Secure and Privacy-Aware Proxy Mobile IPv6 Protocol for Vehicle-to-Grid Networks

Mahmoud Hashem Eiza, Qi Shi and Angelos Marnerides
Department of Computer Science
Liverpool John Moores University
Liverpool L3 3AF, U.K.
{M.Hashemeiza, Q.Shi, A.Marnerides}@ljmu.ac.uk

Thomas Owens
College of Engineering, Design and Physical Sciences
Brunel University London
Uxbridge UB8 3PH, U.K.
Thomas.Owens@brunel.ac.uk

***Abstract*—Vehicle-to-Grid (V2G) networks have emerged as a new communication paradigm between Electric Vehicles (EVs) and the Smart Grid (SG). To ensure seamless communications between mobile EVs and the electric vehicle supply equipment, the support of ubiquitous and transparent mobile IP communications is essential in V2G networks. However, enabling mobile IP communications raise real concerns about the possibility of tracking the locations of connected EVs through their mobile IP addresses. In this paper, we employ certificate-less public key cryptography in synergy with the restrictive partially blind signature technique to construct a secure and privacy-aware proxy mobile IPv6 protocol that addresses the location privacy concerns of EVs. Our proposed protocol ensures the session continuity between an EV and the charging services while protecting the identity and location privacy of the EV. We assess the feasibility of the proposed protocol in terms of the information-theoretic uncertainty derived by the mutual information metric between mobile EVs and their network registration domains and show the high levels of achieved anonymity.**

Keywords—EV; Privacy-aware; Proxy Mobile IPv6; Security; Smart Grid; V2G

I. INTRODUCTION

In parallel with the rapid growth of smart grid (SG) deployments, transportation electrification is one of the major SG-related applications aiming at reducing carbon emissions thus achieving sustainable transportation systems. This has stimulated the development of electric transportation technologies such as electric vehicles (EVs). With the massive number it is anticipated to reach, *e.g.*, up to 10 million EVs on the US roads by 2025 [1], an intelligent management of EV charging loads is envisioned to act as a vital capability for the SG for preventing any overloads initiated at local sub-stations. From the EV users' perspective, the electric vehicle supply equipment (EVSE), *i.e.*, charging spots, should be widely available and easy to reach. Therefore, a variety of residential and public charging spots with different charging capabilities should be available for EVs to use in future V2G networks.

The current standardisation activities ISO/IEC 15118 [2] and SAE J2836 [3] specify the communication interface between EVs and EVSEs in V2G networks. According to the ISO/IEC 15118-2 standard, the IPv6 protocol is adopted as mandatory to acquire an IP address at the network layer and carry out TCP/IP communications [4]. Thus, the IP connection is utilised to exchange information during the charging process and for value added services [2]. Given the realistic fact that a full EV charge could be initiated at different geographical locations, the SG operator or the mobility operator should be able to keep track of the mobile EV and route it to a suitable charging spot. Therefore, it is quite critical to maintain seamless communications between EVs and EVSEs. Using different access technologies such as Power Line Communications (PLC), which is supported by ISO/IEC 15118-3, and WLAN, LTE that are expected to be supported by the currently under development ISO/IEC 15118-6 standard [5], EVs will communicate with the charging infrastructure in different contexts to 1) initiate the charging session, 2) negotiate and access the information required for the next charging/discharging schedule, and 3) terminate the charging session and receive the billing information.

The support of ubiquitous and transparent mobile IP communications is essential in V2G networks in order to maintain the service context between the SG operator and EVs. However, once a two-way communication between an EV and EVSE is established, there is no technical limitation to the amount and type of data that could be obtained from the EV such as its GPS location, the number of *kms* indicated on its odometer, as well as driver-oriented personal data such as the length of time the EV air conditioning was on [6]. For instance, if the DVD player was on in the backseat, it is highly likely that there is more than one person in the EV and one of them is possibly a child. In fact, exposing EV users' privacy and tracking and/or profiling them is very easy using their mobile IP addresses.

A handful of studies has addressed anonymous and privacy-preserving communications in V2G networks after establishing an IP connection (see [7-9]). All aspects of authentication, authorisation, and billing are initialised via the communication protocol once the IP connection is established [10]. However, to the best of our knowledge, no previous work has addressed the security and privacy concerns of mobile IP in V2G networks in order to prevent tracking/profiling of EVs using their mobile IP addresses. In [11], Nguyen *et al.* have suggested Proxy Mobile IPv6 (PMIPv6) protocol for V2G networks. PMIPv6 is a network-based localised mobility management protocol that can support the mobility of an EV without its involvement [12]. Thus, it allows the EV to use the same IPv6 address while moving within the PMIPv6 domain. It also decreases the signalling overhead and has lower handoff latency than host-based protocols such as Mobile IPv6 (MIPv6) [13]. Finally, there is no need to modify the EV protocol stack to join PMIPv6 network. Thus, PMIPv6 makes a good candidate for V2G

networks. Nonetheless, PMIPv6 suffers from many security and privacy threats such as impersonation, man in the middle, and location tracking attacks. Moreover, it has a long authentication latency during handoffs as explained later in Section II-A.

