A New Privacy-aware Mutual Authentication Mechanism for Charging-on-the-Move in Online Electric Vehicles

Rasheed Hussain*, Donghyun Kim†, Michele Nogueira‡, Junggab Son†, Alade O. Tokuta†, Heekuck Oh*
* Department of Computer Science, Innopolis University, Kazan, Russia.
Email: r.hussain@innopolis.ru
† Department of Mathematics and Physics, North Carolina Central University, Durham, USA.
E-mail: donghyun.kim@nccu.edu
‡ Department of Informatics, Federal University of Paraná, Curitiba, Brazil.
E-mail: michele@inf.ufpr.br
§ Department of Computer Science and Engineering Hanyang University, Ansan, South Korea.
Email: hkoh@hanyang.ac.kr

Abstract*—Recently a new concept of online electric vehicle (OLEV) has been introduced in South Korea, where vehicles are propelled through the transmitted energy from the infrastructure installed underneath the road. However, for billing and audit reasons only authentic vehicles with necessary credentials are allowed to charge their batteries and pay the designated amount to the service provider. Moreover, due to the massive budget requirements for such infrastructure, only designated road segments will offer the charging service. As a result, a tradeoff solution to the charging of electric vehicles is needed to both fulfill the charging requirements of the electric vehicles and reduce the upfront costs for the service providers. To obtain electric charge from the charging plates beneath the road, vehicles need to authenticate themselves beforehand for twofold purposes: to bill the vehicles accordingly and to let the revocation authorities revoke the vehicle in case of a dispute. In this paper, we use the core concept of the OLEV and introduce extreme lightweight privacy-aware authentication schemes for charging-on-the-move through the charging plates installed under the road. More precisely we propose two mutual authentication mechanisms between charging plates and the vehicles, a direct authentication and a hash chain-based authentication. In the direct authentication scheme, we leverage multiple pseudonyms for conditional privacy. Vehicles use different pseudonyms every time they use the charging-on-the-move service. Whereas in case of hash chain-based authentication mechanism, the vehicles mutually authenticate with charging plates through service provider. Our proposed authentication mechanisms preserve conditional privacy throughout the protocol and is computationally lightweight than the existing mechanisms.

***Index Terms*—VANET, Electric Vehicle, Wireless Charging, Privacy, Auditability**

I. Introduction

With the advent of alternative fuel vehicle (AFV), it was speculated that the mass production of AFVs would become a showstopper for the industry because of its potential problems, meeting consumer satisfaction, and the low return on investment (RoI) [1]. The problem at that time was that AFV did not outperform conventional fuel cars. However with the advancement in automotive, electronics, and communication technologies, today AFVs can be seen pervading highways. The need for alternative fuel can be realized from many dimensions, economy and environment are of paramount significance among those dimensions. Fuel prices are going high with time and the carbon dioxide (CO_2) emission caused by the fuel is polluting the environment. Therefore, the pressure for reduction in the greenhouse gases has surged the momentum in producing hybrid and electric vehicles.

The milage and cruising range of hybrid and pure electric vehicles is less than that of internal combustion engine vehicles. Therefore the battery of the electric vehicles must be recharged frequently depending upon the commute of the consumers [2]. There are a number of commercial technologies available today to recharge the car battery ranging from plugged-in [3] to wireless charging technology [4]. Moreover to make this technology successful and popular among consumers, there must be charging stations in the nearby vicinities for consumer convenience. Nevertheless, this will create another front for consumer comfort, the users have to stop at the charging stations too often, to charge the car's battery. What future will bring is speculative, but at the moment installing too many charging stations has not been pursued.

To alleviate the aforementioned issues in electric and hybrid cars, a new concept of online electric vehicle (OLEV)[1] has been introduced by Korea Advanced Institute of Science and Technology (KAIST), where vehicles get power from the power-line installed beneath the road surface. OLEV uses a remote wireless charging mechanism where onboard battery is charged from the road segment where charging infrastructure is installed. Unlike conventional vehicles, OLEV functions in an online manner where it uses the power energy received from the power transmitter under the road to propel the vehicle on the road and a partial amount is used to charge the battery as well. OLEV can also be seen as a charging on the move technology and it addresses the previous concerns; however,

[1] http://olev.kaist.ac.kr/en/index.php

security, privacy, auditability, and fairness issues still need to be addressed. OLEV is a promising technology, however governments, power service providers, and legislators may be reluctant to use this technology on a wider range than a simple route-based mechanism due to the cost and security factors. Nevertheless, the wireless charging on the move technology will provide ease of access and comfort to EV users, provided that the security, privacy, auditability and other concerns are equally addressed.

