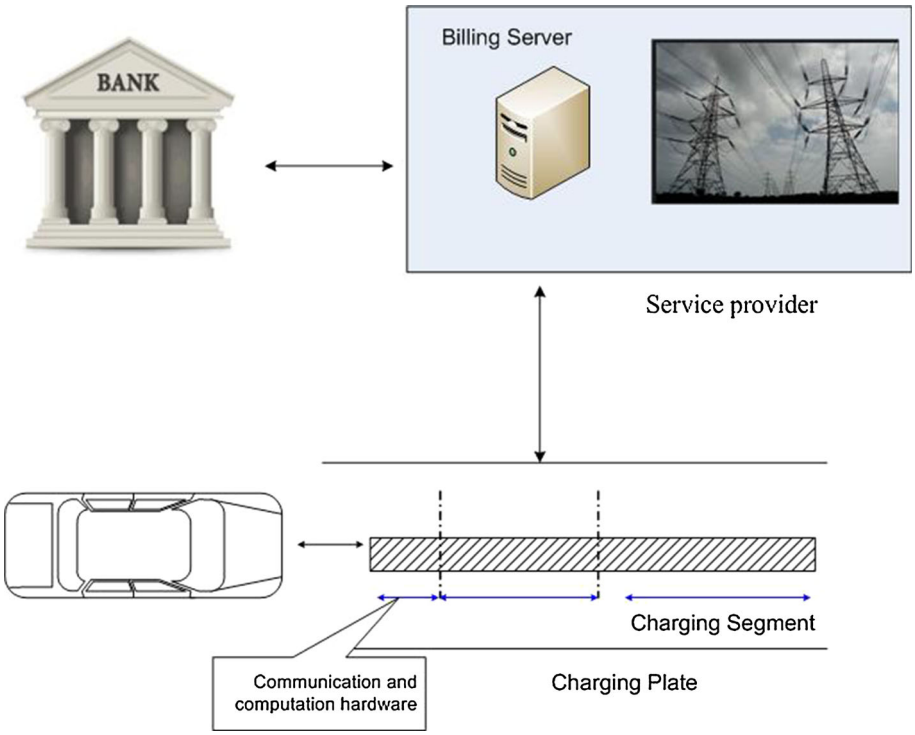

Fig. 1 Network model

2. One of the most important features of wireless charging on the move is the fast operation payment system, as vehicles move with high speed. Therefore, payment methods such as Bitcoin with iterative verification, which is time-consuming, cannot be applied in our scenario. Moreover, the methods which require iterative communications using zero-knowledge proofs are beyond what is considerably practical for wireless charging on the move. Therefore, to make our proposed payment system more efficient, minimizing verification time and the number of exchanged messages are important.
3. 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. Consequently, schemes such as [7], in which anonymity against untrusted parties is not considered and service providers can trace the users with different transactions, are not suitable for our scenario. Therefore, providing anonymity and preserving location privacy against the service provider are the most important requirements that we consider. The service provider cannot track the vehicles unless they use a camera in charging places to record the physical identities of vehicles, which in that case, we cannot provide anonymity.
4. Another parameter is robustness, which means that the method of payment should guarantee a variable price. The amount charged during each transaction may vary, so the methods that are not flexible in terms of different prices are not appropriate for wireless charging. Therefore, an electronic payment method should support a variable price that lets users spend as much money as they need.

5. Traceability is another requirement that we consider in our proposed method because authorities should be able to revoke illegal users from the system. The authorities should be able to trace anonymity whenever it is needed even without users' consent.

3.3 Assumption

The proposed scheme is based on the following assumptions.

The bank is a trusted entity that can only link the real identity of the user to the token number. The 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 the bank connects to the service provider through a secure channel.

Electric vehicle users should make an account for this purpose at the bank, and the payment can be postpaid. They can receive a defined number of tokens and if they do not pay it before the stipulated time, the bank will remove them from the system. Moreover, vehicles are equipped with sensors for defining how much charging they need, which also uses an On-Board Unit (OBU) to communicate with the charging plate wirelessly. Furthermore, they are equipped with tamper-proof devices to perform security operations as well as storage to store security parameters. Moreover, we assume every service provider has its own identity that is known to the entities.

