An Efficient Privacy-preserving Authentication Scheme for Energy Internet-based Vehicle-to-Grid Communication

Prosanta Gope, *Member, IEEE* and Biplab Sikdar, *Senior Member, IEEE*

***Abstract*—The Energy Internet (EI) represents a new electric grid infrastructure that uses computing and communication to transform legacy power grids into systems that support open innovation. EI provides bidirectional communication for analysis and improvement of energy usage between service providers and customers. To ensure a secure, reliable and efficient operation, the EI should be protected from cyber attacks. Thus, secure and efficient key establishment is an important issue for this Internet-based smart grid environment. In this paper, we propose an efficient privacy-preserving authentication scheme for EI-based Vehicle-to-Grid Communication using lightweight cryptographic primitives such as one-way non-collision hash functions. In our proposed scheme, a customer can securely access services provided by the service provider using a symmetric key established between them. Detailed security and performance analysis of our proposed scheme are presented to show that it is resilient against many security attacks, cost effective in computation and communication, and provides an efficient solution for the EI.**

***Index Terms*—Energy internet, mutual authentication, advanced metering infrastructure, smart grids.**

I. Introduction

Energy, science and economy can mutually reinforce each other through new synergies and bring about greater efficiencies. From the perspective of sustainable development of society, the exploitation and utilization of the renewable energy and replacing traditional fossil fuels are important directions for reforming the energy landscape. However, the traditional grid structure makes it difficult to meet the requirements associated with integrating renewables and distributed generation, and incorporate other mechanisms to improve energy efficiency. In order to address these issues, the concept of Energy Internet has been proposed that seeks to integrate Information and Communications Technologies (ICT), cyber-physical systems and power system technologies to develop the next-generation of smart grids [1], [31]. Analogous to the conventional Internet, the idea of EI has been introduced to allow energy to be shared similar to information sharing in the Internet [30]. The fundamental idea behind the EI is to combine economics, information and energy using the power grid as the backbone network to provide an open and egalitarian framework for exchanging energy and associated information. The EI is designed to facilitate the seamless integration of diverse energy sources with the grid, and facilitate the interaction between various elements of the power grid to achieve increase in energy efficiencies [2]. All aspects of a power grid such as generation, transmission, distribution, service provider, operations, markets, and customers will benefit from secure and efficient communication on decisions about energy and information flow [25-26]. Finally, compared with smart grids, EI further integrates other energy networks such as gas for improved energy operations.

Vehicle to Grid (V2G) technology broadly consists of systems that facilitate the bi-directional flow of electrical energy between vehicles and the electrical grid. Electrical energy may flow from the grid to the vehicle to charge the battery and it may also flow in the reserve direction when the grid requires energy (e.g., to provide peaking power). With bi-directional chargers, electric vehicles (EVs) can become participants in the V2G eco-system, and such vehicles are energy assets for the smart grid. EVs need to charge and draw power from the grid when the State of Charge (SOC) of their batteries becomes low. The V2G property of EVs would also allow EVs to deliver power back to the grid and the concept of EI in V2G networks can be used to allow energy to be transported from vehicles to a location where it is used to perform useful work. One of the key benefits of EI in V2G environments is that it allows individuals (e.g., EV owners, households etc.) to trade energy without the need to build their own transmission and distribution networks [31]. With EI-based V2G, the unstable and intermittent energy generated by renewable energy sources (mainly solar and wind energy sources) can be used by EVs two provide two benefits. First, it provides a way to address the large energy demand of EVs through renewable energy sources, thus reducing the potential adverse impact of EVs on power grids. Second, it prevents renewable energy from being wasted when they are generated during low demand periods of traditional (non-EV) loads. This allows more efficient use of energy and can hence facilitate the wider adoption of renewable energy. EI-based V2G systems also have other applications, including power dispatch between cities, power transfer from renewable energy sources to end users, etc.

In addition to the routing of energy between various entities, the exchange of information is an important aspect of the EI and EI-based V2G systems. A number of protocols have been proposed for information exchange in EI based systems. The ISO/IEC/IEEE 18880 standard defines communication protocols and architectures for the EI. It defines the data

P. Gope, is with the Department of Computer Science, University of Sheffield, United Kingdom. (E-mail: prosana.nitdgp@gmail.com)

B. Sikdar is with the National University of Singapore, (Email: bsikdar@nus.edu.sg)

Table I
COMPARATIVE ANALYSIS OF THE RELATED SCHEMES

Scheme	Primitive Used	Mobilty Support	Location Privacy Support
[4]	ECC, Bilinear Pairing	No	No
[5]	ECC, Bilinear Pairing	No	No
[6]	Bilinear Pairing	No	No
[7]	AES-CBC, Hash function	No	No
[8]	Bilinear Pairing, Hash function	No	No
[9]	Bilinear Pairing, Hash function	No	No
[10]	Bilinear Pairing,Hash function	No	No
[11]	PUF, Hash function	No	No
[12-15]	Public-key sign-encryption	Yes	Most of them cannot
[21-25]	Public-key sign-encryption	Yes	Most of them cannot
IEC15118	ECDSA	Yes	No
OCPP	ECDSA	Yes	No
Proposed Scheme	Hash function	Yes	Yes

exchange protocols and the network architecture for integrating various components and participants in the grid, data storage, and application services. ISO/IEC/IEEE 18880 uses wide area communications using TCP/IP, and existing non-TCP/IP networks can connect through multi-protocol gateways. ISO/IEC/IEEE 18881 and ISO/IEC/IEEE 18883 have been developed to address network management and network security issues that are neglected in ISO/IEC/IEEE 18880. In contrast, V2G communications typically just focus on the communication between the vehicles, charging stations, and the grid. In V2G, Electric Vehicle Supply Equipment (EVSE) (i.e., EV chargers), such as those in charging stations, can be shared by many customers. Therefore, a temporal association between the EV and the EVSE has to be initiated for the charging and billing process when the charging cable is inserted. In this regard, some EVs and EVSEs use the IEC 15118 standard for communication. Similarly, EVSEs use Open Charge Point Protocol (OCPP) for communication between the EVSE and the energy management systems. While EI-based V2G has many benefits (as mentioned above), cyber-security of the components and data are big concerns [28-29]. The vehicles themselves face increasingly complex attacks that target not only the vehicle's operation but also its privacy. Threats to privacy include the exposure of the vehicle user's real identity, the vehicle's driving path, location, and disclosure of other private information. Thus, there are significant challenges to the design of security mechanisms for V2G environments and these are further complicated by the topological structure autonomy and fast rate of transformations due to vehicular movement. A number of organizations are working on the development of security solutions for the EI [2-3].

A. Related Work

Secure communication is one of the most important requirements for the EI environment in order to guarantee secure exchange of data at all times. For secure and efficient data exchange between the components, protocols with high security and performance are required. To address this issue, many researchers have proposed several mutual authentication and key establishment schemes suitable for the Advanced Metering Infrastructure (AMI) with various security considerations and goals. Mohammadali et al. [4] proposed two ECC-based identity-based key establishment protocols. The protocols reduce the computational overhead at the smart meter side of the AMI, and they are resilient against replay and desynchronization attacks. However, they are vulnerable to man-in-the-middle, impersonation, and false data injection attacks, and they incur high computational cost during key establishment. Nicanfar et al. [5] introduced two key exchange protocols that are based on the use of a symmetric-key algorithm and ECC. The protocols provide security and scalability for key exchange in smart grids. However, they are vulnerable to false data injection attacks. Moreover, both the protocols incur large computational costs which makes them unsuitable for resource limited devices in smart grids.

Wu and Zhou [6] presented an authentication and key distribution scheme by combining symmetric key and public key cryptographic systems, and the authors claim that their scheme can eliminate man-in-the-middle and reply attacks. Subsequently, Xia and Wang showed that [6] cannot ensure security against man-in-the-middle attacks and they also proposed a new data aggregation scheme [7]. However, Park et al. reported that the scheme presented in [7] is insecure against impersonation attacks [8]. Besides, it cannot address the customer's privacy requirements. Tsai et al. combined an identity-based signature scheme and an identity-based encryption scheme [9] for key distribution in smart grids. Odelu et al. investigated the protocol presented in [9] and demonstrated that it cannot guarantee the security of the session key and the strong credentials privacy of the smart meter [10]. They also introduced a new scheme with a claim that is can reduce computation overheads. However, Chen et al. proved that the scheme presented in [10] is vulnerable to several attacks, and it has large computational and communication costs. Moreover, our analysis shows that the scheme in [10] is weak against man-in-the-middle attacks which may lead to DoS attacks at the server end. In this context, an attacker

Table II
SYMBOLS AND CRYPTOGRAPHIC FUNCTION

Symbol	Definition
ID_{CS}	Identity of charging station
PID_i	Pseudo identity of $User_i$
k_i	Secret key of the $User_i$
psw_i	Password of the $User_i$
β_i	Thumbprint of the $User_i$
SK	Session key ($User_i$ -CS_j)
K_{cu}	Shared secret key between the CS_j and USP
LAI_x	Location area identifier of the entity x
$h(\cdot)$	One-way hash function
$\oplus$	Exclusive-OR operation
$\|$	Concatenation operation