Since the users who charge their batteries will need to pay for the charging to the service provider(s), therefore an efficient, privacy-aware, and an extreme lightweight authentication mechanism is needed so that the vehicles and the charging plates mutually authenticate each other before the charging begins. The authentication process will make sure that the right vehicle is billed to pay the charging cost and to let the revocation authorities revoke the vehicle in case of any dispute. In this paper, we aim at a tradeoff solution to the problems at two extremes. One extreme is the stop-and-charge strategy and another extreme is the online powered vehicle. We make use of the charging technology under the road like OLEV and use this as a charging-on-the-move mechanism. We particularly focus on the extreme lightweight authentication mechanism in the charging process of highly mobile and ephemeral electric vehicles. Our contribution in this work is given by:

1) Keeping in mind the resource constrained charging plates under the road, we propose two extreme lightweight mutual authentication mechanisms for vehicles to charge their batteries on the move.
2) To preserve conditional privacy, we leverage multiple pseudonymous approach where vehicles use different pseudonym in every charging cycle.
3) We avoid computationally expensive cryptographic primitives and use only XOR and hash-based primitives in the authentication protocols which greatly reduce the authentication overhead for both resource-constrained charging plates and onboard units (OBUs).

The structure of the rest of the paper is organized as follows. Section II outlines the state of the art regarding wireless power transfer followed by our problem formulation in section III. In section IV we propose our extreme lightweight authentication mechanisms for the wireless charging and analyze our system in section V. In section VI, we give our concluding remarks with future directions.

II. State of the Art

Today, a number of battery propelled vehicles can be seen on the roads. Such advancement is the result of the technological breakthrough in both electrification and the energy storage technologies. From the studied 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 [5]. Weissenger et al. [5] also outlined the speed range, storage range, and the battery types of vehicles as of 2008. To date, many efficient charging schemes have been proposed in the literature to save the commute time of the drivers [6]. 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 by Musavi et al. where the energy is transferred to the car battery through wireless medium [4]. Musavi et al. carried out a detailed survey regarding wireless power transfer and covered many dimensions such as the distance between the transmitting and receiving entity, cost of the technology and so forth. The concept of green car was introduced in 2009 by KAIST, South Korea by the name of online electric vehicle (OLEV) [7]. The motivation for OLEV was the weight of the battery in electric vehicles, frequent charging, installation and maintenance cost and so forth. To date, remarkable results have been achieved by this project and currently they run prototype buses in the KAIST campus South Korea [8], [9]. Nonetheless, such online vehicle would require massive power-line infrastructure installed under the road. Moreover coverage would be another issue due to cost factor. Therefore a tradeoff solution is essential to benefit from both ends.

In this paper, we propose a tradeoff solution to the currently available electric or hybrid vehicle to charge their batteries on the move. Moreover we address the security and privacy problem faced by such service delivery. In order to transfer the power from charging plates to the vehicles, proper billing mechanism should be in place so that the charging vehicles can be billed and audited accordingly. To make billing and auditing mechanism work, a proper efficient and privacy-aware fast authentication mechanism is essential. The mutual authentication mechanism between the highly mobile vehicles and the static charging plates must be suitable for the resource-constrained charging plates and OBUs. Therefore we propose an extreme lightweight privacy-aware mutual authentication mechanism between the vehicles and the charging plates installed under the road. Our proposed authentication mechanism serves as a baseline for the billing and auditing; however, we only focus on the authentication in this paper and leave the auditing and billing mechanism for future work. Our authentication mechanism consists of two sub-classes from robustness standpoint and provides the service providers with choice to execute one of the two authentication mechanisms based on designated scenarios. Moreover our proposed authentication mechanisms are secure, fast, efficient, and conditionally privacy-preserved.

III. Problem Formulation

In this section we outline the problem by formalizing the system participants, network model, security requirements of the system, and the assumptions on which we base our scheme.

