Hindawi
Wireless Communications and Mobile Computing
Volume 2017, Article ID 5676030, 17 pages
https://doi.org/10.1155/2017/5676030

Research Article

PBF: A New Privacy-Aware Billing Framework for Online Electric Vehicles with Bidirectional Auditability

Rasheed Hussain,[1] Junggab Son,[2] Donghyun Kim,[2] Michele Nogueira,[3] Heekuck Oh,[4] Alade O. Tokuta,[5] and Jungtaek Seo[6]

[1]*Department of Computer Science, Innopolis University, Kazan, Russia*
[2]*Department of Computer Science, Kennesaw State University, Marietta, GA 30060, USA*
[3]*Department of Informatics, Federal University of Paraná, Curitiba, PR, Brazil*
[4]*Department of Computer Science and Engineering, Hanyang University, Seoul, Republic of Korea*
[5]*Department of Mathematics and Physics, North Carolina Central University, Durham, NC 27707, USA*
[6]*Department of Information Security Engineering, Soonchunhyang University, Asan, Republic of Korea*

Correspondence should be addressed to Jungtaek Seo; seojt@sch.ac.kr

Received 8 June 2017; Accepted 29 August 2017; Published 31 October 2017

Academic Editor: Rong N. Chang

Recently an online electric vehicle (OLEV) concept has been introduced, where vehicles are propelled by the wirelessly transmitted electrical power from the infrastructure installed under the road while moving. The absence of secure-and-fair billing is one of the main hurdles to widely adopt this promising technology. This paper introduces a new secure and privacy-aware fair billing framework for OLEV on the move through the charging plates installed under the road. We first propose two extreme lightweight mutual authentication mechanisms, a direct authentication and a hash chain-based authentication between vehicles and the charging plates that can be used for different vehicular speeds on the road. Second, we propose a secure and privacy-aware wireless power transfer on move for the vehicles with bidirectional auditability guarantee by leveraging game theoretic approach. Each charging plate transfers a fixed amount of energy to the vehicle and bills the vehicle in a privacy-aware way accordingly. Our protocol guarantees secure, privacy-aware, and fair billing mechanism for the OLEVs while receiving electric power from the infrastructure installed under the road. Moreover, our proposed framework can play a vital role in eliminating the security and privacy challenges in the deployment of power transfer technology to the OLEVs.

1. Introduction

As the fuel price is going up, alternative fuel vehicles, in particular, electric vehicles, are getting more attention. Previously, electric vehicles were suffering from various issues such as low reliability, high consumer satisfaction, and low return on investment [1]. However, thanks to the recent advancements in automotive, electronics, and communication technologies, electric vehicles have overcome the issues and have become pervasive on the present highways. Still, there are a number of challenges to address in order to make electric vehicles more practical. One of the most crucial problems is that the capacity of the state-of-the-art battery for electric vehicles is not sufficient to drive the cars over a long distance without recharging. It is well known that the battery technology has been slowly improved [2], and thus we can hardly expect to have a much higher capacity battery for electric vehicles in the near future. Meanwhile, as of today, there is a relatively small number of places to recharge the battery of an electric vehicle along a highway [3]. Most of all, compared to the time to refuel a traditional vehicle with a combustion engine, it takes significantly longer to charge the battery through plug-in technology in a charging station [4] or by staying on a wireless charging plate (CP) [5].

Recently, the concept of online electric vehicle (http://olev.kaist.ac.kr/en/index.php) is introduced to alleviate the aforementioned issues of electric vehicles. Electric vehicles with a special onboard unit can obtain the electricity on the

move in a wireless manner while passing over a road surface under which power line is installed. It is envisioned that this new technology will make a significant contribution to expanding the adoption of electric vehicles. Despite the apparent benefits, there are still a number of issues that need to be resolved to aid the wide deployment of online electric vehicles. In particular, consider the problem of designing a proper billing mechanism for this wireless-charging-on-the-move strategy. One straightforward solution would be taking a picture of every vehicle that is entering a road designed for online electric vehicles and sending the flat amount of bill to each one of them. This strategy works well for many vehicles with combustion engine on modern toll plaza at highways where they pay their toll tax in a wireless and efficient manner. However, it is clearly not fair for online electric vehicles with almost fully charged battery to pay the same amount of money paid by those vehicles with the almost empty battery since the driver of a vehicle with the fully charged battery may not want to use online power service to save the cost. In addition, collecting pictures of the vehicles entering every part of the road is almost not possible and also can cause a privacy abuse. Therefore, it is not desirable even though this strategy is widely used for toll tax collection at a toll plaza on the highways. Moreover, recently radio frequency identification (RFID) gained a lot of attention from the service providers and has been widely deployed due to its simple operation and low cost [6–9]. However, our case is completely different from RFID scenario because in our case the requirements for traceability and deniability are critical when compared to RFID authentication and billing. Hence the comparison between RFID-based solutions and our scenario would not be fair.

Motivated by our observations, in this paper, we propose a new secure-and-fair billing framework for online electric vehicles. In detail, we propose to adopt a road which consists of a series of short-and-equal-sized electricity supply segments, each of which serves as a unit for billing. Before an online electric vehicle enters a new segment, it can decide to use the electricity, while moving over the segment, or deny it depending on its current battery level. Once the vehicle decided to use the electricity, it needs to authenticate itself to the segment and obtain a secret to consuming it (see Figure 1). To improve the degree of fairness and service granularity, that is, to be billed for actual use only, it is important to make the segment short. At the same time, to improve the efficiency of the segment, which is the actual rate of the segment used for charging against the portion of the segment used for other use such as authentication, it is crucial to design the authentication protocol to be as lightweight as possible. To guarantee the privacy of each driver and reduce the operation cost, it is highly desirable not to use a camera for billing. Rather than using the camera to take the picture of each vehicle to enter every segment, we propose a wireless communication based conditional privacy mechanism so that the real identity of the driver can be exposed by the revocation authority only if there is a legal need such as refusing to pay after actual electricity consumption. Finally and most importantly, we provide a mutual audit mechanism through which a driver cannot deny the usage of legitimate electricity, as well as the electricity service provider cannot overcharge.

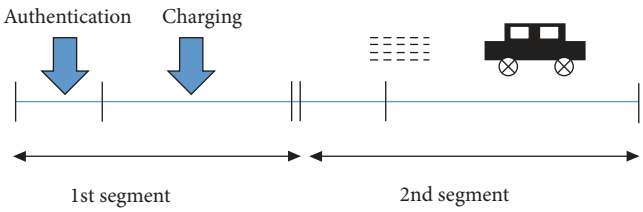


Figure 1: Online electric vehicle can charge its battery while moving after the authentication with the highway segment.

Summary of Contributions. This paper is the extension of our previous work [10]. The preliminary version of this work contains basic mutual authentication mechanism between CP and OBU whereas in the current extended version we address the issues of conditional privacy preservation, two mutual authentication mechanisms, bidirectional auditability, and billing mechanism in the charging-on-the-move environment. Moreover, the extended version also includes a game theoretic approach to guarantee bidirectional auditability in the charging process. To this end, in this paper, we propose a security framework for electric vehicles which supports the following relevant features, and thus the contributions of this paper are as follows.

(a) Bidirectional Audit. We design a mechanism that guarantees privacy-aware bidirectional auditability for both electric power providing authority and the vehicles. To deal with the billing and auditing, we propose a semisimultaneous billing where each vehicle, when it charges its battery, is billed on plate-by-plate basis where each plate delivers a constant amount of energy. In other words, the vehicles are billed with a fixed amount.

(b) Conditional Privacy. We use multiple pseudonymous mechanism to preserve the conditional privacy of the vehicles at every stage of the protocol.

(c) Mutual Authentication. We devise a fast and lightweight authentication mechanism for vehicles and the charging plates keeping in mind the portion of the charging plate designated for authentication.

(d) Game Theoretic Approach. We employ a game theoretic approach to model the proposed bidirectional auditability mechanism in order to establish Nash Equilibrium between the charging plate and the vehicle.

This paper proceeds as follows. Section 2 outlines the literature review regarding wireless power transfer followed by the system model and problem definition in Section 3. In Section 4, we outline our proposed scheme and quantitatively analyze our system in Section 5. In Section 6, we give our concluding remarks.

2. Literature Review

Today, some of world most renowned automobile companies are producing battery propelled vehicles and it is envisioned that soon electric vehicles will outclass the conventional automobiles due to economic and environmental reasons. The technological breakthrough in both electrification technology and the energy storage technology has made it possible for the automobile companies to achieve this milestone. From the studies conducted so far, it can be inferred that, in the near future, most of the fossil fuel propelled vehicles will possibly be replaced by the electric vehicles (see [11]). In [11], Weissinger et al. outlined the speed range, storage range, and the battery types of vehicles till the year 2008. To date, many efficient charging schemes have been proposed in the literature to save the commute time for the drivers [12]. However, the frequency of recharging is still a problem that needs to be addressed.

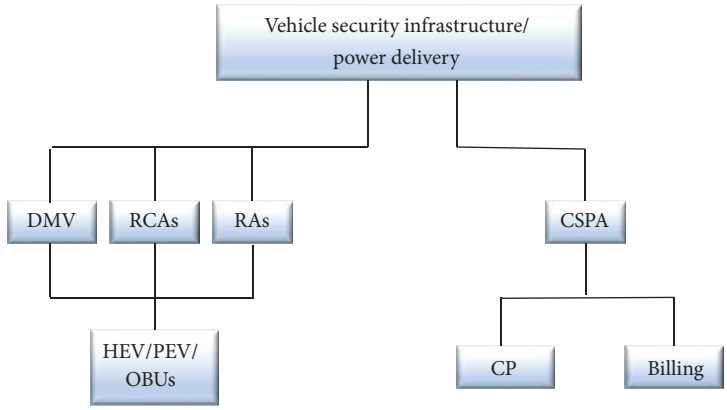
To motivate the use of electric vehicles, a new concept of wireless power transfer (WPT) was introduced [5]. In [5], authors carried out a detailed survey regarding wireless power transfer and covered many dimensions such as the distance between the transmitting and receiving entity, and cost of the technology. The concept of green car was introduced in 2009 by KAIST, South Korea, by the name of online electric vehicle (OLEV) [13]. The motivation for OLEV was the weight and the cost of the battery in electric vehicles, low frequency of charging, fast installation, low maintenance cost, and so forth. To date, remarkable results have been achieved by this project and currently they operate and run prototype buses in the KAIST campus, South Korea [14, 15]. Nonetheless, such online vehicle would require massive power line infrastructure installed under the road. Moreover coverage would be another issue due to the cost factor. For secure WPT, vehicles need to preform mutual authentication with the CPs before the power transfer begins. However, the interconnection time between the CP and OBU is very short. Therefore, it is essential to devise an extreme lightweight and yet efficient authentication mechanism for this purpose. It is to be noted that although there exist sophisticated and efficient authentication mechanisms in VANET [16], these schemes cannot be directly used in our scenario due to the unique features, characteristics, and challenges of the charging on the move.