3.4 Threat Model

In our threat model, we assume that both participating entities (EV and service provider) can be malicious. We consider three kinds of attacks for malicious behavior, namely statement fraudulence, location privacy infringement, and double spending. These behaviors can be malicious in term of bypassing the billing process or refusing to give a charge by the service provider after receiving a token. 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 adversaries can sniff the communication between charging plates and the EVs to collect information for double spending.

4 Proposed Method

In this section, we explain the proposed method of payment for the wireless charging of electric vehicles.

4.1 Baseline

In our proposed method, before using wireless charging services on the move, each user should open an account at the bank, where the bank will store verified users' public keys in its database. Before charging, a vehicle must have enough tokens, which can be withdrawn from the bank. Our method consists of four phases, namely the setup, token withdrawal, charging, and redeeming phases.

Setup phase In this phase, every entity receives the required system parameters and makes necessary keys. Moreover, the user connects the bank for opening an account and paying a deposit.

Token withdrawal phase As the vehicles are equipped with an OBU, they can connect to the bank server to receive a token on the move using VANET through an RSU or LTE through a cellular network.

Charging phase The charging phase can be divided into two parts, verifying the token by the service provider and starting the charging process. The token can be verified before the user reaches the charging plate by connecting to the service provider via an RSU. The charging phase starts when the vehicle reaches the charging plate.

Redeeming phase The service provider can redeem money from the bank with the token and the hash chain received from the users.

4.2 Preliminaries and Initializations

Table 1 shows the notations that we use throughout the rest of the paper. Below are the cryptographic primitives used in our proposed scheme:

1. Actual primitives used in this scheme: hash chain, ELGamal encryption, and BAT signature. We use a token approach for privacy preservation. The token is generated as follows: $sign_b(w_0||+K_j||T_b)$, where w_0 is the root of the hash chain, $+K_j$ is a public key of the token and T_b is timestamp defined by the bank for this token. These values

Table 1 Standard notation used in this paper

Notation	Description
S	Service provider identity
B	Bank identity
PIDj	Token identity
PIDi	Identity of vehicle *i*
$\mathbb{G}, \mathbb{G}_T$	Cyclic group of order q
P	The generator of $\mathbb{G}$ and $\mathbb{G}_T$
x	Private key
s	Secret master key
SK_i	Secret key
P_{Pub}	Public key corresponding to s
PK^+	Public key corresponding to x
α_i	A signature sent by vehicle i
$h(.)$	One way hash function such as MD5
$H(.)$	A MapToPoint hash function such as $H : \{0,1\}^* \rightarrow \mathbb{G}$
$(+K_b, -K_b)$	Public and private key pair of the bank
$E.K_x(M)$	Encryption of the message M with the public key K_x
$sign_i(m)$	Digital signature on message m with the private key of entity i
N_P	Number of segments for charging
$(+Kj, -Kj)$	One time public and private key pair of the *jth* token of the EV
$h_j(w_0)$	Hash chain for the *jth* token of the EV with root w_0
T_i	Timestamp generated by the entity i
$\lfloor f \rfloor$	Floor function: Round a real number (f) down to the next integer
$\lceil f \rceil$	Ceiling function: Round a real number (f) up to the next integer

are signed by the bank and given to the user. In addition, in order for EVs to communicate with the bank and receive tokens in a secret way, we use ElGamal encryption over elliptic curve cryptography (ECC). Let $\mathbb{G}$ be a cyclic group of prime order q, where $\mathbb{G}$ is generated by an element P. Let a random number $x \in Z_q^*$ be chosen as its private key and $PK^+ = xP$ be calculated as its public key.

2. BAT signature [16]: we use a Binary Authentication Tree (BAT), which follows identity-based cryptography, to improve the verification efficiency. The BAT scheme can improve the verification of multiple signatures within a limited interval. Since in wireless charging of EVs, the service provider should verify multiple signatures of differents vehicles within a limited interval, using BAT signature can improve the verification efficiency in our scheme. Let $\mathbb{G}$ and $\mathbb{G}_T$ be cyclic multiplicative groups, where $\mathbb{G}$ and $\mathbb{G}_T$ are generated by P with the same order q. let $\hat{e} : \mathbb{G} \times \mathbb{G}_T \rightarrow \mathbb{G}_T$ be a bilinear map. $H(.)$ is a MapToPoint hash function and $h(.)$ is a one way hash function such as MD5. Let $s \in Z_q^*$ be a secret master key and $P_{Pub} = sP$ its public key. The RSU or the service provider is preloaded with the public parameters $\{\mathbb{G}, \mathbb{G}_T, q, P, P_{Pub}\}$, and PID_i is the identity of vehicle i. To compute the signature, $r_i \in Z_q^*$ is selected randomly to calculate $E_i = r_i P$. With the secret key $SK_i = sH(PID_i)$, the signature $\alpha_i = E_i, F_i$ for the message M_i is calculated as follows:

$$\begin{cases} E_i = r_i P \\ F_i = r_i P_{Pub} + h(M_i, E_i) SK_i \end{cases} \tag{1}$$