A. System Participants

Our proposed model consists of mainly two participating authorities, VANET and power delivery. Power delivery service is exercised by the charging service providing authority (CSPA). VANET further consists of mobile vehicular nodes,

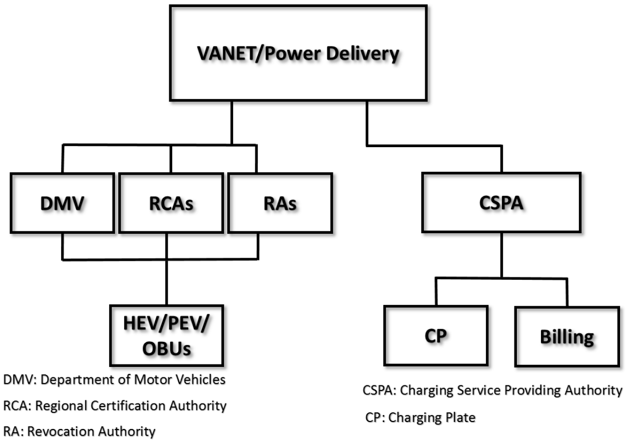

VANET/Power Delivery
DMV
RCAs
RAs
CSPA
HEV/PEV/ OBUs
CP
Billing
DMV: Department of Motor Vehicles
RCA: Regional Certification Authority
RA: Revocation Authority
CSPA: Charging Service Providing Authority
CP: Charging Plate

Fig. 1: Taxonomy of System Participants

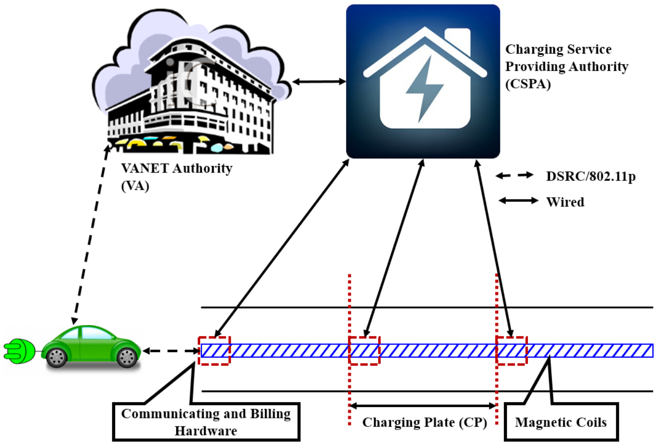

Charging Service Providing Authority (CSPA)
VANET Authority (VA)
DSRC/802.11p
Wired
Communicating and Billing Hardware
Charging Plate (CP)
Magnetic Coils

Fig. 2: Proposed Network Model

registration and revocation authorities. Department of motor vehicles (DMV) is at the top of the hierarchy where every VANET entity should be registered. Vehicular nodes are divided into three categories, combustion engine vehicles (CEVs), hybrid electric vehicles (HEVs), and pure electric vehicles (PEV). However we only focus on HEVs and PEVs in this paper. CSPA owns the hardware installed under the road that consists of the charging material (coils etc.) hereafter referred to as charging plates (CP). CP also has limited communication and computation capability. It is the role of CP to authenticate, bill, and log the OBU after charging, and send the billing log to both CSPA and OBU. However, in this paper we only focus on the efficient and fast authentication process for wireless charging-on-the-move. The Taxonomy of the system participants is shown in Fig 1.

B. Network Model

Our proposed network model is shown in Fig 2. We consider a typical VANET scenario with a fleet of HEVs and PEVs. HEVs and PEVs need to recharge their batteries multiple times a day, depending upon the usage of the vehicle. The charging technology for the batteries is installed under the road where each charging plate consists of additional communication and computation hardware. In order to bill the vehicles accordingly by the service providers and for the vehicles to make sure that they will get what they have paid for, mutual authentication is necessary between the vehicles and the charging plates. Moreover, the whole process right from authentication to billing should be anonymous for the vehicles because the users will not compromise on their privacy as a result of the charging service. Therefore before starting the charging process, vehicles and charging plates mutually authenticate each other. After successful authentication, the designated amount of energy is transferred to the battery and the vehicle is billed accordingly. CPs are connected to CSPA through high-speed backbone whereas the communication among vehicles, VANET authorities, and the CPs is carried out according to dedicated short range communication (DSRC) standard.

C. Security Requirements

The proposed secure and privacy-aware wireless charging mechanism must fulfill the following requirements.

