Efficient, Secure and Privacy-Preserving PMIPv6 Protocol for V2G Networks

Mahmoud Hashem Eiza, Qi Shi, Angelos K. Marnerides, Thomas Owens, and Qiang Ni

***Abstract*—To ensure seamless communications between mobile Electric Vehicles (EVs) and EV power supply equipment, support for ubiquitous and transparent mobile IP communications is essential in Vehicle-to-Grid (V2G) networks. However, it initiates a range of privacy-related challenges as it is possible to track connected EVs through their mobile IP addresses. Recent works are mostly dedicated to solving authentication and privacy issues in V2G networks in general. Yet, they do not tackle the security and privacy challenges resulting from enabling mobile IP communications. To address these challenges, this paper proposes an Efficient, Secure and Privacy-preserving Proxy Mobile IPv6 (ESP-PMIPv6) protocol for the protection of mobile IP communications in V2G networks. ESP-PMIPv6 enables authorised EVs to acquire a mobile IPv6 address and access the V2G network in a secure and privacy-preserving manner. While ESP-PMIPv6 offers mutual authentication, identity anonymity and location unlinkability for the mobile EVs, it also achieves authorised traceability of misbehaving EVs through a novel collaborative tracking scheme. Formal and informal security analyses are conducted to prove that ESP-PMIPv6 meets these security and privacy goals. In addition, via a simulated assessment, the ESP-PMIPv6 is proven to achieve low authentication latency, low handover delay, and low packet loss rate in comparison with the PMIPv6 protocol.**

***Index Terms*—Electric vehicles; Smart grids; Security; Privacy; Proxy Mobile IPv6 (PMIPv6); Vehicle-to-Grid (V2G) Networks**

I. Introduction

VEHICLE-TO-GRID (V2G) networks have emerged in the last decade as a new communication paradigm between electric vehicles (EVs) and the Smart Grid (SG). V2G networks provide charging and value-added services to EVs and empower the vision of clean and smart energy distribution in smart cities. Given the projected growing number of EVs, a variety of residential/public electric vehicle supply equipment (EVSE) (i.e., charging spots) must be widely available and easy to reach to support a smooth operation of V2G networks.

With the utilisation of several access technologies such as Power Line Communications, IEEE 802.11p, and LTE mobile communications, EVs can communicate with the charging infrastructure to initiate a charging session, negotiate and access the information required for the next charging/discharging schedule, and terminate a charging session and receive billing information. The communication interface between an EV and an EVSE in V2G networks is not holistically settled yet as parts of the current standards such as ISO 15118 [1] and SAE J2836 [2] are either under development (e.g., SAE J2836/6) or under review (e.g., ISO 15118-2:2014 [3]).

The ISO 15118-2 standard states that the IPv6 protocol is mandatory for acquiring an IP address and enabling TCP/IP communication for information exchange during the charging process of a given EV [1, 4]. Since an EV may require charging services at different geographical locations (e.g., while moving from its home network to visiting networks), the SG operator or the mobility operator should be able to keep track of the mobile EV and route it to a suitable EVSE. Thus, it is essential to maintain seamless communications between the EV and EVSEs. However, anonymity and location-privacy mechanisms should be applied to maintain the security and privacy of EVs and their users. At the same time, it is necessary to establish a link between an EV and its charging/discharging operations to ensure accountability and authorised traceability should an EV misbehave or abuse the service.

Although support for ubiquitous and transparent mobile IP communications is essential in V2G networks to maintain the smooth operation of its services, it can bring several security and privacy concerns. Enabling IP communications is one of the main reasons that V2G networks are vulnerable to attacks such as message tampering, impersonation, repudiation and location tracking [5]. Once a two-way TCP/IP communication between an EV and an EVSE is established, there is no technical limitation to the amount and type of data that could be obtained from the EV. Such data includes the EV's location, identity, state of charge, charging preferences, and driver-oriented personal data [6]. Thus, tracking locations and infiltrating the privacy and anonymity of the EV's user through the EV's mobile IP address is quite easy in this context.

M. Hashem Eiza is with the School of Physical Sciences and Computing, University of Central Lancashire, Preston PR1 2HE, U.K. (e-mail: MHashemEiza@uclan.ac.uk).

Q. Shi is with the Department of Computer Science, Liverpool John Moores University, Liverpool L3 3AF, U.K. (e-mail: Q.Shi@ljmu.ac.uk).

T. Owens is with the Department of Electronic and Computer Engineering, College of Engineering, Design and Physical Sciences, Brunel University London, London UB8 3PH, U.K. (e-mail: Thomas.Owens@brunel.ac.uk).

Q. Ni and A. K. Marnerides are with the School of Computing and Communications, Lancaster University, Lancaster LA1 4WA, U.K. (e-mails: {Q.Ni, Angelos.Marnerides}@lancaster.ac.uk).

While the aspects of authentication, anonymity and privacy-preserving communications in vehicular and V2G networks have been addressed in the literature (see [7–18]), to the best of the authors' knowledge, no previous work has addressed the security and privacy concerns of enabling mobile IP communications in V2G networks. Given the centralised nature of charging services in V2G networks, a network-based IP mobility protocol such as the Proxy Mobile IPv6 (PMIPv6) protocol [19] can be seen as a reasonable option [20] for handling EV mobility during several charging sessions. Nonetheless, the current implementation of PMIPv6 is prone to several security and privacy threats such as impersonation, man in the middle, and location tracking attacks. Moreover, it has relatively long authentication latency during an EV's handover as explained later in Section III-B.

To rectify the above problems, a secure and privacy-aware PMIPv6 (SP-PMIPv6) protocol for V2G networks was developed in [21]. SP-PMIPv6 achieved the security and location privacy of EVs using certificate-less public key cryptography (CL-PKC) and restrictive partially blind signature (RPBS) techniques. However, these techniques are algorithmically complex and computationally intensive and hence incur high implementation costs. Besides, SP-PMIPv6 focused on a centralised security solution that resulted in high communication overhead every time an EV wants to refresh its pass to access the V2G network. Moreover, it lacks on misbehaviour traceability that is important for deterring "malicious" EVs from misusing the protocol to evade their responsibilities for illegal actions.

To overcome the above weaknesses and alleviate the security and privacy concerns of EVs' users, this paper introduces an Efficient, Secure and Privacy-preserving PMIPv6 (ESP-PMIPv6) protocol for V2G communications, which is a significantly improved and extended version of the work in [21]. ESP-PMIPv6 employs public key cryptography in synergy with an RSA-based blind signature technique, and identity traceability and location unlinkability mechanisms for a balanced and strong provision of efficiency, security and privacy. This paper aids the aspect of security and privacy of mobile IP communications in V2G networks with the following five novel contributions:

1) The ESP-PMIPv6 protocol utilises a novel built-in tagging scheme in an RSA-based blind signature to issue an access pass to an EV. This pass allows an EV to anonymously access a mobile IP-enabled V2G network. At the same time, it prevents any network entity from tracking or profiling the EV's real identity while moving using its acquired mobile IP address.
2) A new proxy-based distributed and collaborative approach to generating access pass trees for each legitimate EV is proposed for the ESP-PMIPv6 protocol. This allows an EV to generate new passes under different identifiers using its current valid access pass. Consequently, the approach achieves stronger location unlinkability and better workload distribution among the authentication and traceability servers used.
3) ESP-PMIPv6 provides a new mechanism for dedicated authorities to initiate a collaborative misbehaviour traceability process for tracking down a misbehaving EV to reveal its identity and location information. They can either initiate a backward trace (i.e., find out the EV's real identity using its access pass) or a forward trace (i.e., given an EV's real identity, find out the locations it has visited).
4) ESP-PMIPv6 achieves a balanced implementation of the security and privacy goals for a mobile IP-enabled V2G network, including mutual authentication between an EV and the network entities, protection against replay, man in the middle, message tampering and impersonation attacks, and EV anonymity and untraceability.
5) The developed ESP-PMIPv6 protocol allows much more efficient access pass authentication and strengthens the aspect of seamless handover with a relatively low authentication delay and low computational complexity.

The rest of this paper is structured as follows. Section II reviews the related works in the literature. Section III presents the preliminaries relevant to the paper. Section IV describes the PMIPv6-enabled V2G network scenario considered for the ESP-PMIPv6 protocol design. Section V presents the developed ESP-PMIPv6 protocol operations in detail. Section VI provides the security and privacy analysis of the protocol. Section VII covers the performance evaluation of ESP-PMIPv6. Finally, Section VIII concludes the paper.

II. Related Works

Aspects of security, privacy and traceability in V2G networks have been addressed in different contexts throughout the literature (see [7–15]). Given the fact that this work is directly related to the PMIPv6 protocol, only the most significant studies on the improvement of the protocol and its variations are reviewed and compared below.

Chaung *et al.* in [22] have proposed a secure password-based authentication mechanism for seamless handover in PMIPv6 networks called SPAM. A mobile node (MN) registers with an Authentication, Authorisation and Accounting (AAA) server to receive authentication credentials on a smart card. When an MN joins a Local Mobility Domain (LMD), the user inserts its smart card and keys in its identity and password to get authentication credentials. These credentials are utilised to perform a mutual authentication with a Mobile Access Gateway (MAG). Chaung et al. integrated SPAM with a bicasting scheme to avoid packet loss problems while performing handover. The authors assumed that the smart cards are tamper-proof; however, most of them are not as shown in [23]. Besides, smart cards are vulnerable to loss and/or theft. Finally, SPAM is also susceptible to password guessing attacks.

Kong *et al.* in [24] and [25] utilised the AAA infrastructure to authenticate a given MN in PMIPv6 networks. However, both works inherit high packet loss and inefficient authentication problems during handover. In this paper, the

latency caused by the AAA server is overcome, since an EV executes only a single AAA authentication phase when it first joins the V2G network and subsequently the introduced pass is used. Hence, the (re)authentication latency is avoided during any handover while the EV joins a new MAG. Lee and Chung [26] proposed two secure authentication procedures for PMIPv6, but similar to Kong *et al.*, they did not consider the handover procedure. In particular, their handover was still based on the original PMIPv6 procedure that naturally results in high handover authentication latency.

