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). In order 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 raises 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 (SP-PMIPv6) protocol for V2G networks. SP-PMIPv6 achieves low authentication latency while protecting the identity and location privacy of the mobile EV. We evaluate the SP-PMIPv6 protocol in terms of its authentication overhead and the information-theoretic uncertainty derived by the mutual information metric to show the high level of achieved anonymity.**

Keywords—Electric Vehicle (EV); Privacy-aware; Proxy Mobile IPv6 (PMIPv6); Security; Smart Grid (SG); V2G Networks.

I. Introduction

Transportation electrification is one of the major Smart Grid (SG)-related applications aiming at achieving sustainable transportation systems. This has stimulated the development of electric transportation technologies such as Electric Vehicles (EVs). With the projected massive number of EVs, anticipated to reach up to 10 million on US roads by 2025 [1], intelligent management of EVs charging loads is a vital capability for the SG to prevent overloads 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 Vehicle-to-Grid (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 mandatory to acquire an IP address at the network layer and carry out TCP/IP communications to exchange information during the charging process and for value added services [2, 4]. Given the 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 a mobile EV and route it to a suitable charging spot. Therefore, it is quite critical to maintain seamless communications between EVs and EVSE. EVs can use different access technologies in V2G networks such as Power Line Communications (PLC), WLAN, and LTE [5]. Hence, they can 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; 3) terminate the charging session and receive the billing information.

Although the support of ubiquitous and transparent mobile IP communications is essential in V2G networks, 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 data can be the EV's 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]. In fact, exposing EV users' privacy and tracking and/or profiling them is very easy using their mobile IP addresses.

A handful of studies have addressed anonymous and privacy-preserving communications in V2G networks after establishing an IP connection [7-9]. 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 [10], Nguyen *et al.* have suggested the 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 [11], and allows the EV to use the same IPv6 address while moving within a PMIPv6 domain. Moreover, there is no need to modify the EV protocol stack to enable it to join a PMIPv6 network.

While PMIPv6 makes a good candidate for V2G networks, it suffers from many security and privacy threats such as impersonation, man in the middle, and location tracking attacks. Moreover, it has relatively long authentication latency as explained later in Section II-A. To rectify the above problems, in this paper, a secure and privacy-aware PMIPv6 (SP-PMIPv6) protocol for V2G networks is proposed. Thus, the focus of this work is the security and privacy issues related to mobile IP at the network layer and how they may be addressed. Employing the certificate-less public key cryptography in synergy with the restrictive partially blind signature (RPBS) technique, this paper makes two novel contributions: 1) The SP-PMIPv6 protocol reduces significantly the authentication overhead in the standard

This work has been partially supported by the European Union's Horizon 2020 Research and Innovation Programme under Grant Agreement no. 644262 as part of the Wi-5 project.

PMIPv6 by introducing the *pass* authentication, which guarantees a seamless handover with minimum authentication delay; 2) SP-PMIPv6 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 employed in SP-PMIPv6 protocol. Section III describes the V2G network scenario and the security goals. Section IV introduces the proposed SP-PMIPv6 protocol. Section V provides an analysis and evaluation of the SP-PMIPv6 protocol. Section VI highlights the benefits of the proposed scheme through a brief comparison with related work. Finally, Section VII concludes the paper and discusses future work.

II. Preliminaries

A. *PMIPv6 Protocol Operations in V2G Networks*

The PMIPv6 handles the EV mobility within a PMIPv6 local mobility domain (LMD) through the following network entities: 1) A Local Mobility Anchor (LMA) that maintains binding cache entries for tracking the locations of the EVs in its domain and directing traffic intended for them towards their current location; 2) Mobile Access Gateways (MAG) that are responsible for performing the mobility signalling with the LMA on behalf of the EVs; 3) The Authentication, Authorisation and Accounting (AAA) Server that is responsible for authenticating an EV and authorising it to access the LMD. Fig. 1 shows the PMIPv6 signalling flow.