SR-1 The conditional privacy of the charging entity's location and the user must be preserved during the authentication.
SR-2 Due to the resource constraints of the CP, the communication between CP and OBU, and between CP and CSPA must be minimal.
SR-3 The proposed mutual authentication between OBU and CP should be extremely lightweight keeping in mind the resource constraints of the CP.
SR-4 In case of any misbehavior and/or a dispute, revocation authorities should be able to revoke the culprit through an efficient revocation mechanism.

D. Assumptions

Our proposed scheme is based on the following assumptions:

1) VANET is incrementally deployed and a number vehicles (both HEV and PEV) are equipped with OBU and tamper-resistant module (TRM) to carry out the secure computation.
2) 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, CPs and OBUs are non-trustworthy.
3) Every vehicle is also pre-loaded with a pool of pseudonyms (traceable by revocation authorities) for privacy reasons.
4) CPs are equipped with hardware that is capable of lightweight secure computation and communication.
5) The charging process is not automatic and it can be started with the consensus of the driver if the battery needs to be recharged.

IV. Proposed Fast and Privacy-aware Mutual Authentication for EV Charging

In this section we outline our proposed mutual authentication scheme based on the foundations laid in the previous section. We start with the baseline for the proposed scheme and then describe the privacy-aware mutual authentication in detail.

A. Baseline

In VANET scenario, before using the wireless charging service, vehicles must register with DMV to initialize their TRM and stores security parameters and pseudonyms in it, and also register with CSPA to get the charging service on the move. Whenever a vehicle[2] enters the road section with charging capability, it opts for either charging or not charging. If the vehicle selects charging, then it has to mutually authenticate with the CP. We propose two very lightweight mutual authentication mechanisms, one is based on only hash and XOR functions and inspired from Chuang et al.'s scheme [10], while the second one is based on the hash chain. The former is a direct authentication between CP and OBU whereas the latter is authentication through CSPA. In the former scheme, CP incurs minimum communication delay whereas in the latter, CP incurs minimum computation delay. Both of the proposed scheme are suited for specific purposes that are explained in the next section. After successful authentication, the charging process starts and CP sends the billing information to both OBU and CSPA. The billing is fixed on per CP basis.

B. Preliminaries and Initializations

1) System Initialization: Notations in Table 1 will be used throughout the paper. We use pseudonymous approach for privacy preservation. In addition, in order to save the individual secret keys K_{sym} and K_V in the revocation authorities (RAs), we use ElGamal encryption algorithm over elliptic curve cryptography (ECC). 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 $x \in \mathbb{Z}_q^*$ as its private key and computes $PK^+ = xP$ as its public key. DMV then uses threshold based secret share scheme [11] and divides x into j parts where j is the number of revocation authorities, each RA_i holds a share x_i and $x_i \in (x_1, x_2, x_3, ..., x_j)$. 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.

2) TRM Installation: Only DMV is authorized to install the TRM in the vehicle for the first time after purchase or re-purchase. The owner of the vehicle has to personally visit 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 $(\mathbb{G}, q, P, PK^+, c_V, inc_V)$. Additionally DMV also preloads TRM with vehicles individual secret key K_V and pseudonym generation key K_{sym}.

TABLE I: Legend for symbolic notations

Notation	Explanation
$\mathbb{G}$	Cyclic group of prime order q
P	The generator of $\mathbb{G}$
r	Random nonce
x,x_i	Private master key and i-th 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
$H(\cdot)$	A MaptoPoint hash function as $H : \{0,1\}^* \rightarrow \mathbb{G}$
$h(\cdot)$	Collision-resistant hash function
$\oplus$	Exclusive OR operation
$\|\|$	Concatenation function

3) Pseudonyms Assignment: DMV generates n number of pseudonyms for each vehicle by taking vehicles secret counter c_V and increment it by vehicle V's incrementing factor inc_V. The pseudonyms are generated as follows: $PS^i_{OBU} = \{(\alpha)_{K_{sym}} \| (\alpha \oplus ID)_{K_V} \| n_i\}_{K^-_{DMV}}$ where $\alpha = c_V + n_i \cdot inc_V$, n_i is the current count of generated pseudonym (note that it may not be linear), and ID is the vehicular ID. 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 $X_{OBU} = h(PS^1_{OBU} \| PS^2_{OBU} \| ... \| PS^n_{OBU})$ 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 serves as a trapdoor in revocation. The aforementioned keys are encrypted with public master key using ElGamal encryption as follows:

$$\delta_1 = rP, \delta_2 = (K_{sym} \| K_V) \oplus H(rPK^+)$$

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 and collude 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 pseudonym in message until necessary, otherwise.