In [27], Kang *et al.* proposed an enhanced user authentication scheme in PMIPv6 networks to overcome the shortcomings of the smartcard-based authentication scheme developed by Alizadeh *et al.* [28]. Alizadeh's scheme involves three stages: i) registration phase where a user keys in its password into the smartcard that communicates with the AAA server to register; ii) mutual authentication phase where the smartcard (i.e., MN) and a MAG authenticate each other; and iii) password change phase where the user can change its password in the smartcard and repeat the process. According to Kang *et al.*, Alizadeh's scheme is vulnerable to offline password guessing, MN and/or MAG impersonation, and session-key-derived attacks. Hence, they proposed an enhancement that uses biometric information and a dynamic identity to mitigate the security drawbacks of Alizadeh's scheme. Nonetheless, as mentioned earlier, smart cards are not tamper-proof and vulnerable to loss and/or theft. Besides that, neither of these two schemes proposed a mechanism for an authorised traceability should the MN misbehave.

Taha and Shen have proposed an anonymous and location privacy-preserving scheme (ALPP) for mobile IPv6 heterogeneous networks [29]. ALPP includes two subschemes: 1) anonymous home binding update to add anonymity and location privacy to mobile IPv6 binding updates; and 2) anonymous return routability to protect the anonymity of return routability control messages. The authors utilised onion routing to repeatedly encrypt the transmitted messages at each intermediate node to achieve location privacy of mobile nodes. To authenticate a MN to its foreign gateway and keep the computational cost of the certificate management process minimised, ALPP uses CL-PKC. However, the utilisation of onion routing in ALPP makes it computationally expensive. Besides that, many works have shown the susceptibility of onion routing when adversaries have access to large fractions of its input-output links [30].

As already mentioned, the work in [21] aimed to overcome the aforementioned constraints from the literature. However, there were still issues of computational complexity within the generation of the RPBS-based pass, whereas the herein reported work (as clearly described in Section V) is much simpler and more efficient. Moreover, the work in [21] was mainly targeting a centralised security scheme where the capabilities of pass tagging, proxy-based distributed pass issuing and misbehaved EV tracking are not considered.

In contrast to the above, the approach presented in this paper operates in a distributed fashion to accomplish these new capabilities. It allows an EV to utilise a valid pass to acquire other passes for use at different MAGs. These anonymous and apparently unlinked passes strengthen the preservation of the EV's identity and location privacy, if it does not misbehave. Otherwise, tags embedded in the passes help an authority to revoke the EV's privacy protection by tracking down its real identity, used passes and visited MAGs to construct a trace of activities for the investigation of its misbehaviour. Such traceability can deter the misuse of the services offered by the new ESP-PMIPv6 protocol.

TABLE I – NOTATIONS

m	A message
CA	Certificate Authority
TS	Traceability Server
PK, SK	A pair of public/private keys
r	A random number where $r \in \mathbb{Z}_N^*$
P_{pub}	The public key of a certificate authority (CA)
$H(\cdot)$	A secure hash function
$Enc(\cdot)$	A symmetric encryption function
$PKE(\cdot)$	A public key encryption function
M	The access *pass* template
TPK_{EV1}, TSK_{EV1}	The temporary public/private keys of EV1
T	A ticket
Ψ	The requested access *pass* expiration time
S_{key}	A random symmetric session key
PI	A unique access *pass* identifier
TC	The terms and conditions of the provided service
Ω	TS's signature on M and TPK_{EV1}
PID	A random pseudo identity
Δd	Random delay during the handover process
λ	Arrival rate of EVs at a MAG

III. PRELIMINARIES

In this section, the RSA-based blind signature scheme and the basic PMIPv6 protocol operations in V2G networks are introduced. The main notations used throughout this paper are given in Table I.

A. RSA-based Blind Signature

The first RSA-based blind signature scheme was proposed in [31] to enable a requester R to obtain a signature on a message m without revealing anything about m to the signing authority (SA). This provides message anonymity to R. Let N be a large public parameter defined by SA, and (PK, SK) be its public and private keys, respectively. The requester R generates a random number $r \in \mathbb{Z}_N^*$, computes $m` \equiv m \cdot r^{PK} \ (mod\ N)$ where $r^{PK}$ is a blinding factor and $m < N$, and sends $m`$ to SA. Upon receiving the message, SA computes $S` \equiv (m`)^{SK} \ (mod\ N)$ and sends $S`$ to R. Based on received $S`$, R calculates $S \equiv S` \cdot r^{-1} \ (mod\ N) \equiv (m`)^{SK} \cdot r^{-1} \ (mod\ N) \equiv m^{SK} \cdot r^{PK \cdot SK} \cdot r^{-1} \ (mod\ N) \equiv m^{SK} \ (mod\ N)$, which is SA's signature on m. Here, $r \cdot r^{-1} \equiv 1 \ (mod\ N)$ and $r^{PK \cdot SK} \equiv r \ (mod\ N)$.

B. PMIPv6 Protocol in V2G Networks

The EV mobility is handled within a PMIPv6 LMD through the following network entities [19]: 1) the Local Mobility Anchor (LMA); 2) the MAGs; and 3) the AAA Server.

LMA maintains binding cache entries for tracking the locations of EVs in its domain and directs traffic intended for them towards their current locations. MAGs are responsible for performing the mobility signalling with LMA on behalf of EVs. Finally, the AAA server is responsible for authenticating EVs and authorising them to access the LMD. Fig. 1 shows the PMIPv6 signalling flow when EV1 joins the LMD and performs a handover from MAG1 to MAG2. The Corresponding Node (CN) in Fig. 1 could be any entity in the SG charging infrastructure such as a central aggregator (CAG), charging and billing server, *etc*. The messages utilised in this process are: Router Solicitation (RS), Proxy Binding Update (PBU), Proxy Binding Acknowledgment (PBA), and Router Advertisement (RA).

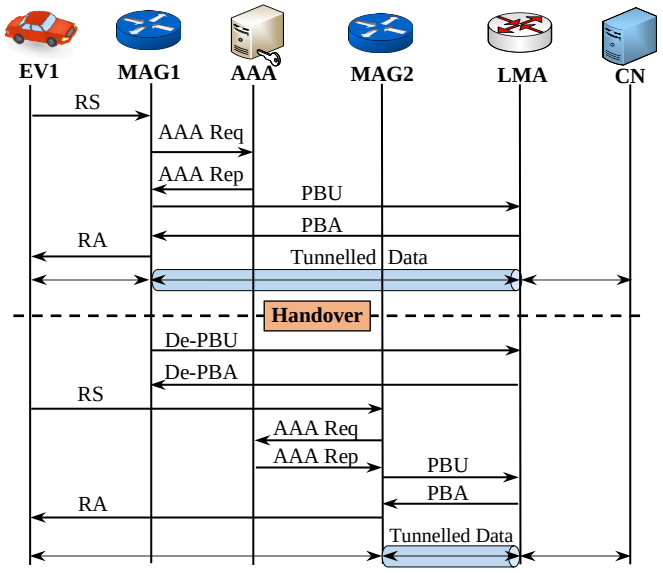


Fig. 1. PMIPv6 Signalling Flow in V2G Network [21]

IV. PMIPv6-Enabled Vehicle-to-Grid (V2G) Network

A. System Model

The V2G network model considered in this paper is illustrated in Fig. 2. It is assumed that the PMIPv6-enabled V2G network (i.e., the LMD) serves a city, which represents a local SG. This model is targeted at personal EVs and does not include other electric forms of transportation such as electric buses. The investigation of a wider V2G network model is outside the scope of this paper and left for future work.

When EV1 acquires an IPv6 address, it can retain this address as long as it is moving within the LMD. It should be noted that the Traceability Server (TS) in Fig. 2 is not part of the standard PMIPv6 scenario. Thus, it has no access to the PMIPv6 network and only communicates with AAA through a secure channel. Note that there is only one TS in the network. TS is added to provide traceability in the proposed ESP-PMIPv6 protocol as to be explained later in Sections V and VI. It is assumed that a trusted third party (i.e., neither the SG operator nor the mobility operator) manages the TS.

In Fig. 2, MAGs, LMA and AAA are managed either by the SG operator or a mobility operator, which handles communications in the SG. LMA keeps track of the location of EV1 and directs its data traffic to the corresponding MAG. MAGs do not maintain binding cache entries for mobile EVs. The TS and AAA server keep certain information regarding the requested access passes from EVs for traceability purposes, as to be explained later in Section V.

To maintain session continuity and preserve the service context between EV1 and the CN, EV1 should keep the same IPv6 address while moving among different networks. In this way, the data from CN can be routed to EV1 through the LMA to the MAG it is attached to. However, once the current service session is over, EV1 can acquire a new IPv6 address to achieve a higher level of location unlinkability.

Finally, each EV that wishes to access the LMD has to follow *TC*, the terms and conditions of the provided service. *TC* is publicly known by every entity in the system and defines the validity scope of the access being granted to an EV to prevent it from being abused for any other purposes.

B. System Security & Key Management Assumptions

It is assumed that the communication between LMA and a MAG is protected using IPSec Encapsulating Security Payload (ESP) in transport mode with mandatory integrity protection [19]. A certificate authority (CA) exists and is trusted by all entities in the system. Each entity in the system is assumed to have a certificate *Cert*, which contains its identity and public key issued by CA. The CA publishes the system parameters (P_{pub}, PK_{AAA}, PK_{TS}, H, $Enc(\cdot)$), where P_{pub} is CA's public key, PK_{AAA} and PK_{TS} are the public keys of AAA and TS, respectively, H is a secure hash function such as SHA-3, and $Enc(\cdot)$ is a symmetric encryption algorithm. Moreover, over the secure channel between them, TS and AAA are mutually authenticated to each other prior to the system start.

Each MAG in the system is assumed to be verified through its $Cert_{MAG}$ and registered at the AAA server. These MAGs are authorised to act as proxies for TS or AAA for the purpose of issuing access pass trees, as to be explained later in Section V-D. AAA delivers the list of all legitimate MAGs in the system to MAGs, and EVs when they register to access the LMD, as to be explained in Section V-B. If this list is updated (e.g., new authorised MAGs are added, or a MAG updates its key), MAGs will receive the updated list from AAA while EVs will get the list when they renew their access passes. If a MAG is revoked from the MAG list for being compromised or distrusted, AAA broadcasts the revoked MAG(s) to all other MAGs to avoid any passes issued by the revoked MAG(s). In this case, EVs that possess any passes issued by the revoked MAG(s) can no longer use them but can still use their original access pass or passes issued by other MAGs. Hence, their access to the LMD will not be interrupted.