(say Eve) can capture the initial message (Msg_1 in [10]), alter the message, and then send the altered message Msg_1^e to the service provider (SP). The SP can only decide about the validity of a request message (Msg_1^e) after completing the whole process, i.e., after receiving the response message (Msg_3 in [10]). Consequently, each request is stored in a buffer, where several intensive pairings first need to be computed, followed by submission response. This buffer needs to be kept open until a response from the smart meter (SM) is received. As a consequence, the memory can easily overflow if a large number of invalid requests are sent, since the invalid requests cannot be distinguished due to the late detection of the forged messages. In [11], the authors have considered the physical security of the smart meter and they proposed an authentication scheme by using the concept of physical unclonable functions (PUFs). In addition to [4-11], some recent studies on privacy issues in V2G communications have appeared in literature [12-15,21-25]. In these schemes, privacy of the car owner is considered as an important concern. However, in these schemes an EV needs to perform several computationally inefficient cryptographic primitives such as group signature, sign-encryption, etc. Besides, most of these schemes cannot ensure the location privacy of the EV user, which is essential for securely monitoring the status of the EV and efficiently providing services to the EV user. Table I compares related work to our approach with respect to the primitive used, ability for mobility support, and location privacy.

B. Our Contribution

In this paper, we first introduce a new model for EI-based V2G communication. Subsequently, we propose a lightweight authentication and key establishment scheme for EI-based V2G communication. The major contributions of this paper can be summarized as follows:

- A new model for EI-based V2G communication, which allows an EV user to seamlessly charge or discharge the battery of his/her vehicle from the charging stations located in different geographical locations. However, the charging/discharging rate may vary based on the location of the charging station.
- An efficient privacy-preserving authentication protocol, which provides several key security properties including Authentication Key Exchange (AKE) security, privacy of the user, protection against eavesdropping or interception attacks, protection against man-in-the middle attacks, and location privacy, which are all requirements for secure EI-based V2G communication [32-33]. There are some existing schemes which can ensure most of the security requirements for EI-based V2G communication. However, they use computationally expensive public-key cryptographic primitives. On the contrary, the proposed scheme is based lightweight cryptographic primitives such as one-way hash function and exclusive-OR operation, which creates significantly less computational overhead on the resource limited user's device (as shown in Table V).
- Most of the existing schemes including the existing underlying communication protocols such as IEC15118 and OCPP for V2G communications are vulnerable to some of the well-known security attacks such as man-in-the middle attacks, impersonation attacks, etc. Therefore, we provide a rigorous formal security analysis of our proposed scheme using the BR93-model [18] to show that it is secure against such attacks.
- A comparative study of the proposed scheme with closely related existing schemes. It is shown that the proposed scheme is secure and computationally efficient, and requires significantly lower overhead for establishing a session key between an user's device and the charging station, as compared to the related existing schemes.

The remainder of this paper is organized as follows. In Section II, we present our system and adversary model. In Section III we introduce the proposed scheme. The formal security analysis and performance analysis of the proposed scheme are presented in Section IV and Section V, respectively. Finally, conclusions are drawn in Section VI. The symbols and cryptographic functions of the proposed scheme are defined in Table II.

II. SYSTEM AND ADVERSARY MODEL

A. System Model for EI-based V2G Communication

Fig. 1 shows the system model for an EI-based V2G environment, which consists of three major components: a set of EV users each with a mobile device (MD) connected to the Internet, a set of charging stations (CSs), and a utility service provider (USP). The USP consists of two components: power generation, distribution, and management center (PGDMC) and data center (DC). Each user is required to register their EV with the USP. Then, the USP maintains all the user information in its data center. In this network model, the USP is an organization that is responsible for procuring electricity from various vendors. The USP also supplies electricity to charging stations in different locations. These charging stations may be owned by several private companies. A user may charge/discharge the batteries of his/her EV from/to any of the CSs. However, the charging/discharging rate may vary based on the location of the CS. For example, the charging/discharging rate of the CSs located at commercial area

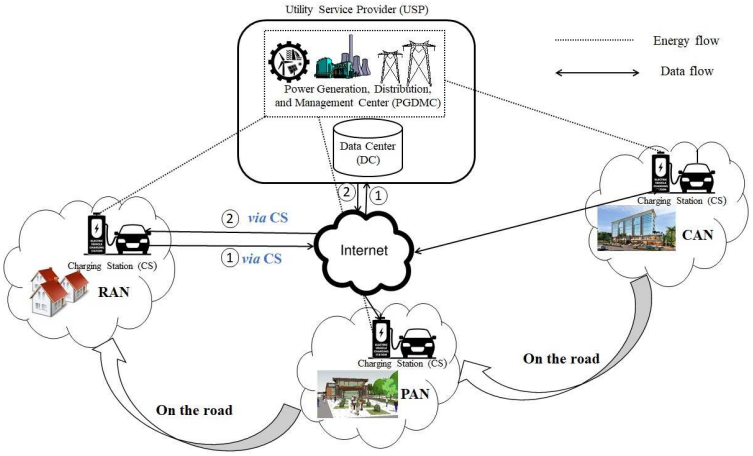

Figure 1. System model for the proposed scheme.

networks (CANs) may be higher than others. On the other hand, the charging/discharging rate of public area networks (PANs) may be lower than residential area networks (RANs). We assume that a secure channel is available between an EV user and the USP during the initial registration. Subsequently, each user with a mobile device communicates with the CS through the Internet. A CS may communicate with the USP through the public Internet or private networks. In this model, two types of flows, i.e., energy flows (shown by dotted lines) and data flows (shown by solid lines) have been considered. All the entities (user, CS and USP) need to authenticate themselves before sharing any information. Because of the public network based communication used in the system environment, there is a possibility of various attacks, such as replay, man-in-the middle, and impersonation attacks. In our scheme, users use biometrics (e.g., fingerprints) in addition to a password for two-factor authentication.

B. Adversary Model

During user registration, a user and the USP interact through a secure channel. On the other hand, during the execution of the proposed authenticated key agreement scheme, all parties communicate through an insecure public channel. In this context, we consider the Dolev-Yao threat model (DY model) [29], where an adversary may eavesdrop, modify, or delete the messages exchanged during transmission. Now, due to the usage of public networks and wireless communication in this EI-based V2G environment, there is a possibility of several attacks, such as impersonation, man-in-the middle, replay attacks, etc. The user's privacy is another important issue in this environment. Also, an adversary can impersonate as a legitimate user and try to obtain services. Similarly, a charging station may impersonate as others and ask for higher charges from a user. Hence, there is a need for an authenticated key agreement scheme by which the legitimacy of the entities can be verified, and also both the user and CS can establish a session key.

III. Proposed Scheme

In this section, we present our proposed lightweight authentication protocol for EI-based V2G communication, where a user ($User_i$) who has mobile device MD_i with Internet connectivity requests charging of his/her EV's battery from a charging station CS_j. In this regard, both $User_i$ and CS_j need to authenticate each other with the help of the USP. After successful mutual authentication between $User_i$ and CS_j, both entities will establish a session key *SK* for their secure communication. Our proposed scheme consists of the following two phases: user registration and authentication.

A. User Registration Phase

Each user first needs to register with the USP. The registration process consists of the following steps:

Step R1: $User_i$ sends the registration request along with its identity ID_i to the USP through the secure (out-of-band) channel.

Step R2: Upon receiving the request, the USP creates an account and inserts a new row in its database. It then randomly generates a unique pseudo identity PID_i, a secret key k_i, and also generates a set of shadow identities $SID = \{sid_1, sid_2, \cdots, sid_n\}$, which are later used in case of loss of synchronization between the USP and $User_i$. Next, the USP composes a message with $\{PID_i, k_i, SID\}$ and sends it to $User_i$ through the secure channel. Finally, the USP stores $\{PID_i, k_i, SID\}$ in its database for further interaction with $User_i$.

Step R3: Upon receiving $\{PID_i, k_i, SID\}$ from the USP, the user inputs his/her biometrics (e.g., thumbprint) β_i and password psw_i and computes $k_i^* = k_i \oplus h(\beta_i || psw_i)$. Finally, $User_i$ stores $\{PID_i, k_i^*, SID\}$ in his/her mobile device for further communication with the USP.