To rectify the above problems, in this paper, we propose a secure and privacy-aware PMIPv6 protocol for V2G networks. The focus of this paper is the security and privacy issues related to mobile IP at the network layer. With the employment of certificate-less cryptography in synergy with the restrictive partially blind signature (RPBS) technique, the novel contribution of this paper is two folds. First, the proposed protocol reduces significantly the authentication overhead in PMIPv6 by introducing the *pass* authentication. Thus, it guarantees a seamless handover with minimum authentication delay. Secondly, it provides a strong location privacy for the EV against attempts to track its location in the PMIPv6 domain.

The rest of this paper is structured as follows: Section II states the preliminaries we will utilise in our scheme whereas Section III is dedicated at describing the V2G network scenario and the security goals. Section IV introduces the proposed secure and privacy-aware PMIPv6 protocol. Section V provides the analysis and evaluation of the proposed protocol in terms of its security and privacy-preserving capabilities whereas Section VI strengthens the benefits of our scheme under a brief comparison with related work. Finally, Section VII concludes the paper and discuss on future work.

II. PRELIMINARIES

A. PMIPv6 Protocol Operations in V2G Networks

The PMIPv6 protocol introduces the following network entities to handle the EV mobility within a PMIPv6 local mobility domain (LMD). The Local Mobility Anchor (LMA) that maintains a binding cache entry for tracking the locations of each mobile EV and directing its traffic towards its current topological location. The Mobile Access Gateway (MAG) that is responsible for performing the mobility-related signalling with the LMA on behalf of an EV. Finally, the Authentication, Authorisation and Accounting (AAA) Server that is responsible for authenticating an EV to ensure that it is allowed to access the LMD. Fig. 1 shows the PMIPv6 signalling flow.

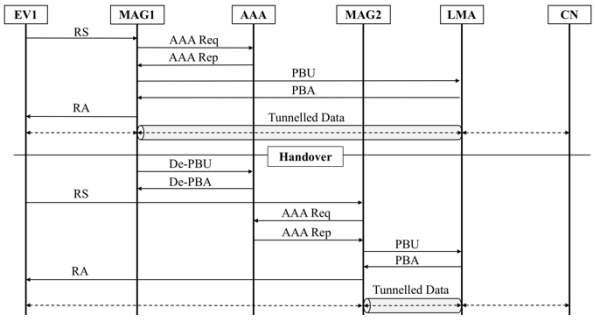

Fig. 1. PMIPv6 Signalling Flow

According to Fig. 1, when an EV joins a LMD, it sends a Router Solicitation (RS) message to attach to a MAG in the LMD, which we denote by MAG1, that authenticates the EV by using its identifier *EV_ID*, which was included in RS message, to request authentication by the AAA server. In the scenario of a successful authorisation for joining the LMD, MAG1 sends a Proxy Binding Update (PBU) message to the LMA that contains *EV_ID*. The LMA updates its binding cache entries and sends a Proxy binding Acknowledgment (PBA) to MAG1 that contains the Home Network Prefix (HNP), and subsequently establishes a bidirectional tunnel to MAG1. Finally, MAG1 sends a Router Advertisement (RA) message to the EV that contains the HNP. Upon receiving the RA message, the EV configures its IPv6 address to communicate with the corresponding node (CN). When the EV performs a handover, from MAG1 to MAG2, MAG1 and the LMA exchange De-PBU and De-PBA messages to update the LMA's binding entries. Subsequently MAG2 authenticates the EV again as explained before and updates the current location of the EV at LMA. Finally, it obtains the same HNP for the EV so it can continue using the same IPv6 address as long as it is moving within the same LMD.

B. Certificate-less Public Key Cryptography (CL-PKC)

Let $(\mathbb{G}_1, +)$ and $(\mathbb{G}_2, .)$ be two cyclic groups of prime order q and the bilinear pairing is a map $e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_2$ where $e(aP, bQ) = e(P, Q)^{ab}$ for all $P, Q \in \mathbb{G}_1$ and $a, b \in \mathbb{Z}_q^*$. A trusted Key Generation Centre (KGC) chooses three random generators P, P_0, $P_1 \in \mathbb{G}_1$, three secure hash functions H_0: $\{0, 1\}^* \rightarrow \mathbb{G}_1$, H_1: $\{0, 1\}^* \rightarrow \mathbb{Z}_q^*$, and H_2: $\mathbb{G}_1^4 \times \mathbb{G}_2^4 \rightarrow \mathbb{Z}_q^*$ and a random master key $s \in \mathbb{Z}_q^*$. KGC then sets $P_{pub} = sP$ as its public key and publishes the system parameters $(\mathbb{G}_1, \mathbb{G}_2, e, q, P_{pub}, P, P_0, P_1, H_0, H_1, H_2, Enc)$ where *Enc* is a symmetric encryption algorithm [14].