DMV maintains a database against each vehicle whose TRM is initialized by DMV and saves the credentials of each vehicle $(ID, c_V, inc_V, X_{OBU})$. Pseudonyms are maintained by DMV and indexed with the value of n (the counter of pseudonym and to be discussed later) as shown in Fig. 2(a). Moreover the same kind of table is also anonymously maintained by RAs as shown in Fig. 2(b). In other words, the pseudonyms do not carry any information that would enable

[2] The term '*vehicle*' throughout the rest of the paper should be read as either HEV or PEV. For the sake of simplicity we use the term vehicle instead of charging vehicles.

RAs to link them to the owner. The pseudonyms can be linked to the original owner and/or sender only when RAs collude and decrypt the stored encrypted keys necessary for revocation. Now we outline the mutual authentication mechanisms.

C. Direct Mutual Authentication (DMA)

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

$$CSPA \rightarrow DMV : MSK_i(i = 1, 2, 3, ..., l)$$

MSK_i is a hash chain based master secret key which is based on a secret s and $MSK_l = h^l(s)$. Each MSK_i is used for a designated amount of time and it is updated by CSPA after regular intervals. After that, DMV also sends X_{OBU} of the registered vehicles to CSPA for records.

$$DMV \rightarrow CSPA : X_{OBU}$$

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

1) Vehicle Registration with CSPA: The vehicle, most precisely its OBU must register with CSPA before charging. We assume that there exists a secure channel between CSPA and the vehicle. The registration of the vehicle proceeds as follows. The vehicle starts with the password (PWD_{OBU}) and upon access, the CSPA calculates some security parameters for the vehicle and sends it back to the OBU. Different steps and their description is given below:

1) $OBU \rightarrow CSPA : PWD_{OBU}, X_{OBU}$. OBU sends these values to CSPA on a secure channel. If PWD_{OBU} is valid, then the protocol will proceed.
2) CSPA calculates the following 3 values, i.e. 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 and these values are sent back to the OBU.

$$H_1 = h(s \| X_{OBU})$$
$$H_2 = h^2(s \| X_{OBU})$$
$$H_3 = MSK_i \oplus H_1$$

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

2) Authentication between OBU and CP: After the registration phase with CSPA, vehicle is eligible for charging its battery on the move with the registered parameters and the legitimate pseudonym pool. When the vehicle passes through the section of the road where charging technology is installed, it communicates with the charging plate. The phenomenon is same as hi-pass technology; however, the amount deducted as a charging fee, or the amount that is to be paid depends upon the application development or depends upon the suitability of the service provider.

The vehicle starts with selecting a pseudonym from the available pool and proceeds with authentication process with the selected pseudonym anonymously. The comprehensive mutual authentication steps are given below:

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

$$c_1 = h(H_2) \oplus PS^i_{OBU}$$
$$c_2 = h(PS^i_{OBU}) \oplus X_{OBU}$$
$$c_3 = h(h(PS^i_{OBU}) \| c_2 \| H_3)$$
$$\delta_4 = r_{OBU} \oplus PS^i_{OBU}$$

2) Then OBU sends CP, the above calculate values along with H_3.