B. Authentication Phase

To accomplish communication security, $User_i$ has to go through an authentication process each time before obtaining services from charging station CS_j. The authentication phase of the proposed scheme comprises of the following steps:

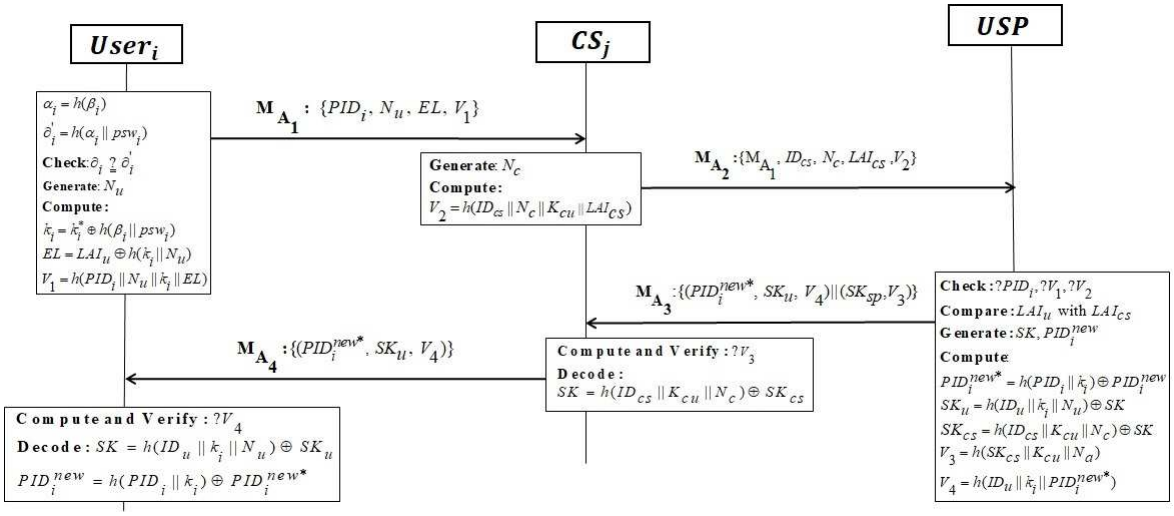

Figure 2. Steps and computations in the key agreement phase of proposed scheme.

Step 1: $User_i$ inputs his/her thumbprint β_i and password psw_i into his/her mobile device MD_i. The mobile device then computes $\alpha_i = h(\beta_i)$ and $\partial_i^{'} = h(\alpha_i||psw_i)$, and validates the user's legitimacy. If the user's validation is successful, then the device calculates $k_i = k_i^* \oplus h(\beta_i||psw_i)$. After that, the user generates a nonce N_u and finds his/her location area identity, LAI_u, using the MD's location service. Next, $User_i$ computes $EL = LAI_u \bigoplus h(k_i||N_u)$, a key-hash response $V_1 = h(PID_i||N_u||k_i||EL)$, and subsequently composes a message $\mathrm{M_{A_1}} : \{PID_i, N_u, EL, V_1\}$ and sends it to charging station CS_j.

Step 2: Upon arrival of message $\mathrm{M_{A_1}}$, charging station CS_j generates a nonce N_c and computes $V_2 = h(ID_{cs}||N_c||K_{cu}||LAI_{cs})$, where LAI_{cs} denotes the location area identifier of charging station CS_j. Next, CS_j composes a message $\mathrm{M_{A_2}} : \{\mathrm{M_{A_1}}, ID_{cs}, N_c, LAI_{cs}, V_2\}$ and sends it to the USP.

Step 3: Upon arrival of message $\mathrm{M_{A_2}}$, the USP first locates PID_i in its database and then computes and validates the key hash responses V_1 and V_2. Next, the USP decodes LAI_u from EL and then compares and validates LAI_u with LAI_{cs}. If the validation is successful, the USP generates a key SK and a new pseudo identity PID_i^{new}. It then computes $PID_i^{new*} = PID_i^{new} \bigoplus h(PID_i||k_i)$, $SK_u = h(ID_u||k_i||N_u) \bigoplus SK$, $SK_{cs} = h(ID_{cs}||K_{cu}||N_a) \bigoplus SK$, $V_3 = h(SK_{cs}||K_{cu}||N_c)$, and $V_4 = h(SK_u||k_i||PID_i^{new*})$. Next, the USP composes a message $\mathrm{M_{A_3}} : \{(PID_i^{new*}, SK_u, V_4)||(SK_{cs}, V_3)\}$ and sends $\mathrm{M_{A_3}}$ to charging station CS_j.

Step 4: Upon arrival of the response message $\mathrm{M_{A_3}}$ from the USP, the charging station first computes and validates the key-hash response V_3. If the validation is successful, CS_j decodes the session key $SK = h(ID_{cs}||K_{cu}||N_a) \bigoplus SK_{cs}$ and composes a new message $\mathrm{M_{A_4}} : \{(PID_i^{new*}, SK_u, V_4)\}$ and then sends it to $User_i$.

Step 5: Upon arrival of message $\mathrm{M_{A_4}}$, $User_i$ first verifies the key-hash response V_4. If the validation is successful, $User_i$ computes and decodes the session key $SK = h(ID_u||k_i||N_u) \bigoplus SK_u$, and the new pseudo identity $PID_i^{new} = PID_i^{new*} \bigoplus h(PID_i||k_i)$ for the next round.

The entities involved in the protocol will stop the execution of the scheme if any of the above verification steps is unsuccessful. For dealing with the loss of synchronization problem, instead of the pseudo identity PID_i, $User_i$ needs to select one of the unused shadow identities sid_x from $SID = \{sid_1, sid_2, \cdots, sid_n\}$ and send it in message $\mathrm{M_{A_1}}$. On receiving this message and after successfully validating the user, the USP generates a new pseudo identity and securely sends it in message $\mathrm{M_{A_3}}$ by using the secret key k_i. At the end of the authentication process, both $User_i$ and the USP delete the used shadow identity sid_x from their storage. Also, in the proposed scheme, $User_i$ can only use almost t shadow identities, where $t < n - 1$. After that, the user needs to request for reloading. In this context, the user sends a "Re-Load" message to the USP. On receiving that message, the USP generates a new set of shadow identities and then securely sends it in message $\mathrm{M_{A_3}}$ by using the secret key k_i. Details of this phase are depicted in Fig. 2.

Remark 1: In our proposed scheme, if a user needs to charge or discharge his/her vehicle multiple times in a day, then he/she needs to go through the authentication process each time, even if the same EV is used. Besides, since one of the goals of the proposed scheme is to achieve location privacy, we do not keep any footprint of the CSs. Therefore, even if the EV uses the same CS multiple times, it needs to execute the proposed anonymous authentication process. Since our proposed scheme is based on lightweight cryptographic primitives such as hash functions, it has a lower computational cost (execution times are shown in Table III and Table IV). Besides, from Table IV we can see that the communication cost of the proposed scheme is significantly less than the other schemes. On the other hand, in our proposed scheme, we allow a user to have a single account for multiple EVs, which will avoid any increase in the credential storage requirement.

Remark 2: Now, we consider the scenario where two users $User_i$ and $User_j$ share a vehicle. In such cases, during registration the USP will generate two sets of security

credentials $\{PID_i, k_i, SID_i\}$ and $\{PID_j, k_j, SID_j\}$ under the same account and send them to $User_i$ and $User_j$, respectively. After receiving their credentials, both the users securely store them in their respective mobile devices (as shown in Step R3). Now, when $User_i$ uses the vehicle then he/she needs to use $\{PID_i, k_i, SID_i\}$ to get through the authentication process. Similarly, when user $User_j$ uses the vehicle then he/she is required to use $\{PID_j, k_j, SID_j\}$ in order to authenticate with the USP. In this way, the proposed scheme can support the scenario where a vehicle is shared among multiple users. However, in this context, the storage complexity at the USP will increase linearly with the number of shared users.

IV. Formal Security Analysis

This section presents the formal security proof of the proposed scheme. We first demonstrate that our proposed scheme is secure.

A. Definitions and Assumptions

Bellare and Rogaway introduced a theoretical security proof for an authentication and key exchange protocol for a symmetric two-party case, which we refer to as the BR93-Model [18]. During the authentication process only the USP can authenticate a user, and a CS needs to forward the authentication request of the user to the USP. Thus, we assume that the communication between the CS and USP is secure, so that the USP and the CS can be regarded as a single participant and we call it the service agent (SA).

1) Complexity Assumptions: The security of our proposed scheme is based on the secure one-way hash function, which can be regarded as a pseudorandom function [19]. Therefore, we first introduce the security definitions of pseudorandom functions and show their game environments that will be used for the security proofs of the proposed scheme.