Each legitimate entity A in the system that has an identity ID_A, including EVs, MAGs, the LMA and the AAA server, sends a request to the KGC that includes its ID_A and a secret key K_A to obtain its partial private key. This request is encrypted using P_{pub}. The KGC then generates a partial private key $D_A = s \times Q_A$ where $Q_A = H_0(ID_A)$, encrypts it using K_A, and sends it back to A. Upon receipt of D_A, A selects a random number $x_A \in \mathbb{Z}_q^*$ and computes its private key $SK_A = x_A D_A$ and its public key $PK_A = (X_A, Y_A)$ where $X_A = x_A P$ and $Y_A = x_A P_{pub}$. Finally, we define $g = e(P, Q_A)$ and $y = e(Y_A, Q_A)$ to be used later in the RPBS technique. It is noted that in CL-PKC, the entity A does not need a certificate from a trusted authority thus saving the computation overhead needed for certificate management.

C. Certificate-less Restrictive Partially Blind Signature

The blind signature scheme was firstly introduced in [15] to enable a requester to obtain a signature on a message M without revealing anything about M to the signer. In [16], the restrictive blind signature technique is introduced to allow the requester to obtain a signature on a message M not known to the signer but the choice of M is restricted and must conform to specific rules. The partial blind signature (PBS) technique was introduced in [17] to allow the signer to produce a signature on M where the signature contains common agreed information that stays clearly visible despite the blinding process. The restrictive partially blinded signature (RPBS) technique is introduced as a PBS that also satisfies the property of restrictiveness. In this paper, we adopt the CL-RPBS scheme that was introduced in [18].

III. PROBLEM DESCRIPTION

A. V2G Network Model & Assumptions

The V2G network model considered in this paper is illustrated in Fig. 2. EV1 is mobile and connects to the EVSE

and the charging infrastructure at different places using different access technologies. Thus, a vertical handover will occur when necessary that allows EV1 to continue its connection. The MAGs, the LMA, and AAA server will be managed by either the SG operator or by the mobility operator that handles the communications in the SG. The EVSE could be managed by a third party such as an EV manufacturer. As shown in Fig. 2, the LMA keeps track of the location of EV1 and directs the data traffic to the corresponding MAG. MAGs do not maintain binding cache entries for the mobile EVs. The CN in Fig. 2 could be any entity in the SG charging infrastructure such as the central aggregator (CAG), charging and billing server, *etc*. In order to keep the session continuity and preserve the service context between EV1 and the CN, EV1 should maintain the same IPv6 address while moving.

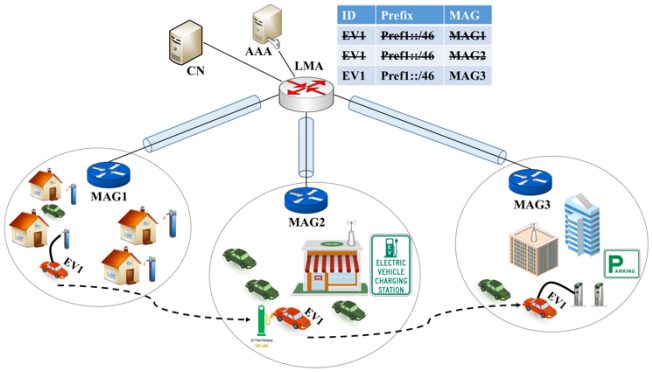

Fig. 2. PMIPv6-enabled Vehcile-to-Grid Network

In this paper, we assume that the LMD is a city or a state, which represents a local SG. Thus, when EV1 acquires an IPv6 address, it can retain this address as long as it is moving within the LMD, *i.e.*, intra domain handover is always possible. Inter domain handover between different LMDs is outside the scope of this paper and is left for our future work. Finally, we assume that EV1 is equipped with a logical interface to hide the different access technologies to the IPv6 stack in order to retain the same IPv6 address after the handover [19].

B. Security Model

The communication between LMA and MAG is protected using IPSec Encapsulating Security Payload (ESP) in transport mode with mandatory integrity protection as required by the PMIPv6 standard [12]. The KGC is trusted by all entities in the network. Moreover, since CL-PKC scheme is utilised, the KGC is not aware of the private key for any entity in the network. There is no trust relationship between the EV and the MAGs or LMA. Finally, we assume that a pre-shared keys (*PSK*) are distributed for all legitimate entities in the network in a secure way.

C. Security & Performance Requirements

In order to protect the EV's privacy and ensure that the LMA or other network entities cannot track the locations of a given EV while it is communicating with the charging infrastructure, we define the following security and performance requirements.