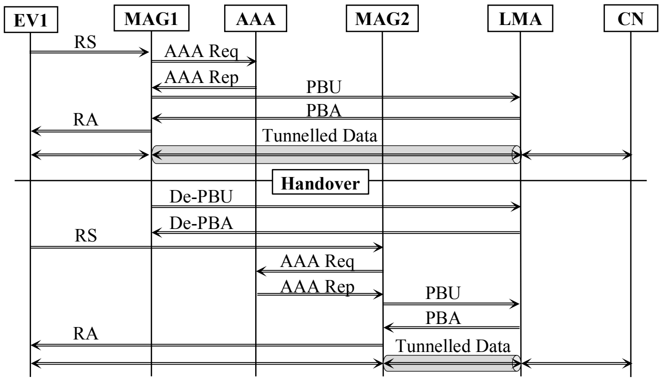


Fig. 1. PMIPv6 Signalling Flow

When an EV joins a PMIPv6 LMD, it sends a Router Solicitation (RS) message to attach to a MAG, denoted as MAG1 in Fig. 1. MAG1 identifies the EV by using its identifier *EV_ID* included in the RS message and requests authentication by the AAA server. If successful, 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. Then MAG2 authenticates the EV again, as explained earlier, and updates EV's current location at the LMA. Finally, it obtains the HNP for the EV. Hence, the EV 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 $(\mathbb{G}_2, \cdot)$ be two cyclic groups of prime order q, and $e : \mathbb{G}_1 \times \mathbb{G}_1 \rightarrow \mathbb{G}_2$ be a bilinear pairing that is a map 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 $s \in \mathbb{Z}_q^*$. The KGC then sets $P_{pub} = sP$ as its public key and publishes the system parameters $(\mathbb{G}_1, \mathbb{G}_2, e, q, P_{pub}, P, P_0, P_1, H_0, H_1, H_2, Enc(\cdot))$ where $Enc(\cdot)$ is a symmetric encryption algorithm [12].

Each legitimate entity A in the system with 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}. On receipt of this request, the KGC 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 the encrypted D_A, A decrypts it with K_A and selects a random number $x_A \in \mathbb{Z}_q^*$ used in computing its private key as $SK_A = x_A D_A$ and its public key as $PK_A = (X_A, Y_A)$ 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, A is not dependant on a valid certificate from a trusted authority. Moreover, the KGC is not aware of the private key of A.

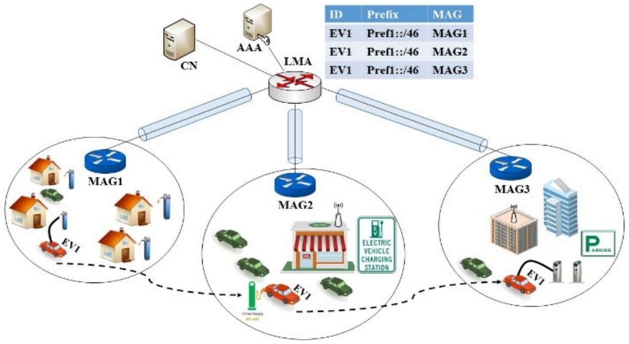
C. *Restrictive Partially Blind Signature (RPBS)*

The blind signature scheme aims to enable a requester to obtain a signature on a message M without revealing anything about M to the signer [13]. The restrictive blind signature technique was introduced in [14] to allow a requester to obtain a signature on M not known to the signer. However, the choice of M is restricted and must conform to specific rules. The partial blind signature (PBS) technique was introduced in [15] 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 RPBS technique was introduced as a PBS that also satisfies the property of restrictiveness. In this paper, the Certificate-less RPBS (CL-RPBS) scheme is adopted, which was introduced in [16].

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 EVSE and the charging infrastructure at different places using different access technologies. A vertical handover will occur when necessary to allow EV1 to continue its connection. The MAGs, the LMA, and the AAA server will be managed either by 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 maintain session continuity and preserve the service context between EV1 and the CN, EV1 should maintain the same IPv6 address while moving.



ID	Prefix	MAG
EV1	Pref1::/46	MAG1
EV1	Pref1::/46	MAG2
EV1	Pref1::/46	MAG3

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

In this paper, we assume that the PMIPv6-enabled V2G network (*i.e.* the LMD) is that of a city or a state and represents a localised SG. Thus, when EV1 acquires an IPv6 address, it can retain this address as long as it is moving within the LMD. Inter-domain handover between different LMDs is outside the scope of this paper. It is assumed that EV1 is equipped with a logical interface to hide the different access technologies from the IPv6 stack to retain the same IPv6 address after a handover [17].