$$OBU \rightarrow CP : c_1, c_2, c_3, H_3, \delta_4$$

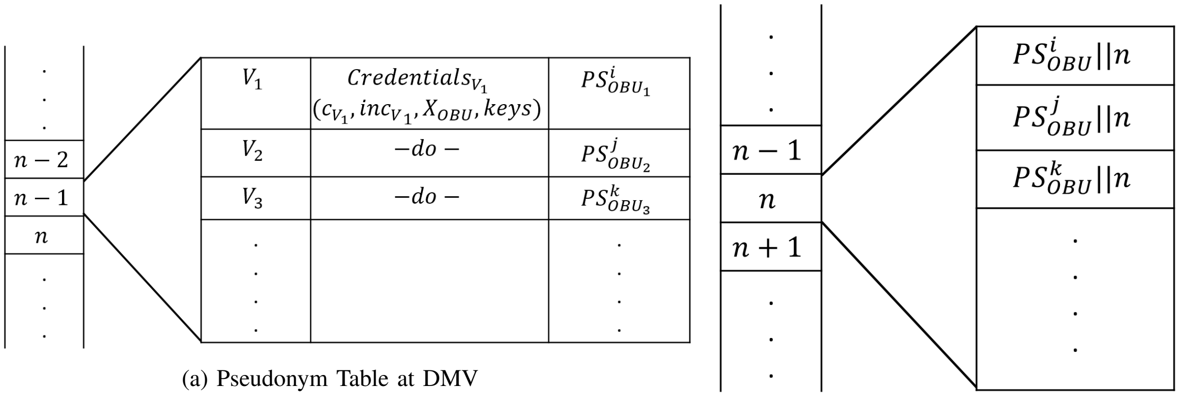
3) CP executes the following steps.
   a. Start with H_3 and extract the secret H_1 as $MSK_i \oplus H_1 \oplus MSK_i$.
   b. It calculates H_2 and extracts PS^i_{OBU} from c_1.
   c. CP also extracts r_{OBU} from δ_4 which is used in the construction of session key.
   d. Then it checks for the value c_2 if it is equal to $h(PS^i_{OBU}) \oplus X_{OBU}$.
   e. And check if c_3 is equal to the retrieved values $h(h(PS^i_{OBU}) \| c_2 \| H_3)$ then the OBU is authenticated, otherwise the authentication fails. It is to be noted that there will be a fixed number of tries, failing which will halt the authentication process.

After successful authentication, OBU and CP initiate the protocol to construct a session key SK_{OBU-CP} which is used for the later communication and billing parameters. The initialization of session key from CP serves as an acknowledgement to authentication as well. The OBU would not have been authenticated otherwise. CP extracts X_{OBU}, PS^i_{OBU}, and r_{OBU} from c_2, c_1, and δ_4 respectively. CP selects its nonce as r_{cp} and calculates session key as $SK_{OBU-CP} = h(PS^i_{OBU} \| r_{OBU} \| r_{cp})$. CP also calculates the following parameters.

$$ID_J = h(r_{OBU} \| ID_{cp})$$
$$c_4 = ID_J \oplus r_{cp}$$
$$c_5 = r_{cp} \oplus h(h(PS^i_{OBU}))$$
$$c_6 = h(r_{cp} \| c_4 \| c_5)$$
$$c_7 = H_1 \oplus h^2(PS^i_{OBU})$$

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.

$$CP \rightarrow OBU : c_4, c_5, c_6, c_7$$



V_1	$Credentials_{V_1}$ $(c_{V_1}, inc_{V_1}, X_{OBU}, keys)$	$PS^i_{OBU_1}$
V_2	$-do-$	$PS^j_{OBU_2}$
V_3	$-do-$	$PS^k_{OBU_3}$
. . . .		. . . .

(a) Pseudonym Table at DMV

$PS^i_{OBU}\|\|n$
$PS^j_{OBU}\|\|n$
$PS^k_{OBU}\|\|n$
. . . .

(b) Pseudonym Table at RAs

Fig. 3: Pseudonym History tables at DMV and RAs

From the above reply message, OBU extracts r_{cp} from c_4 and checks if c_6 is equal to $h(r_{cp}\|c_4\|c_5)$. If the information is correct, then the OBU authenticates CP as well and computes the session key $SK_{OBU-CP} = h(PS^i_{OBU}\|r_{OBU}\|r_{cp})$, 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 charging process will start based on the established session key SK_{OBU-CP}.

When these two entities (OBU and CP) authenticate each other then the charging will start. At the end of each charging at CP_i, a unit cost C_i will be accumulated to the account of the OBU against its presented PS^i_{OBU}. At the end of the whole charging, both OBU and CSPA will have the log of the charge and the OBU will be billed accordingly which will be verifiable by both CSPA and the OBU.