Anyone that receives the message M_i, α_i can verify the signature $\alpha_i = E_i, F_i$ if Eq. (2) holds; the proof is given in the "Appendix".

$$\hat{e}(F_i, P) = \hat{e}(E_i + h(M_i, E_i) H(PID_i), P_{Pub}) \tag{2}$$

Moreover, all the signatures $\{\alpha_{k_1}, \alpha_{k_1+1}, \ldots, \alpha_{k_2}\}$ can be verified by Eq. (3). The details of the proof are presented in the "Appendix".

$$\hat{e}\left(\sum_{i=k_1}^{k_2} F_i, P\right) = \hat{e}\left\{\sum_{i=k_1}^{k_2} [E_i + h(M_i, E_i) H(PID_i)], P_{Pub}\right\} \tag{3}$$

Therefore, the group based authentication can significantly reduce the computational cost for a large number of aggregated signatures. Moreover, the authors in [16] proposed an Up-to-Bottom binary verification based on the BAT signature. The goal of this verification scheme is to find bogus signature in these signatures $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. In this scheme, the authentication starts from the root node of the tree. If the root node, which is the aggregate signature to all signatures at the leaf-nodes, is valid, all the signatures in the leaf-nodes are legal. Otherwise, it verifies the aggregate signature of the left node or the right node to find a leaf node which is associated with the bogus signature. The authors show that this method of verification can reduce the signature verification complexity, even under a worse case with k bogus messages, so this method is appropriate for transplanting in our approach.

4.3 Detailed Description

In this subsection, we explain each phase of our method in detail. Our proposed method is the offline payment method. In our scheme, we assume that EVs can connect to the bank and the service provider through an RSU or they can use LTE and a cellular network to

communicate with the bank and the service provider when they move on the road. The whole process of our proposed method for wireless charging of EVs is shown in Fig. 2.

4.3.1 Setup Phase

In this phase, the initial authentication has already been performed in the trusted registration authority (RA), and every entity receives the required system parameters and makes their own private and public keys. The system follows the ECC method for encryption and decryption and the BAT method for the signature, so the corresponding public and private keys can be calculated as mentioned in Sect. 4.2. Also, the initial authentication can be performed between the EVs and the bank. Then, the user can make an account with the bank to receive tokens that can be used for charging services on the road. The structure of the token will be described in the following sub-section. Moreover, electric vehicles are equipped with a tamper-proof module to carry out secure computation and preserve the security of keys.