From mutual authentication standpoint, Chuang and Lee [17] proposed a hash-based authentication mechanism called trust-extended authentication mechanism (TEAM). TEAM adopts the concept of transitive trust relationships where a normal vehicle becomes the trusted entity after successful authentication and can delegate the authentication process in the absence of the authorities. Moreover TEAM does not protect the privacy since original ID is shared during authentication. On the other hand, even if a normal vehicle successfully authenticates itself, it does not guarantee that the vehicle will not be malicious while delegating authentication function. Therefore, we believe that the transitive trust may lead to even worst situation from security standpoint in VANET.

Billing is an important requirement in commercial networks and it can be abstractly divided into two classes, time-based billing and content-based billing. In the former, nodes (subscribers or consumers) pay the service fee based on time, for instance, the Internet access charges, and in the latter case, nodes pay based on the content they receive where the specific content costs a constant amount of money, for example, downloading a song from iTunes and so forth [18]. A number of billing mechanisms have been proposed for wireless mesh networks [19, 20] and commercial VANET applications [18, 21]. In [18], the authors propose a portable authentication/authorization/accounting (AAA) framework for purchasing services from the RSUs. They use signature-based and key policy attribute-based encryption (KP-ABE) in their billing mechanism to attain localized fine-grained access control and also employ E-coin. In another work, Yeh and Lin [21] proposed a local and proxy-based authentication and billing scheme to lessen the long-distance communication overhead. They also proposed an incentive-aware multihop forwarding for vehicles in the VANET. They use batch verification mechanism in their scheme to fulfill the security requirements and signature-based communications. However, our service scenario is different because we deal with the charging plates installed underneath the road and such sophisticated cryptographic primitives will cause enormous delay. Therefore, aforementioned schemes are not directly applicable in our scenario.

Recently, some considerable results were appeared for the OLEVs. Zhao et al. proposed a new billing scheme which could detect free-riders, who charge their vehicle without payment, by checking their battery level before and after a charging plate [22]. The free-riders could charge by getting closer to authenticated and billed vehicles. However, this is an unrealistic solution as vehicles should not be on the same charging segment, which is 50 m long or longer than one mile according to their description, to avoid to be treated as a free-rider. All vehicles in traffic jam must pay for charging even if they do not want to charge. Saxena and Choi proposed a bilinear pairing based authentication scheme for flexible charging in vehicle-to-grid networks [23]. However, their proposed scheme is not compatible with our environment as they considered a wired charging which vehicles need to be connected to for a relatively longer time period. Li et al. proposed a fast authentication scheme with segmented charging plates for wireless charging [24]. Their simulation results show that the proposed scheme is highly efficient as it takes only 0.11 ms to verify vehicles. However, their system model needs to have a gap between charging pads to prevent the free-riders. The two neighboring charging pads should be separated by 0.8 m while the length of charging pads is 0.4 m, and thus this setting makes the system have low utilization of charging. Heavy vehicles, which need more energy to move, would be discharged slowly on the road.

In this paper, we, to the best of our knowledge, for the first time propose a secure and privacy-aware mechanism to transfer the electric power to propel the vehicles moving on the road where the power transfer technology is installed underneath the road in the form of charging plates. Moreover our proposed scheme also guarantees bidirectional audit.



DMV: department of motor vehicle
RCA: regional certification authority
RA: revocation authority
CSPA: charging service providing authority
CP: charging plate

Figure 2: Taxonomy of system participants.

First we propose two lightweight and fast privacy-aware mutual authentication mechanisms between the vehicles and the charging plates installed under the road. The two authentication mechanisms can be adapted with different vehicular speeds and the length of the charging plates. Then we propose a secure charging mechanism for vehicles with bidirectional auditability guarantee where vehicle is billed in a semisimultaneous manner on the per-plate basis. We also employ a game theoretic approach for modeling and guaranteeing auditability by establishing Nash Equilibrium between the charging plates and the vehicles.

3. System Model and Problem Statement

3.1. System Participants and Network Model. Our proposed system model consists of electric vehicles and an electric power delivery infrastructure. Electric power delivery service is exercised by the charging service providing authority (CSPA) that is responsible for providing the vehicles with the electric charge through charging plates and billing them accordingly. The charging infrastructure is installed under the surface of the road and each road segment of a certain length is covered by the charging plates. The charging plates also have hardware for communication and computation purpose and these plates are responsible for authentication prior to battery charging, billing, and logging the audit information. These charging plates communicate with both vehicles and CSPA back and forth during the charging and the billing process. We also introduce some components from vehicular ad hoc network (VANET) that are frequently assumed in VANET. These components are used by electric vehicles (throughout the paper, the terms "vehicle," "vehicular node," and "OBU" are used interchangeably and we mean electric vehicle collectively by these terms) for initialization and registration. These components include vehicle management, registration, and revocation authorities. The department of motor vehicles (DMV) is at the top of the hierarchy where every vehicle should be registered beforehand. Revocation authorities are leveraged to revoke the identity of the vehicle when needed with the consent from law enforcement authorities (police or judiciary) in the form of a warrant. There may be heterogeneous types of vehicles on the road, but for ease of understanding, we focus only on the electric vehicles in this paper. Therefore, our proposed scheme can be easily implemented in the VANET framework, which is one of the most popular and promising future vehicular infrastructures.

The taxonomy of the system participants is shown in Figure 2 and the network model is shown in Figure 3. We consider a fleet of electric vehicles on the road where these vehicles receive electric power from the power line installed beneath the road, depending upon the usage of the vehicle. It can be seen in Figure 1 that road segment consists of the power line distribution technology installed beneath the road in the form of charging plates. A portion of the charging plate is leveraged for authentication purpose and the rest of the charging plate is used for transferring the electrical energy to the vehicle (see Figure 1). Vehicles mutually authenticate with the charging plates before receiving electric power from the plates. After successful authentication, the fixed designated amount of electrical energy is transferred to the battery and the vehicle is billed accordingly. The communication channel between vehicles, registration, and revocation authorities, and the charging plates is based on Dedicated Short Range Communication (DSRC) (https://www.fcc.gov/wireless/bureau-divisions/mobility-division/dedicated-short-range-communications-dsrc-service) standard whereas charging plates are connected to the charging service providers through high-speed wired links.

In our network model, bidirectional auditability is of paramount importance because the vehicle wants to get the energy if it has paid for it and similarly the service provider must receive the amount of due amount if the electrical charge is transferred to the vehicle. Therefore, in the next

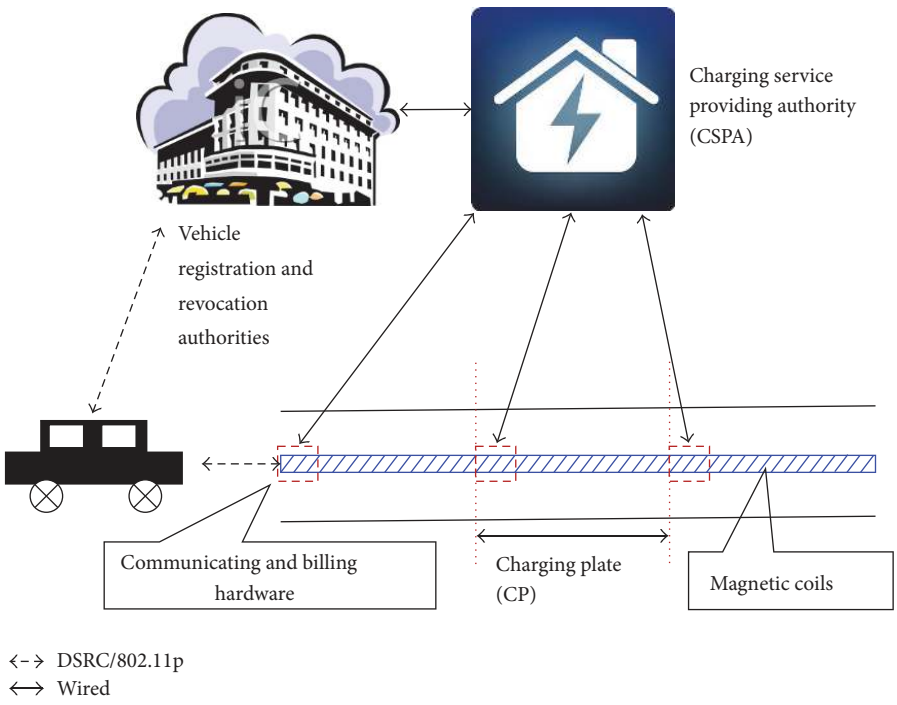


Figure 3: The network model.

subsection, we outline the bidirectional auditability problem by leveraging game theoretic approach.

3.2. Problem Definition. Based on the aforementioned system and network model, we outline our problem statement. The problem statement is multidimensional and covers a number of aspects for the unique environment of wireless charging. The wireless-charging-on-the-move phenomenon has a unique set of requirements and thus introduces new problems. Firstly, due to the billing and audit, both charging plates and vehicles must mutually authenticate each other. However, due to the high speed of vehicles and the small size of the charging plate, the authentication mechanism should be extremely lightweight and fast. Secondly, in order to make the wireless charging service on the move, user satisfaction is going to be a major challenge from the privacy standpoint. In other words, the users will prefer to make the charging and billing mechanism anonymous. Therefore, a conditional privacy-aware and yet secure mechanism should be in place to cover the whole charging and billing process. Thirdly, the vehicles and the service providers should be able to carry out bidirectional auditability where both parties should be able to verify the amount of charge and the respective bill.

In order to argue on the bidirectional auditability, we employ a game between the user and CP as an instance of the Guest-Host problem (GHP). In the GHP, guest and host at a hotel make sure that both of them are audited in a fair way. In game theoretic approach, an important stage called Nash Equilibrium (NE) is achieved where each player is assumed to be aware of the equilibrium strategies of the opponent(s). In NE, no player can gain anything by changing only his/her own strategy. In other words, during the game, a stage is reached where no player can benefit from changing its strategy while other players keep their existing strategy. Therefore, the current set of strategies and their payoff collectively constitute NE. In our proposed scheme, an uncooperative game theoretic approach will be explained in the later section.