Definition 1: *Let f be a polynomial-time computable function and $AdvH = |\Pr[H^f = 1] - \Pr[H^{f'} = 1]|$ denote the advantage of an algorithm H, controlled by a probabilistic polynomial-time adversary $\mathcal{A}$, in distinguishing f from another function f'. We say that f is a (n, q, ε)-secure pseudorandom function if there is no feasible algorithm H that can distinguish f from f' with advantage $AdvH \geq \varepsilon$, while making at most q oracle queries to f or a truly random function f' and running at most n times by playing the following game:*

Initialization: *A challenger $\mathbb{C}$ interacting with $\mathcal{A}$ picks a random bit $b \in \{0, 1\}$ to determine the function f_b, where f_0 is a pseudorandom function and f_1 is a truly random function.*

Training Phase: *$\mathcal{A}$ issues q queries, $x_1, \cdots, x_q$ to $\mathbb{C}$, where $x_i \in \{0, 1\}^*$ are binary strings of arbitrary length. The challenger responds to these queries by sending $f_b(x_i)$ to $\mathcal{A}$ for $i = 1, \cdots, q$, where $f_b(x_i) \in \{0, 1\}^l$ and l is a fixed positive integer.*

Guess: *$\mathcal{A}$ outputs $b' \in \{0, 1\}$ as a guess of b. $\mathcal{A}$ wins this game if $b' = b$. We define the advantage of $\mathcal{A}$ winning the game as $Adv_{f_0,\mathcal{A}} = |\Pr[b' = b] - \frac{1}{2}|$.*

According to the pseudorandom function assumption, no probabilistic polynomial-time adversary can win the above game with non-negligible advantage.

2) Security Model and Notations: **Protocol Participants:** $\prod^s_{A,B}$ denotes the oracle which plays the role of *A* to interact with *B* in session *s*, and $\prod^t_{A,B}$ denotes the oracle which plays the role *B* to interact with *A* in session t, where $A, B \in I$, $s, t \in N$, I is the set of identities of the players such as a user and the service agent who participate in the protocol, and N is the set of positive integers.

Protocols: The proposed authentication scheme uses a three-party authentication and key exchange scheme. However, the protocol can be reduced to a de facto two-party setting protocol. Therefore, we define a two-party authentication and key exchange protocol as follows.

Definition 2: *A two-party authentication and key exchange protocol P, is formally specified by an efficiently computable function $\prod$ on the following inputs:*

k: The length of the security parameter used in the protocol.

A: The identity of the initiator of P, where $A \in I$.

B: The identity of the intended partner of P, where $B \in I$.

x: The secret information, where $x \in \{0, 1\}^*$.

$\mathfrak{K}$: The conversation in P so far.

r: The random coin flips of the sender or initiator, where $r \in \{0, 1\}^+$.

The output of $\prod(k, A, B, x, \mathfrak{K}, r) = (m, \delta, \alpha)$ is defined as follows:

m: The next message to be sent, where $m \in \{0, 1\} \bigcup \{*\}$, where $\{*\}$ specifies that the initiator sends no message.

δ: The decision, where $\delta \in \{\mathbb{A}, \mathbb{R}, *\}$, and $\mathbb{A}$, $\mathbb{R}$, and $*$ denote accept, reject, and no decision, respectively.

α : The private output, where $\alpha \in \{0, 1\}^* \bigcup \{*\}$ and $\{*\}$ denotes that the initiator does not have any private output.

3) Adversary Model: An adversary $\mathcal{A}$ is a probabilistic polynomial-time Turing machine during the execution of protocol P. $\mathcal{A}$ can control the channel between *A* and *B* by eavesdropping on the messages sent by *A* and *B*, modifying these messages, and compromising the session secrets shared between A and B. These behaviors can be modeled by the following queries.

$Execute(\prod^s_{A,B}, \prod^t_{B,A})$: This query models all kinds of passive attacks, where a passive adversary can intercept all the data exchanged between $\prod^s_{A,B}$ and $\prod^t_{B,A}$ in a session of P.

$Send(\prod^s_{A,B}, m)$: This query models active attacks, where an adversary sends a message m to $\prod^s_{A,B}$ and obtains a response message according to the proposed scheme.

$Reveal(\prod^s_{A,B})$: This query models the exposure of session keys (known session key attacks) in a particular session s.

$Corrupt(\prod^s_{A,B})$: This query models the revelation of long-term secret keys. This query models passive attacks.

$Test(\prod^s_{A,B})$: When $\prod^s_{A,B}$ has accepted and shared a session key, adversary $\mathcal{A}$ can make this query and try to distinguish a real session key from a random string.

4) Security Definitions: Before defining the notion of mutual authentication security, we first briefly review the definition of a matching conversation.

Definition 3 (Matching Conversations): *An authenticated key exchange protocol P is a message-driven protocol and the goal of P is to achieve a matching conversation. We first define a protocol session of a party A as $(A, B, s, \texttt{role})$ where B*

is the identity of A's partner, s is the session identifier, and `role` *can be either* `initiator` *or* `responder`*. A P with two protocol sessions between a party A and a party B are of the form $(A, B, s,$* `initiator`*$)$ and $(A, B, t,$* `responder`*$)$, respectively. Two sessions are said to be a matching conversation involving A and B if their session identifiers are identical and the initiator and responder parties are A and B. If a protocol P consists of more than two sessions and each pair of sessions in sequence is a matching conversation, then P is said to be a protocol of matching conversations.*

We define mutual authentication based on the definition of matching conversation as follows. P is a mutual authentication protocol if for any polynomial time adversary $\mathcal{A}$: (1) matching conversation implies acceptance and (2) acceptance implies matching conversation. The first condition says that if the sessions of two parties consists of a matching conversation, then the parties accept the authentication of each other. The second condition says that if each party accepts the authentication with the other party in a conversation, then the probability that there is no matching conversation between them is negligible. Formally, mutual authentication (MA) security is defined as:

Definition 4: *An authentication protocol P is **MA-Secure** (i.e., P satisfies **MA-Security**) if:*

(1) Matching conversation implies acceptance: If oracles $\prod_{A,B}^{s}$ and $\prod_{B,A}^{t}$ have matching conversations, then both oracles accept the authentication of each other, AND

(2) Acceptance implies matching conversations: The probability of event $NoMatching^{\mathcal{A}}(k)$ is negligible, where k is a security parameter and $NoMatching^{\mathcal{A}}(k)$ is the event that there exist i, j, A, and B such that $\prod_{A,B}^{i}$ is accepted but there is no oracle $\prod_{B,A}^{j}$ which is engaged in a matching conversation.

The event $NoMatching^{\mathcal{A}}(k)$ can also be denoted as $Succ_{P}^{MA}(\mathcal{A})$ which is the probability that a polynomial-time adversary $\mathcal{A}$ can successfully impersonate one of the two interactive entities who want to authenticate each other in P.

Authentication Key Exchange (AKE) Security: In an execution of an **MA-Secure** authentication protocol P, a polynomial-time adversary $\mathcal{A}$ interacts with two fresh oracles: $\prod_{A,B}^{s}$ and its partner $\prod_{B,A}^{t}$. At the end of the execution, $\mathcal{A}$ issues a *Test* query to one of the two fresh oracles. Then the real session key or a random string is returned to $\mathcal{A}$ according to the value of a random bit b. Finally, $\mathcal{A}$ outputs a bit b' and terminates the game. The **AKE-Advantage**, $Adv_{P}^{AKE}(\mathcal{A})$, is defined as $|\Pr[b = b'] - 1/2|$. We give a formal definition of **AKE-Security** below:

Definition 5 *A protocol P is* **AKE-Secure** *if it satisfies the following properties:*

(1) At the beginning the adversary engages in the execution of P with $\prod_{A,B}^{s}$ and its partner $\prod_{B,A}^{t}$. Then both oracles can accept and share the same session key with each other.

*(2) P is **MA-Secure**.*

(3) For every probabilistic polynomial-time adversary $\mathcal{A}$, $Adv_{P}^{AKE}(\mathcal{A})$ is negligible.

When a *Test* query is issued before finishing the execution of the protocol, the game is played as per the above definition if the session key is generated by any one of the two fresh parties. Otherwise, the *Test* query will be rejected.

B. Formal Security Analysis of the Proposed Scheme

The proposed scheme is based on hash functions, which can be considered as secure pseudorandom functions [19]. In this section, we show that the proposed scheme is provably secure based on the pseudorandom function assumption. As mentioned earlier, even though our proposed scheme is based on a three-party authentication and key exchange protocol, it can be reduced to a two-party authentication and key exchange protocol.

Lemma 1: If h is a $(n_0, q_0, \varepsilon_0)$-secure pseudorandom function family with negligible ε_0, then the proposed authentication scheme is **MA-Secure**.

Proof: Assume that there is a polynomial-time adversary $\mathcal{A}$ who can break MA-Security of the proposed protocol P with non-negligible probability $Succ_{P}^{MA}(\mathcal{A})$. We construct a polynomial time algorithm $\mathcal{F}$ using $\mathcal{A}$ to show that $\mathcal{F}$ can break the pseudorandom function with non-negligible advantage, thus providing a contradiction. Also, $Succ_{P}^{MA}(\mathcal{A}) = \Pr[Succ_{User}] + \Pr[Succ_{SA}] - \Pr[Succ_{User}, Succ_{SA}] \leq \Pr[Succ_{User}] + \Pr[Succ_{SA}]$, where $Succ_{User}$ and $Succ_{SA}$ are the events that $\mathcal{A}$ successfully impersonates as a legitimate user and SA, respectively, to pass authentication. Therefore, we split the proof into two cases, one for SA impersonation and the other for user impersonation.