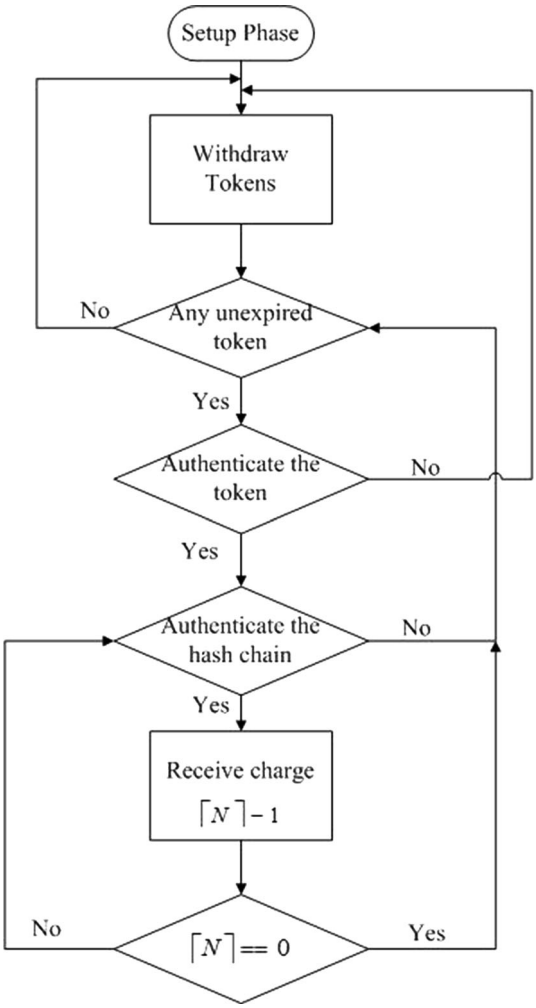

Fig. 2 Flowchart of the proposed method for charging an EV

4.3.2 Token Withdrawal Phase

After the setup phase, whenever users want to receive a new token, they can connect to the bank through VANET or by using a cellular network on the road. We assume that authentication can be done between EVs and the bank server that a secure channel is present between them. The user accesses the public key and uses the identity of the bank to verify its signature, and then the vehicle is preloaded with the system parameters $\{\mathbb{G}, \mathbb{G}_T, q, P, +K_j\}$ and the identity PID_j for each token. Then, the token withdrawal phase starts, as shown in Fig. 3. This phase can be performed in two steps as follows:

(1) In the first step, users who have a valid account with the bank can request the token. They send the message contained in the public key $+\mathrm{K_j}$, the identity PID_j, and the root of hash chain w_0 for the requested token. Moreover, the hash chain has a limited length of n defined by the maximum number of the charging plate segments.

(2) In the second step, the bank will give them a token, which consists of its signature on the public key $+\mathrm{K_j}$, the root of the hash chain $\mathrm{w_0}$ related to this token, the token identity $\mathrm{PID_j}$, and the timestamp $\mathrm{T_b}$ generated by the bank. The token will expire after timestamp $\mathrm{T_b}$, and the user should request a new token if the token is not spent during this time.

4.3.3 Charging Phase

The charging phase takes place in two sub-phase. The first sub phase is carried out before the EV reaches the charging place, and we assume that the EV and the service provider can exchange messages with a secure channel present between them. The second sub-phase takes place when the EV reaches the charging plate. As shown in Fig. 4, Steps 1 through 3 is for verifying the token and the user by the service provider. The user should connect to the service provider through an RSU or by using a cellular network. Steps 4 through 9 are carried out when the user reaches the charging plate, where the user connects to the service provider through the charging plate. In the following, we explain the entire process in detail.

(1) First, the user sends a message (signed by the bank) to the charging plate concatenated with the number of segments N_P that it needs for charging. We should remark that N_P can be a fraction that shows how much of a charge the EV needs. Then, the service provider checks the validity of the signature. We remark that each token has a unique identity and a public key, so the identity of the vehicle will remain unknown to the service provider.