B. *Security Model*

The communication between the LMA and the MAG is protected using IPSec Encapsulating Security Payload (ESP) in transport mode with mandatory integrity protection [11]. The KGC is trusted by all entities in the network. There is no trust relationship between the EV and the MAGs or the LMA. It is assumed that a pre-shared key (*PSK*) is distributed to all legitimate EVs in the LMD and to the AAA server in a secure way. The KGC publishes a list of the available MAGs and the AAA server in the LMD together with their corresponding public keys. Finally, it is assumed that MAGs cannot be compromised.

C. *Security & Performance Requirements*

In order to protect the EV's privacy and prevent its location being tracked through its mobile IP address, the following security and performance requirements are imposed.

1) Mutual authentication between the EV and the MAG to prevent impersonation attacks and unauthorised access to the PMIPv6 domain.
2) Identity and location privacy for all mobile EVs. No entity in the network including the LMA, the AAA server, and the MAGs should be able to track the location of the EV using its acquired mobile IPv6 address. For instance, in the scenario of Fig. 2, the LMA is able to track the identity and the location of the connected EV, which should be prevented.
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 SP-PMIPv6 Protocol

A. *Pass Generation*

Each EV that wants to join the LMD has to register its identity with the AAA server and request a *pass*. This *pass* is only used to access the PMIPv6-enabled V2G network whereas the aspects of billing and rewarding related to the charging and discharging processes are handled after establishing the IP connection. The AAA server generates the *pass* using a message M from the EV, which is unknown to the AAA server, and sets an expiration time Ψ to indicate when the *pass* expires, which stays visible in the *pass*. We suggest Ψ is 24 hours. It is assumed that the AAA server will not keep track of the passes generated for a particular EV, the *pass* is used by an EV to authenticate itself to a MAG every time it performs a handover and when it joins the LMD for which the *pass* is issued. The CL-RPBS technique ensures that the MAG cannot establish the real identity of an EV when it sees its *pass*. The steps taken to generate a *pass* for an EV denoted as EV1 are described as follows:

1) EV1 generates a message $M = u_A P_0 + P_1$ where $u_A \in \mathbb{Z}_q^*$ is a random number kept secret at EV1. It then sends the following request to the AAA server $Enc_{PSK}(ID_{EV1}, M, t_1, Sig_{EV1}(H_1(ID_{EV1} \parallel M \parallel t_1)))$, where t_1 is the current timestamp and Sig_{EV1} is the digital signature of EV1.
2) Recall that *PSK* is a pre-shared key that EV1, as a legitimate network entity, shares with the AAA server to secure its request. Having validated the request, the AAA server chooses randomly $r \in \mathbb{Z}_q^*$ and $J \in \mathbb{G}_1$, calculates $U = rP$, $a = e(P, J)$, $b = e(M, J)$, $z = e(M, D_{AAA})$ and a pair-wise key $k_1 = e(D_{AAA}, Q_{EV1})$ and sends $Enc_{PSK}(U, a, b, z, t_2, HMAC_{k1}(U \parallel a \parallel b \parallel z \parallel t_2))$ back to EV1. Here $HMAC(\cdot)$ is the message authentication code. The AAA server stores the following tuple $\{ID_{EV1}, M\}$.
3) Upon message reception, EV1 calculates $k_1 = e(D_{EV1}, Q_{AAA})$ and authenticates the message using $HMAC(\cdot)$. If the message is valid, EV1 chooses randomly $(\alpha, \beta, u, v, \delta, \mu) \in \mathbb{Z}_q^{*6}$, and calculates $M' = \alpha M + \beta P$, $A = e(M', Q_{AAA})$, $z' = z^{\alpha} y^{\beta}$, $a' = a^{u} g^{v}$, $b' = a^{u\beta} b^{u\alpha} A^{v}$, $U' = \delta Q_{AAA} + U + \mu P$, $c = H_2(M', U', A, z', a', b') + \delta H_1(\Psi)$, $c' = cu$, and sends $Enc_{PSK}(c, t_3, HMAC_{k1}(c \parallel t_3))$ to the AAA server.
4) The AAA server checks the message integrity and if it is confirmed, calculates $S_1 = J + cSK_{AAA}$ and $S_2 = cD_{AAA} + rH_1(\Psi)P_{pub}$. It sends $Enc_{PSK}(S_1, S_2, t_4, HMAC_{k1}(S_1 \parallel S_2 \parallel t_4))$ 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, EV1 generates a new PID each time it attaches to a new MAG.