If TS and/or AAA decide to update their keys, the CA will publish an updated list of the system parameters to all entities in the system. To minimise the effect of this change to the current issued access passes, the update process is expected to take effect overnight. Besides that, this update is assumed to be

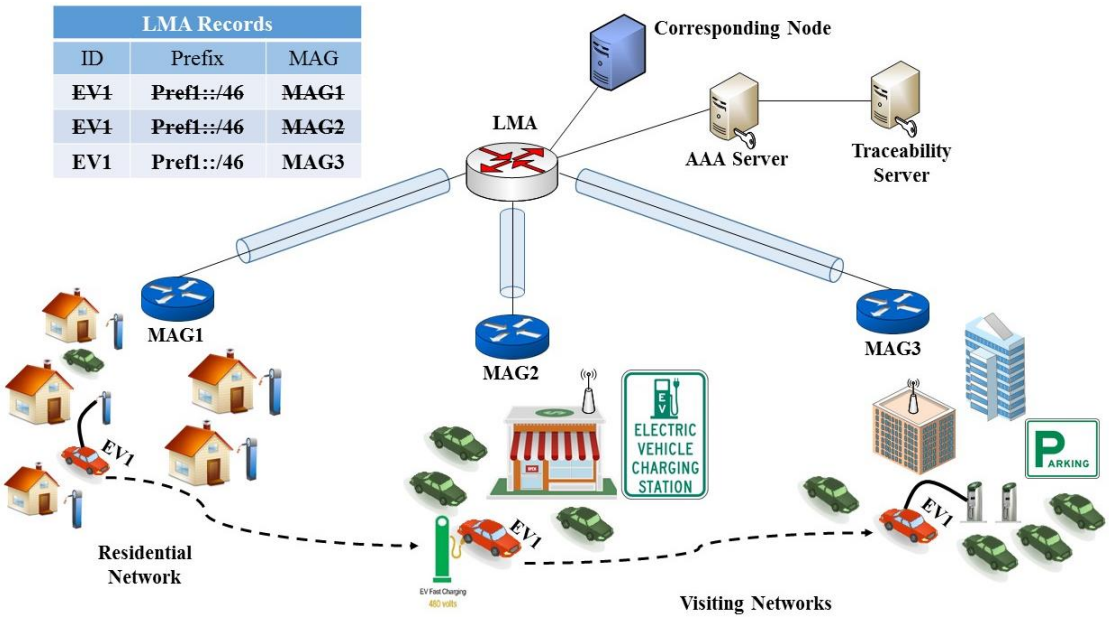


Fig. 2. PMIPv6-enabled V2G Network

infrequent given the nature of the TS and AAA servers' roles and their security measures. It is worth noting that EVs' access pass validity is limited to 24 hours, as explained later. In addition, an old key pair and its updated one can coexist for up to 24 hours. During this brief period, the old key pair can still be used for the verification of the previously created access passes but it cannot be used to issue new passes. Only the updated key pair can issue and verify new access passes. After the coexisting period, all the previously created access passes are expired, so the old key pair becomes invalid. Hence, the effect of updating the PK and SK keys of AAA, TS, and even MAGs on the previously created access passes is kept minimal.

Note that in case a key pair needs to be revoked immediately without the above coexisting period, the MAG revocation case discussed earlier can be applied to invalidate all relevant passes even if they have not expired.

C. Threat Model

In Fig. 2, any network entity can be considered as an adversary if it misbehaves or deviates from its legitimate operations. Due to the openness of wireless communications and the deployment of MAGs in an unfenced environment, two types of adversary are considered here: external and internal.

An external adversary is an entity outside the network that can capture messages and analyse packets transmitted between the communicating entities to spot their identities, track their locations, and reveal the contents of transmitted packets if it possesses the corresponding decryption keys. Thus, it can perform attacks such as man in the middle, replay, message tampering, and impersonation. An internal adversary is an entity within the network (e.g., a compromised MAG), or a misbehaving EV, which engages in similar illicit activities. A misbehaving EV can perform a repudiation attack to evade its responsibilities (e.g., not paying for consumed power) and abuse the service.

The following assumptions are made in the threat model adopted. First, the LMA, TS and AAA server are semi-trusted in the sense that they always perform their assigned operations correctly and do not collude directly or indirectly for illicit operations. However, they may misbehave independently, and even collude with some MAGs and EVs, for gathering EVs' private information. Secondly, MAGs always keep correct EV records required, which will be specified in the next section, and offer authorised access to them. However, MAGs may conspire with other MAGs and EVs in addition to the collusion in the first assumption.

V. Efficient, Secure & Privacy-Preserving PMIPv6 (ESP-PMIPv6) Protocol

A. ESP-PMIPv6 Security and Privacy Objectives

To protect an EV's privacy and prevent possible attacks due to enabling mobile IP communications in V2G networks, the following main security, privacy and performance requirements are imposed:

1) Mutual authentication between the EV and the network entities including the AAA server, TS, and MAGs to prevent impersonation attacks and unauthorised access to the mobility domain.
2) Anonymity and location privacy for all mobile EVs. No entity in the network including LMA, AAA, TS and MAGs is able to illegitimately reveal an EV's real identity or track its locations using its acquired mobile IPv6 address. Moreover, external adversaries should not be able to spot the EV's ID from intercepted messages.
3) Message integrity and confidentiality. All the transmitted messages among the network entities must be protected against replay attacks or exposing an EV's real identity or utilised keys.
4) Forward and Backward traceability. An authorised entity

should be able to trace an EV's real identity using its access pass should that EV misbehave. Moreover, given an access pass, an authorised entity should be able to find a full trace of the EV's movements within the mobility domain.

5) Low computation complexity and authentication latency especially during handover to ensure seamless communications between EVs and the SG.

B. Access Pass Generation

To join a LMD, each EV must register its identity with the AAA server and request an anonymous access *pass*. The pass is only used to access the PMIPv6-enabled V2G network, whereas the aspects of billing and rewarding related to the charging/discharging processes are handled after establishing the IP connection. In the following, the steps needed to generate an anonymous access pass for an EV, denoted as EV1, are described, which are also illustrated in Fig. 3 with message validation details omitted for easier understanding:

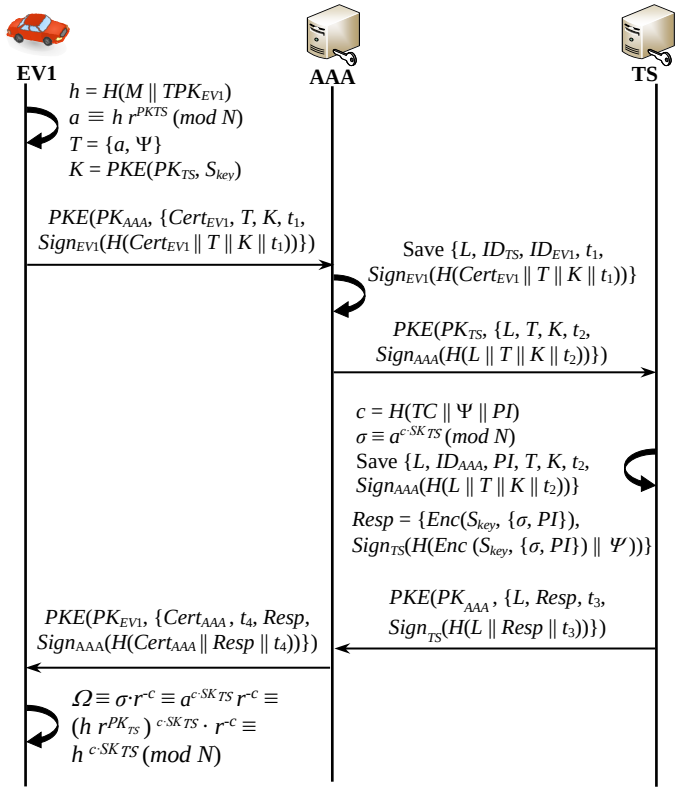


Fig. 3. ESP-PMIPv6 – Access Pass Generation Process

1) EV1 fills in an access pass template M tied to the terms and conditions TC of the provided service. Then, it generates a pair of temporary public and private keys (TPK_{EV1}, TSK_{EV1}), and computes $a \equiv h{\cdot}r^{PK_{TS}}\ (mod\ N)$, where $h = H(M \parallel TPK_{EV1})$ and $r \in \mathbb{Z}_N^*$ is a random number. Based on a, it formulates a ticket $T = \{a, \Psi\}$ where Ψ is the requested access pass expiration time. Note that Ψ is chosen by EV1 from a list of available times offered by AAA. This means that multiple access passes are likely to have the same expiration time, so Ψ cannot be used to track down a particular EV by adversaries. It is assumed that Ψ is limited to 24h. This is essential to make sure that the issued access pass will expire quickly and thus require EV1 to renew it. In this way, it becomes even harder for adversaries to track down a particular EV through its current access pass as to be discussed in Section VI.

   Afterwards, EV1 computes $K = PKE(PK_{TS}, S_{key})$, where S_{key} is a random symmetric session key and PK_{TS} is TS's public key. EV1 then sends its request $PKE(PK_{AAA}, \{Cert_{EV1}, T, K, t_1, Sign_{EV1}(H(Cert_{EV1} \parallel T \parallel K \parallel t_1))\})$ to AAA. Here, $Cert_{EV1}$ is EV1's public key certificate, t_1 is a timestamp, and $Sign_{EV1}$ is EV1's signature on $Cert_{EV1}$, T, K and t_1.

2) Having validated the received request via $Cert_{EV1}$ and $Sign_{EV1}$, AAA chooses a unique session label L and saves $\{L, ID_{TS}, ID_{EV1}, t_1, Sign_{EV1}(H(Cert_{EV1} \parallel T \parallel K \parallel t_1))\}$ in its records, where ID_{TS} and ID_{EV1} are the identities of TS and EV1, respectively. Recording EV1's signature $Sign_{EV1}$ is essential for holding it accountable for the access pass request. In case EV1 misbehaves, the record can be used to track it down as will be detailed in Section VI-D. Afterwards, AAA submits $PKE(PK_{TS}, \{L, T, K, t_2, Sign_{AAA}(H(L \parallel T \parallel K \parallel t_2))\})$ to TS for the issuance of the requested access pass.