3.3. Assumptions. Our proposed scheme is based on the following assumptions.

(a) Electric vehicles are equipped with onboard unit (OBU) and Tamper-Resistant Module (TRM) to carry out the secure computation. It is to be noted that messages are constructed inside TRM and the security parameters (keys) are saved into TRM. TRM takes care of the message construction according to its configuration. The modules that give the data as input to the TRM can still provide TRM with wrong information.

(b) DMV is a trustworthy entity and only DMV is authorized to initialize the TRM and store necessary security parameters and keys in it, whereas CSPA, charging plates, and OBUs are not trustworthy.

(c) For a single charging plate, a fixed amount of charge is transferred to vehicles and a fixed amount of bill is charged to the customer, and thus this constitutes a semistatic and fixed billing system. This can be extended to detect the exact amount of energy transferred to vehicles.

(d) We use the energy encryption scheme [25] to prevent free-riders who charge their vehicles without payment by being located on the same charging plates with a legal paid vehicle.

3.4. Threat Model. In our threat model, we consider that both participating parties (charging plates and vehicles) may be malicious. Their behavior can be malicious in terms of either bypassing the billing process or overcharging the energy receiving entity. Besides, the CSPA can also abuse the privacy of the electric power consumer vehicle by either exposing their location information or selling out their location-based profile to other third parties such as ads agencies. Moreover, both passive and active adversaries are considered who can sniff the communication between charging plate and OBU, modify it, or forge it. We argue that the adversaries will have more resources than the participating entities. However, the timeliness of possible attack is a challenging front for the adversaries where the possible attacks must be performed within the stipulated time that is equal to the duration of the charging and billing.

3.5. System Requirements and Security Models. Based on the system and threat models, we argue that the proposed scheme is secure if it satisfies the following security models.

(S-1) Mutual authentication: whenever a vehicle is moving on the authentication section and the vehicle needs to charge battery, both the vehicle and the charging plate can authenticate each other to prevent illegal charging and illegal payment. Also, an illegal vehicle and an illegal charging plate cannot pass the authentication protocol.

(S-2) Bidirectional auditability: while transferring electric power to the vehicle, bidirectional auditability must be guaranteed. In other words, a billing and provided electric power message can be verified by both a vehicle and a CSPA. Also, the billing procedure must be verifiable by all the entities, that is, OBU, CSPA, and DMV to prevent the vehicle overbilled and the CSPA underpaid.

(S-3) Conditional privacy: the conditional privacy of the vehicle's location and the user must be preserved. The identity of a vehicle owner should be revoked to the power supplier only if it is legally necessary, for example, in case the user refuses to pay. Therefore, with this requirement fulfilled, attackers cannot obtain the user identity.

Additionally, the proposed authentication and billing framework must fulfill the following requirements.

(R-1) Due to the resource constraints of the charging plate and the speed of the vehicle, the communication between charging plate and OBU and between charging plate and CSPA must be sufficiently efficient. Moreover, the authentication mechanism must be very fast and lightweight.

(R-2) At the time of charging, both the players should be in the Nash Equilibrium state.

4. Proposed Bidirectional Auditability in Online Electric Vehicle

In this section, we outline the proposed power transfer and billing mechanism and the bidirectional audit between the charging plate and the OBU by a game theoretic approach.

4.1. Baseline. Before using the wireless electric energy transfer service on the move, vehicles must have registered with the DMV to initialize their TRM and to store the security parameters and pseudonyms in it. Additionally, the vehicles must also register with the CSPA to get the necessary security parameters, required to the charging plates at authentication stage. Charging plates are installed under the designated road segments by CSPA and are equipped with hardware that is capable of carrying out secure computation and communication operations for authentication and billing purpose. Whenever a vehicle (the term *"vehicle"* throughout the rest of the paper should be read as electric vehicle; for the sake of simplicity, we use the term vehicle instead of charging vehicles) enters the road section with power line underneath it, it opts for either obtaining the electric power or not. If the vehicle selects the power reception, then it has to mutually authenticate with the charging plate. We propose two very fast and lightweight mutual authentication mechanisms; one is based on only hash and XOR functions and inspired by the Chuang and Lee's scheme [17], while the second one is based on the hash chain. The former is a direct authentication between charging plate and OBU whereas the latter is authentication through CSPA. In the former scheme, charging plate incurs minimum communication delay, whereas, in the latter, charging plate incurs minimum computation delay. Both of the proposed schemes are suited for specific purposes that are explained later in the paper. After successful authentication, the power transfer process starts and charging plate sends the billing information to both OBU and CSPA. The billing is fixed on per charging plate basis. To preserve users' privacy, we use pseudonymous approach and vehicles change their pseudonyms at every charging plate at the time of charging. We also model the billing and audit as a game between OBU and charging plate where both of them must achieve the Nash Equilibrium state.

4.2. Preliminaries and Initializations

4.2.1. System Initialization. Notations in the Notations section are employed throughout the paper. We achieve user privacy through pseudonymous. In addition, in order to store the individual secret keys of the vehicles, that is, K_{sym} and K_V in the database of revocation authorities (RAs), we use ElGamal encryption algorithm over elliptic curve cryptography (ECC) due to its proven security. Let $\mathbb{G}$ be a cyclic group of prime order q, where $\mathbb{G}$ is generated by a generator P. First of all, DMV chooses a random number $x \in \mathbb{Z}^*$ as its private key and computes $\text{PK}^+ = xP$ as its public key. DMV then uses threshold based secret share scheme [26] and divides x into j parts, where j is the number of revocation authorities, each RA_i holds a share x_i, and $x_i \in (x_1, x_2, x_3, \ldots, x_j)$. In order to construct x from individual x_i,

RAs must elect one of them to be group leader and construct x from combination of x_i. For the selection of group leader, any available efficient group leader election mechanism in the networks can be used.

4.2.2. TRM Installation. Only DMV is authorized to install the TRM in the vehicle for the first time after purchase or repurchase. The owner of the vehicle has to personally visit the DMV for the installation and/or initialization of the TRM. After confirming the credentials of the vehicle and its owner, DMV initializes TRM and saves the system parameters in the TRM including $(\mathbb{G}, q, P, \mathrm{PK}^+, c_V, \mathrm{inc}_V)$. Additionally DMV also preloads TRM with vehicle's individual secret key K_V and pseudonym generation key K_{sym}.

4.2.3. Pseudonyms Assignment. DMV generates n number of pseudonyms for each vehicle by taking vehicle's secret counter c_V and increments it by vehicle V's incrementing factor inc_V. The pseudonym is a complex value that also contains trapdoor for revocation. The format of generic pseudonym is given by $\mathrm{PS}^i_{\mathrm{OBU}} = \{(\alpha)_{K_{\mathrm{sym}}} \parallel (\alpha \oplus \mathrm{ID})_{K_V} \parallel n_i\}_{K^-_{\mathrm{DMV}}}$, where $\alpha = c_V + n_i \cdot \mathrm{inc}_V$, n_i is the current count of generated pseudonym (note that it may not be linear), and ID is the vehicle's identity. Then DMV stores these pseudonyms in its database and indexes it with the value of n. After all pseudonyms are generated for the vehicles, DMV saves these pseudonyms in vehicle's TRM along with another value $X_{\mathrm{OBU}} = h(\mathrm{PS}^1_{\mathrm{OBU}} \parallel \mathrm{PS}^2_{\mathrm{OBU}} \parallel \cdots \parallel \mathrm{PS}^n_{\mathrm{OBU}})$ and sends the anonymous pseudonyms to RAs as well. In order to help in revocation, TRM also encrypts both K_{sym} and K_V and sends it to RAs which serve as a trapdoor in revocation. The aforementioned keys are encrypted with public master key using ElGamal encryption as follows:

$$\begin{aligned} \delta_1 &= rP, \\ \delta_2 &= \left(K_{\mathrm{sym}} \parallel K_V\right) \oplus H\left(r\mathrm{PK}^+\right). \end{aligned} \tag{1}$$

r is a random nonce selected by the TRM for this encryption, then it sends $\{\delta_1, \delta_2\}$ to RAs. However, RAs can only decrypt the keys K_{sym} and K_V when they have a warrant to do so after colluding to construct x from individual x_i. The reason for saving encrypted keys in RAs database is twofold: RAs use these keys to revoke a vehicle in case of any dispute and for privacy reasons; we do not want RAs to link pseudonyms and/or extract c_V and inc_V from the beacons until necessary, otherwise.

It is also to be noted that when a vehicle consumes all the pseudonyms it has in the pseudonym pool, it needs to obtain a batch of fresh pseudonyms from the DMV. The vehicle does not need to be physically present at DMV, rather it can obtain the pseudonyms from DVM by connecting through Internet. We assume that the existing pseudonym refilling strategies can be used [27–30]. Now we outline the two mechanisms for mutual authentication and billing.

4.3. Direct Mutual Authentication (DMA). In the direct approach, OBU and CP mutually authenticate each other without the intervention of CSPA. First of all, CSPA creates l number of master secret keys MSK based on hash chain by selecting a secret s, where $\mathrm{MSK}_i = h^i(s)$ and sends the key to DMV as follows:

$$\mathrm{CSPA} \longrightarrow \mathrm{DMV} : \mathrm{MSK}_i \quad (i = 1, 2, 3, \ldots, l). \tag{2}$$

MSK_i is a hash chain-based master secret key which is based on a secret s and $\mathrm{MSK}_l = h^l(s)$. In other words, each MSK_i is used for a designated amount of time, and CSPA updates MSK_i after regular intervals. Since MSK_i is distributed by CSPA, it can be updated in timely manner by CSPA and vehicles will receive the updated MSK_i in their next registration phase with CSPA. After that, DMV also sends X_{OBU} of the registered vehicles to CSPA for records

$$\mathrm{DMV} \longrightarrow \mathrm{CSPA} : X_{\mathrm{OBU}}. \tag{3}$$

Each vehicle has a pool of legitimate traceable pseudonyms from DMV and at the time of authentication, any pseudonym from the pool can be used to start charging. The vehicle will be billed based on the used pseudonym.