Subsequently, EV1 sends $PKE(PK_{MAG1}, \{PID1, pass_{EV1}, t_5, H_0(PID1 \| pass_{EV1} \| t_5)\})$ within the RS message to MAG1, where $PKE(\cdot)$ is a public key encryption function and PK_{MAG1} is MAG1's public key.

When MAG1 receives the RS message, it 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 $e(S'_2, P) = e(H_1(\Psi)U' + H_2(M', U', A, z', a', b')Q_{AAA}, P_{pub})$, then the $pass_{EV1}$ is verified and EV1 is authorised to join the LMD. If this is the case, 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 $Enc_{PID1}(\text{HNP}, t_6, H_0(\text{HNP} \| t_6))$ within the RA message to EV1, which validates the received message and configures its IPv6 address as illustrated in Fig. 3.

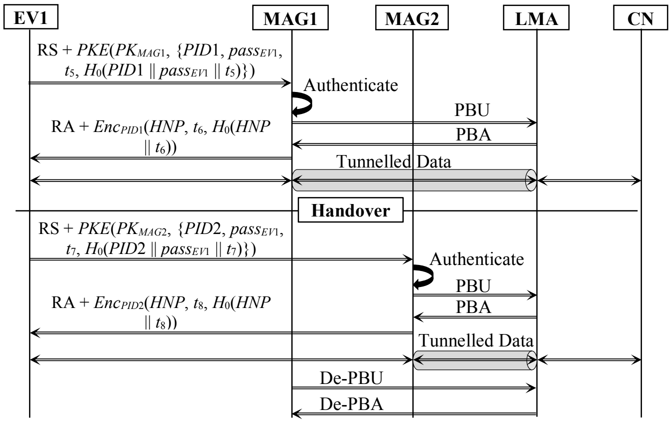

EV1
MAG1
MAG2
LMA
CN
RS + $PKE(PK_{MAG1}, \{PID1, pass_{EV1}, t_5, H_0(PID1 \| pass_{EV1} \| t_5)\})$
Authenticate
PBU
RA + $Enc_{PID1}(HNP, t_6, H_0(HNP \| t_6))$
PBA
Tunnelled Data
Handover
RS + $PKE(PK_{MAG2}, \{PID2, pass_{EV1}, t_7, H_0(PID2 \| pass_{EV1} \| t_7)\})$
Authenticate
PBU
RA + $Enc_{PID2}(HNP, t_8, H_0(HNP \| t_8))$
PBA
Tunnelled Data
De-PBU
De-PBA

Fig. 3. SP-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 above but with a new $PID2$. In SP-PMIPv6, we propose to delay the transmission of the De-PBU and De-PBA messages, shown in Fig. 3, from MAG1 to the LMA by a random value Δd. The reason is to avoid the possible linkage of the 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 $PID2$. Thus, within Δd, the LMA maintains two entries with different PIDs for the same vehicle EV1. However, to the LMA, it appears they are the identities of two different EVs.

It is worth noting that within Δd, the data packets sent to EV1 will be directed to MAG1 and MAG2 while EV1 is only attached to MAG2, thus causing extra resource consumption. However, Δd can be assigned a very small value. With a large number of EVs joining and leaving the network, the LMA would not be able to link two pseudo identities to the same EV as discussed later in Section V-A.

V. Security Analysis & Performance Evaluation

A. Security & Privacy Analysis

This section provides an analysis of the security and privacy properties of the proposed SP-PMIPv6 protocol in order to determine whether or not it satisfies the security and performance requirements specified in Section III-C.

Identity and Location Privacy. In order to illustrate this property, the following questions are answered:

- 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 CL-RPBS technique, the MAG cannot establish the real identity of EV when it sees its *pass* even with help from the AAA server, which holds the real identity of EV and M.
- Can external adversaries track an EV or reveal its identity? All the authentication messages of the SP-PMIPv6 protocol are encrypted. Thus, the utilised *pass* cannot be disclosed to external adversaries to allow them to track the location of an EV if it is assumed that the MAGs cannot be compromised internally, which was assumed earlier.
- Can the LMA track the locations of an EV? The real identity of an EV is hidden and *PIDs* are utilised instead. Therefore, the LMA cannot link different *PIDs* to the same EV, so it is unable to track the EV's locations.