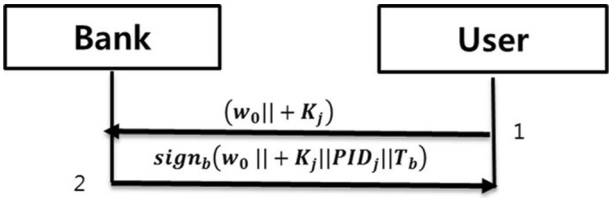

Fig. 3 Token withdrawn phase

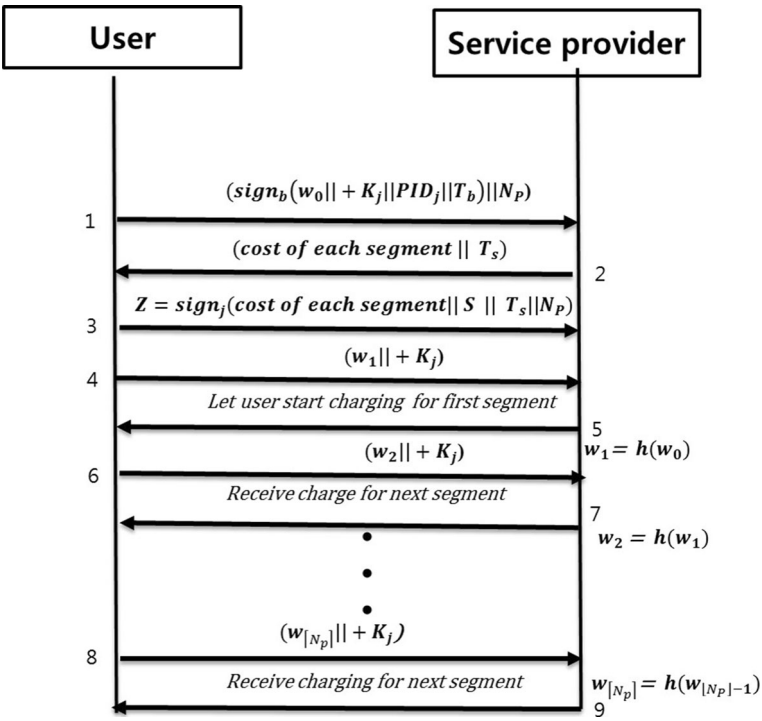

Fig. 4 Charging phase

(2) If the signature is valid, the service provider sends a message that contains the cost of each segment of the charging plate, its identity, and the timestamp to the user. The timestamp is used to prevent reply attacks.

(3) The user signs this message with the token's private key and sends it to the charging plate. With this signed message, the service provider not only has the assurance of the message and the token owner authenticity, but it will also be used to redeem the token from the bank. The service provider checks the validity of this message with the public key of the token.

Steps 4 through 9 are carried out when the users reach the charging plate. Before receiving a charge from each segment, they need to reveal one value of the hash chain sequentially. Since different vehicles may enter the charging plate, each of the messages is defined by the public key of its token. Moreover, the charging plate can verify each value by only checking the hash function and the previous value of the hash chain related to the token ($w_{n-1} = h(w_n)$). If the hash chain value is valid, the service provider lets the user receive the charge from the first segment. We should remark that the user will avoid disclosing the next value of the hash chain to the service provider if the service provider refuses to give the user an electric charge from this segment. However, after receiving a charge from the first segment, the user reveals another value of the hash chain to receive a charge from the next segment. This process will continue until the user receives a charge from the N_P^{th} segment.

We would like to mention that to improve the fairness and to decrease misbehaviors of the service providers, we use the hash chain in our method. However, there is a small

possibility that an untrusted service provider would refuse to give a charge in the last segment (9th Step of Fig. 4) after receiving the hash chain from the user. That being said, the chance of this is negligible since the benefit for cheating one segment is not only smaller than giving a charge in the last segment but also only hurts the service provider's reputation.

4.3.4 Redeeming Phase

The service provider gives the message, which it receives in Step 1 and Step 3 of the charging phase, accompanied with the hash chain to the bank for redeeming the token $(Y||Z||hashchain)$. In this message, Y contained K_j defines which token should be redeemed, and the hash chain reveals that the service provider has given a charge to the user. The bank can check that this message belongs to a real person, as the message contains the service provider's identity, so only the specific service provider can redeem this token.

5 Analysis

In this section, we first discuss different attack scenarios that can happen in our proposed scenario. Then, we compare our method with schemes proposed for plug-in electric vehicles.

5.1 Attack Scenarios

We consider three kinds of attacks, namely, location privacy infringement, double spending, and statement fraudulence. For each of them, we explain the possible scenario and discuss how our method can resist them.

5.1.1 Location Privacy Infringement

Scenario The adversary can be when either the charging plate or the outsider tries to collect information about the EVs to track them. The adversary can access the encrypted message between the users and service providers and the signed message between users and service providers.

Discussion Since we assume that a secure channel established between EVs and the bank, the attackers cannot recognize token withdrawn by the specific EV. Moreover, since tokens are independent of each other, the adversary cannot link them to each other. Therefore, our method provides privacy of EVs to third parties.

5.1.2 Double Spending

Scenario Double spending may be preferred by an adversary who uses the reply attack or the owner of a token to reutilize the already-spent token. Both of these are discussed in case 1 and case 2, respectively, as follows:

Case 1: The adversary can access the messages exchanged between the owner of the tokens and the service provider. Since they do not possess the secret key of that token, they cannot spend it with another service provider. Moreover, as the signed messages

with the private key of the token contain the time of spending, they will not be able to spend this token with the same service provider either. Moreover, the service provider will not let users spend the hash chain more than one time, so if two different charging plates are operated by the same service provider, an adversary may not be able to use the same messages in two different charging plates belonged to the same service provider.
Case 2: The owners of the tokens who has access the ticket's private key can only spend the token more than once. However, double spending by the user only endangers his privacy and does not provide any benefit for them. Moreover, owners who spent the token multiple times can be detected by the bank, and users cannot also spend the hash chain more than one time with the same service provider.