1) Mutual authentication between the EV and the MAG to prevent impersonation attacks and unauthorised access to the PMIPv6 domain.
2) Location and identity privacy for all mobile EVs. No entity in the network including the LMA, MAGs or adversaries should be able to link the real identity of the EV with its location using its acquired mobile IPv6 address. For instance, as shown in Fig. 2, the LMA is able to track the identity and the locations of the connected EV.
3) Low authentication latency during the handover. As can be seen in Fig. 1, the AAA server is utilised to authenticate an EV every time it joins the LMD or performs a handover between two MAGs. The authentication latency should be minimised to ensure seamless communications between the EV and the SG.

IV. The Proposed Protocol

A. Pass Generation

Each EV that requires to use the SG charging services, *i.e.*, join the V2G network, has to register its identity with the AAA server and request a *pass*. The AAA server generates the *pass*, which contains a message M from the EV that is unknown to AAA server, and an expiration time Ψ to indicate when the *pass* expires, which stays visible in the *pass*. We suggest Ψ is taken to be 24 hours. It is assumed that the AAA server will not keep track of the generated passes for a particular EV. The *pass* is used by an EV to authenticate itself to a MAG every time it performs a handover or joins the LMD for which the *pass* is issued. The restrictive partially blind signature technique is used to ensure that the MAG cannot link or reveal the real identity of an EV when it sees its *pass*. The steps taken to generate a *pass* for an EV, which is denoted as EV1, are described as follow.

1) EV1 generates a message $M = u_A P_0 + P_1$ where $u_A \in \mathbb{Z}_q^*$ is a random number and is kept secret at EV1. Subsequently it sends the following request to the AAA server: $Enc_{PSK}(ID_{EV1}, M, t_1, Sig_{EV}(H_1(ID_{EV1} \| M \| t_1)))$, where t_1 is the current timestamp and Sig_{EV} is the digital signature of EV.
2) We recall that *PSK* is a pre-shared key that EV1, as a legitimate network entity, shares with the AAA server which the AAA server relies on to authenticate EV1 and validate the received request. The AAA server chooses randomly $r \in \mathbb{Z}_q^*$ and $Q \in \mathbb{G}_1$, calculates $U = rP$, $a = e(P, Q)$, $b = e(M, Q)$, $z = e(M, SK_{AAA})$ and a pair-wise key $k_1 = e(SK_{AAA}, Q_{EV1})$ and sends $Enc_{PSK}(U, a, b, z, t_2, HMAC_{k1}(U \| a \| b \| z \| t_2))$ back to EV1. Both ID_{EV1} and M will be stored in the AAA server.
3) Upon message reception, EV1 calculates $k_1 = e(SK_{EV1}, Q_{AAA})$ and checks the message integrity. Following, EV1 chooses randomly $(c, \beta, u, v, \lambda, \mu) \in \mathbb{Z}_q^{*6}$, and calculates $M' = \alpha M + \beta P$, $A = e(M', Q_{AAA})$, $z' = z^{\alpha} y^{\beta}$, $a' = a^u g^v$, $b' = a^{u\beta} b^{u\alpha} A^v$, $U' = \lambda Q_{AAA} + U + \mu P$, $c = H_2(M', U', A, z', a', b') + \lambda H_1(\Psi)$, $c' = cu$, and sends $Enc_{PSK}(c, t_3, HMAC_{k1}(c \| t_3))$ to the AAA server.
4) The AAA server checks the message integrity and calculates $S_1 = Q + cSK_{AAA}$ and $S_2 = cD_{AAA} + rH_1(\Psi)P_{pub}$. It sends $Enc_{PSK}(S_1, S_2, t_4, HMAC_{k1}(S_1 \| S_2 \| t_4))$ to EV1.

5) Finally, EV1 checks if the following equations hold $e(P, S_1) = ay^c$ and $e(M, S_1) = bz^c$. If yes, it calculates $S'_1 = uS_1 + vQ_{AAA}$ and $S'_2 = S_2 + \mu H_1(\Psi)P_{pub}$. The restrictive partially blind signature on M' and Ψ is (U', z', c', S'_1, S'_2) and the $pass_{EV1}$ is $\{(M', \Psi), (U', z', c', S'_1, S'_2)\}$.

B. Initial Mobility Session

When EV1 attaches to MAG1, it generates a pseudo identity *PID1* as follows. $PID1 = r_A H_0(IP_{EV1})$ where $r_A \in \mathbb{Z}_q^*$ is a random number that is generated every time EV1 attaches to a new MAG and IP_{EV1} is the current obtained IPv6 address of EV1. If IP_{EV1} is not available, then it will be taken to be all zeroes. Thus, *PID1* will be different each time EV1 attaches to a new MAG. After that, EV1 sends $Enc_{PSK}(PID1, pass_{EV1}, t_5, H_0(PID1 \| pass_{EV1} \| t_5))$ within the RS message to MAG1.