4.3.1. Vehicle Registration with CSPA. The vehicle, most precisely its OBU, must register with CSPA before charging. We assume a secure channel between CSPA and the vehicle. The registration of the vehicle proceeds as follows. The vehicle starts with the already shared password and upon successful access, the CSPA calculates some security parameters for the vehicle and sends it back to the OBU. The different steps and their descriptions are given below:

(a) $\mathrm{OBU} \rightarrow \mathrm{CSPA} : \mathrm{PWD}_{\mathrm{OBU}}, X_{\mathrm{OBU}}$. OBU sends these values to CSPA on a secure channel. If $\mathrm{PWD}_{\mathrm{OBU}}$ is valid, then the protocol will proceed.

(b) CSPA calculates the following 3 values, that is, H_1, H_2, and H_3. H_1 is used as a secure parameter kept by CSPA. H_2 and H_3 are the authentication parameters that are sent back to the OBU

$$\begin{aligned} H_1 &= h\left(s \parallel X_{\mathrm{OBU}}\right), \\ H_2 &= h^2\left(s \parallel X_{\mathrm{OBU}}\right), \\ H_3 &= \mathrm{MSK}_i \oplus H_1. \end{aligned} \tag{4}$$

(c) CSPA registers the OBU by sending the hash function $h()$, H_2, and H_3 to the OBU and recording these parameters by storing them in its database against the value of X_{OBU}.

$\mathrm{CSPA} \rightarrow \mathrm{OBU} : X_{\mathrm{OBU}}, h(), H_2, H_3.$

4.3.2. Authentication between OBU and CP. After completing the registration phase with CSPA, when the vehicle passes through the section of the power line-enabled road, it starts authentication process with the charging plate. The vehicle starts the authentication process by selecting a pseudonym from its pool of pseudonyms. Then it starts the power receiving process with the selected pseudonym in an anonymous way. The partial per charging bill is prepared based

on the presented pseudonym in the authentication/charging process. It is to be noted that a fixed amount of electric power is delivered to the vehicle's power reception module and it costs the user a fixed amount. The comprehensive mutual authentication steps are given below:

(a) OBU selects a pseudonym $\mathrm{PS}^i_{\mathrm{OBU}}$, $i = 1, 2, 3, \ldots, n$, from its pool and calculates the following parameters:

$$\begin{aligned} c_1 &= h(H_2) \oplus \mathrm{PS}^i_{\mathrm{OBU}}, \\ c_2 &= h\left(\mathrm{PS}^i_{\mathrm{OBU}}\right) \oplus X_{\mathrm{OBU}}, \\ c_3 &= h\left(h\left(\mathrm{PS}^i_{\mathrm{OBU}}\right) \parallel c_2 \parallel H_3\right) \\ \delta_4 &= r_{\mathrm{OBU}} \oplus \mathrm{PS}^i_{\mathrm{OBU}}. \end{aligned} \tag{5}$$

(b) Then OBU sends CP, the values calculated in previous step along with H_3

$$\mathrm{OBU} \longrightarrow \mathrm{CP} : c_1, c_2, c_3, H_3, \delta_4. \tag{6}$$

(c) CP executes the following steps:

(i) Start with H_3 and extract the secret H_1 as $\mathrm{MSK}_i \oplus H_1 \oplus \mathrm{MSK}_i$.

(ii) It calculates H_2 from H_1 and extracts $\mathrm{PS}^i_{\mathrm{OBU}}$ from c_1.

(iii) CP also extracts r_{OBU} from δ_4 which is used in the construction of session key.

(iv) Then it checks for the value c_2 if it is equal to $h(\mathrm{PS}^i_{\mathrm{OBU}}) \oplus X_{\mathrm{OBU}}$.

(v) And it checks if c_3 is equal to the retrieved values $h(h(\mathrm{PS}^i_{\mathrm{OBU}}) \parallel c_2 \parallel H_3)$, then the OBU is authenticated; otherwise the authentication fails. It is to be noted that there will be a fixed number of tries, of which failing will halt the authentication process.

After successful authentication, OBU and CP initiate the protocol to construct a session key $\mathrm{SK}_{\text{OBU-CP}}$ which is used for the later communication and billing parameters. The initialization of session key from CP serves as an acknowledgment to authentication as well. The OBU would not have been authenticated, otherwise. At this point CP already extracted X_{OBU}, $\mathrm{PS}^i_{\mathrm{OBU}}$, and r_{OBU} from c_2, c_1, and δ_4, respectively. Now CP selects a nonce as r_{cp} and calculates session key as $\mathrm{SK}_{\text{OBU-CP}} = h(\mathrm{PS}^i_{\mathrm{OBU}} \parallel r_{\mathrm{OBU}} \parallel r_{\mathrm{cp}})$. CP also calculates the following parameters:

$$\begin{aligned} \mathrm{ID}_J &= h\left(r_{\mathrm{OBU}} \parallel \mathrm{ID}_{\mathrm{cp}}\right), \\ c_4 &= \mathrm{ID}_J \oplus r_{\mathrm{cp}}, \\ c_5 &= r_{\mathrm{cp}} \oplus h\left(h\left(\mathrm{PS}^i_{\mathrm{OBU}}\right)\right), \\ c_6 &= h\left(r_{\mathrm{cp}} \parallel c_4 \parallel c_5\right), \\ c_7 &= H_1 \oplus h^2\left(\mathrm{PS}^i_{\mathrm{OBU}}\right). \end{aligned} \tag{7}$$

$\mathrm{ID}_{\mathrm{cp}}$ is the ID of the charging plate. After calculating the above values, CP constructs an authentication reply message and sends it back to OBU. This authentication reply means that OBU has been authenticated and other parameters will be sent for the session key calculation. The following authentication reply message is sent to OBU:

$$\mathrm{CP} \longrightarrow \mathrm{OBU} : c_4, c_5, c_6, c_7. \tag{8}$$

From the above reply message, OBU extracts r_{cp} from c_4 and ID_J and checks if c_6 is equal to $h(r_{\mathrm{cp}} \parallel c_4 \parallel c_5)$. If the information is correct, then the OBU authenticates CP as well and computes the session key $\mathrm{SK}_{\text{OBU-CP}} = h(\mathrm{PS}^i_{\mathrm{OBU}} \parallel r_{\mathrm{OBU}} \parallel r_{\mathrm{cp}})$, extracts H_1 from c_7, and stores it as a security parameter.

At this point in time, the mutual authentication is completed and the electric power reception process will start based on the established session key $\mathrm{SK}_{\text{OBU-CP}}$.

When these two entities (OBU and CP) authenticate each other, then the vehicle will receive the designated amount of power from the road (CP). At the end of each phase of the charging plate at CP_i, a unit cost C_i will be accumulated to the account of the OBU against its presented $\mathrm{PS}^i_{\mathrm{OBU}}$. At the end of the whole power transfer from a number of charging plates, both OBU and CSPA will have the log of the amount of transferred power and the OBU will be billed accordingly which will be verifiable by both CSPA and the OBU. The whole authentication process in case of DMA is shown in Figure 4.

4.4. Pure Hash Chain-Based Authentication (PHA). For a fast moving vehicle, the DMA approach can be applied where computation is done locally by the charging plate; however, DMA may incur reasonable computation delay. Therefore, we propose another indirect authentication mechanism based on hash chain carried out by CSPA where computation delay is minimum whereas a small communication delay is introduced. Moreover this mechanism is most favorable for low speed vehicles. DMV provides the OBU with n pseudonyms $\mathrm{PS}^i_{\mathrm{OBU}}$, $i = 1, 2, 3, \ldots, n$, and hash chain corresponding to each pseudonym $h(\mathrm{PS}^i_{\mathrm{OBU}}), h^2(\mathrm{PS}^i_{\mathrm{OBU}}), \ldots, h^n(\mathrm{PS}^i_{\mathrm{OBU}})$. We assume that, for the sake of charging its battery, the vehicle registers with the CSPA based on some designated policy. In other words, the car uses a new hash chain based on the designated interval in the policy. Authentication process takes place as follows:

(a) The vehicle registers with CSPA and sends one of the hash chain heads $h^n(\mathrm{PS}^i_{\mathrm{OBU}})$ to CSPA

$$\mathrm{OBU} \longrightarrow \mathrm{CSPA} : h^n\left(\mathrm{PS}^i_{\mathrm{OBU}}\right), X_{\mathrm{OBU}}, \mathrm{Cert}_{\mathrm{OBU}}. \tag{9}$$

(b) At the time of authentication and request for charging, the vehicle must provide CP with a member hash from the registered hash chain $h^{n-1}(\mathrm{PS}^i_{\mathrm{OBU}})$

$$\mathrm{OBU} \longrightarrow \mathrm{CP} : h^{n-1}\left(\mathrm{PS}^i_{\mathrm{OBU}}\right), X_{\mathrm{OBU}}. \tag{10}$$

(c) CP forwards this value to the CSPA

$$\mathrm{CP} \longrightarrow \mathrm{CSPA} : \mathit{timestamp}, h^{n-1}\left(\mathrm{PS}^i_{\mathrm{OBU}}\right), X_{\mathrm{OBU}}. \tag{11}$$

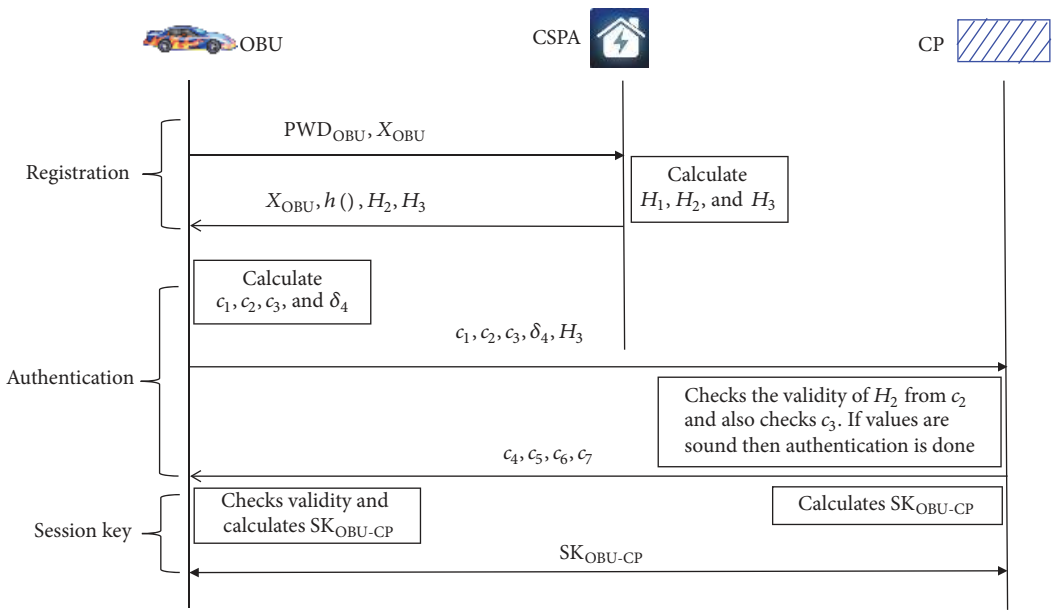


Figure 4: Authentication process in DMA scenario.