In the following, the ability of the LMA to link two *PIDs* with a particular EV after performing handover between two adjacent MAGs is investigated. For this analysis, it is assumed that there are only two MAGs in the network. Assume N is the set of all EVs in the binding cache entries 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 us assume that the arrival of new EVs at MAG_j follows a Poisson arrival process with an 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. We utilise the mutual information (MI) $I(Y; X)$ metric that measures the amount of reduction in 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 $PID2$. $I(Y; X)$ is defined as

$$I(Y;X) = H(Y) - H(Y \mid X) \tag{1}$$

where $H(Y)$ measures the amount of information the LMA knows about Y and $H(Y|X)$ 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 rewrite (1) as follows

$$I(Y,X) = \sum_{y} p(y)\, log_2\, p(y) - \sum_{x,y} p(x,y)\, log_2 \frac{p(x)}{p(x,y)} \tag{2}$$

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 when t is set to 1 second.

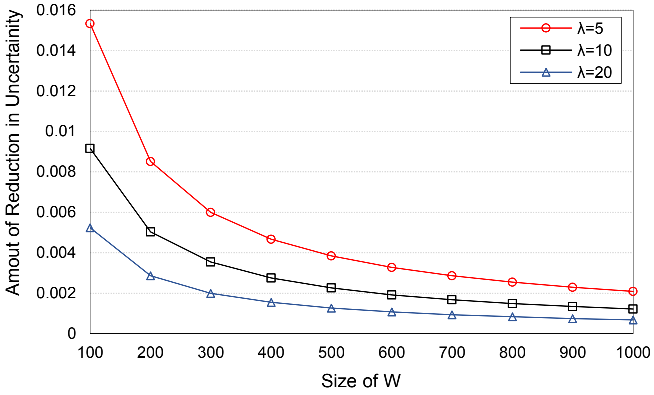


Fig. 4. Amount of Reduction in Uncertainty

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 outcome demonstrates that the LMA stays uncertain about whether $PID1$ and $PID2$ belong to EV1 even though the network has only two MAGs. Therefore, SP-PMIPv6 protocol ensures high level of anonymity for mobile EVs at the LMA.

Mutual Authentication. The SP-PMIPV6 protocol achieves mutual authentication between an EV and the AAA server and between the EV and the MAG to which it is attached. At *pass* generation, the EV sends its ID_{EV}, M, and a signature to the AAA server. This information is encrypted with *PSK* that the EV shares with the AAA server. The AAA server authenticates the EV via its signature and saves its information. When the EV attaches to the MAG, the EV sends its *pass* with which the MAG can authenticate the EV as a legitimate user that is authorised to join the LMD. When the MAG replies with the RA message that is encrypted using $PID1$, the EV authenticates the MAG as well.

Stolen *pass* attack resistance. As mentioned earlier, the AAA server does not save the *pass* it signed for a particular EV. Thus, even if it is compromised, the attacker cannot steal the *pass*. Furthermore, the EV is required to obtain a new *pass* every 24 hours. Hence, even if it is stolen, it can only benefit the attacker for a limited period.

B. Performance Evaluation – Authentication Latency

In this section, the performance of the proposed protocol SP-PMIPv6 is evaluated in terms of the authentication latency by comparing it with that of the PMIPv6 protocol with the traditional AAA server architecture shown in Fig. 1.