Following the reception of the RS message, MAG1 validates it and verifies the $pass_{EV1}$, if it has not expired, as follows: It computes $A = e(M', Q_{AAA})$, $a' = e(P, S'_1)y^{-c'}$ and $b' = e(M', S'_1)\, z'^{-c'}$. If the following equation holds $e(P, S'_2) = e(H_1(\Psi)U' + H_2(M', U', A, z', a', b')Q_{AAA}, P_{pub})$, then the $pass_{EV1}$ is verified and EV1 is authenticated. Consequently, MAG1 sends a PBU message to the LMA that contains *PID1*. The LMA creates a new binding entry for *PID1* and sends back a PBA message to MAG1. MAG1 then sends $Enc_{PSK}(ID_{MAG}, HNP, t_6, H_0(ID_{MAG1} \| HNP \| t_6))$ within the RA message to EV1. Finally, EV1 validates the received RA message and configures its IPv6 address as illustrated in Fig. 3. In this way, MAG1 authenticates EV1 without communicating with the AAA server. Due to the adopted RPBS scheme, MAG1 is not able to reveal the real identity of EV1.

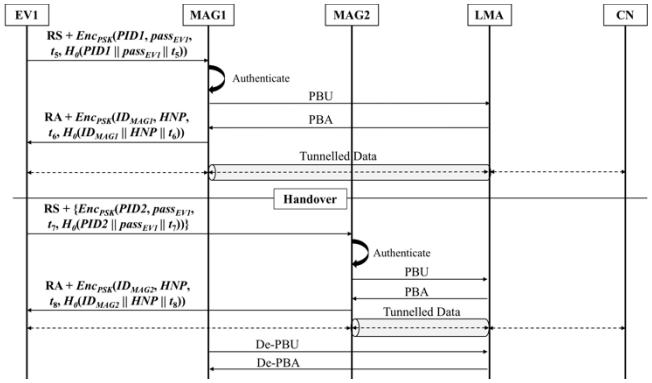

Fig. 3. Secure and Privacy-aware PMIPv6 Signalling Flow

C. Mobility Session Handover

When EV1 moves to a new location and detaches from MAG1 to attach to MAG2 the authentication process is performed as described before but with a new pseudo identity *PID2*. In our scheme, we propose to delay the transmission of the De-PBU and De-PBA messages, as can be seen in Fig. 3, from MAG1 to the LMA by a random value Δd. The reason for that is to avoid the possible linkage between two pseudo identities *PID1* and *PID2* of EV1 at the LMA. Otherwise, the LMA will be able to link the deregistered *PID1* with the newly registered *PID2*. Table 1 shows the binding entries at the LMA after performing the handover. It can be noticed that within Δd, the LMA maintains two entries with different pseudo identities for the same vehicle EV1. However, to the LMA it looks like they are the identities of two different vehicles.

TABLE I. Binding Cache Entries at LMA within Δd

ID	Prefix	MAG
PID1	Pref1::/46	MAG1
PID2	Pref1::/46	MAG2

It is worth noting that within Δd, the data packets to the EV will be sent to MAG1 and MAG2 while the EV is only attached to MAG2. This will cause extra resource consumption. However, Δd can be assigned with a very small value. With the large numbers of EVs joining and leaving the network, the LMA would not be able to link two pseudo identities to the same EV. This is further discussed in Section V-A.

V. Security & Privacy Analysis

This section provides the analysis of the security and privacy properties of our proposed protocol in order to verify whether it satisfies the security requirements defined in Section III-C.

Identity and Location Privacy. In order to illustrate this property, we answer the following questions.

- Can the AAA server track the locations of an EV? The AAA server does not save the generated *pass* thus it is not aware of when and where the EV will use this *pass*.
- Can the MAG reveal the identity of an EV? Due to the utilisation of the RPBS technique, the MAG cannot link the real identity of EV with the *pass* even with help from the AAA server, which holds the real identity of EV and *M*, especially as the EV generates a new *PID* each time it attaches to a new MAG.
- Can the adversaries track an EV or reveal its real identity? All the authentication messages and PMIPv6 signalling messages are encrypted using the *PSK*. Besides that, *PIDs* are used in PMIPv6 control messages thus adversaries cannot link the utilised *pass* with the real identity of the EV, even if a *pass* was obtained by an adversary, it would be changed within the next 24 hours.
- Can the LMA track the locations of an EV? In fact, the real identity of an EV is hidden and *PIDs* are utilised instead. Therefore, the LMA cannot link two *PIDs* with the real identity of an EV.

In the following, we investigate the ability of the LMA to link two *PIDs* with a particular EV after performing the handover between two adjacent MAGs. For this analysis, we assume that we only have two MAGs in the network.