5.1.3 Fraudulent Statement

Scenario Fraudulence can be preferred by users who try not to pay or pay for the service less than what they utilize, and also by the service provider who tries not to give a charge after receiving money. Both of these conditions will be discussed in case 1 and the case 2, respectively, as below:

Case 1: The amount of money determined by the service provider concatenated with his identity should be signed by the user with the token's private key. Then, the service provider lets the user start charging after receiving the first value of the hash chain related to the token. If the signature is not valid or the user prevents the hash chain value from being sent, the user will not receive a charge.
Case 2: For fairness, in our method, each token has a hash chain. The root of this hash chain is signed by the bank, and the service provider can redeem the token by giving the token and the hash chain to the bank. Moreover, the charging plate is divided into segments and the service provider gives a charge for each segment after receiving the next value of the hash chain. If the service provider does not give a charge to the user, the user will refuse to reveal the hash chain, so the service provider cannot redeem the token entirely. However, the user receives a charge from the last segment after revealing the hash value related to this segment, so there is a chance that the service provider does not give a charge for the last segment after receiving the hash value related to this segment. However, given that the service provider has a public identity and that the benefit for cheating on one segment is not only smaller, but actually only hurts the service provider's reputation. Therefore, the probability of the service provider cheating becomes smaller. Moreover, to prevent collusion between service providers, whether the users receive a charge or not, they should use each token only once.

5.2 Comparison with Other Methods

In this section, we compare different features of our method with the proposed methods of Ho et al. [6] and Nikanfar et al. [14]. These schemes are proposed for plug-in electric vehicles. To the best of our knowledge, there is no method for wireless charging of the electric vehicle on the move, so we compare our method with these schemes, which have more similarities with the wireless charging of electric vehicles on the move.

As shown in Table 2, our method is offline and so it cannot prevent double spending, but it does decrease the overhead communication, which is necessary for wireless charging on the move. Moreover, double spending can be detected by the bank in our system.

Table 2 Compare methods

	Ho et al. [6]	Nikanfar et al. [14]	Proposed method
Feature	Online	Online	Offline
Location privacy	✔	✔	✔
Robustness	✔	✔	✔
Detect double spending	✔	✔	✔
Prevent double spending	✔	✔	✗
Prevent fraudulent statement	✔	✗	✔
Track illegal user	✗	✔	✔

Nikanfar et al. [14] do not consider preventing fraudulence in their method. Therefore, a service provider can refuse to give a charge after receiving a user's information. In our method, by using the hash chain, we try to prevent fraudulence so as to be fair to service providers and users. However, for the last segment, the service provider can avoid giving a charge after receiving the hash chain related to this segment. Moreover, as Ho et al. [6] 's method provides unconditional privacy, tracking is only possible with user approval. Therefore, tracking an illegal user is impossible in this scheme. Furthermore, they use zero-knowledge proofs, which makes their method more complex. In addition, users need to send multi-proofs to the service provider during charging, which makes it unsuitable for wireless charging on the move.

6 Conclusion

In this paper, we have discussed different payment methods and their problems for wireless charging on the move. Moreover, we have presented an anonymous payment method against service providers that is appropriate for wireless charging on the move. As the efficiency is an important factor for wireless charging on the move, we try to reduce using signatures and exchanging messages with service providers during the charging process. Also, by using independent tokens, we provide location privacy. To obtain a fair payment method, we have used the hash chain. In our proposed system, we have assumed the cooperation of the bank, which not only provides the signed tokens but can also detect double spending and open all transactions in case of any dispute.

Acknowledgments This research was supported in part by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2016-H8501-16-1018) supervised by the IITP (Institute for Information & communications Technology Promotion). This research was also supported in part by the NRF (National Research Foundation of Korea) grant funded by the Korea government MEST (Ministry of Education, Science and Technology) (No. NRF-2015R1D1A1A09058200).

Appendix

Signature Verification

As mentioned in [16], an RSU or a service provider with access to the $\{\mathbb{G}, \mathbb{G}_T, q, P, P_{Pub}\}$ parameters can verify the signature $\alpha_i = E_i, F_i$ on the message M_i as follows:

$$\hat{e}(F_i, P) = \hat{e}(E_i + h(M_i, E_i)H(PID_i), P_{Pub}).$$

This is proved below:

$$\begin{aligned}\hat{e}(F_i, P) &= \hat{e}(r_i P_{Pub} + h(M_i, E_i)SK_i, P) = \hat{e}(r_i P_{Pub}, P) \cdot \hat{e}(h(M_i, E_i)SK_i, P) \\ &= \hat{e}(r_i P, P_{Pub}) \cdot \hat{e}(h(M_i, E_i)sH(PID_i), P) = \hat{e}(E_i, P_{Pub}) \cdot \hat{e}(h(M_i, E_i)H(PID_i), P_{Pub}) \\ &= \hat{e}(E_i + h(M_i, E_i)H(PID_i), P_{Pub}).\end{aligned}$$

The computation cost to verify the above signature is one multiplication and two pairing operations.