D. Pure Hash Chain based Authentication

The first approach was a direct communication between CP and OBU and most of the computation was carried out by the resource-constrained CP hardware. For a fast moving vehicle the first approach can be applied where computation is done locally by the CP; however, due to resource constraints, first approach may incur reasonable computation delay. Therefore we propose another indirect authentication mechanism where computation delay is minimum whereas a small communication delay is introduced. Moreover this mechanism is most favorable for low speed vehicles. The indirect authentication is carried out by CSPA and it is based on a pure hash-chain strategy. DMV provides the OBU with n pseudonyms $PS^i_{OBU}, i = 1, 2, 3, ..., n$ and hash chain corresponding to each pseudonym $h(PS^i_{OBU}), h^2(PS^i_{OBU}), ..., h^n(PS^i_{OBU})$. We assume that for the sake of charging the vehicle's battery, the vehicle registers with the CSPA every day. In other words, the car uses a new hash chain every day. The simple authentication takes place as follows:

1) The vehicle registers with CSPA and sends one of the hash chain head to CSPA $h^n(PS^i_{OBU})$.

$$OBU \rightarrow CSPA : h^n(PS^i_{OBU}), X_{OBU}, Cert_{OBU}$$

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

$$OBU \rightarrow CP : h^{n-1}(PS^i_{OBU}), X_{OBU}$$

3) CP forwards this value to the CSPA.

$$CP \rightarrow CSPA : timestamp, h^{n-1}(PS^i_{OBU}), X_{OBU}$$

4) 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.

$$CSPA \rightarrow CP : Auth.Status, \{SK_{OBU-CP}\}_{K^+_{OBU}}$$
$$CP \rightarrow OBU : \{SK_{OBU-CP}\}_{K^+_{OBU}}$$

5) If the authentication is successful then the charging process can be started, otherwise the process halts. It is to be noted that one hash chain is long enough to charge battery of the vehicle once and for all for a day. For the next day, the vehicles can register another hash chain. This process will still preserve the conditional privacy of the OBU.

The users will be allowed to try for a certain number of times, failing which will halt the authentication process and block the user for a stipulated amount of time. Moreover, the billing process will be same as in the first approach; however, the CP has to communicate with CSPA back and forth during authentication.

V. Quantitative Evaluation and Analysis

A. Security and Privacy Analysis

The security of our proposed scheme depends upon the collision resistance property of the one-way hash function. Given any m, it is easy to compute $h(m)$, and computationally very difficult to calculate the value of m from $h(m)$. The most basic security requirement of our proposed scheme is mutual authentication between CP and OBU. With our proposed lightweight authentication protocol which is an extended version of Chuang et al.'s [10] protocol, mutual authentication is guaranteed before starting the charging process. In both DMA and PHA, CP, CSPA and OBU mutually authenticate each other through a computationally lightweight mechanism that incurs phenomenally low cost. If the underlying hash mechanism is secure, then our proposed authentication can be considered secure. However the effect of keys compromise can be critical for our proposed scheme. From the OBU perspective, compromise of K_V does not have dire consequences because the adversary $\mathcal{A}$ can get only a part of the pseudonym, not the whole pseudonym. In case of the compromise of both K_{sym} and K_V, $\mathcal{A}$ can, not only manipulate pseudonyms, but also can reuse them.

It is also worth noting that it is the duty of CSPA to make sure the freshness of the session key and use different session keys in different charging for security reasons. Our proposed scheme also preserves conditional privacy of the users during authentication process. We do not use any real identity that could lead to the actual user, instead we use a series of legitimate pseudonyms. The anonymous pseudonyms are subject to revocation by RAs in case of a dispute.

Theorem V.1. *In case of any dispute, the node in question can be revoked and the pseudonym in question is linkable to the actual user by the revocation authorities.*

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 cipher text $c = \{\delta_1, \delta_2\}$ as follows: $PS^i_{OBU} = \delta_2 \oplus H(x\delta_1) = (K_{sym}\|K_V) \oplus H(rPK^+) \oplus H(rxPK^+)$. When RAs decrypt the keys K_{sym} and K_V, then revocation is almost done, all RAs have to do is to decrypt the $(\alpha)_{K_{sym}}$ and then extract ID of the vehicle from the pseudonym. ■

Lemma V.2. *It is hard to impersonate other OBU in the process of mutual authentication followed by power transfer. In other words, it is hard to get away with impersonation attack.*

Proof: Before starting the charging 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 CP with c_1 and c_3 that contain H_2 and H_3 respectively. At the registration phase, H_2 is associated to the X_{OBU} of the current authenticating vehicle. Therefore 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.

Therefore 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 PS^i_{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, therefore it is hard for anybody to impersonate other OBU with a pseudonym. ■

The following corollary naturally follows:

Corollary 1. *Replaying the authentication request message and/or Pseudonym will not benefit the malicious intent of the user.*

The argument is divided into two parts. Replaying a message with the same pseudonym result in the existence of previous charging records with this information. Upon successful authentication, the CSPA maintains a log with timestamp and billing information against the used pseudonym. Let an OBU charges its battery at CP_x at particular time t_i after successful authentication, 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 be charged 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.