(d) CSPA validates the hash, checks if $h(h^{n-1}(PS^i_{OBU})) = h^n(PS^i_{OBU})$, and replies accordingly. CSPA also replaces $h^n(PS^i_{OBU})$ with $h(h^{n-1}(PS^i_{OBU}))$. In addition to authentication, CSPA also provides the CP with a session key SK_{OBU-CP} and saves it in its database with time and the X_{OBU}. It is to be noted that CSPA issues a single session key for all the plates for a particular vehicle and a particular hash chain

$$\begin{aligned} &\text{CSPA} \\ &\longrightarrow \text{CP} : \textit{Auth.Status}, SK_{OBU-CP}, \{SK_{OBU-CP}\}_{K^+_{OBU}}, \\ &\text{CP} \longrightarrow \text{OBU} : \{SK_{OBU-CP}\}_{K^+_{OBU}}. \end{aligned} \quad (12)$$

(e) If the authentication is successful, then charging plate will transfer the electric power to the vehicle; otherwise the process halts. It is to be noted that one hash chain is long enough to use it for the whole day. For the next day, the vehicles can register another hash chain. This process will still preserve the conditional privacy of the OBU.

The protocol for pure hash chain-based authentication mechanism is given in Figure 5.

4.5. Power Transfer, Billing, and Auditability. Once the mutual authentication is completed between the charging plate and OBU, the vehicle starts to receive the power from the road (CP) semisimultaneously with billing. More precisely, the vehicle is billed at the charging plate level. At the end of the charging process, the total bill is accumulated both at OBU and the CSPA. The process is explained in case of both direct and indirect authentication as shown in Figures 6 and 7, respectively.

4.5.1. Online Electric Power Transfer and Billing in DMA. In case of DMA, CSPA has access to the pseudonym used in the authentication process through CP. Therefore, after a successful authentication and establishment of a session key, vehicle requests for the electric power and presents the charging plate and CSPA with the pseudonym and other parameters for the billing purpose. The series of steps are given below:

$$\begin{aligned} &\text{OBU} \longrightarrow \text{CP} : \left\{\textit{timestamp} \parallel \textit{ChargingReq.} \parallel PS^i_{OBU} \parallel h_{K_V}(\alpha)\right\}_{SK_{OBU-CP}}, \\ &\alpha = \left(\textit{timestamp} \parallel \textit{ChargingReq.} \parallel PS^i_{OBU}\right), \\ &\text{CP} \longrightarrow \text{OBU} : \left\{\textit{Ack}, \textit{timestamp} \parallel PS^i_{OBU} \parallel h_{K_V}(\alpha)\right\}. \end{aligned} \quad (13)$$

At this point, CP starts billing and sends the bill log to OBU and to CSPA. The bill is logged against two values, X_{OBU} and the consumed pseudonym PS^i_{OBU},

$$\begin{aligned} &\text{CP} \longrightarrow \text{CSPA} : \\ &\left(\textit{timestamp} \parallel PS^i_{OBU} \parallel X_{OBU} \parallel Cost_{CP_i}\right), \\ &\text{CSPA} : Cost_{X_{OBU}} = \sum_{i=1}^{n} Cost_{CP_i}. \end{aligned} \quad (14)$$

In case of DMA, the CSPA accumulates all partial billing information from individual CPs and bill the OBU accordingly. It is worth noting that we use a constant cost per charging plate. For our current proposed scheme, we consider fixed energy transfer and fixed price per certain amount of transferred energy. These parameters can be set by the service provider(s). On part of service provider(s), fixed

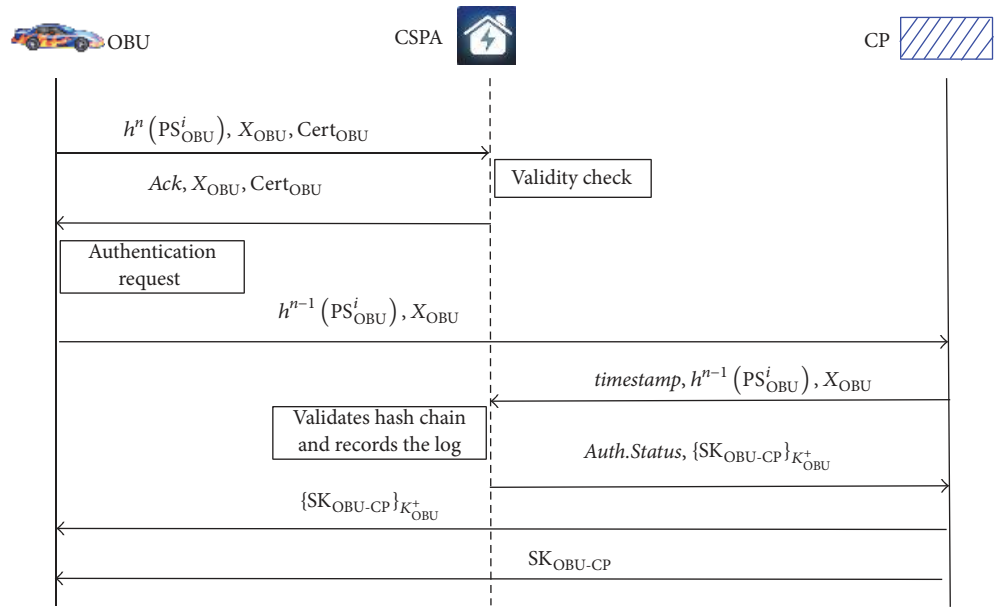


Figure 5: Authentication process in PHA scenario.

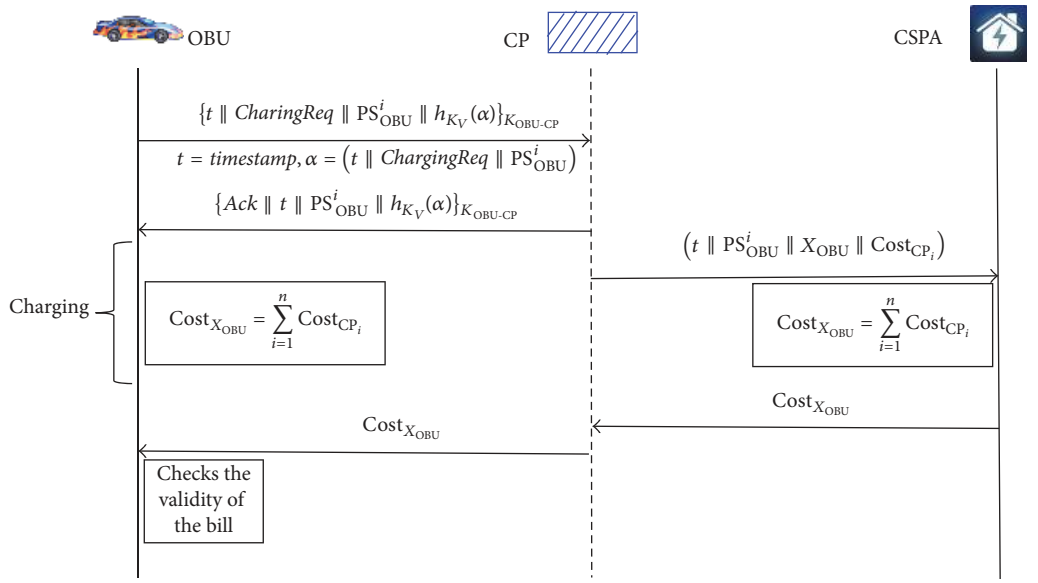


Figure 6: Power transfer and billing process in DMA scenario.

amount of energy transfer and thus fixed price would be easy to implement and faster, whereas, for customers, dynamic billing makes more sense. However, some tradeoff solution will suffice. In the current setup, if the price is fixed per unit, and the value/volume of unit is kept small, then we can compare this scheme with the dynamic billing. For instance, depending on the demand of the customers, x units of charge could be transferred to the customer and the customer will be billed accordingly. It is also worth noting that fixed billing mechanism will alleviate the problem of free-riders that would otherwise be possible in dynamic environment if the security keys are compromised.

4.5.2. Online Electric Power Transfer and Billing in PHA. In case of PHA, the CSPA does not have access to individual pseudonyms; rather it maintains the billing information based on the X_{OBU} value. After successful authentication, OBU requests for online power transfer and the power transfer begins. Meanwhile, CSPA bills the cost for the current CP and accumulates it to the account against X_{OBU}

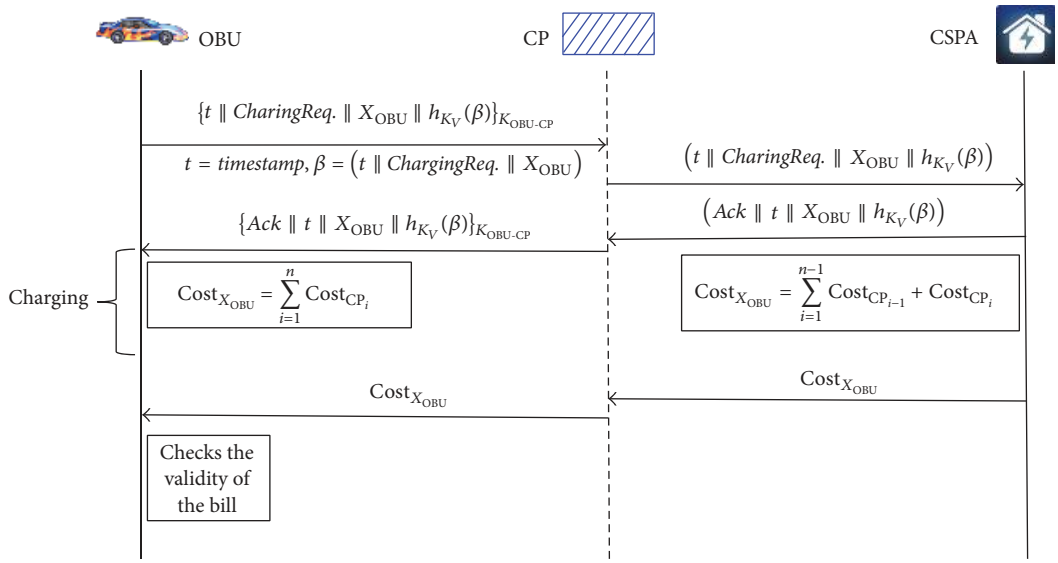


Figure 7: Power transfer and billing process in PHA scenario.