Verifying the Group Signature

To reduce the computation cost and improve the efficiency, Jian et al. [16] introduce the BAT signature in which $n = 2^h$ vehicles $\{V_1, V_2, V_3, \ldots, V_n\}$ with corresponding signatures $\{\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n\}$ can construct a Binary Authentication Tree. In this tree, each leaf node contains the signatures of a vehicle, and each inner node is associated with an aggregate signature that contains signatures of the whole leaf nodes in this sub-tree. Moreover, the root of the tree includes an accumulation of all signatures at the leaf-nodes. For verifying all the signatures $\{\alpha_{k_1}, \alpha_{k_1+1}, \ldots, \alpha_{k_2}\}$, the following equation should hold:

$$\hat{e}\left(\sum_{i=k_1}^{k_2} F_i, P\right) = \hat{e}\left\{\sum_{i=k_1}^{k_2}[E_i + h(M_i, E_i)H(PID_i)], P_{Pub}\right\},$$

which can be proven as follows:

$$\begin{aligned}\hat{e}\left(\sum_{i=k_1}^{k_2} F_i, P\right) &= \hat{e}\left\{\sum_{i=k_1}^{k_2} r_i P_{Pub} + h(M_i, E_i)SK_i, P\right\} = \hat{e}\left(\sum_{i=k_1}^{k_2} r_i P_{Pub}, P\right) \cdot \hat{e}\left(\sum_{i=k_1}^{k_2} h(M_i, E_i)SK_i, P\right) \\ &= \hat{e}\left(\sum_{i=k_1}^{k_2} r_i P_{Pub}, P\right) \cdot \hat{e}\left(\sum_{i=k_1}^{k_2} h(M_i, E_i)sH(PID_i), P\right) \\ &= \hat{e}\left(\sum_{i=k_1}^{k_2} E_i, P_{Pub}\right) \cdot \hat{e}\left(\sum_{i=k_1}^{k_2} h(M_i, E_i)H(PID_i), P_{Pub}\right) \\ &= \hat{e}\left\{\sum_{i=k_1}^{k_2}[E_i + h(M_i, E_i)H(PID_i)], P_{Pub}\right\}.\end{aligned}$$

The computation cost for verifying the k aggregate signatures contains k multiplications, k one-way hash, and 2 pairing operations. Cleary, using the BAT signature can effectively lower the computation cost.

References

1. Hawkins, T. R., Singh, B., Majeau-Bettez, G., & Strømman, A. H. (2013). Comparative environmental life cycle assessment of conventional and electric vehicles. *Journal of Industrial Ecology, 17*(1), 53–64.
2. Valsera-Naranjo, E., Sumper, A., Lloret-Gallego, P., Villafafila-Robles, R., & Sudria-Andreu, A. Electrical vehicles: State of art and issues for their connection to the network. (2009). In *Proceeding of IEEE international conference on electrical power quality and utilisation*, pp. 1–3.