Case 1 (SA Impersonation): Assume that $\mathcal{A}$ can impersonate as a SA with probability ϵ'. If $\mathcal{A}$ wants to be successfully authenticated by a user (say U_i) using $\prod_{User,SA}^{s}$ controlled by $\mathcal{F}$, $\mathcal{A}$ must correctly send $V_4 = h(SK_u||k_i||PID_i^{new*})$. In the following game, $\mathcal{F}$ will exploit the ability of $\mathcal{A}$ to break the pseudorandom function assumption with $\epsilon' \leq 4\epsilon_0 + 2^{-k}$, where k is the security parameter. $\mathcal{F}$ plays the game in *Definition 1* with challenger $\mathcal{C}$ as follows.

Initialization: Let the long-term secret key k_i be k-bit long. $\mathcal{C}$ picks a random bit $b \in \{0, 1\}$ and sets up a secure one-way hash function h_b where $h_0 = h_{k_i}$ is a pseudorandom function and h_1 is a random function. If $\mathcal{F}$ simulates the game by using h_1 to interact with $\mathcal{A}$, we call this game a *random experiment*. On the other hand, if $\mathcal{F}$ uses h_0 to simulate the game, we call this game a *real experiment*. The goal of $\mathcal{F}$ is to correctly guess if $h_b = h_0$ or $h_b = h_1$ (i.e., $b = 0$ or $b = 1$).

Training: $\mathcal{F}$ simulates $\prod_{User,SA}^{s}$ and $\prod_{SA,User}^{t}$ to interact with $\mathcal{A}$ by answering the following queries:

- $Execute(\prod_{User,SA}^{s}, \prod_{User,HG}^{t})$: $\mathcal{F}$ uses h_b given by $\mathcal{C}$ as h_{k_i} in the protocol. $\mathcal{F}$ also randomly generates k_h and PID_i^{new} and then computes $PID_i^{new*} = h(PID_i||k_i) \oplus PID_i^{new}$, $SK_u = h(ID_u||k_i||N_u) \oplus SK$, and $V_4 = h(SK_u||k_i||PID_i^{new*})$. Subsequently, $\mathcal{F}$ simulates $\prod_{User,SA}^{s}$ and $\prod_{SA,User}^{t}$ with the help of h_b, PID_i^{new*}, SK_u, and V_4.
- $Send(\prod_{User,SA}^{s}, m)$: $\prod_{User,SA}^{s}$ sends the request message $m = \{PID_i, N_u, V_1\}$ of the protocol. $\prod_{User,SA}^{s}$ first validates V_1 by querying h_b and then finds PID_i in its database and then checks the correctness of V_1 by querying h_b.
- $Send(\prod_{SA,User}^{t}, m)$: If $m = \{PID_i, N_u, V_1\}$, then $\prod_{SA,User}^{t}$ computes $PID_i^{new*} = h(PID_i||k_i) \oplus PID_i^{new}$, $k_h^{HG} = h(ID_u||k_i||N_u) \oplus SK$, and $V_4 =$

$h(SK_u||k_i||PID_i^{new*})$. $\prod_{SA,User}^{t}$ then responds by sending $\{PID_i^{new*}, SK_u, V_4\}$ to $\mathcal{A}$.

Challenge: First, $\mathcal{A}$ queries $Send(\prod_{User,SA}^{s}, m)$ to trigger the protocol. $\prod_{User,SA}^{s}$ then sends $m = \{PID_i, N_u, V_1\}$ to $\mathcal{A}$. Then $\mathcal{A}$ generates the authentication response parameter V_4 with success probability $\Pr[Succ_{SA}] = \varepsilon'$. Thus, $\mathcal{A}$ queries $Send(\prod_{SA,User}^{t}, \{PID_i^{new*}, SK_u, V_4\})$. After receiving this query, $\mathcal{F}$ issues a query $x^* = h(SK_u||k_i)$ to h_b and obtains the output $V_4^* = h(SK_u||k_i||PID_i^{new*})$.

Guess: Finally, $\mathcal{F}$ outputs a guess bit $b' \in \{0,1\}$. If $V_4^* = V_4$ then $\mathcal{F}$ outputs 0; otherwise, $\mathcal{F}$ outputs a random bit 0 or 1.

The analysis of the probability that $\mathcal{F}$ can successfully distinguish between the given h_b (i.e., $b = b'$) can be divided into two cases: under a real experiment (i.e., $b = 0$), and under a random experiment (i.e., $b = 1$). In the case of a real experiment, $\mathcal{A}$ can successfully send the correct authentication information to win the game with probability ε'. Hence, $\mathcal{F}$ will output $b' = 0$ with probability ϵ' when $\mathcal{A}$ sends correct authentication information under a real experiment. However, if $\mathcal{A}$ sends wrong information, $\mathcal{F}$ can only make a random guess for b, and thus $\mathcal{F}$ will output $b' = 0$ with probability $(1 - \varepsilon')/2$. Thus, when $b = 0$, $\Pr[b = b'|b = 0] = \varepsilon' + (1 - \varepsilon')/2$. In the case of random experiments, $\mathcal{A}$ can only send the correct authentication information by random guessing and the probability of a correct guess is 2^{-k}. Thus, when $b = 1$, $\mathcal{F}$ outputs $b' = 1$ with probability $(1 - 2^{-k})/2$ (i.e., $\Pr[b = b'|b = 1] = (1 - 2^{-k})/2$). Combining the two cases, we have

$$\begin{aligned}\Pr[b = b'] &= \Pr[b = b', b = 0] + \Pr[b = b', b = 1] \\ &= (\varepsilon' + (1 - \varepsilon')/2)1/2 + ((1 - 2^{-k})/2)1/2 \\ &= 1/2 + \epsilon'/4 - 2^{-(k+2)}.\end{aligned}$$

Thus we have

$$\begin{aligned}\varepsilon_0 &\geq |Pr[b = b'] - 1/2| \\ &= \epsilon'/4 - 2^{-(k+2)}. \\ \Rightarrow \epsilon' &\leq 4\varepsilon_0 + 2^{-k}.\end{aligned}$$

Case2 (User Impersonation): Suppose that $\mathcal{A}$ can impersonate as a user with probability ε''. If $\mathcal{A}$ wants to be accepted by $\prod_{SA,User}^{t}$, then $\mathcal{A}$ has to send out the correct authentication information. Thus $\mathcal{F}$ plays the same game as in Case 1 with $\mathcal{C}$.

Initialization: $\mathcal{C}$ selects a hash function h_b according to a random bit $b \in \{0,1\}$ for answering the queries from $\mathcal{F}$ where $h_0 = h_{k_i}$ is a pseudorandom function and h_1 is a random function.

Training: $\mathcal{F}$ first selects the required N_u and PID_i in the protocol. $\mathcal{F}$ then simulates $\prod_{User,SA}^{s}$ and $\prod_{SA,User}^{t}$ by answering $Execute(\prod_{User,SA}^{s}, \prod_{SA,User}^{t})$ and $Send(\prod_{User,SA}^{s}, m)$. The simulations of these oracles are similar to those in Case 1.

Guess: $\mathcal{F}$ outputs a guess $b' \in \{0,1\}$ according to PID_i and V_1. If PID_i and V_1 are valid, then $\mathcal{F}$ outputs 0, implying $h_b = h_{k_i}$; otherwise it outputs a random bit 0 or 1.

The probability that $\mathcal{A}$ successfully sends out the correct PID_i and V_1 is ε'' in the real experiment and 2^{-k} in the random experiment. Following the analysis of Case 1, we have

$$\begin{aligned}\Pr[b = b'] &= 1/2 + \varepsilon''/4 - 2^{-(k+2)} \\ \Rightarrow \varepsilon'' &\leq 4\epsilon_0 + 2^{-k}.\end{aligned}$$

Combining Case 1 and Case 2,

$$\begin{aligned}Succ_P^{MA}(\mathcal{A}) &\leq \Pr[Succ_{SA}] + \Pr[Succ_{User}] \\ &= \varepsilon' + \varepsilon'' \\ &\leq 8\epsilon_0 + 2^{-(k-1)}.\end{aligned}$$

From the above, ε_0 is non-negligible, which contradicts the assertion in the lemma's statement that ε_0 is negligible. Thus we can conclude that the proposed authentication scheme is MA-Secure. ■

Lemma 2: If h is a $(n_0, q_0, \varepsilon_0)$-secure pseudorandom function family with negligible ε_0, then the proposed scheme is **AKE-Secure**.

Proof: In Lemma 1 we have proved that the proposed protocol P is MA-Secure. Now, consider an adversary $\mathcal{A}$ who can break AKE-Security of P with non-negligible $Adv_P^{AKE}(\mathcal{A}) = \varepsilon$. We construct a simulator $\mathcal{F}$ using the ability of $\mathcal{A}$ to break the pseudorandom function assumption [20]. $\mathcal{F}$ plays the following game, as given in Definition 3, with a challenger $\mathcal{C}$.