3) After the successful validation of the received request via $Sign_{AAA}$, TS yields a unique access pass identifier PI and applies $T = \{a, \Psi\}$ to compute $c = H(TC \parallel \Psi \parallel PI)$. Afterwards, TS computes $\sigma \equiv a^{c \cdot SK_{TS}}\ (mod\ N)$, and extracts S_{key} from K with its private key SK_{TS}. Similar to AAA, TS records $\{L, ID_{AAA}, PI, T, K, t_2, Sign_{AAA}(H(L \parallel T \parallel K \parallel t_2))\}$ for traceability purposes. TS creates $Resp = \{Enc(S_{key}, \{\sigma, PI\}), Sign_{TS}(H(Enc(S_{key}, \{\sigma, PI\}) \parallel \Psi))\}$. Finally, TS sends $PKE(PK_{AAA}, \{L, Resp, t_3, Sign_{TS}(H(L \parallel Resp \parallel t_3))\})$ to AAA.

4) Upon the message reception and successful validation via its signature, AAA transfers $PKE(PK_{EV1}, \{Cert_{AAA}, t_4, Resp, Sign_{AAA}(H(Cert_{AAA} \parallel Resp \parallel t_4))\})$ to EV1.

5) EV1 decrypts the received message using SK_{EV1} and S_{key} and then validates it via $Sign_{AAA}$ and $Sign_{TS}$. If positive, it calculates $\Omega \equiv \sigma{\cdot}r^{-c} \equiv a^{c \cdot SK_{TS}} \cdot r^{-c} \equiv (h{\cdot}r^{PK_{TS}})^{c \cdot SK_{TS}} \cdot r^{-c} \equiv h^{c \cdot SK_{TS}}\ (mod\ N)$, which is TS's signature on M and TPK_{EV1} due to $h = H(M \parallel TPK_{EV1})$. This signature is tagged with PI through c for EV1's traceability, and its validity is restricted by TC and Ψ included in c. The access pass for EV1 is thus $pass_{EV1} = \{ID_{TS}, M, TPK_{EV1}, \Omega, \Psi, PI\}$.

Note that EV1's keys (TPK_{EV1}, TSK_{EV1}) are uniquely associated with its $pass_{EV1}$, as TPK_{EV1} is certified via h by TS although it does not know the key. This allows EV1 to use the keys for authentic communications with MAGs as to be shown below. It should also be noted that (TPK_{EV1}, TSK_{EV1}) are not used during this process (i.e., communications with the AAA and TS servers) to make sure that EV1's anonymity is maintained, and traceability will only be possible via the mechanism to be explained later. EV1 can change this pair of keys for each new access pass.

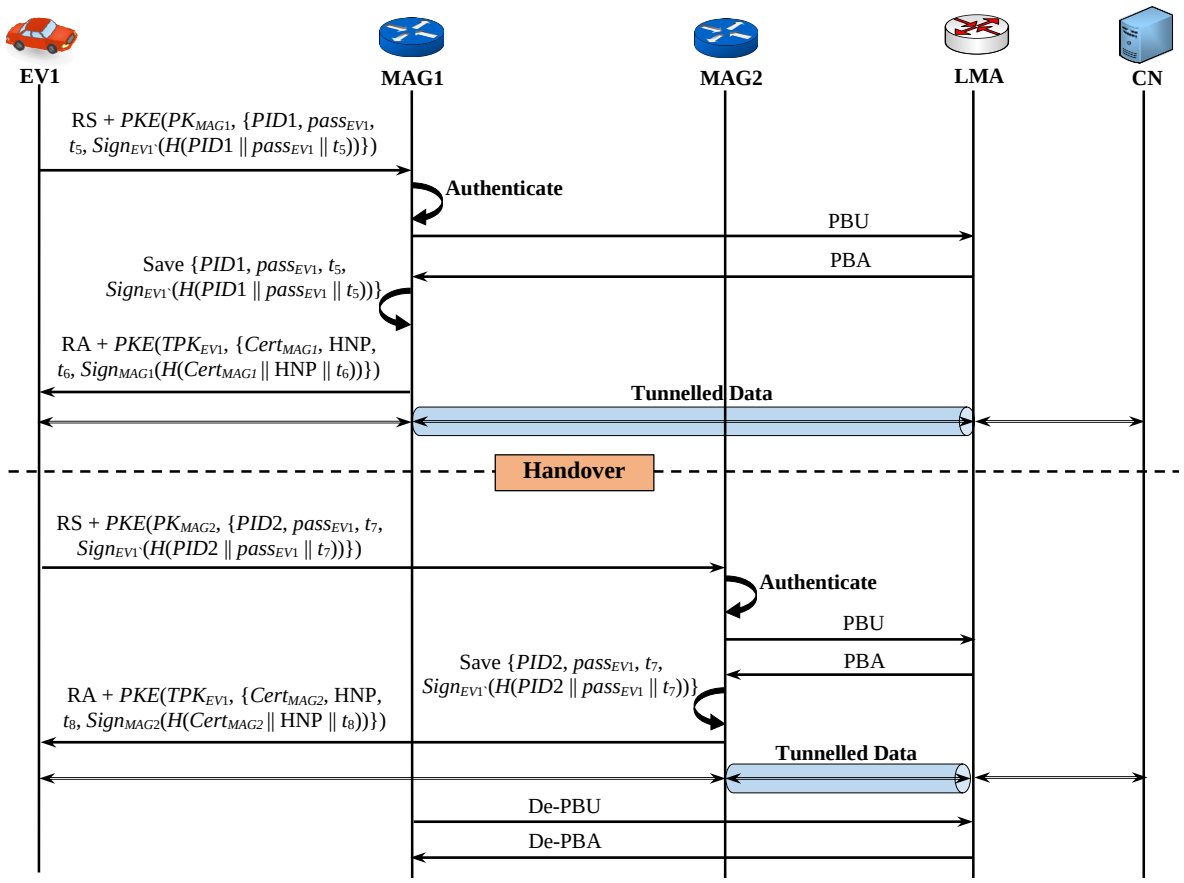


Fig. 4. ESP-PMIPv6 – Establishing Mobility Sessions and Handover Signalling

C. *Establishing Mobility Sessions & Handover Processes*

When EV1 attaches to a MAG denoted as MAG1, it generates a random pseudo identity *PID*1, which is produced every time EV1 attaches to a new MAG. EV1 then sends $PKE(PK_{MAG1}, \{PID1, pass_{EV1}, t_5, Sign_{EV1`}(H(PID1 \| pass_{EV1} \| t_5))\})$ within the RS message to MAG1. Note that EV1 uses $TSK_{EV1}$ to generate $Sign_{EV1`}$ and it does not send its long-term public key certificate to MAG1.

Following the reception and decryption of the RS message, MAG1 confirms that $pass_{EV1}$ is not expired and *M* follows the correct template as follows. MAG1 computes $c = H(TC \| \Psi \| PI)$ and $h` = H(M \| TPK_{EV1})$. It checks if $\Omega^{PK_{TS}} \equiv h^{`c} \pmod N$ holds. If yes, then $pass_{EV1}$ is verified and EV1 is authenticated and authorised to join LMD. Subsequently, MAG1 sends a PBU message to LMA, which contains *PID*1. LMA creates a new binding entry for *PID*1 and sends back a PBA message to MAG1. MAG1 then saves $\{PID1, pass_{EV1}, t_5, Sign_{EV1`}(H(PID1 \| pass_{EV1} \| t_5))\}$ for the traceability purposes, and sends $PKE(TPK_{EV1}, \{Cert_{MAG1}, HNP, t_6, Sign_{MAG1}(H(Cert_{MAG1} \| HNP \| t_6))\})$ within the RA message to EV1 where HNP is the Home Network Prefix. Finally, EV1 validates the received message, authenticates MAG1 via its signature and configures its IPv6 address using HNP. The above process is illustrated in Fig. 4 with the message validation or authentication details omitted for easier understanding.

Now, data from the CN can be routed to EV1 based on the newly created binding entry at LMA that points to MAG1, where EV1 under pseudo identity *PID*1 is currently attached. Note that routing data packets is based on LMA's advertisement of reachability of that network prefix, as shown in Fig. 2.

Later on, as shown in Fig. 4, an authentication is performed when EV1 moves to a new location, detaches from MAG1 and uses a new *PID*2 to attach to another MAG signified as MAG2. In this case, a new access pass $pass_{EV1`}$ might be used along with *PID*2, which will be discussed further in the next sub-section. It can be observed in Fig. 4 that the transmission of the De-PBU and De-PBA messages between MAG1 and LMA is delayed by a random value Δd. This is done to deter the LMA capability to link the deregistered *PID*1 with the newly registered *PID*2. Therefore, within Δd, LMA maintains two entries with different PIDs for EV1 while, to LMA, they appear as two different identities of two different EVs. Note that within Δd, data packets from the CN will be routed to both MAG1 and MAG2 while EV1 is only attached to MAG2, causing extra resource consumption. However, Δd is assigned a very small value to keep the delayed deregistration impact minimum on the network performance. Once the deregistration is complete, data will be routed based on the only record LMA has for EV1 under *PID*2. In this way, the CN can keep the communication session with EV1 during and after the handover from MAG1 to MAG2.

While not communicating with AAA, as shown in Fig. 4, the

protocol reduces the communication overhead during the handover, but some security issues could arise in case a MAG is compromised. As mentioned earlier, the list of MAGs is updated and disseminated by AAA to EVs when they register/renew their passes. It is possible that EV1 communicates with a compromised MAG that is not spotted yet by AAA. On one hand, the impact of such a MAG on EV1 is very limited since the compromised MAG will be able to neither reveal the real identity of EV1 nor benefit from stealing its pass, as to be detailed later in Sections VI-B and VI-C. On the other hand, EV1 could be denied access to the LMD by the compromised MAG. To mitigate this problem, AAA or the mobility operator could observe the operations of MAGs periodically to ensure they are not compromised. The investigation of this solution is outside the scope of this paper and left for future work.

D. Access Pass Trees

ESP-PMIPv6 allows an EV to utilise its valid access pass to apply for new passes with different identifiers. This enables the EV to use different passes at different MAGs, which makes the illegitimate linkage of the EV's identities and locations much harder, so as to achieve higher levels of privacy protection and anonymity.

Note that the EV can simply repeat the access pass issuing process in Fig. 3 to obtain multiple passes from AAA. However, this centralised solution is likely to lead to a bottleneck problem at AAA, which causes delays to the access pass issuing, when it receives a large number of pass requests. Thus, a distributed approach is proposed below for generating a tree of new access passes for the EV from its valid pass granted by AAA.

The main idea underpinning the approach is to allow the authorised MAGs to act as a proxy of AAA or TS to issue new access passes from a valid pass of the EV without any involvement of AAA and TS. Hence, such pass generation does not incur extra workloads on AAA or TS and allows the workloads to be distributed among the authorised MAGs. Also, adding these MAGs to the issuance of access passes makes the illicit linkage of the EV's identities and locations even more difficult, because such linkage necessitates the compromise of more network entities such as the MAGs.