Anonymity Quantification. Let assume *N* is the set of all EVs in the binding cache entry table at the LMA and *W* is a subset of *N* where $1 \leq |W| \leq |N|$. The EVs in *W* are attached to MAG_i and are highly likely to perform a handover to MAG_j where MAG_i and MAG_j are geographically adjacent to each other. Let assume that the arrival of new EVs at MAG_j follows a Poisson arrival process with arrival rate λ. Let *X* and *Y* be two discrete random variables with marginal probability functions $p(x)$ and $p(y)$, respectively. *X* represents the probability that EV1 with *PID1* detaches from MAG_i while *Y* represents the probability that EV1 attaches to MAG_j with a new *PID2* right away, *i.e.*, performs a handover.

It is worth noting that the LMA cannot assign different probabilities to the members of W and it only knows about the occurred handover after Δd. In general, the degree of anonymity d in the network can be measured as follows [20]

$$d = \frac{H(Y)}{H_M} \quad (1)$$

where H_M is the maximum entropy of the system and $H(Y)$ measures the amount of information the LMA knows about Y. However, in our case, the degree of anonymity is not a suitable measurement considering that we need to know how much knowing X will reduce uncertainty about Y. Therefore, instead of d, we use the mutual information (MI) $I(Y; X)$ that measures the amount of reduced uncertainty about Y given the realisation of X. Hence, it measures how much knowing that EV1 with *PID1* detaches from MAG_i reduces the uncertainty of the LMA that EV1 attaches to MAG_j with *PID2*. $I(Y; X)$ can be written as

$$I(Y; X) = H(Y) - H(Y \mid X) \quad (2)$$

where $H(Y \mid X)$ is the conditional entropy that measures the amount of information needed to describe Y given that the value of X is known. Using $p(x)$ and $p(y)$ notation, we can write (2) as follows

$$I(Y, X) = \sum_{y} p(y) \log_2 p(y) - \sum_{x,y} p(x, y) \log_2 \frac{p(x)}{p(x, y)} \quad (3)$$

where $p(x, y)$ is the joint probability distribution function of X and Y. We define $p(x) = \frac{1}{W}$ as the probability that EV1 detaches from MAG_i and $p(y) = \frac{1}{W} \cdot \frac{1}{\lambda t+1}$ as the probability that EV1 attaches to MAG_j after detaching from MAG_i. λt is the average number of arrivals per t units. Fig. 4 shows the amount of reduction in uncertainty about Y with respect to the size of W and the mean arrival rate λ.

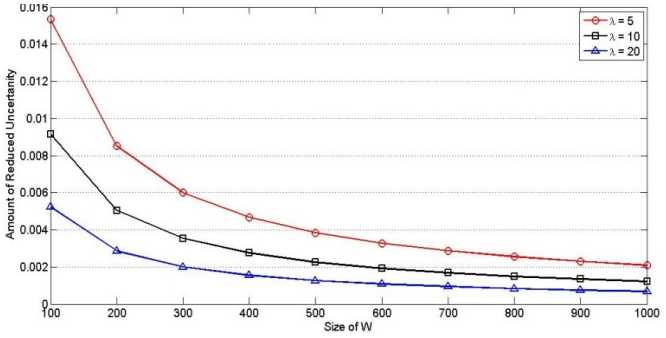

Fig. 4. Amount of Reduction in Uncertainty

It can be observed in Fig.4 that for the LMA, the amount of reduction in uncertainty decreases when both the size of W and the arrival rate λ increase. This resulted outcome demonstrates that the LMA stays uncertain about whether *PID1* and *PID2* belong to EV1 even though the network has only two MAGs. Therefore, our proposed protocol ensures high levels of anonymity for mobile EVs at the LMA.

Mutual Authentication. The proposed scheme achieves mutual authentication between an EV and the AAA server and between the EV and the MAG to which it is attached. At the *pass* generation, the EV sends its ID_{EV} and M to the AAA server. This information is encrypted with the *PSK* the EV shares with the AAA server. Thus, the AAA server authenticates the EV and saves its information along with M. When it is attached to the MAG, the EV is authenticated on two levels. Firstly, it encrypts the information within RS with the *PSK*, which is securely delivered to the MAG by the AAA server for use and then deletion, so it is authenticated as a legitimate user. Secondly, it has a valid *pass* thus it is authorised to join the LMD. When the MAG replies with the RA message that is encrypted using *PSK*, the EV authenticates the MAG as well.

Stolen *pass* attack resistance. It should be noted that the AAA server does not save the *pass* it signed for a particular EV. Thus, even if the AAA server is compromised, the attacker cannot steal the *pass*. Moreover, all the authentication messages in the network are protected by the *PSKs* and the EV is required to obtain a new *pass* every 24 hours so even if the *pass* is stolen, it can only benefit the adversary to a limited extent.