Initialization: $\mathcal{C}$ picks a random bit $b \in \{0,1\}$ and sets up a secure hash function h_b for answering the queries from $\mathcal{F}$, where $h_0 = h_{k_i}$ is a pseudorandom function and h_1 is a random function.

Training: $\mathcal{F}$ selects the required N_g and SID_i in the protocol. $\mathcal{F}$ then simulates $\prod_{User,SA}^{s}$, and $\prod_{SA,User}^{t}$ by answering $Execute(\prod_{HG,SA}^{s}, \prod_{SA,HG}^{t})$ and $Send(\prod_{User,SA}^{s}, m)$, respectively. The simulations of these oracles are similar to those in the proof of Lemma 1.

• $Test(\prod_{User,SA}^{s})$: If k_h of $\prod_{User,SA}^{s}$ is generated, then $\mathcal{F}$ randomly chooses $c \in \{0,1\}$, and returns the real session key k_h if $c = 0$ or a random string for $c = 1$. Otherwise, $\mathcal{F}$ returns $\perp$, denoting meaninglessness.

• $Test(\prod_{N,E}^{t})$: The simulation is the same as the one above.

Challenge: After querying $Execute(\prod_{HG,SA}^{s}, \prod_{SA,HG}^{t})$, $\mathcal{A}$ sends a $Test$ query to $\mathcal{F}$.

Guess: After querying $Test(\prod_{User,SA}^{s})$ or $Test(\prod_{SA,User}^{t})$, $\mathcal{A}$ outputs a bit $b = 0$ if it thinks that the responding string is the real session key; otherwise, it outputs $b = 1$. Finally, $\mathcal{F}$ outputs $b' = 0$ if $b' = b$; otherwise $\mathcal{F}$ outputs $b' = 1$.

The analysis of the probability of the event $b = b'$ is similar to that in the proof of Lemma 1. $\mathcal{A}$ can win the game by successfully guessing $b = b'$ with probability $(\varepsilon + 1/2)$ under a real experiment (i.e., $b = 0$). Also, $\mathcal{A}$ can only guess if $b = b'$ with probability $1/2$ under a random experiment (i.e., $b = 1$). If $\mathcal{A}$ successfully guesses $b = b'$, then $\mathcal{F}$ will output $b' = 1$. Therefore, the probability of $b = b'$ and $b = 0$ is $(\varepsilon + 1/2)1/2$,

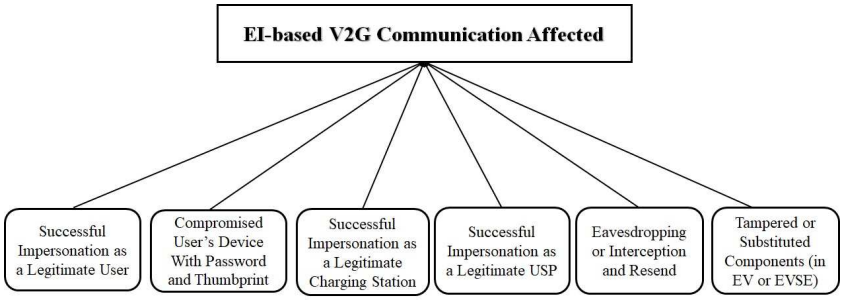

Figure 3. Attack Tree.

and the probability of $b = b'$ and $b = 1$ is 1/4. Thus we have

$$\begin{aligned} \Pr[b = b'] &= \Pr[b = b', b = 0] + \Pr[b = b', b = 1] \\ &= (\varepsilon + 1/2)1/2 + 1/4 \\ &= 1/2 + \epsilon/2 \\ \Rightarrow \epsilon_0 &\geq \Pr[b = b'] - 1/2 \\ &= \epsilon/2 \end{aligned}$$

From the above, ε_0 is non-negligible, and thus a contradiction occurs. Therefore, $Adv_P^{AKE}(\mathcal{A})$ is negligible for each polynomial-time adversary $\mathcal{A}$ and P is AKE-Secure. ■

C. Informal Security Analysis

So far, we have formally proved that the proposed scheme can ensure AKE-security, which is imperative to achieve security against impersonation attacks or replay attacks, session key security, etc. In this subsection we use the attack tree shown in Fig. 3 to show how the proposed scheme ensures some of the important security properties which are necessary for EI-based V2G communications.

1) *Protection Against Impersonation or Forgery Attacks*: In the proposed scheme, if an adversary tries to impersonate as a legitimate user $User_i$, then he/she needs to send a valid authentication request $\mathrm{M_{A_1}}$: $\{PID_i, N_u, EL, V_1\}$. However, the adversary cannot provide the thumbprint β_i and password psw_i. Therefore, he/she cannot use the mobile device and compute $k_i = k_i^* \oplus h(\beta_i||psw_i)$, $EL = LAI_u \bigoplus h(k_i||N_u)$, and a valid key-hash response $V_1 = h(PID_i||N_u||k_i||EL)$, which are essential to authenticate with the USP. On the other hand, if the adversary tries to impersonate as a legitimate service provider, then he/she must know the secret keys K_{cu} and k_i. Without knowing the secrets K_{cu} and k_i, the adversary cannot generate valid key-hash responses $V_3 = h(SK_{cs}||K_{cu}||N_c)$ and $V_4 = h(SK_u||k_i||PID_i^{new*})$. In our EI-based V2G communications model, charging/discharging rates vary based on the location. A charging station CS_j may try to cheat the $User_i$ by providing a false location identity LAI_{cs} to the USP and demand an inaccurate amount from the user. The proposed scheme will be able to detect such forgery attempts in the following way: the USP decodes LAI_u from the EL and then compares and validates LAI_u with LAI_{cs}. If the validation is successful, then only the USP will proceed with the execution of the further steps. Otherwise, the USP will terminate the execution of the protocol and take necessary against the CS. Similarly, an user may intentionally provide a forged LAI_u in order to pay a lower amount for charging or ask for a higher amount for discharging. The USP will similarly be able to detect such attempts. Next, we consider a scenario where the user's mobile device is lost or stolen. The adversary may try to use this device to impersonate as a legitimate user. However, in our proposed scheme we have considered multi-factor security and the adversary cannot provide the valid thumbprint β_i and password psw_i. Hence, he/she will not be able to proceed with further execution of the protocol. In this way, we can ensure security against impersonation and forgery attacks.
2) *Privacy of the User*: In the proposed scheme, the user needs to use a valid pseudo identity PID_i for each session, which cannot be used twice. Therefore, no one except the service provider can a recognize the activity of the user. Besides, in case of loss of synchronization, the user needs to use one of the unused shadow identities sid_j from $SID = \{sid_1, \cdots, sid_n\}$. After that, the user deletes sid_j from its memory. Therefore, changing the pseudonym in each session ensures identity intractability. This approach of the proposed scheme is quite useful for achieving privacy against eavesdropper (PAE).
3) *Protection Against Eavesdropping or Interception Attacks*: In the proposed scheme, an adversary cannot reuse the message $\mathrm{M_{A_1}}$: $\{PID_i, N_u, EL, V_1\}$ since PID_i changes in each session. The adversary cannot reuse message $\mathrm{M_{A_2}}$ since a new random number N_c is used in each session. Similarly, an adversary also cannot resend the messages $\mathrm{M_{A_3}}$ and $\mathrm{M_{A_4}}$ since key-hash response messages V_3 and V_4 change in each session and they are generated based on the challenges N_u and N_c, respectively. In this way, we ensure security against replay attacks.
4) *Protection Against Compromised User's Device*: Next, we consider a scenario when an attacker hijacks the car with the user's device and forces the legitimate user to input his/her password and thumbprint and then change the password and the thumbprint. After that, the adversary may try to ask for charging/discharging services from the USP. In order to address this issue, the

Table III
PERFORMANCE COMPARISON BASED ON SECURITY FEATURES

Scheme	SP1	SP2	SP3	SP4	SP5	SP6
Mohammadali et al. [4]	Yes	Yes	No	No	Yes	No
Nicanfar et al. [5]	No	No	No	No	No	No
Wu et al. [6]	No	No	No	No	No	No
Xia et al. [7]	No	No	Yes	No	No	No
Tsai et al. [9]	Yes	Yes	Yes	Yes	No	No
Odelu et al. [10]	Yes	Yes	Yes	Yes	Yes	No
Proposed Scheme	Yes	Yes	Yes	Yes	Yes	Yes
SP1: Privacy of customer; **SP2:** Privacy against eavesdropper; **SP3:** Resilience against man-in-the-middle attacks;						
SP4: Forward secrecy; **SP5:** Session key security; **SP6:** Resilience against DoS attacks						