More specifically, after the EV has successfully attached to a MAG via the process in Fig. 4 using a valid access pass, it can request the MAG for a new pass if needed. In this case, the MAG serves as a proxy of AAA (i.e., AAA-proxy). The EV then randomly selects another MAG as a proxy of TS (i.e., TS-proxy) based on the list obtained from AAA at the registration phase. As the AAA-proxy MAG has already confirmed the validity of the EV's access pass received, they can follow the process in Fig. 3 to get a new pass issued by the TS-proxy MAG. The new access pass should bear the same expiration time as the current pass. This ensures that when the original access pass granted by AAA is expired, all the passes issued directly or indirectly from it are also expired, as the EV is no longer eligible for further services from any MAGs after the expiration time.

Similarly, the EV can use the new access pass to obtain another pass from two different MAGs during a visit to one of them before it expires. This means that the EV can obtain a tree of access passes from the original pass received from AAA. To avoid overloading a MAG with a large number of new pass requests, each MAG limits the number of new passes issued to an EV to one only, based on a single valid pass.

The process in Fig. 3 is now applied to elaborate the above idea to show how EV1 gets a new access pass $pass_{EV1}$` based on its valid pass $pass_{EV1}$ from two MAGs, MAG_i as an AAA-proxy and MAG_j as a TS-proxy. By replacing AAA and TS in Fig. 3 with MAG_i and MAG_j respectively, the first stage of the process performed by EV1 remains largely unchanged. Here, the expiration time Ψ for the new access pass is inherited from the one in $pass_{EV1}$. $Cert_{EV1}$ in the encrypted message is replaced by ID_{MAGj}, the identity of the TS-proxy, as MAG_i has already confirmed the validity of public key TPK_{EV1} associated with $pass_{EV1}$. The signature in the encrypted message is signed with the private key TSK_{EV1} paired with confirmed TPK_{EV1}.

The second stage executed by MAG_i in Fig. 3 is still the same except that MAG_i needs to confirm the use of the same expiration time Ψ for both passes. Afterwards, there is no change to the rest of the pass generation process. As illustrated in Fig. 3, MAG_i saves $\{L`, ID_{MAGj}, PI, t_1`, Sign_{EV1}(H(ID_{MAGj} \| T` \| K` \| t_1`))\}$, while $MAG_j$ records $\{L`, ID_{MAGi}, PI`, T`, K`, t_2`, Sign_{MAGi}(H(L` \| T` \| K` \| t_2`))\}$, after the generation of new pass $pass_{EV1}$` for the traceability purposes.

From the above description, it is evident that MAG_i can see $pass_{EV1}$ but not $pass_{EV1}$`, whereas $MAG_j$ knows the identifier $PI$` of $pass_{EV1}$` but not $pass_{EV1}$. In other words, neither of them can link the two passes together. As only $pass_{EV1}$ is used to produce $pass_{EV1}$`, the MAGs cannot see any information on EV1's real identity either.

Although MAG_j has issued $pass_{EV1}$`, it has no information to infer that EV1 has been located at $MAG_i$. Also, when using $pass_{EV1}$` at another MAG different from MAG_i and MAG_j, the third MAG can see that $pass_{EV1}$` was issued by $MAG_j$, but it is unable to find out any previous MAGs that EV1 has visited, as the issuance of $pass_{EV1}$` by MAG_j does not mean that EV1 has visited MAG_j. This protects EV1's location privacy.

Note that EV1 has the choice of whether to use a new access pass after a handover to a different MAG. This decision depends on the level of anonymity/privacy that EV1 requires.

E. Authorised Identity and Location Tracking

Assume that EV1 misbehaved and there is a legal requirement to reveal its real identity and/or trace its movements within LMD, and that AAA has been authorised to perform the task. Three cases are considered here: i) a pass used by EV1 is given as $pass_{EV1}$`, so the task is to trace backwards to discover EV1's real identity; ii) the real identity of EV1 is given, so the task is to trace forward for the collection of all the passes used by EV1; and iii) all the passes of EV1 have been provided, so the task is to find out all the MAGs visited by EV1 using these access passes. Obviously, these cases can be

combined to handle other scenarios. For example, given a pass, reveal EV1's real identity and identify all its used passes and visited MAGs. In the following, each case is explained in detail.

i) Here, the main idea is to explore the recorded links between EV1's access passes, which are kept by AAA, TS and MAGs as illustrated in Figures 3 and 4. As any pass issued by a TS-proxy MAG is always based on another pass produced earlier, this link can be established via the records saved by the MAG and its associated AAA-proxy MAG. Similarly, the earlier access pass can be used to identify another one from which the pass was granted. This backward tracking process continues until the pass issued by TS is reached, which then enables the AAA server to reveal the real identity of EV1.

The above idea is implemented by the following steps.

a) Suppose that the correctness of the given access pass $pass_{EV1}` = \{ID_{MAGj}, M`, TPK_{EV1}`, \Omega`, \Psi, PI`\}$ has been confirmed. AAA then sends a signed request to TS-proxy $MAG_j$, which issued $pass_{EV1}`$, for its saved record with identifier $PI`$ listed in $pass_{EV1}`$. The message is expressed as $PKE(PK_{MAGj}, \{PI`, t_9, Sign_{AAA}(H(PI` \| t_9))\})$.

b) After the successful decryption and validation of the received request, MAG_j searches its records based on given $PI`$. As $MAG_j$ issued $pass_{EV1}`$, it should have the record $R_j = \{L`, ID_{MAGi}, PI`, T`, K`, t_2`, Sign_{MAGi}(H(L` \| T` \| K` \| t_2`))\}$, as presented in Section V-D. MAG_j then sends the record back to AAA as $PKE(PK_{AAA}, \{R_j, t_{10}, Sign_{MAGj}(H(R_j \| t_{10}))\})$.

c) Upon receipt of MAG_j's response, AAA decrypts the message and confirms the presence of $PI`$ in the message as well as the message validity via $Sign_{MAGj}$. It then verifies $Sign_{MAGi}$ in received $R_j$ to assure its correctness. Afterwards, based on $MAG_i$'s identity $ID_{MAGi}$ and its label $L`$ listed in R_j, AAA transfers a signed request to MAG_i for its stored record labelled with $L`$, which is represented as $PKE(PK_{MAGi}, \{L`, t_{11}, Sign_{AAA}(H(L` \| t_{11}))\})$.

Note that for any failure of AAA's verifications, it asks MAG_j to re-transmit its record. As assumed in Section IV-C, MAGs always keep correct records required. Hence, if MAG_j has operated normally, AAA should eventually receive the correct record requested. However, it is possible that MAG_j is compromised and issued the pass to EV1 illicitly without a valid request from an AAA-proxy MAG. In this case, MAG_j would fail to provide a valid record to AAA. Thus, the traceability of ESP-PMIPV6 is to hold MAG_j accountable for the misbehaviour of EV1. This problem can be mitigated by using multiple TS-proxy MAGs to jointly issue a pass, which is not covered in this paper. The above discussion also applies to AAA-proxy MAGs.

d) After the decryption and validity confirmation of AAA's request, MAG_i uses received $L`$ to locate its record $R_i = \{L`, ID_{MAGj}, PI, t_1`, Sign_{EV1`}(H(ID_{MAGj} \| T` \| K` \| t_1`))\}$. As stated in Section V-D, $MAG_i$ accepted EV1's pass generation request only after its successful attachment to $MAG_i$. This means that $MAG_i$ has another saved record $R_i` = \{PID1, pass_{EV1}, t_5, Sign_{EV1`}(H(PID1 \| pass_{EV1} \| t_5))\}$ for EV1 as defined in Fig. 4, where $PI$ in $R_i$ also appears in $pass_{EV1} = \{ID_{TS}, M, TPK_{EV1}, \Omega, \Psi, PI\}$. Hence, $MAG_i$ used $PI$ to find $R_i`$. Afterwards, it sends its signed response $PKE(PK_{AAA}, \{R_i, R_i`, t_{12}, Sign_{MAGi}(H(R_i \| R_i` \| t_{12}))\})$ to AAA.

e) Having decrypted and verified MAG_i's message successfully, AAA examines the validity of $Sign_{EV1`}$ and $pass_{EV1}$ in received $R_i`$. It also confirms the correctness of the signature in R_i using items $T`$ and $K`$ in R_j received earlier from MAG_j.

After the successful completion of the above verifications, AAA uses $pass_{EV1}$ to repeat above steps *a*) and *b*) to obtain a record $R_{TS} = \{L, ID_{AAA}, PI, T, K, t_2, Sign_{AAA}(H(L \| T \| K \| t_2))\}$ from the issuer TS of $pass_{EV1}$. Based on label L in R_{TS}, AAA can locate its record $R_{AAA} = \{L, ID_{TS}, ID_{EV1}, t_1, Sign_{EV1}(H(Cert_{EV1} \| T \| K \| t_1))\}$ to reveal the real identity ID_{EV1} of EV1. In the case where $pass_{EV1}$ was not produced by TS, AAA applies $pass_{EV1}$ to repeat steps *a)* to *e)*. This process continues until the pass issued by TS is found.

ii) To handle the second case, the above process needs to be reversed. That is, given the real identity ID_{EV1} of EV1, AAA gets hold of its record R_{AAA} and uses label L in R_{AAA} to request record R_{TS} from TS in similar ways to those described in step *e*) above. AAA then extracts the identifier PI of EV1's first pass $pass_{EV1}$ from R_{TS}. Afterwards, it sends a signed request to all the MAGs for passes issued for identifier PI. The formal message definition is omitted hereafter, as it is similar to those used in the first case.

Upon receipt of the request, every AAA-proxy MAG checks its records based on received PI. Similar to step *d*), if two records are identified, the MAG sends them to AAA. If no records are received after a set period, AAA concludes that EV1 has not requested any extra pass from MAGs. Otherwise, for the records received from each MAG, one of them contains EV1's access pass, and the other records its pass generation request including the corresponding TS-proxy identity and a label. The identity and the label allow AAA to acquire a record from the TS-proxy MAG in similar ways to steps *a*) to *c*). This record contains the identifier of the pass issued by the TS-proxy MAG. After the collection of all such identifiers, AAA broadcasts them to all the MAGs for gathering further passes and identifiers. This is repeated until no more identifiers have been reported.