VI. Comparison with Related Work

The security and privacy issues in V2G networks and in PMIPv6/MIPv6 networks have been addressed separately in the literature. Next, we give a brief overview of some related works.

Jie *et al*. [9] propose a secure and efficient authentication scheme with privacy preserving for V2G networks. The scheme allows the EVSE to authenticate EVs anonymously and manage them dynamically. The authentication scheme is based on a revocable group signature, vector commitment scheme and an ID-based restrictive partially blind signature technique. Each entity in the system acquires a pair of public/private keys from a trusted authority (TA). The CAG then assigns a permit to each eligible EV that allows it to connect to the SG. The permit is generated using the RPBS technique. After verifying the permit, the local aggregator (LAG) generates a group membership certificate for the EV, which allows it to join the V2G network. The proposed scheme suffers from the key escrow problem inherited from ID-based public key cryptography, *i.e.*, a dishonest TA can forge the signature of any entity while the entity can also deny its own signature.

Liu *et al*. [8] present a role-dependant privacy-preservation scheme (ROPS) to achieve secure interaction between an EV and the SG. The authors specified three roles in which an EV interacts with the SG: energy demand, energy storage and energy supply. In each role, the EV has dissimilar security and privacy concerns. Therefore, Liu *et al*. proposed a set of interlinked sub protocols to incorporate different privacy considerations when EV acts as a customer, storage or a generator. The proposed sub protocols utilise the ring signature, fair blind signature and proxy re-encryption techniques to prevent the LAG from correlating the EV's real identity with its sensitive information. It also depends on a central authority (CA) to assign pseudonyms to EVs and LAGs. Considering the large number of network entities and pseudonyms the CA has to manage, the CA is the bottleneck of the proposed scheme.

In the context of securing the PMIPv6 protocol, Chaung *et al.* propose a secure password based authentication mechanism for seamless handover in PMIPv6 networks called SPAM [13]. The mobile node (MN) registers with the AAA server to receive the authentication credentials on a smart card. When MN joins the LMD, the user inserts the smart card and keys in his identity

and a password to get the authentication credentials. These credentials are utilised to perform a mutual authentication with a MAG. Chaung *et al.* integrate SPAM with a bicasting scheme to avoid the packet loss problem while performing the handover. The authors assumed that the smart cards are tamper-proof; however, most of them are not as shown in [21]. Besides, smart cards are vulnerable to loss and/or theft and SPAM is vulnerable to password guessing attacks.

Taha and Shen proposed ALPP; an anonymous and location privacy preserving scheme for MIPv6 heterogeneous networks [22]. ALPP consists of two sub schemes: anonymous home binding update (AHBU) and anonymous return routability (ARR) to add anonymity and location privacy to MIPv6 binding updates and return routability control messages, respectively. The authors combined onion routing and the anonymiser to encrypt repeatedly the transmitted messages at each hop to resist traffic analysis attacks and increase the achieved location privacy of MNs. The ALPP scheme utilised CL-PKC to authenticate a MN to its foreign gateway (FG) while preserving its anonymity. A FG in ALPP acts as a KGC for an attached MN. Although, the utilisation of CL-PKC reduces the computational overhead of the certificate management process, onion routing is computationally expensive and many studies have shown its susceptibility to different entities having some access to large fractions of input-output links [23].

Our paper differs from these studies in that we identify the security and privacy challenges of applying PMIPv6 in V2G networks and propose a novel solution to address these challenges. The utilisation of anonymous credentials for EVs while connecting to V2G networks does not address the EVs location privacy concerns because they can still be tracked and identified through their mobile IP addresses. Therefore, our proposed protocol complements the reported works in the literature to achieve EV security and privacy.

VII. Conclusion and Future Work

In this paper, we investigated the utilisation of PMIPv6 in V2G networks and identified the security and privacy concerns of EVs in this context. To achieve seamless communications between EV and charging services while protecting the identity and location privacy of EV, we have proposed a secure and privacy-aware PMIPv6 protocol for V2G networks. Our proposed solution utilises in synergy the CL-PKC and RPBS technique to achieve mutual authentication, identity and location privacy, message integrity and reduced authentication latency. Moreover, it achieves high levels of anonymity for EVs by reducing the amount of uncertainty about the identity of EV at the LMA. For future work, we intend to extend the proposed protocol for inter domain handover, *i.e.*, across different LMDs. Besides that, we will implement the proposed protocol and construct a test bed to assess its performance.

References

[1] OSIsoft, LLC , "Electric Vehicles and the Smart Grid Get a Boost from eMotorWerks Intelligent Charging Stations," 28 July 2015. [Online]. Available:https://www.osisoft.com/company/press_releases/Press_Releases__Media/Electric_Vehicles_and_the_Smart_Grid_Get_a_Boost_from_eMotorWerks_Intelligent_Charging_Stations.aspx. [Accessed 30 Sept 2015].