with timestamp information. The series of steps are given below:

$$\text{OBU} \longrightarrow \text{CP} : \left\{timestamp \parallel ChargingReq. \parallel X_{\text{OBU}} \parallel h_{K_V}(\beta)\right\}_{\text{SK}_{\text{OBU-CP}}}, \quad (15)$$

$$\beta = (timestamp \parallel ChargingReq. \parallel X_{\text{OBU}}).$$

The CP forwards the request to CSPA where CSPA constructs a reply message for the OBU. Meanwhile when CP receives the reply message from CSPA, the vehicle will start receiving power and CSPA will record the cost for the current charging plate

$$\text{CSPA} \longrightarrow \text{CP} : \left(timestamp \parallel X_{\text{OBU}} \parallel h_{K_V}(\beta)\right). \quad (16)$$

CP forwards the message to OBU accordingly whereas CSPA calculates the bill for current CP and accumulates with the partial bills from previous CPs

$$\text{CSPA} : \text{Cost}_{X_{\text{OBU}}} = \sum_{i=1}^{n-1} \text{Cost}_{\text{CP}_{i-1}} + \text{Cost}_{\text{CP}_i}. \quad (17)$$

This way, CSPA calculates the bill partially simultaneously with charging process which is the motive of our GHP game. We will discuss our OBU-CP game in the next subsection.

4.6. Revocation. In this subsection, we outline our efficient revocation mechanism.

The proposed protocol preserves the users' privacy; however in case of any misbehavior and/or bypassing the protocol, the users are subject to revocation. We incorporate an efficient revocation mechanism through which RAs can efficiently revoke the identity of the participating node. As we know the revocation functionality is distributed among a number of RAs rather than a single RA. These RAs share a part of the secret part of the share. When there is a need for revocation, the RAs collude, get a judicial warrant, and construct the secret from the shares. It is to be noted that RAs may select a session leader among them to carry out the decryption process. The encrypted keys K_{sym} and K_V are stored in RAs. When RAs obtain the secret x, they decrypt the aforementioned keys from ciphertext (δ_1, δ_2). In order to decrypt the encrypted keys, RA proceeds with the following steps.

Take the secret value x and calculate the following value:

$$\text{dec}((\delta_1, \delta_2), x) = \delta_2 \oplus H(x\delta_1). \quad (18)$$

By replacing δ_2 and δ_1 with the original values, we get

$$\begin{aligned} \text{dec}((\delta_1, \delta_2), x) &= \left(K_{\text{sym}} \parallel K_V\right) \oplus H\left(r\text{PK}^+\right) \\ &\quad \oplus H(x\delta_1), \\ \text{dec}((\delta_1, \delta_2), x) &= \left(K_{\text{sym}} \parallel K_V\right) \oplus H(rxP) \\ &\quad \oplus H(x\delta_1), \\ \text{dec}((\delta_1, \delta_2), x) &= \left(K_{\text{sym}} \parallel K_V\right) \oplus H(rxP) \\ &\quad \oplus H(rxP), \\ \text{dec}((\delta_1, \delta_2), x) &= \left(K_{\text{sym}} \parallel K_V\right). \end{aligned} \quad (19)$$

After decrypting the keys, RA takes the pseudonym in question and extract the trapdoor in it in order to revoke the node. As aforementioned, every pseudonym has the trapdoor value. RA decrypts $(\alpha)_{K_{\text{sym}}}$ and then decrypts $(\alpha \oplus \text{ID})_{K_V}$. Then RA extracts the ID from the value $\alpha \oplus \text{ID}$ that corresponds to the pseudonym in question. This way the pseudonym in question and hence the node are revoked by the RAs.

5. Security and Privacy Analysis

In this section, we prove that the proposed scheme satisfies the three security models.

5.1. Bidirectional Auditability. Secure bidirectional auditability is provided through semisimultaneous billing procedure incorporated into our proposed scheme. Each charging plate is capable of transferring a fixed amount of electrical energy to the battery and billing the vehicle with a fixed amount. Since vehicles use either individual pseudonyms $\mathrm{PS}^i_{\mathrm{OBU}}$ or the combined hash value X_{OBU}, the final bill is the combination of the costs of individual charging plates. Each OBU knows the cost per charging plate, and it records the cost in its log as well. Both CSPA and OBU can verify the individual and final bill of the power transfer in a liable and a nonrepudiate manner. It is also worth noting that it is the duty of CSPA to make sure of the freshness of the session key and use different session keys for different charging plates for security reasons. For session key update frequency and mechanism, existing techniques can be used. The behavior of both charging plate and OBU from security perspective is depicted by the game $\mathcal{G}$ where they establish NE during charging transaction. For the detailed description of bidirectional auditability game, please refer to the Appendix.

5.2. Conditional Privacy. Our proposed scheme also preserves conditional privacy of the users during electric power transferring and billing process. We do not use any real identity that could lead to the actual user; instead we use a series of legitimate pseudonyms.

Moreover in order to measure the privacy and the anonymity of the vehicles, we calculate the entropy of the user denoted by $\mathcal{H}$. The anonymity set needed for entropy calculation is, the set of active vehicles at the certain time t that are in the process of charging their batteries. Let U be the anonymity set and let p_{U_i} be the probability that the node U_i is the target vehicle whose anonymity is being calculated or U_i is under surveillance by adversary $\mathcal{A}$, where $\forall U_i \in U$, $\sum_{i=1}^{|U|} p_{U_i} = 1$. The entropy $\mathcal{H}$ of the target user U_i in the anonymity set U is given by $\mathcal{H} = -\sum_{i=1}^{|U|} p_{U_i} \times \log_2 p_{U_i}$. Since our anonymity set is U, the possible outcomes can be $|U|$ assuming the fair distribution and the probability of each outcome will be $1/|U|$. If the distribution is normal and the occurrence of the nodes to be related to the pseudonyms in question is equally likely, then the maximum entropy is also given by the following formula: $\mathcal{H}_{\max} = -\sum_{i=1}^{|U|} p_{U_i} \times \log_2 p_{U_i} = \log_2 p_{U_i}$.

Theorem 1. *Conditional privacy is always guaranteed by the proposed scheme and in case of any dispute, the node in question is revoked and the pseudonym in question is linkable to the actual user.*

Proof. In order to proceed with revocation, RAs get the warrant from the authorities and then look into the n values of the message in question that are provided to RAs in order to figure out which pseudonym was used. After that, RAs collude and construct x from individual x_i related to the pseudonym in question and the session leader decrypts the keys from ciphertext $c = \{\delta_1, \delta_2\}$ as follows: $\mathrm{PS}^i_{\mathrm{OBU}} = \delta_2 \oplus H(x\delta_1) = (K_{\mathrm{sym}} \parallel K_V) \oplus H(r\mathrm{PK}^+) \oplus H(rxP)$. When RAs decrypt the keys K_{sym} and K_V, then revocation is almost done, and what all RAs have to do is to decrypt the $(\alpha)_{K_{\mathrm{sym}}}$ and then extract ID of the vehicle from the pseudonym. □

Lemma 2. *It is hard to impersonate other OBUs in the process of online power transfer. In other words, it is hard to get away with billing procedures manipulation.*

Proof. Before starting the power transfer procedure, the vehicles have to register with CSPA in both direct and hash chain-based authentication and provide CSPA with X_{OBU}. And at the authentication stage, OBU has to provide the CP with c_1 and c_3 that contain H_2 and H_3, respectively. At the registration phase, H_2 is associated with the X_{OBU} of the current authenticating vehicle. Therefore, for any adversary $\mathcal{A}$ with H_2' without knowing the secret s, it will be hard to calculate valid c_1, c_2, and c_3 at the authentication phase. Thus the values sent to the CP for authentication will be c_1', c_2', c_3', and H_3' all of which must have association with the X_{OBU} of the pseudonym $\mathrm{PS}^i_{\mathrm{OBU}}$. Arguing on the collision resistance of the hash function used, it can be inferred that the probability of calculating the right values with not knowing the X_{OBU} is small (Section 5.3); therefore, it is hard for anybody to impersonate other OBUs with a pseudonym. □

The following corollary naturally follows.

Corollary 3. *Replaying the power transfer request message and/or pseudonym will not benefit the malicious intent of the user.*

The argument is divided into two parts. Replaying a message will result in the existence of previous power transfer records with this information. Upon successful power transfer, the CSPA maintains a log with timestamp and billing information against the used pseudonym. Let an OBU charge its battery at CP_x at particular time t_i after successful authentication, and the log is recorded at CSPA with the used pseudonym and other credentials. At t_{i+j}, the OBU again uses the message, then there are two possibilities. First, the OBU must have already been authenticated before sending this message; in that case, it will receive the power accordingly; secondly if it is not authenticated, then CSPA must have figured out that the record already existed and that the OBU was malicious. In either case, the OBU cannot benefit from such behavior. The same argument stands for the pseudonym as well.

5.3. Mutual Authentication. The most basic security requirement of our proposed scheme is mutual authentication between charging plate and OBU. With our proposed lightweight authentication protocol which is an extended version of Chuang and Lee's [17] protocol, mutual authentication is guaranteed before starting the charging process. Our proposed scheme at its essence is based on hashing and XOR functions. We assumed that the hash function has the

Table 1: Computation cost incurred by different operations.

Operation	Cost		
	$T_{\text{auth-OBU}}$	$T_{\text{auth-CP}}$	CSPA
Direct authentication	$3H + 2EO$ 2.28 μsec	$6H + 5EO$ 4.56 μsec	—
Hash chain-based authentication	$1D$	—	$1H + 1E$
Revocation	$T_{\text{rev}} = 1.56 + 2(T_\gamma + T_H + T_{\text{dec}})$		

collision resistance and the one-wayness properties. Hence, the hash function satisfies following definition [31].

Definition 4 (collision resistance one-way hash function). On input$(m, 1^*)$, for a deterministic polynomial-time algorithm A, every positive polynomial $p(\cdot)$, and all sufficiently large n's, a function $f : \{0,1\}^* \to \{0,1\}^n$ satisfies the following probability:

$$\begin{aligned}&\Pr\left[A\left(f\left(m\right), 1^n\right) \in f^{-1}\left(f\left(m\right)\right)\right]\\ &= \Pr\left[f\left(m\right) = f\left(m'\right)\right] < \frac{1}{p\left(n\right)},\end{aligned} \tag{20}$$

where m' is another input of f.