The transmission delay between EVs and MAGs as well as MAGs and the LMA is taken to be 10 *ms*, while the transmission delay between MAGs and the AAA server is taken to be 160 *ms* as mentioned in [18], which is assumed to include the time needed to authenticate the EV as well. In SP-PMIPv6, the MAG needs to perform five pairing operations and two exponentiation operations to verify the *pass*. The time needed to perform a single exponentiation operation is T_{exp} = 1.1 *ms* and the corresponding pairing operation is T_{par} = 3.1 *ms* with pre-computation on Intel Pentium 4 3.0-GHz machine [19]. Thus, the *pass* verification process takes 17.7 *ms*. Besides that, there is one PKC operation, one $Enc(\cdot)$ operation, and two hash operations H_0 as shown in Fig. 3. It is assumed that the time needed to perform the $Enc(\cdot)$ and H_0 operations is negligible considering the small size of the messages. It is assumed that RSA-1024 is utilised for the PKC operation. The RSA-1024 encryption operation takes 0.03 *ms* while the decryption takes 0.6 *ms* [20]. Thus, the authentication latency is estimated to be 10 + 0.03 + 0.6 + 17.7 + 10 = 38.33 *ms*. In PMIPv6 protocol, the authentication latency is 10 + 160 + 10 = 180 *ms*. Therefore, we can clearly argue that the SP-PMIPv6 protocol reduces the authentication latency by 78.7% in comparison to the standard PMIPv6 protocol.

VI. Comparison with Related Work

The security and privacy issues in V2G networks and in PMIPv6/Mobile IPv6 (MIPv6) networks have been addressed separately in the literature. A brief overview of some related works follows.

Jie *et al.* [9] proposed 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, a vector commitment scheme, and an ID-based RPBS 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. After verifying the permit, the local aggregator (LAG) generates a group membership certificate for the EV, which allows it to join the V2G network. This scheme suffers from the key escrow problem inherited from the ID-based PKC.

Liu *et al.* [8] presented 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 an 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 this scheme.

In the context of securing the PMIPv6 protocol, Chaung *et al.* proposed a secure password based authentication mechanism for seamless handover in PMIPv6 networks called SPAM [21]. The mobile node (MN) registers with the AAA server to receive authentication credentials on a smart card. When the MN joins the LMD, the user inserts the smart card and then keys in his/her identity and a password to get the authentication credentials. These credentials are utilised to perform a mutual authentication with the MAG. The authors assumed that the smart cards are tamper-proof; however, most of them are not as shown in [22]. 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 networks [23]. 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, which 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 its input-output links [24].

This paper differs from the above studies in that it identifies the security and privacy challenges of applying PMIPv6 in V2G networks and proposes 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, the proposed protocol complements the work reported in the literature to potentially deliver higher levels of EV's identity and location privacy in V2G networks.

VII. Conclusion & Future Work

In this paper, the utilisation of PMIPv6 in V2G networks has been investigated and the security and privacy concerns of EVs in this context identified. In order to achieve seamless communications between an EV and the SG while protecting the identity and location privacy of the EV, a secure and privacy-aware PMIPv6 protocol (SP-PMIPv6) for V2G networks has been proposed. SP-PMIPv6 synergistically exploits the CL-PKC and the RPBS schemes to achieve mutual authentication and identity and location privacy. Moreover, it achieves a high level of anonymity for EVs by decreasing the amount of reduction in uncertainty about the identity of an EV at the LMA on handover. Besides, SP-PMIPv6 achieves low authentication latency in comparison to the standard PMIPv6. For future work, intention is to extend the SP-PMIPv6 protocol to cover inter-domain handover and assess its performance in a real-time test bed based on Software Defined Networking (SDN), which is currently under development [25].

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] 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.

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

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

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

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

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

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

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

[18] L-Y. Yeh, J-G. Chang, W. Huang and Y-L. Tsai, " A Localized Authentication and Billing Scheme for Proxy Mobile IPv6 in VANETs," in *Proc. ICC*, Ottawa 2012, pp. 993-998.

[19] M. Wen, R. Lu, K. Zhang, J. Lei, X. Liang and X. Shen, " PaRQ: A Privacy-Preserving Range Query Scheme Over Encrypted Metering Data for Smart Grid," IEEE Trans. Emerging Topics Computing, vol. 1, no. 1, pp. 178-191, July 2013.

[20] Crypto++, "Crytpo++ Library 5.6.2 – a Free C++ class library of cryptographic schemes," 31 Aug 2015. [Online]. Available: http://www.cryptopp.com/ [Accessed 21 Oct 2015].

[21] 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.

[22] 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.

[23] 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.

[24] 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].

[25] Wi-5, "Wi-5 – What to do With the Wi-Fi Wild West," 01 Feb 2015. [Online]. Available: http://wi5.eu/. [Accessed 01 Oct 2015].