B. 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.

In the computation overhead, we consider the authentication cost incurred by OBU and CP denoted by $T_{auth-OBU}$ and $T_{auth-CP}$ 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 in our proposed scheme is given by:

$$\begin{aligned} T_{rev} = Cost(&Search_{pseu-Table} + Cost(DervieK_{sym}, K_V) \\ &+ Cost(Decryption) \end{aligned}$$

$$T_{rev} = 2T_{\gamma} + 2T_{mul} + 2T_H + 2T_{dec}$$

T_{γ} is the time incurred by the table search $Search_{pseu-Table}$, 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 [11], 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:

$$T_{rev} \quad = 1.56 + 2(T_{\gamma} + T_H + T_{dec})$$

We also discuss the authentication processing time by both OBU and CP. According to [10], $SHA - 2$ 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 $1H + 1E$, E is the encryption operation.

C. Discussion

It is to be noted that, we cannot compare our proposed scheme with OLEV project directly because they are using short length segments for online-vehicle, whereas we leverage these inductive coils to recharge the battery. The weight of the battery must also be a tradeoff between the cost of the battery and the cost of the infrastructure for online vehicle.

We compare the two authentication strategies and their effect 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 CP are communicating directly. Therefore the only parameter that could affect the performance of DMA and PHA, is the length of the CP. If we consider the normal speed of the vehicle, then PHA will favor the lengthier CP 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 CP is only used as intermediary. However, in case of PHA, the session key is constructed by only CSPA. Moreover the OBUs must save the hash chain of the currently used pseudonyms in the on-board 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.

VI. Conclusion

In this paper, we proposed an efficient, fast, and privacy-aware mutual authentication mechanism for wireless charging in electric vehicles. The power transfer technology is installed under the road in the form of charging plates and a segment of a particular length of the road constitute 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. In the direct mutual authentication, charging plate and OBU authenticate each other directly without communicating with CSPA whereas in case of hash chain-based approach, the authentication is carried out through CSPA. We aim to address the billing, bidirectional auditability, and robust charging mechanism in the future and integrate it with our lightweight mutual authentication.

Acknowledgment

This research was supported in part by the MSIP (Ministry of Science, ICT and Future Planning), Korea, under the ITRC (Information Technology Research Centre) support programs (IITP-2015-H8501-15-1007, IITP-2015-H8501-15-1018) supervised by the IITP (Institute for Information & communications Technology Promotion).

References

[1] J. Romm, “The car and fuel of the future,” *Energy Policy*, vol. 34, no. 17, pp. 2609 – 2614, 2006. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0301421505001734

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

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

[4] F. Musavi, M. Edington, and W. Eberle, “Wireless power transfer: A survey of ev battery charging technologies,” in *Energy Conversion Congress and Exposition (ECCE), 2012 IEEE*, Sept 2012, pp. 1804–1810.

[5] C. Weissinger, D. Buecherl, and H. Herzog, “Conceptual design of a pure electric vehicle,” in *Vehicle Power and Propulsion Conference (VPPC), 2010 IEEE*, Sept 2010, pp. 1–5.

[6] A. Hoke, A. Brissette, D. Maksimovic, A. Pratt, and K. Smith, “Electric vehicle charge optimization including effects of lithium-ion battery degradation,” in *Vehicle Power and Propulsion Conference (VPPC), 2011 IEEE*, Sept 2011, pp. 1–8.

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

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

[9] I.-S. Suh and J. Kim, “Electric vehicle on-road dynamic charging system with wireless power transfer technology,” in *Electric Machines Drives Conference (IEMDC), 2013 IEEE International*, May 2013, pp. 234–240.

[10] M.-C. Chuang and J.-F. Lee, “Team: Trust-extended authentication mechanism for vehicular ad hoc networks,” in *Consumer Electronics, Communications and Networks (CECNet), 2011 International Conference on*, April 2011, pp. 1758–1761.

[11] C. Zhang, R. Lu, X. Lin, P.-H. Ho, and X. Shen, “An efficient identity-based batch verification scheme for vehicular sensor networks,” in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE.* IEEE, 2008, pp. 246–250.