In the proposed scheme, each authentication interval contains 9 hash values. An attacker may try to pass the authentication session without any information. In this case, the attacker has to generate exactly same 9 values. The probability of success for this kind of attack is given by

$$\prod_{i=1}^{9} \Pr\left[A\left(f\left(m_i\right), 1^n\right) = U_i\right] < \frac{1}{9 \cdot p\left(n\right)}, \tag{21}$$

where U_i is input of the algorithm A, and it is chosen by the attacker. Since the probability is a negligible if n is large enough, hence our proposed authentication can be considered secure. However, the effect of keys compromise can be critical for our proposed scheme. From the OBU perspective, compromising K_V does not have dire consequences because the adversary $\mathcal{A}$ can get only a part of pseudonym, not the whole pseudonym. In case of compromising both K_{sym} and K_V, $\mathcal{A}$ can not only manipulate pseudonyms, but can also reuse them. Moreover our system can prevent the secret sharing attack because a vehicle must authenticate itself prior to charging its battery. Since the charging plate authenticates the user, therefore, two users cannot use the same secret and/or reuse it because timestamp and the local log of the usage of charging plate or CSPA will stop the vehicles from doing so. In other words, the protocol must follow these steps: (i) registration, (ii) authentication, and (iii) power transfer.

6. Evaluation

6.1. Computation and Communication Overhead. In this subsection, we consider the computation and communication overhead incurred by the OBU and CP in the process of mutual authentication and power transfer. Table 1 shows the computation overhead incurred by our proposed scheme and Table 2 outlines the communication overhead incurred by our proposed scheme. In the computation overhead, we consider the authentication cost incurred by OBU and CP denoted by $T_{\text{auth-OBU}}$ and $T_{\text{auth-CP}}$, respectively, and the cost of revocation denoted by T_{rev} in the direct authentication method. When OBU mutually authenticates with CP, it performs $3H + 2EO$ operations, where H denotes the *hash operation* and EO denotes the *exclusive OR* operation. CP performs $6H + 5EO$ operations. The cost of revocation T_{rev} in our proposed scheme is given by

Table 2: Communication cost incurred by the proposed scheme.

Operation	Cost
DMA	$71 + u$
PHA	135 bytes

$$T_{\text{rev}} = 2T_\gamma + 2T_{\text{mul}} + 2T_H + 2T_{\text{dec}}. \tag{22}$$

T_γ is the time incurred by the pseudonym search table, T_{mul} is the time required for point multiplication, T_H is the time required to calculate hash, and T_{dec} is the time required for symmetric decryption. In [26], T_{mul} is found for a supersingular curve with embedding $k = 6$ over $\mathbb{F}_{3^{97}}$ to be equal to 0.78 ms. Hence the above equations can be written as

$$T_{\text{rev}} = 1.56 + 2\left(T_\gamma + T_H + T_{\text{dec}}\right). \tag{23}$$

We also discuss the authentication processing time by both OBU and CP. According to [17], $SHA2$ hash operation takes 0.76 μsec. Therefore, OBU takes about 2.28 μsec and CP takes about 4.56 μsec. It is worth noting that since the XOR operation time is usually a single clock on CPUs which is infinitesimally small, therefore, we ignore it. In case of the hash chain-based authentication, OBU cost is only $1D$, where D denotes the decryption operation. CSPA incurs $1H + 1E$, and E is the encryption operation.

We also calculate the authentication overhead. In case of DMA, the communication overhead is equal to $71 + u$, where u is the size of the pseudonym. We assume $SHA{-}512$ as a hash function and consider the [32] implementation of timestamp which is 6 bytes. Similarly, in case of PHA the communication overhead is fixed and incurs 135 bytes where timestamp is 6 bytes, *ChargingReq.* is 1 byte, X_{OBU} is 64 bytes, and $h_{K_V}(\beta)$ is also 64 bytes.

6.2. Comparison with Existing Mechanisms. To the best of our knowledge, the most relevant work to our proposed

scheme is [24]. We compare our proposed scheme with [24] from performance, modeling, efficiency, and number of messages. Li et al. used cryptographic techniques to provide authentication between moving vehicles and charging pads. Furthermore, the length of the charging pad is 0.4 m in [24]. It is worth noting that keeping the length of the charging plate too short will not only increase the authentication overhead, but also make it difficult to manage the billing. Our proposed scheme on the other hand does not use cryptographic primitives for authentication and therefore with only XOR and hash operations, our proposed scheme clearly outperforms [24]. Additionally, in order to perform authentication, OBU and CP have to exchange 5 messages whereas 9 messages are exchanged in [24] during authentication. The speed is also a crucial factor to consider in [24]. With such a short charging pad, the vehicles will have no choice but to move slow on the charging pad to complete authentication.

6.3. Length of Charging Plate. The efficiency of the power transfer and the auditability depends upon the length of the charging plate. Therefore, the length of the charging plate must be a tradeoff between the authentication and billing delay and the time required to acquire the specified amount of electrical power from the charging plate. The plate should not be too short where a vehicle cannot receive the promised amount of power after spending most of the time on the authentication and billing. Similarly the plate should not be too long, where mutual auditability is at stake and semisimultaneous audit is not possible. To date, the size of the segment is not fixed; however, OLEV project considers the length of the segment to be 5 m which is still controversial because of the authentication and billing overhead incurred by the number of segments. Another important point is that the length of the segment is a design feature where the amount of electrical power, authentication and billing delay, and the time to acquire the guaranteed charge should be taken into account. In our scenario, we argue that the authentication delay incurred by both OBU and charging plate is less than a microsecond (optimistically) due to the design of authentication scheme. Therefore, the uniformity of the pickup devices installed in the vehicles and the capacity of delivering electrical power by the charging plates will play a vital role in deciding the length of the plate.

6.4. Discussion. In this subsection, we analyze the effect of the two authentication strategies on the efficiency and the design parameters. In DMA, OBU and CP have to perform relatively more operations as compared to PHA; nevertheless the time consumed by these operations (hash and XOR) is less than encryption operation. That is why we argue that, in performance, DMA will outperform PHA. Secondly, in DMA, both parties are involved in setting up the session key with mutual agreement. The communication cost is minimum since OBU and charging plate are communicating directly. Therefore, the only parameter that could affect the performance of DMA and PHA is the length of the charging plate. If we consider the normal speed of the vehicle, then PHA will favor the lengthier charging plate than DMA, because of the communication delay incurred by the PHA. On the other hand, PHA does not cost any computation delay because the processing is carried out at resource rich CSPA and charging plate is only used as intermediary bridge between vehicles and CSPA. However, in case of PHA, the session key is constructed by one entity, CSPA. Moreover OBUs must save the hash chain of the currently used pseudonyms in the onboard storage thereby incurring storage cost. Therefore, we can argue that these two methods can be used in different circumstances that fit the necessary conditions for direct and hash-based authentication. For normal scenarios, DMA will be the fair choice because of its security, auditability guarantee, and robustness.

7. Conclusion and Future Directions

In this paper, we proposed a secure, privacy-aware, and bidirectional auditable mechanism for wireless power transfer in online electric vehicles. The power transfer technology is installed under the road in the form of charging plates where a segment of the road constitutes a charging plate containing a hardware module for communication and lightweight computation. In our proposed scheme, the vehicles use multiple pseudonymous strategy to mutually authenticate with the charging plate and then expedite the power transfer. Meanwhile electric power service provider bills the vehicles on per charging palate basis. Our proposed scheme provides secure and privacy-aware bidirectional auditability where the billing process is verifiable by both parties. Moreover we also present the game theoretic approach to validate the bidirectional auditability.

In the future, we aim to implement the system to have a deeper insight into the performance issues. Moreover we also aim to relax the assumption of fixed per-plate charging cost. We will focus on a more robust mechanism where the vehicles will have choice to buy the charge according to their convenience. We will address the complexity involved in such robust charging and its billing mechanism.

Appendix

A. Bidirectional Auditability Game

We formalize the bidirectional auditability as an instance of the Guest-Host problem (GHP) with game theoretic approach. In the GHP, a guest wants to use the hotel for a few days and does not want to get a bill (no) greater than the actual use, whereas the host wants to charge the bill to the guest for the actual (or more) use but wants to make sure that the guest does not deny the actual use. In our scenario, OBU can be assumed as guest and the charging plate as the host.

We explain the bidirectional auditability between OBU and charging plate with the help of an uncooperative game $\mathcal{G}$ which is defined as a triplet $(\mathcal{P}, \mathcal{S}, \mathcal{PO})$. $\mathcal{P}$ is the set of players of the game, $\mathcal{S}$ is the set of strategies followed by the players, and $\mathcal{PO}$ is the set of payoff functions as a result of the players' strategies.

A.1. Players. The set of players $\mathcal{P} = \{\text{OBU}, \text{CP}\}$ corresponds to the set of OBUs and the CP. There can be multiple OBUs

serviced by the CP, but we assume that, at certain instant of time, only single OBU will be entertained at the start of the CP. Without loss of generality, multiple OBUs can recharge their batteries after successful authentication.

A.2. Strategy/Move. In our game, each of the two players follows two strategies, either *Cooperate* (C) or *Deviate* (D), and thus $S_i = \{C, D\}$. Moreover in cooperation state, each player makes a move that produces a better payoff. By cooperating, a vehicle changes its pseudonym every time it charges the battery and the CP bills it accordingly, whereas, in case of deviation, OBU misbehaves and does not follow the protocol or CP overcharges the bill against OBU.

A.3. Payoff Function. We formulate a payoff function for both players of the game. The payoff function $\mathcal{PO}(t)$ is given by

$$\mathcal{PO}_i(t) = a_i(t) - \text{cost}_i(t). \quad \text{(A.1)}$$

$a_i(t)$ is the advantage of player i at time t and $\text{cost}_i(t)$ is the cost of achieving $a_i(t)$. It is to be noted that $a_i(t)$ depends upon the successful battery charging and the normal billing and $\text{cost}_i(t)$ depends upon the pseudonym change for charging and the authentication overhead for both CP and OBU.

In game $\mathcal{G}$, the players do not know the strategic behavior of the opponent unless the complete billing has been done. Since we have only two strategic behaviors from the set $S_i = \{C, D\}$, there is 50% probability for the players to guess the behavior of the opponent keeping in mind its payoff.