Table IV
EXECUTION TIME OF VARIOUS CRYPTOGRAPHIC OPERATIONS

Operation	User's Device (HTC One Smartphone)	USP/CS (Intel Core i5-4300 Machine)
T_{mp}	5.12 ms	2.6 ms
T_m	21.86 ms	14.5 ms
T_b	8.67 ms	3.78 ms
$T_{cert_{gen}}$	55.946 ms	-
$T_{cert_{ver}}$	-	17.237 ms
T_h	0.0186 ms	0.011 ms
T_e	7.235 ms	2.338 ms
T_s	0.0584 ms	0.041 ms

Table V
PERFORMANCE COMPARISON BASED ON COMPUTATION COST (IN MS) AND COMMUNICATION COST

Scheme	User's Device	USP/CS	Communication Cost
Mohammadali et al. [4]	$2T_{mp}+T_m+T_{cert_{gen}}+3T_h \approx 88.15$	$3T_{mp}+T_m+T_{cert_{ver}}+4T_h \approx 57.87$	2340-bits
Nicanfar et al. [5]	$3T_{mp}+T_m+T_{cert_{gen}}+T_h \approx 93.24$	$4T_{mp}+T_m+T_{cert_{ver}}+4T_h+T_s \approx 63.77$	2176-bits
Wu and Zhou [6]	$2T_{mp}+T_m+T_{cert_{gen}}+T_h+T_s \approx 92.38$	$3T_{mp}+T_m+T_{cert_{ver}}+3T_h+T_s \approx 57.88$	4064-bits
Xia and Wang [7]	$T_s+ 4T_h \approx 0.13$	$T_s+ 4t_h \approx 0.085$	3296-bits
Tsai and Lo [9]	$4T_{mp}+T_e+5T_h \approx 27.85$	$3T_{mp}+T_e+ 2T_b+5T_h \approx 23.22$	6880-bits
Odelu et al. [10]	$3T_{mp}+T_e+ 6T_h \approx 22.74$	$2T_{mp}+T_e+ 2T_b+6T_h \approx 15.32$	2912-bits
Proposed Scheme	$6T_h \approx 0.15$	$8T_h \approx 0.88$	1802-bits
T_{mp}: Time Required for a multiplication point operation; T_m: Time Required for a multiplication operation;			
T_e:Time Required for of a modular exponential operation; T_s:Time Required for a symmetric encryption/decryption;			
T_b:Time Required for a bilinear pairing; T_h: Time Required for a hash operation;			
$T_{cert_{gen/ver}}$: Time Required for a certificate generation/verification operation			

legitimate user needs to inform such an incident to the USP as soon as possible. After that, the USP will block the user's account. In addition, the USP can also place a limit on the weekly or monthly charging/discharging amount for an user. In this way, we can address the scenario of compromised user devices.

5) *Protection Against Physical Attacks*: In the proposed scheme we assume that all the devices (such as user's mobile device, EV, EVSE) are tamper proof. Therefore, if an adversary attempts to perform any physical attacks, they can be resisted by the hardware. In addition, in order to deal with physical attacks, devices with embedded physical uncloneable functions (PUFs) [11] can also be used. Any attempt to tamper with the PUF changes the behavior of the device and renders the PUF useless, thereby making it possible to detect any tampering attempts.

V. PERFORMANCE EVALUATION

This section evaluates and compares the performance of the proposed scheme with respect to other authentication schemes for smart grids. We first consider several imperative security properties such as forward secrecy, session key security, etc. for analyzing the performance of our proposed authentication scheme on the security front with respect to other schemes ([4], [5], [6], [7], [9]). Table III shows that the schemes

presented in [4], [5], [6], [7], [9], and [10] fail to guarantee *all* the imperative security properties. Although Odelu et al.'s scheme can provide various security features, it is not robust against DoS attacks (as discussed in Section 1). In contrast, the proposed scheme can ensure all the important security features (as shown in Table III). For instance, in our proposed scheme, the USP can quickly make a decision against an invalid authentication request, which helps our scheme to be resilient against DoS attacks. Next, we evaluate the performance of the proposed scheme in terms of the computation and communication costs. In this regard, we first conduct simulations of the cryptographic operations used by all the schemes on an Ubuntu 12.04 virtual machine with an Intel Core i5-4300 dual-core 2.60 GHz CPU (operating as the USP/CS). To simulate a customer's mobile device, we use a HTC One smartphone with ARM Cortex-A9 MPCore processor operating at 890 MHz. We use the JPBC library Pbc-05.14 [21] and the JCE library [22] for evaluating the computation times of different cryptographic operations used in the proposed scheme and [4], [5], [6], [7], [9], and [10]. From Table IV we can see that the performance of the proposed scheme in terms of computation and communication costs is better than the others. Next, if we consider the existing standards such as IEC 15118 and OCPP protocol for V2G communications, then we find that like [4], [5], and [6], their authentication and key-establishment schemes are based on the computationally expensive ECDSA crypto-system, where each signature generation takes 23.81 ms (at the user's device) and each signature verification (at the USP) takes 17.56 ms. Besides, according to [32] and [33], these protocols also suffer from several security issues (such as insecure against man-in-the middle attacks, network impersonation attacks, DoS attacks, etc.) and challenges. These protocols also expose some important information such as customer name, vehicle identification number, charging location, and charging schedule, which affects the customer's privacy. Here, we argue that our lightweight authentication and key establishment scheme can easily be used by these underlying communication protocols (such as IEC 15118 and OCPP) so that they can address all the underlying security issues and ensure an enhanced security level along with higher degree of efficiency.

Next, in order to comprehensively evaluate the practicality of the proposed scheme, we consider the scalability of the proposed scheme when deployed by organizations that own charging stations. Since companies with large number of charging stations do not exist yet, we use traditional gasoline refueling companies to obtain representative numbers. In the USA, the biggest service providers are Shell (13727 stations), Chevron (6075 stations) and Exxon (5800 stations) [34]. Current battery charging technologies for EVs may be classified as either slow (energy flow rates of 2-6 KW) or rapid charging (upto 150 KW) [35]. We consider EV models Nissan LEAF (2018), Tesla Model S 100D and Mitsubishi Outlander PHEV (2018) that come with battery capacities of 40 KHh, 100 KWh and 13.8 KWh, respectively. Assuming a fast charging station with energy flow rate of 50 KWh, the empty to full charging time for these vehicles is 1 hour, 2 hours and 40 minutes, respectively. While a 150 KW rapid charger takes 1 hour to charge the Tesla Model S 100D battery, the Nissan and Mitsubishi models do not support this technology. Thus we use one hour as a representative time for charging current EVs in charging stations. The number of charging points in CSs varies. For traditional (petrol) filling stations, even in larger stations, studies indicate the average number is 18 (in Florida, [36]), i.e., 18 vehicles can fill up at the same time. We use 18 as the number of charging points in a CS and thus, 18 authentication requests are generated from a CS every hour. Now, based on Table V, the communication cost for the proposed protocol is 1802 bits = 226 bytes. On the other hand, TCP + IP + Ethernet overhead = 20 + 20 + 24 = 64 bytes and during the authentication process 4 messages are required to be exchanged. Therefore, the total communication overhead = 226 + 4×64 = 482 bytes (approx. 500). The computation time required at the USP is 0.00088 sec for verifying an authentication request. Using Shell as an example, we have $13800 \times 18 = 248400$ authentication requests per hour (Shell has 13800 refilling stations). Therefore, the amount of CPU time required every hour for verifying these transactions is $0.00088 \times 248400 = 219$ seconds. A simple personal computer or low end server can easily handle such computational requirements. The communication requirement of these authentication requests is $500 \times 248400 = 124200000$ bytes every hour = 276000 bits/sec = 276 Kbps. Thus, we conclude that the proposed scheme can provide all the important security properties and has lower (and practical) computation and communication costs, and is hence suitable for EI-based V2G communication.

VI. Conclusion

Secure and efficient key exchange is critical for ensuring secure data exchange in the Energy Internet. Aiming at the problem of safe communication between EV users, the USP and CSs, this paper proposed an efficient privacy-preserving authentication scheme for EI-based Vehicle-to-Grid communication. In this regard, only lightweight cryptographic primitives such as one-way non-collision hash functions have been considered. We quantified the performance of our scheme using theoretical analysis and simulation tools. Our scheme is resilient against many security attacks, efficient in computation and communication, and compares favorably with existing related schemes.

Acknowledgment

This research was supported by the National Research Foundation, Prime Minister's Office, Singapore under its Corporate Laboratory@University Scheme, National University of Singapore, and Singapore Telecommunications Ltd. This research was supported in part by Singapore Ministry of Education Academic Research Fund Tier 1 (R-263-000-C13-112). The authors would like to thank all the five reviewers for their insightful comments and valuable suggestions.

References

[1] J. Rifkin, "The third industrial revolution," Engineering and Technology, vol. 3, no. 7, pp. 26-27, 2008.

[2] Z. Y. Dong, "Towards an intelligent future energy grid," The University of Sydney, New South Wales, 2016.

[3] V. C. Gungor et al., "A Survey on Smart Grid Potential Applications and Communication Requirements," IEEE Transactions on Industrial Informatics, vol. 9, no. 1, pp. 28-42, 2013.