Once done, AAA has obtained all the passes of EV1 apart from those that have not been used to generate other passes. Hence, AAA applies a similar way to obtain them from the MAGs via a broadcast message. If such a missing

access pass has been given to at least one MAG for attachment, it should be in the MAG's records as shown in Fig. 4, so AAA can obtain it from that MAG. It is possible that some of these passes have never been used in any way at all, so AAA is unable to get them from the MAGs. In this case, the existence of these passes has no help to the current investigation. If necessary, they can be barred for future use (e.g., via a black list of their identifiers).

iii) Finally, for the third case, AAA can first run the second case *ii*) to collect all the pass identifiers of EV1. It then broadcasts them to all the MAGs. Every MAG, which has attachment records associated with some of these identifiers, sends the records to AAA. This allows AAA to collate a list of all the MAGs visited by EV1 and construct a full trace of where and when the misbehaved EV1 moved within LMD.

F. Location Tracking Complexity

To keep the location tracking complexity and signalling overhead low, the number of new passes that can be requested by an EV from a MAG is limited to one only, as mentioned earlier in Section V-D. Hence, the maximum number of access passes obtained by an EV is limited to the number of MAGs it attaches to in LMD. While allowing an EV to acquire more access passes means higher anonymity levels, its impact will be higher loads on MAGs and a higher signalling overhead to track an EV. Therefore, this assumption keeps the balance between the EV's level of anonymity and location tracking complexity. On the other hand, since access passes are limited by an expiration time Ψ, the search for records at MAGs, AAA and TS can be optimised to target the date when that pass was issued. Consequently, location tracking complexity is kept low and the number of messages among AAA, MAGs and TS is also kept minimum.

G. ESP-PMIPv6 Scalability

As stated in section IV-A and illustrated in Fig. 2, the system model considered in this work is limited to a city and explicitly targets personal EVs. It is also assumed that one TS exists to serve the ESP-PMIPv6 objectives. However, scalable mobile IP management in V2G networks is of paramount importance especially when the number of EVs increases. Hence, the scalability of ESP-PMIPv6 is discussed herein to show that the assumption of one TS in a LMD is reasonable in this context, and ESP-PMIPv6 is scalable and can be extended to more than one city. The following three cases are considered:

1) *Intra-LMD Scalability with one TS and one AAA server*. Assume a large city such as Liverpool, UK that has a population of 469230 [35] and a ratio of 323 cars/vans per 1000 people [36] (i.e., an estimate of 151561 cars/vans in the city). Assume that all these cars/vans are personal EVs and one V2G network exists in the city. Moreover, assume that all EVs require their access passes at the same time (i.e., they request the access pass generation described in Section V-B simultaneously). According to Fig. 3, the cryptographic operations conducted at the AAA server and TS would take approximately 11*ms* using the speed benchmarks of RSA-2048 on a 2.7 GHz CPU [37]. Therefore, serving all the EVs' requests would take approximately 28 minutes, assuming the requests are processed sequentially one by one. In reality, servers can process multiple requests in parallel, so the time could be reduced significantly.

   Note that the assumptions above (i.e., all cars/vans are personal EVs and requesting the pass generation at the same time) are exaggerated to show the worst-case scenario. The probability of all EVs asking for the pass generation at the same time is very slim, given that Ψ is limited to 24 hours and can be chosen to be less than that. Even in the worst-case scenario, the protocol's total processing time is reasonable and can be considerably shortened by employing powerful servers.

2) *Intra-LMD Scalability with multiple TSs and AAA servers*. As noted in Fig. 3, the identity of the TS is included in the record saved by the AAA, and similarly the identity of the AAA is kept in the record stored by the TS. Hence, the use of multiple TSs within a LMD is envisioned in the ESP-PMIPv6 protocol design to handle a high volume of requests for access passes in the same way as the pass issuance by MAGs. This scalability helps to expand the coverage of a LMD to more than one city.

3) *Inter-LMD Scalability*. From the above case of multiple TSs and AAA servers, it is evident that the proposed ESP-PMIPv6 protocol can also be applied to multiple LMDs by distributing and operating the TSs and AAA servers in different LMDs, assuming that the certified long-term public keys of all the entities involved in the protocol are valid and their associated signatures can be verified across different LMDs. However, there are some issues of security, privacy, roaming agreements, and synchronisation among LMAs' records in different LMDs when an EV crosses several LMDs using different access passes. A comprehensive investigation of these issues is outside the scope of this paper and is left for future work.

VI. Security & Privacy Analysis

A. Mutual Authentication Formal Validation with BAN Logic

In the following, BAN logic is utilised to validate the mutual authentication property of the ESP-PMIPv6 protocol. BAN logic, named after its developers: Mike Burrows, Martín Abadí, and Roger Needham in [32], is based on model logic and uses logical postulates and definitions to analyse authentication protocols. This allows the assumptions and goals of an authentication protocol to be abstractly stated in belief logic. According to BAN logic, an authentication protocol is proved successful if the belief state of the communicating entities, after running the protocol, contains the protocol goals. Table II shows the notation used in BAN logic for the ESP-PMIPv6 proof below.

The following logical postulates are also defined to be used in the proof:

TABLE II – NOTATIONS IN BAN LOGIC FOR ESP-PMIPV6 VALIDATION

$P \mid\equiv X$	P believes X (or P believes that X holds)
$P \lhd X$	P sees X
$P \mid\sim X$	P has once said X
$P \mid- X$	P said X in the current run
$P \Rightarrow X$	P has complete control over X
$fresh(X)$	X is fresh and recent
$P \overset{K}{\leftrightarrow} Q$	P and Q share a secret key K
$\overset{K}{\rightarrow} P$	P has K as a public key and its corresponding private key is K^{-1}, which is only known to P
$P \overset{X}{\Leftrightarrow} Q$	X is a secret known only to P and Q
$\{X\}_K$	X is encrypted under the key K

$$\frac{P \mid\equiv P \overset{K}{\leftrightarrow} Q,\ \ P \lhd \{X\}_K}{P \mid\equiv Q \mid\sim X} \quad (1)$$

meaning that if P believes that K is a secret key shared with Q and P sees X encrypted with K, then P believes that Q has once said X.

$$\frac{P \mid\equiv \overset{K}{\rightarrow} Q,\ \ P \lhd \{X\}_{K^{-1}}}{P \mid\equiv Q \mid\sim X} \quad (2)$$

meaning that if P believes that K is a public key of Q and P sees X encrypted with K^{-1}, then P believes that Q has once said X.

$$\frac{P \mid\equiv fresh(X),\ \ P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid- X} \quad (3)$$

meaning that if P believes that X is fresh and recent, and P believes that Q has once said X, then P believes that Q still believes X (i.e., Q said X in the current run).

$$\frac{P \mid\equiv Q \Rightarrow X,\ \ P \mid\equiv Q \mid\equiv X}{P \mid\equiv X} \quad (4)$$

meaning that if P believes that Q has complete control over X and P believes that Q believes X, then P believes X (i.e., P trusts Q on the truth of X).

$$\frac{P \mid\equiv (X,Y)}{P \mid\equiv X,\ \ P \mid\equiv Y} \quad (5)$$

meaning that if P believes in a message consisting of X and Y, then P believes X and P believes Y.

$$\frac{P \mid\equiv fresh(X)}{P \mid\equiv fresh(X,Y)} \quad (6)$$

meaning if P believes that X, part of a message, is fresh, then P believes that the entire message (X, Y) is fresh.

Following the notation in Fig. 3, the following messages are given for the full run of the protocol:

$\mathcal{M}_1$: $EV1 \rightarrow AAA$: $\{Cert_{EV1}, T, K, t_1, \{H(Cert_{EV1} \parallel \mathrm{T} \parallel K \parallel t_1)\}_{PK^1_{EV1}}\}_{PK_{AAA}}$

$\mathcal{M}_2$: $AAA \rightarrow TS$: $\{L, T, K, t_2, \{H(L \parallel T \parallel K \parallel t_2)\}_{PK^1_{AAA}}\}_{PK_{TS}}$

$\mathcal{M}_3$: $TS \rightarrow AAA$: $\{L, Resp, t_3, \{\mathrm{H}(L \parallel Resp \parallel t_3)\}_{PK^1_{TS}}\}_{PK_{AAA}}$

$\mathcal{M}_4$: $AAA \rightarrow EV1$: $\{Cert_{AAA}, t_4, Resp, \{H(Cert_{AAA} \parallel Resp \parallel t_4)\}_{PK^1_{AAA}}\}_{PK_{EV1}}$

In the following, the security goal of ESP-PMIPv6 in achieving mutual authentication among the entities is proven:

i) Mutual authentication between EV1 and AAA. To achieve this aim, two objectives can be formalised as follows:

O_1: $AAA \mid\equiv EV1 \mid- \mathcal{M}_1$ and O_2: $EV1 \mid\equiv AAA \mid- \mathcal{M}_4$

Using the logical postulates (1) to (6) above, the following logical steps can be obtained:

1- $AAA \lhd \{Cert_{EV1}, T, K, t_1, \{H(Cert_{EV1} \parallel \mathrm{T} \parallel K \parallel t_1)\}_{PK^1_{EV1}}\}_{PK_{AAA}}$ [$\mathcal{M}_1$]

2- $\overset{PK_{AAA}}{\longrightarrow} AAA$ [Assumption]

3- $AAA \lhd \{Cert_{EV1}, T, K, t_1, \{H(Cert_{EV1} \parallel \mathrm{T} \parallel K \parallel t_1)\}_{PK^1_{EV1}}\}$ [1, 2]

4- $AAA \mid\equiv$ EV1 $\mid\sim \{H(Cert_{EV1} \parallel \mathrm{T} \parallel K \parallel t_1)\}$ [3, (2)]

5- $AAA \mid\equiv$ EV1 $\mid\sim \{Cert_{EV1}, T, K, t_1\}$ [4]

6- $AAA \mid\equiv fresh(\{Cert_{EV1}, T, K, t_1\})$ [3, 4, 5]

7- $AAA \mid\equiv fresh(\{Cert_{EV1}, T, K, t_1, \{H(Cert_{EV1} \parallel \mathrm{T} \parallel K \parallel t_1)\}\})$ [6, (6)]

8 - $AAA \mid\equiv EV1 \mid- \mathcal{M}_1$ [7, (3)]

Hence, O_1 is proved. Similarly, O_2 can be proved using the same logic above. Therefore, ESP-PMIPv6 achieves mutual authentication between EV1 and AAA.

ii) Mutual authentication between EV1 (also AAA) and TS. To achieve this aim, two objectives can be formalised as follows:

O_3: $TS \mid\equiv EV1 \mid- \{T, K\}$ and O_4: $EV1 \mid\equiv TS \mid- \{Resp\}$

Using the logical postulates (1) to (6), the following derivation can be obtained:

1- $TS \lhd \{L, T, K, t_2, \{H(L \parallel T \parallel K \parallel t_2)\}_{PK^1_{AAA}}\}_{PK_{TS}}$ [$\mathcal{M}_2$]

2- $\overset{PK_{TS}}{\longrightarrow} TS$ [Assumption]

3- $TS \lhd \{L, T, K, t_2, \{H(L \parallel T \parallel K \parallel t_2)\}_{PK^1_{AAA}}\}$ [1, 2]

4- $TS \mid\equiv AAA \mid\sim \{H(L \parallel T \parallel K \parallel t_2)\}$ [3, (2)]

5- $TS \mid\equiv AAA \mid\sim \{L, T, K, t_2\}$ [4]

6- $TS \mid\equiv EV1 \mid\sim \{T, K\}$ [5, (4), (5)]

7- $TS \mid\equiv fresh(\{L, T, K, t_2\})$ [3, 4, 5]

8- TS $\mid\equiv fresh(\{L, T, K, t_2, \{H(L \parallel T \parallel K \parallel t_2)\}\})$ [7, (6)]

9- $TS \mid\equiv AAA \mid- \mathcal{M}_2$ [8, (3)]

10 - TS $\mid\equiv EV1 \mid- \{T, K\}$ [6, 8, 9]

Hence, O_3 is proved. Similarly, O_4 is proved as follows:

1- $EV1 \lhd \{Cert_{AAA}, t_4, Resp, \{H(Cert_{AAA} \parallel Resp \parallel t_4)\}_{PK^1_{AAA}}\}_{PK_{EV1}}$ [$\mathcal{M}_4$]

2- $EV1 \mid\equiv AAA \mid- M_4$ [O_2]

3- $EV1 \mid\equiv TS \mid\sim Resp$ [2, (4), (5), (1)]

4- $AAA \mid\equiv fresh(Resp)$ [$\mathcal{M}_3$]

5- $EV1 \mid\equiv fresh(Resp)$ [4, (4)]

6- $EV1 \mid\equiv TS \mid- \{Resp\}$ [5, (3)]

Therefore, ESP-PMIPv6 achieves mutual authentication between EV1 (also AAA) and TS. The achievement of mutual authentication of ESP-PMIPv6 between EV1 and MAG1 (and MAG2) can be proven similarly using the steps taken in this sub-section. The proof is omitted due to limited space.

B. Mutual Authentication – Informal Proof

In Fig. 3, EV1 sends its identity information via its public key certificate $Cert_{EV1}$ to AAA in step 1 for the initiation of an access pass generation process. Consequently, AAA authenticates EV1 and verifies its request for a pass by checking its signature $Sign_{EV1}$ with the public key in $Cert_{EV1}$. Similarly, for each subsequent step there is a signature involved to allow the message recipient to verify the message authenticity, as

defined in Fig. 3. Particularly, TS's signature in the last message received by EV1 enables it to authenticate that TS has indeed issued the pass.

In addition, as illustrated in Fig. 4, when EV1 attaches to MAG1, it sends its $pass_{EV1}$ and a signature $Sign_{EV1}$` yielded using private key TSK_{EV1} paired with public key TPK_{EV1} tied to $pass_{EV1}$. This allows MAG1 to authenticate that EV1 is the right user of the pass and hence authorised to join LMD. When MAG1 replies with the RA message, EV1 can authenticate MAG1 through its $Cert_{MAG1}$ and $Sign_{MAG1}$ in the message.

It can be noticed, from Fig. 3, that neither TS nor AAA saves the generated access pass (i.e., $pass_{EV1}$) of EV1. In fact, AAA cannot form $pass_{EV1}$, because it does not even have the blind signature σ signed by TS, which is a crucial part of the pass issuance. On the other hand, although TS creates σ, it does not have the blind factor r that is essential for the calculation of signature Ω in $pass_{EV1}$. Thus, even if AAA or TS is compromised, the pass cannot be stolen from them for impersonation attacks.

Finally, assume that MAG1 is compromised and $pass_{EV1}$ is stolen by an attacker. Then the stolen pass cannot be used to access LMD, because the attacker still needs EV1's temporary private key TSK_{EV1} known only by EV1, to use $pass_{EV1}$. Thus, it defeats impersonation attacks.

C. EV's Anonymity & Location Privacy

To illustrate this property, the possibilities of revealing the identity and/or tracking the locations of a given EV, denoted as EV1, by each of the system entities are discussed below:

1) As stated before, both AAA and TS do not save $pass_{EV1}$ and cannot produce it either. Instead, AAA records $\{L, ID_{TS}, ID_{EV1}, t_1, Sign_{EV1}(H(Cert_{EV1} \| T \| K \| t_1))\}$, while TS keeps $\{L, ID_{AAA}, PI, T, K, t_2, Sign_{AAA}(H(L \| T \| K \| t_2))\}$, as shown in Fig. 3. Thus, neither AAA nor TS are aware of when and where EV1 will use its access pass. Those saved records are not sufficient to track EV1 unless both AAA and TS collude directly with MAGs for such an illicit operation. As assumed in the threat model in Section IV-C, they do not have such collusion.
2) A pair of MAGs, MAG_i and MAG_j, can be used as the proxies of AAA and TS by EV1 to get a new access pass $pass_{EV1}$` from its existing pass $pass_{EV1}$. As pointed out in Section V-D, this pass generation process involves no information on EV1's real identity, and neither of the two MAGs can link the two passes together. MAG_j is unaware that EV1 is located at MAG_i, and any other MAG cannot infer from $pass_{EV1}$` that EV1 has visited MAG_i. Even if both MAG_i and MAG_j collude, the only gain is to establish the link between the two passes and let MAG_j know EV1's location at MAG_i. However, if EV1 has no intention to visit MAG_j or visits it with a different pass, the collusion gives them no benefit in terms of revealing EV1's real identity and linking its different locations. Obviously, to establish a linkage to EV1's other locations, MAG_i and MAG_j have to collude with the other MAGs that EV1 has visited or will visit. Thus, the more access passes EV1 has, the more difficult for such collusion to work.
3) A MAG cannot spot the real identity of EV1 when it receives any of EV1's passes, as each access pass only contains an identifier bearing no link to EV1's real identity. The only way to reveal EV1's real identity is for the MAG to collude directly with AAA and TS. Again, it is already assumed that such collusion is not feasible.
4) All the messages between EV1 and MAG1 (or MAG2) in Fig. 4 are encrypted. Thus, the utilised $pass_{EV1}$ cannot be disclosed to external adversaries to track down the locations of EV1. Even if a given MAG is compromised and $pass_{EV1}$ is leaked, EV1 can acquire multiple passes from different MAGs as discussed earlier, so it is able to use different access passes at different MAGs. This hinders the possibility of illicitly linking EV1's location at the compromised MAG to its other locations at different MAGs, because the disclosed pass bears no direct link to EV1's other passes as pointed out earlier.
5) Finally, at LMA, PIDs are utilised instead of an EV's real identity. Thus, LMA cannot track down any of EV's locations as it cannot link different PIDs to the same EV.

D. Unlinkability & Traceability

The ESP-PMIPv6 protocol aims to enable the integration of anonymity, unlinkability and traceability for providing strong privacy protection to legitimate EVs while holding misbehaving EVs accountable for their actions. In the following, the unlinkability property is illustrated in which the ability of LMA to link two PIDs to a particular EV is discussed. For this analysis, it is assumed that the system only has two geographically adjacent MAGs. Secondly, the ability of ESP-PMIPv6 to fully trace a misbehaving EV and reveal its real identity is illustrated.

For the analysis of unlinkability, let $\mathcal{N}$ be the set of all EVs in the binding cache entries of the LMA and $\mathcal{W} \subseteq \mathcal{N}$, where $\mathcal{W}$ contains all EVs that are attached to MAG_i and are highly likely to perform a handover to MAG_j, which is geographically adjacent to MAG_i. Assume that the arrival of new EVs at MAG_j follows a Poisson arrival process with an arrival rate λ. Let $\mathcal{X}$ and $\mathcal{Y}$ be two discrete random variables with marginal probability distribution functions $\mathcal{P}(x)$ and $\mathcal{P}(y)$, respectively. $\mathcal{X}$ represents the probability that an EV with a pseudo identity $PID1$ detaches from MAG_i, while $\mathcal{Y}$ represents the probability that the EV attaches to MAG_j with a new identity $PID2$. In order to measure, at LMA, the reduction in uncertainty about $\mathcal{Y}$ given that $\mathcal{X}$ has happened, the mutual information $I(\mathcal{X}; \mathcal{Y})$ metric is utilised and defined below:

$$I(\mathcal{X};\mathcal{Y}) = \sum_{y\in\mathcal{Y}} \sum_{x\in\mathcal{X}} \mathcal{P}(x,y)\, log\left(\frac{\mathcal{P}(x,y)}{\mathcal{P}(x)P(y)}\right), \quad (7)$$

where $\mathcal{P}(x, y)$ is the joint probability distribution function of $\mathcal{X}$ and $\mathcal{Y}$. $I(\mathcal{X}; \mathcal{Y})$ can also be expressed as:

$$I(\mathcal{X}; \mathcal{Y}) = \mathcal{H}(\mathcal{Y}) - \mathcal{H}\,(\mathcal{Y} \mid \mathcal{X}), \quad (8)$$

where $\mathcal{H}(\mathcal{Y})$ is the amount of information that LMA knows

about $\mathcal{Y}$, and $\mathcal{H}(\mathcal{Y} \mid \mathcal{X})$ is the conditional entropy that measures the uncertainty remaining about $\mathcal{Y}$ after knowing $\mathcal{X}$. Let $\mathcal{P}(x) = \frac{1}{|\mathcal{W}|}$ be the probability that the EV detaches from MAG_i, and $\mathcal{P}(y) = \frac{1}{|\mathcal{W}|} \cdot \frac{1}{\lambda \cdot t + 1}$ is the probability that the EV attaches to MAG_j after detaching from MAG_i, where $\lambda \cdot t$ is the average number of arrivals per t units.

Fig. 5 shows the amount of reduction in uncertainty about $\mathcal{Y}$, expressed in bits, with respect to the size of $\mathcal{W}$ and λ when t is set to 1*s*.