[2] International Standards Organisation (ISO), "Road vehicles -- Vehicle to grid communication interface -- Part 1: General information and use-case definition," 15 Apr 2013. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=55365. [Accessed 29 Sept 2015].

[3] Society of Automotive Engineers (SAE), "J2836/1: Use Cases for Communication Between Plug-in Vehicles and the Utility Grid," 08 Apr 2010. [Online]. Available: http://standards.sae.org/j2836/1_201004/. [Accessed 30 Sept 2015].

[4] Society of Automotive Engineers of Japan, Inc., "Industry Standards," Society of Automotive Engineers of Japan., Available at: http://www.jsae.or.jp/e07pub/yearbook_e/2014/docu/28_industry_standards.pdf, 2014.

[5] International Standards Organisation (ISO), "ISO/DIS 15118-6 Road vehicles -- Vehicle to grid communication interface -- Part 6: General information and use-case definition for wireless communication," 11 Sept 2015. [Online]. Available: http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=62982. [Accessed 30 Sept 2015].

[6] Australian Government - Data.gov.au, "Smart-Grid Smart-City Electric Vehicle Trial Data - Datasets," 22 Sept 2015. [Online]. Available: https://data.gov.au/dataset/smart-grid-smart-city-electric-vehicle-trial-data. [Accessed 28 Sept 2015].

[7] 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, Dec 2013.

[8] H. Liu, H. Ning, Y. Zhang, Q. Xiong and L.T. Yang, "Role-Dependent Privacy Preservation for Secure V2G Networks in the Smart Grid," *IEEE Trans. Information Forensics and Security*, vol. 9, no. 2, pp. 208-220, Feb 2014.

[9] C. Jie, Z. Yueyu and S. Wencong, "An Anonymous Authentication Scheme for Plugin Electric Vehicles Joining to Charging/DischargingStation in Vehicle-to-Grid (V2G) Networks," *China Communications*, vol. 12, no. 3, pp. 9-19, Mar 2015.

[10] M. Marc and S. Hartmut, "Plug-and-Charge and E-Roaming – Capabilities Of The ISO/IEC 15118 For The E-Mobility Scenario," *AT - Automation Technology,* vol. 62, no. 4, pp. 241–248, Apr 2014.

[11] T-T. Nguyen, C. Bonnet and J. Harri, "Proxy mobile IPv6 for electric vehicle charging service: Use cases and analysis," in *Proc. PIMRC*, London, 2013, pp. 127-131.

[12] S. Gundavelli, K. Leung, V. Devarapalli, K. Chowdhury, B. Patil, "Proxy Mobile IPv6", *RFC 5213*, August 2008.

[13] M-C Chuang, J-F Lee and M-C Chen, "SPAM: A Secure Password Authentication Mechanism for Seamless Handover in Proxy Mobile IPv6 Networks," *IEEE System Journal*, vol. 7, no. 1, pp. 102-113, Feb 2013.

[14] S.S. Al-Riyami and K.G. Paterson, "Certificateless public key cryptography," *Advances in Cryptology*-Asiacrypt, 2003, pp. 452-473.

[15] D. Chaum, "Blind signatures for untraceable payments," in *Proc. CRYPTO*, 1983, pp. 199-203.

[16] S. Brands, "Untraceable off-line cash in wallets with observers, " in *Proc. CRYPTO*, 1993, pp. 302-318.

[17] M. Abe and E. Fujisaki, "How to data blind signatures," *Advances in Cryptology-Asiacryp*'96, LNCS, vol. 1163, Springer-Verlag, 1996, pp. 244-251.

[18] C. Wang and R. Lu, "A certificateless restrictive partially blind signature scheme," in *Proc. IIHMSP*, Harbin 2008, pp. 279-282.

[19] T. Melia and S. Gundavelli, "Logical Interface Support for multi-access enabled IP Hosts", Internet-Draft, March 2015.

[20] C. Diaz, S. Seys, J. Claessens and B. Preneel, "Towards measuring anonymity," in *Proc. PET'02*, Germany 2002, pp. 184-188.

[21] M. Alizadeh, K. Sakurai, M. Zamani, S. Baharun and H. Anada, "Cryptanalysis of "A Secure Password Authentication Mechanism for Seamless Handover in Proxy Mobile IPv6 Networks"," *International Journal of Computer Science and Business Informatics*, vol. 15, no. 4, pp. 40-48 , July 2015.

[22] S. Taha and X. Shen, "ALPP: anonymous and location privacy preserving scheme for mobile IPv6 heterogeneous networks," *Security and Communication Networks*, vol. 6, no. 4, April 2013.

[23] G. Danzis, "Measuring anonymity: a few thoughts and a differentially private bound," [Online]. Avaliable: http://www0.cs.ucl.ac.uk/staff/G.Danezis/papers/Danezis-MeasuringThoughts.pdf [Accessed 01 Oct 2015].