Definition A.1. The best response $\text{br}_i(S_{j\in[C,D]})$ on the part of a player i is a move such that

$$\text{br}_i\left(S_{j\in[C,D]}\right) = \max\left(\mathcal{PO}_i\left(s_i\right)\right). \quad \text{(A.2)}$$

In other words, the best response of a player i will be such that it results in a maximum payoff. If the two players unknowingly strategically give best responses to each other in the game, then the opponent will not have any chance to deviate from the game and the result of the game is called Nash Equilibrium (NE). When the game reaches an NE, then the players cannot increase their payoff by changing their strategy or deviating from the best response strategy.

A.4. Nash Equilibrium in $\mathcal{G}$. In NE, every player plays its best response and correctly anticipates that its opponent will do the same. In Table 3, we outline the possible moves made by each player.

In our game, there is only one NE which is achieved through (C, C). It is worth noting that a game may have more than one Nash Equilibrium depending upon the nature of the game. In our game, the best strategy for OBU is to choose "C" no matter what charging plate chooses between "C" and "D". This is because the only way for OBU to maximize its payoff in the form of battery charge and fair billing is to choose "C" at the expense of the cost incurred by changing pseudonym and shared authentication overhead. OBU may not know the strategy of the charging plate. The "D" strategy will cause the loss which is unfair auditability leading to revocation for both CSPA and the OBU. Therefore, from the strategic Table 3, $(1, 1)$ is the best response from both sides, where they cannot increase their payoff by changing their strategy.

Table 3: Strategic moves of the players in the game $\mathcal{G}$.

OBU	CP	
	C	D
C	1, 1	1, 0
D	0, 1	−1, −1

Notations

$\mathbb{G}$:	Cyclic group of order q
P:	The generator of $\mathbb{G}$
r_x:	Random nonce from entity x
x, x_i:	Private master key and ith share of x
PK^+:	Public key corresponding to x
K^+_{DMV}, K^-_{DMV}:	Public private key pair of DMV for signing pseudonyms
c_V:	Vehicle V's secret initial counter used in pseudonym generation
inc_V:	Incrementing factor for pseudonyms
K_{sym}:	Vehicle V's AES symmetric key used in pseudonym generation
K_V:	V's individual secret key
PS^i_{OBU}:	Vehicle V's ith pseudonym
MSK:	Hash chain-based master secret key
X_{OBU}:	Hash of the overall pseudonym pool
Cert_{OBU}:	OBU's anonymous certificate issued by a certification authority
PWD_{OBU}:	OBU's initial password to log in to the system in order to start registration
$H(\cdot)$:	A MapToPoint hash function as $H : \{0, 1\}^* \to \mathbb{G}$
$h(\cdot)$:	Collision-resistant hash function
$\oplus$:	Exclusive OR operation
$\|$:	Concatenation function.

Disclosure

The preliminary version of this paper was published in Proceedings of the IEEE 11th International Conference on Mobile Ad-Hoc and Sensor Networks (MSN 2015) [10]. The funding sponsors had no role in the design of the study; in the simulations, analyses, or interpretation of results; in the writing of the manuscript; and in the decision to publish the results.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this manuscript.

Acknowledgments

This work was supported by the National Research Foundation of Korea (NRF) grant funded by the Korean government (MSIP: Ministry of Science, ICT & Future Planning) (no. 2016M2A8A4952280). This work was supported by the Soonchunhyang University Research Fund.

References

[1] J. Romm, "The car and fuel of the future," *Energy Policy*, vol. 34, no. 17, pp. 2609–2614, 2006.

[2] S. Li and C. C. Mi, "Wireless power transfer for electric vehicle applications," *IEEE Journal of Emerging and Selected Topics in Power Electronics*, no. 99, 2014.

[3] J. Timpner and L. Wolf, "Design and evaluation of charging station scheduling strategies for electric vehicles," *IEEE Transactions on Intelligent Transportation Systems*, vol. 15, no. 2, pp. 579–588, 2014.

[4] G. Li and X. Zhang, "Modeling of plug-in hybrid electric vehicle charging demand in probabilistic power flow calculations," *IEEE Transactions on Smart Grid*, vol. 3, no. 1, pp. 492–499, 2012.

[5] F. Musavi, M. Edington, and W. Eberle, "Wireless power transfer: A survey of EV battery charging technologies," in *Proceedings of the 4th Annual IEEE Energy Conversion Congress and Exposition, ECCE 2012*, pp. 1804–1810, September 2012.

[6] H. Zhu, Y. Zhao, S. Ding, and B. Jin, "An improved forward-secure anonymous RFID authentication protocol," in *Proceedings of the 7th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM '11)*, pp. 1–5, September 2011.

[7] K. Dietrich, "Anonymous rfid authentication using trusted computing technologies," in *Radio Frequency Identification: Security and Privacy Issues, ser. Lecture Notes in Computer Science*, S. Ors Yalcin, Ed., vol. 6370, pp. 91–102, Springer, Berlin Heidelberg, 2010.

[8] W. Xie, L. Xie, C. Zhang, Q. Zhang, and C. Tang, "Cloud-based RFID authentication," in *Proceedings of the IEEE International Conference on RFID*, pp. 168–175, May 2013.

[9] P. D'Arco and A. de Santis, "On ultralightweight RFID authentication protocols," *IEEE Transactions on Dependable and Secure Computing*, vol. 8, no. 4, pp. 548–563, 2011.

[10] 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.

[11] C. Weissinger, D. Buecherl, and H.-G. Herzog, "Conceptual design of a pure electric vehicle," in *Proceedings of the 2010 IEEE Vehicle Power and Propulsion Conference, VPPC 2010*, September 2010.

[12] A. Hoke, A. Brissette, D. Maksimović, A. Pratt, and K. Smith, "Electric vehicle charge optimization including effects of lithium-ion battery degradation," in *Proceedings of the 7th IEEE Vehicle Power and Propulsion Conference (VPPC '11)*, pp. 1–8, September 2011.

[13] Y. J. Jang, Y. D. Ko, and S. Jeong, "Optimal design of the wireless charging electric vehicle," in *Proceedings of the 2012 IEEE International Electric Vehicle Conference (IEVC '12)*, pp. 1–5, March 2012.

[14] Y. D. Ko and Y. J. Jang, "The optimal system design of the online electric vehicle utilizing wireless power transmission technology," *IEEE Transactions on Intelligent Transportation Systems*, vol. 14, no. 3, pp. 1255–1265, 2013.

[15] I.-S. Suh and J. Kim, "Electric vehicle on-road dynamic charging system with wireless power transfer technology," in *Proceedings of the 2013 IEEE International Electric Machines and Drives Conference (IEMDC '13)*, pp. 234–240, May 2013.

[16] D. Huang, S. Misra, M. Verma, and G. Xue, "PACP: An efficient pseudonymous authentication-based conditional privacy protocol for VANETs," *IEEE Transactions on Intelligent Transportation Systems*, vol. 12, no. 3, pp. 736–746, 2011.

[17] M.-C. Chuang and J.-F. Lee, in *Proceedings of the International Conference on Consumer Electronics, Communications and Networks (CECNet)*, pp. 1758–1761, April 2011.

[18] L.-Y. Yeh and J.-L. Huang, "PBS: a portable billing scheme with fine-grained access control for service-oriented vehicular networks," *IEEE Transactions on Mobile Computing*, vol. 13, no. 11, pp. 2606–2619, 2014.

[19] H. Zhu, X. Lin, R. Lu, P.-H. Ho, and X. S. Shen, "SLAB: A secure localized authentication and billing scheme for wireless mesh networks," *IEEE Transactions on Wireless Communications*, vol. 7, no. 10, pp. 3858–3868, 2008.

[20] H.-Y. Lee and Y.-B. Lin, "Credit pre-reservation mechanism for UMTS prepaid service," *IEEE Transactions on Wireless Communications*, vol. 9, no. 6, pp. 1867–1873, 2010.

[21] L.-Y. Yeh and Y.-C. Lin, "A proxy-based authentication and billing scheme with incentive-aware multihop forwarding for vehicular networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 15, no. 4, pp. 1607–1621, 2014.

[22] X. Zhao, J. Lin, and H. Li, "Privacy-preserving billing scheme against free-riders for wireless charging electric vehicles," *Mobile Information Systems*, vol. 2017, no. 1325698, Article ID 1325698, p. 1, March 2017.

[23] N. Saxena and B. J. Choi, "Authentication Scheme for Flexible Charging and Discharging of Mobile Vehicles in the V2G Networks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 7, pp. 1438–1452, 2016.

[24] H. Li, G. Dán, and K. Nahrstedt, "Portunes+: privacy-preserving fast authentication for dynamic electric vehicle charging," *IEEE Transactions on Smart Grid*, vol. 8, no. 5, pp. 2305–2313, 2017.

[25] Z. Zhang, K. T. Chau, C. Qiu, and C. Liu, "Energy encryption for wireless power transfer," *IEEE Transactions on Power Electronics*, vol. 30, no. 9, pp. 5237–5246, 2015.

[26] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, "An efficient identity-based batch verification scheme for vehicular sensor networks," in *Proceedings of the in INFOCOM, 2008*, pp. 246–250, 2008.

[27] Z. Ma, F. Kargl, and M. Weber, "Pseudonym-on-demand: A new pseudonym refill strategy for vehicular communications," in *Proceedings of the IEEE 68th Vehicular Technology Conference*, pp. 1–5, September 2008.

[28] J. Benin, M. Nowatkowski, and H. Owen, "Unified pseudonym distribution in VANETs," in *Proceedings of the 6th Annual IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob '10)*, pp. 529–533, October 2010.

[29] J. Petit, C. Bosch, M. Feiri, and F. Kargl, "On the potential of PUF for pseudonym generation in vehicular networks," in *Proceedings of the 2012 IEEE Vehicular Networking Conference (VNC '12)*, pp. 94–100, November 2012.

[30] M. M. E. A. Mahmoud, S. Taha, J. Misic, and X. Shen, "Lightweight privacy-preserving and secure communication protocol for hybrid Ad Hoc wireless networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 8, pp. 2077–2090, 2014.

[31] O. Goldreich, *Foundations of Cryptography*, Cambridge University Press, 2001.

[32] J. Harri, F. Filali, and C. Bonnet, "Rethinking the overhead of geo-localization information for vehicular communications," in *Proceedings of the 2007 IEEE 66th Vehicular Technology Conference, VTC 2007-Fall*, pp. 2111–2115, October 2007.