[4] Mohammadali, M. Sayad Haghighi, M. H. Tadayon, and A. Mohammadi Nodooshan, "A Novel Identity-Based Key Establishment Method for Advanced Metering Infrastructure in Smart Grid," IEEE Transactions on Smart Grid, pp. 1-1, 2016.

[5] H. Nicanfar and V. C. M. Leung, "Multilayer Consensus ECC-Based Password Authenticated Key-Exchange (MCEPAK) Protocol for Smart Grid System," IEEE Transactions on Smart Grid, vol. 4, no. 1, pp. 253-264, 2013.

[6] D. Wu and C. Zhou, "Fault-tolerant and scalable key management for smart grid," *IEEE Trans. Smart Grid*, vol. 2 no. 2 pp. 371-378 Jun. 2011.

[7] J. Xia and Y. Wang, "Secure key distribution for the smart grid," IEEE Trans. Smart Grid, vol. 3 no. 3 pp. 1437-1443 Aug. 2012.

[8] J. H. Park, M. Kim, and D. Kwon, "Security weakness in the smart grid key distribution proposed by Xia and Wang" *IEEE Trans. Smart Grid*, vol. 4 no. 3 pp. 1613-1614 Sep. 2013.

[9] J.-L. Tsai and N.-W. Lo, "Secure Anonymous Key Distribution Scheme for Smart Grid," *IEEE Transactions on Smart Grid*, vol. 7, no. 2, pp. 906–914, 2016.

[10] V. Odelu, A. K. Das, M. Wazid, and M. Conti, "Provably Secure Authenticated Key Agreement Scheme for Smart Grid," *IEEE Transactions on Smart Grid*, 2016, DOI: 10.1109/TSG.2016.2602282.

[11] P. Gope, and B. Sikdar, "Privacy-Aware Authenticated Key Agreement Scheme for Secure Smart Grid Communication," *IEEE Transactions on Smart Grid* DOI:10.1109/TSG.2018.2844403, 2018.

[12] M. Mustafa, N. Zhang, and Z. Fan, "Smart electric vehicle charging: Security analysis," in Proc. IEEE PES ISGT, Washington, DC, USA, Feb. 2013, pp. 1–6.

[13] H. Guo, Y. Wu, and M. Ma, "UBAPV2G: A unique batch authentication protocol for vehicle-to-grid communications," IEEE Trans. Smart Grid, vol. 2, no. 4, pp. 707–714, Nov. 2011.

[14] H. Liu, H. Ning, and L. Yang, "Role-dependent privacy preservation for secure V2G networks in the smart grid," IEEE Trans. Inf. Forensics Security, vol. 9, no. 2, pp. 208–220, Feb. 2014.

[15] Z. Yang, S. Yu, and C. Liu, "P^2: Privacy-preserving communication and precise reward architecture for V2G networks in smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 697–706, Dec. 2011.

[16] .Pbc library. Tech. rep. http://crypto.standford.edu/pbc/(accessed on 16 April 2017).

[17] Oracle Technology Network. Java Cryptography Architecture (JCA). [Online].

[18] M. Bellare and P. Rogaway, "Entity Authentication and Key Distribution," *Advances in Cryptology - Crypto 1993, D. Stinson, ed.* pp. 110-125, Springer-Verlag, 1993.

[19] B. Schneier, *Applied Cryptography (2nd edn),* pp. 197-211, John Wiley & Sons, New York, 1996.

[20] A. Menezes and S. Wanstone, *Handbook of Applied Cryptography*. Boca Raton, FL, USA: CRC Press, 1996.

[21] H. Liu, H. Ning, Y. Zhang and L-T. Yang, "Aggregated-Proofs Based Privacy-Preserving Authentication for V2G Networks in the Smart Grid," *IEEE Trans. Smart Grid,* vol. 66, no. 3, pp. 1722–1733, 2012.

[22] A. Abdallah and X. Shen, "Lightweight Authentication and Privacy-Preserving Scheme for V2G Connections," *IEEE Transactions on Vehicular Technology* vol. 3, no. 4, pp. 2615–2629, 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. 11, pp. 1438–1452, 2017.

[24] D. He, S. Chan and M. Guizani, "A Privacy-friendly and efficient secure communication framework for V2G networks," *IET Communications* vol. 12, no. 3, pp. 304–309, 2018.

[25] Y. Zhang, S. Gjessing, H. Liu, H. Ning, L-T. Yang and M. Guizani, "Securing vehicle-to-grid communications in the smart grid," *IEEE Wireless Communications* vol. 20, no. 6, pp. 66–73, 2018.

[26] P. Gope, and B. Sikdar, "An Efficient Privacy-Friendly Hop-by-Hop Data Aggregation Scheme for Smart Grids," *IEEE Systems Journals*, 10.1109/JSYST.2019.2899986, 2019.

[27] P. Gope, and B. Sikdar, "Lightweight and Privacy-Friendly Spatial Data Aggregation for Secure Power Supply and Demand Management in Smart-Grids," *IEEE Transactions on Information Forensics & Security*, DOI:10.1109/TIFS.2018.2881730, 2018.

[28] A.-S. Sani et al., "Cyber security framework for Internet of Things-based Energy Internet," *Future Generation Computing Systems,* doi.org/10.1016/j.future.2018.01.029, 2018.

[29] A. Jindal, N. Kumar and M. Singh, "Internet of energy-based demand response management scheme for smart homes and PHEVs using SVM," *Future Generation Computing Systems,* doi.org/10.1016/j.future.2018.04.003, 2018.

[30] J. Shen, T. Zhou, F. Wei, X. Sun and Y. Xiang, "Privacy-Preserving and Lightweight Key Agreement Protocol for V2G in the Social Internet of Things," *IEEE Internet of Things Journal* vol. 4, no. 4, pp. 2526–2536, 2017.

[31] K. Zhou, S. Yang and Z. Shaoa, "Energy Internet: The business perspective," *Applied Energy* vol. 178, no. 15, pp. 212–222, 2016.

[32] S. Lee et al., "Study on Analysis of Security Vulnerabilities and Countermeasures in ISO/IEC 15118 Based Electric Vehicle Charging Technology," *International Conference on IT Convergence and Security (ICITCS),* doi: 10.1109/ICITCS.2014.7021815, 2014.

[33] C. Alcaraz, J. Lopez and S. Wolthusen, "OCPP Protocol: Security Threats and Challenges," *IEEE Trans. Smart Grid,* vol. 8, no. 5, pp. 2452–2459, 2017.

[34] https://247wallst.com/retail/2017/04/21/10-retailers-that-control-americas-gasoline-sales

[35] Y. Ligen, H. Vrubel and H. Girault, "Mobility from Renewable Electricity: Infrastructure Comparison for Battery and Hydrogen Fuel Cell Vehicles," *World Electric Vehicle Journal,* vol. 9, no. 1, 2018.

[36] Florida Department of Transportation, *Trip Generation Characteristics of Large Gas Stations/Convenience Stores and Student Apartments*, https://fdotwww.blob.core.windows.net/sitefinity/docs/default-source/content/planning/systems/programs/sm/tripgen/trip-generation-of-convenience-stores.pdf.

Prosanta Gope (M'18) received the PhD degree in computer science and information engineering from National Cheng Kung University (NCKU), Tainan, Taiwan, in 2015. He is currently working as a Lecturer in the department of Computer Science (Cyber Security) at the University of Sheffield, UK. Prior to this, Dr. Gope was working as a Research Fellow in the department of Computer Science at National University of Singapore (NUS). His research interests include lightweight authentication, authenticated encryption, access control system, security in mobile communication and cloud computing, lightweight security solutions for smart grid and hardware security of the IoT devices. He has authored over 50 peer-reviewed articles in several reputable international journals and conferences, and has four filed patents. He received the Distinguished Ph.D. Scholar Award in 2014 from the National Cheng Kung University, Tainan, Taiwan. He currently serves as an Associate Editor of the IEEE INTERNET OF THINGS JOURNAL, IEEE SENSORS JOURNAL, the SECURITY AND COMMUNICATION NETWORKS and the MOBILE INFORMATION SYSTEMS JOURNAL.

Biplab Sikdar (S'98-M'02-SM'09) received the Ph.D. degree in electrical engineering from the Rensselaer Polytechnic Institute, Troy, NY, USA, in 2001. He was on the faculty of Rensselaer Polytechnic Institute from 2001 to 2013, first as an Assistant and then as an Associate Professor. He is currently an Associate Professor with the Department of Electrical and Computer Engineering, National University of Singapore, Singapore. His research interests include computer networks, and security for IoT and cyber physical systems. Dr. Sikdar is a member of Eta Kappa Nu and Tau Beta Pi. He served as an Associate Editor for the IEEE Transactions on Communications from 2007 to 2012. He currently serves as an Associate Editor for the IEEE Transactions on Mobile Computing.