3. Dutta, P. (2013). Coordinating rendezvous points for inductive power transfer between electric vehicles to increase effective driving distance. In *Proceeding of international conference on connected vehicles and expo (ICCVE), IEEE*, pp. 649–653.
4. Suh, N., Cho, D., & Rim, C. T. (2011). Design of on-line electric vehicle (OLEV). Plenty lecture at 2010 CIPR Design Conference in Nantes, France. In A. Bernard (Ed.), *Global product development* (pp. 3–8). Berlin: Springer.
5. Ko, Y. D., Jang, Y. J., & Jeong, S. Mathematical modeling and optimization of the automated wireless charging electric transportation system. (2012). In *Proceeding of IEEE international conference on automation science and engineering (CASE)*, pp. 250–255.
6. Au, M. H., Liu, J. K., Fang, J., Jiang, Z. L., Susilo, W., & Zhou, J. (2014). A new payment system for enhancing location privacy of electric vehicles. *IEEE Transactions on Vehicular Technology, 63*(1), 3–18.
7. Rivest, R. L., & Shamir, A. (1997). PayWord and MicroMint: Two simple micropayment schemes. In M. Lomas (Ed.), *Security protocols 1996, LNCS* (Vol. 1189, pp. 69–87). Heidelberg: Springer.
8. Foley, S. N. (2003). Using trust management to support transferable hash-based micropayments. In R. N. Wright (Ed.), *Financial cryptography (FC) 2003, LNCS* (Vol. 2742, pp. 1–14). Berlin: Springer.
9. González, A. G. (2004). PayPal: the legal status of C2C payment systems. *Computer Law & Security Review, 20*(4), 293–299.
10. Zormati, A. (2004). Prepaid payment card that can be instantly recharged remotely by coupon. Google Patents.
11. Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. Retrieved November 12, 2011. http://bitcoin.org/bitcoin.pdf
12. Reid, F., & Harrigan, M. (2013). An analysis of anonymity in the bitcoin system. *Security and privacy social networks* (pp. 197–223). New York: Springer.
13. Miers, I., Garman, C., Green, M., & Rubin, A. D. Zerocoin: Anonymous distributed e-cash from bitcoin. In *Proceeding IEEE symposium on security and privacy (SP)*, pp. 397–411.
14. Nicanfar, H., Hosseininezhad, S., TalebiFard, P., & Leung, V. C. (2013). Robust privacy-preserving authentication scheme for communication between electric vehicle as power energy storage and power stations. In *Proceedings IEEE INFOCOM*, pp. 3429–3434.
15. Neuman, B. C., & Medvinsky, G. (1995). Requirements for network payment: The netcheque perspective. In *Proceeding IEEE Compcon'95*, San Francisco, pp. 32–36.
16. Jiang, Y., Shi, M., Shen, X., & Lin, C. (2009). BAT: A robust signature scheme for vehicular networks using binary authentication tree. *IEEE Transactions on Wireless Communications, 8*(4), 1974–1983.

Zeinab Rezaeifar received her B.S. in Communication Engineering, from Shahid Bahonar University of Kerman, Iran in 2008 and M.S. degree in Network Communication Engineering, from Isfahan University of Technology, Iran in 2012. Currently she is working toward the Ph.D. degree in Computer Engineering from Hanyang University, South Korea. His main research interests include security issues in wireless charging of Electric Vehicle (EV), routing in VANET (Vehicular Ad Hoc NETworks), information security and privacy issues in VANET, DTN (Delay Tolerant Network) in VANET, and security issues in Content Centric Networks (CCN).

Rasheed Hussain received his B.S. in Computer Software Engineering from N-W.F.P University of Engineering and Technology, Peshawar, Pakistan in 2007, M.S. degree in Computer Engineering from Hanyang University, South Korea in 2010, and Ph.D. degree in Computer Engineering from Hanyang University, South Korea in February 2015. Currently he is an assistant professor in Department of Computer Science and Engineering, Innopolis University, Russia. His main research interests include information security and privacy issues in Vehicular Ad Hoc NETworks (VANET), information dissemination in VANET, VANET applications and services, cloud computing, smart grid security, location-based services, Security and Privacy issues in Internet of Things (IoT), Big Data, and VANET-based clouds.

Sangjin Kim received his B.S. in Computer Software Engineering from N-W.F.P University of Engineering and Technology, Peshawar, Pakistan in 2007 and M.S. degree in Computer Engineering from Hanyang University, South Korea in 2010. Currently he is working toward the Ph.D. degree in Computer Engineering from Hanyang University, South Korea. In 2012, he joined the faculty of the Department of Computer Science and Engineering, Korea University of Technology and Education, where he is currently a professor.

Heekuck Oh received his B.S. degree in Electronics Engineering from Hanyang University in 1983. He received his M.S. and Ph.D. degrees in Computer Science from Iowa State University in 1989 and 1992, respectively. In 1994, he joined the faculty of the Department of Computer Science and Engineering, Hanyang University, ERICA campus, where he is currently a professor. His current research interests include network security and cryptography. Prof. Oh is the senior executive vice president of Korea Institute of Information Security & Cryptology, and is a member of Advisory Committee for Digital Investigation in Supreme Prosecutors Office of the Republic of Korea. He is also a member of Advisory Committee for Internet Security under Korea Communications Commission.