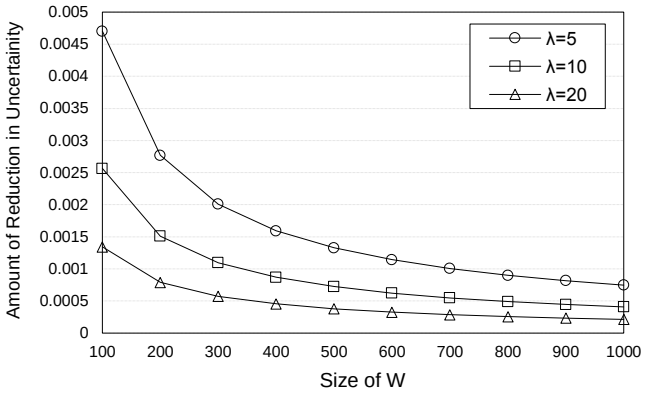


Fig. 5. Amount of Reduction in Uncertainty

Fig. 5 shows that the reduction in uncertainty decreases when the sizes of both $\mathcal{W}$ and λ increase. Thus, in such circumstances, LMA stays uncertain about whether *PID*1 and *PID*2 belong to the same EV even when considering geographically adjacent MAGs. In other words, ESP-PMIPv6 ensures high levels of unlinkability for the EV at LMA.

In addition, as pointed out in the previous sub-section, the EV's different access passes bear neither any direct link among them nor any indication on which MAGs the EV has visited. Also, they show no information linkable to the real identity of the EV.

Regarding the traceability property of ESP-PMIPv6, Section V-E has presented the methods for tracking down the real identity of a misbehaved EV and collating a list of all its used passes and visited MAGs. This indicates that ESP-PMIPv6 can trace the misbehaved EV and present its movement within LMD so as to hold it accountable for its misbehaviour. As shown in Fig. 3 and 4, the EV is always required to present its signatures when it contacts the AAA server and any MAG that records such signatures. Each of these signatures can only be produced with a private key associated with an access pass or the public-key certificate (only for contact with AAA) of the EV, and the key is known only by the EV. Thus, the collated list of its used access passes and visited MAGs mentioned above provides undeniable evidence about the EV's activities within LMD. Thus, it defeats repudiation attacks by misbehaving EVs.

VII. Performance Evaluation & Simulation Results

In this section, the performance of ESP-PMIPv6 is evaluated through a simulation assessment using the OMNet++ 4.6 network simulator [33] and the EV mobility model in the Simulation for Urban MObility (SUMO) mobility simulator [34]. Simulation results of ESP-PMIPv6, PMIPv6 and SP-PMIPv6 [21] are compared to show the efficiency of ESP-PMIPv6.

A. Simulation Setup

The simulation scenario represents a 10 km^2 urban area of Manhattan grid where charging spots and MAGs are uniformly distributed. Vehicles start their journey from their home network and follow predefined routes to workplaces or shopping centres, where public charging spots are installed (i.e. visiting networks). Vehicles are either fully charged at home or recharged on the way. For this simulation, vehicles use WLAN connectivity to communicate with MAGs. The CN in this scenario represents the billing/charging server in the SG domain. The average velocity of vehicles on the roads is changed from 20 *km*/*h* to 60 *km*/*h*. The handover occurs approximately every 1 *km*. Vehicles stop at the charging spot for 15 minutes on average. The simulation parameters are summarised in Table III.

TABLE III – Simulation Parameters

Simulation Area	10 km^2
Mobility Model	Manhattan grid
Communication range	≈ 100*m*
Application	Background data packets over UDP
WLAN connectivity	IEEE 802.11b
Simulation time	60 minutes
Number of Runs	10
Number of Vehicles	100
Average Stop Time	15 minutes

Note that the time needed to perform *Enc*(·) and hash operations is neglected, given the small size of the messages. The following performance metrics are considered:

- Authentication latency: represents the average time needed to authenticate and authorise an EV to join the LMD and start data transmission.
- Handover delay: is the average time needed to perform all the authentication and authorisation needed when an EV switches its attachment from one MAG to another.
- Packet loss rate: shows on average the percentage of packets lost with respect to the packets sent from the CN to an EV especially when a handover occurs.

B. Simulation Results

Fig. 6 shows the authentication latency for each of the protocols examined in this simulation. It can be noticed that both SP-PMIPv6 and ESP-PMIPv6 outperform PMIPv6 in terms of lower authentication latency over different average speeds. Unlike PMIPv6 that must communicate with AAA to authenticate and authorise an EV, the use of access pass authentication avoids this journey and thus achieves lower authentication latency. Due to the utilisation of less intensive computational techniques, ESP-PMIPv6 achieves lower authentication latency than SP-PMIPv6. In ESP-PMIPv6, a MAG only needs to perform two exponentiation operations to

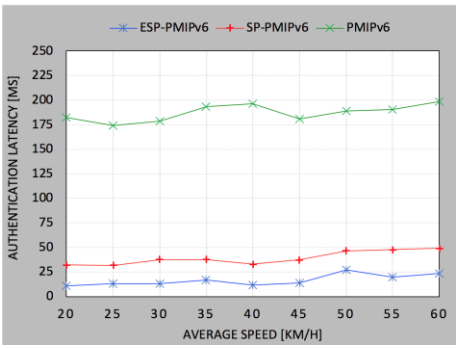


Fig. 6. Authentication Latency

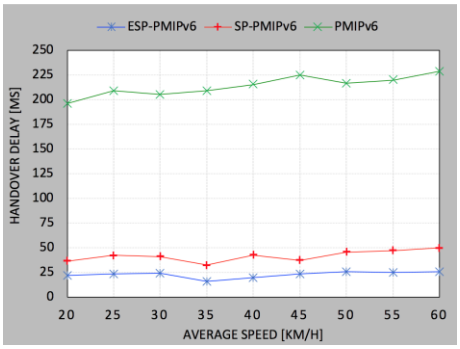


Fig. 7. Handover Delay

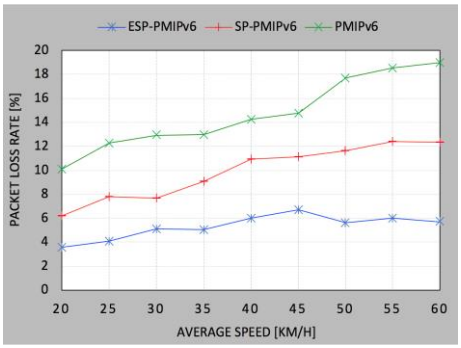


Fig. 8. Packet Loss Rate

verify an access pass. However, in SP-PMIPv6, it needs five pairing operations in addition.

Similar to Fig. 6, Fig. 7 shows the excellent performance of the developed ESP-PMIPv6 in comparison to PMIPv6. The handover process in ESP-PMIPv6 is performed without communicating with AAA. Thus, it saves time and incurs low handover delay. Finally, Fig. 8 clearly shows the advantage of the smooth handover process achieved by the ESP-PMIPv6 protocol. It can be observed that the packet loss rate of ESP-PMIPv6 is lower than those of PMIPv6 and SP-PMIPv6. In general, a higher average speed contributes to a higher packet loss rate because more handovers may occur. In this case, it is of great importance to keep the handover delay as low as possible to ensure continuous and seamless data transmission between an EV and the CN.

VIII. Conclusion & Future Work

In this paper, the security and privacy concerns of enabling mobile IP communications in V2G networks have been investigated. To achieve seamless communications between an EV and the SG while protecting the EV's identity and location privacy, the novel ESP-PMIPv6 protocol for V2G networks has been developed. ESP-PMIPv6 employs an RSA-based blind signature incorporating a built-in tagging technique via access pass identifier *PI* and limited validity Ψ as well as terms and conditions *TC*. This coupled with the new proxy-based distributed and collaborative access *pass* generation and trace-back mechanisms, enables the ESP-PMIPv6 protocol to achieve mutual authentication, anonymity and location privacy, and authorised traceability. This has been evident via the formal security analysis using BAN logic. Furthermore, the simulation results indicate that ESP-PMIPv6 has much lower authentication latency and handover delay than the standard PMIPv6 and SP-PMIPv6. Thus, ESP-PMIPv6 achieves lower packet loss rates and consequently ensures seamless communications between an EV and the CN.

For future work, it is intended to extend ESP-PMIPv6 to cover a wider V2G network model and inter-domain handover and assess its performance on a real-time testbed.

References

[1] 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 2017].

[2] 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 2017].

[3] International Standards Organisation (ISO), "Road vehicles -- Vehicle-to-Grid Communication Interface -- Part 2: Network and application protocol requirements," April 2014. [Online]. Available: https://www.iso.org/standard/55366.html. [Accessed 30 Sept 2017].

[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] Z. M. Fadlullah, T. Taleb, A. V. Vasilakos, M. Guizani, and N. Kato, "DTRAB: Combating against attacks on encrypted protocols through traffic-feature analysis," *IEEE/ACM Trans. Netw.*, vol. 18, no. 4, pp. 1234–1247, Aug 2010.

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

[8] A. Abdallah and X. Shen, "Lightweight Authentication and Privacy-Preserving Scheme for V2G Connections," *IEEE Trans. Veh. Technol.*, vol. 66, no. 3, pp. 2615 – 2629, Mar 2017.

[9] N. Saxena and B. J. Choi, "State of the Art Authentication, Access Control, and Secure Integration in Smart Grid," *Energies*, vol. 8, no. 10, pp. 11883-11915, Oct 2015.

[10] 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. Veh. Technol.*, vol. 3, no. 4, pp. 1722-1733, Dec 2012.

[11] D.T. Hoang, P. Wang, D. Niyato and E. Hossain, "Charging and Discharging of Plug-In Electric Vehicles (PEVs) in Vehicle-to-Grid (V2G) Systems: A Cyber Insurance-Based Model," *IEEE Access*, vol. 5, pp. 732 – 754, Jan 2017.

[12] 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 Comm.*, vol. 20, no. 6, pp. 66-73, Dec 2013.

[13] 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. Info. Forensics and Security*, vol. 9, no. 2, pp. 208-220, Feb 2014.

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

[15] H. Wang, B. Qin, Q. Wu, L. Xu and J. Domingo-Ferrer, "TPP: Traceable Privacy-Preserving Communication and Precise Reward for Vehicle-to-Grid Networks in Smart Grids," *IEEE Trans. Info. Forensics and Security*, vol. 10, no. 11, pp. 2340 – 2351, Nov 2015.

[16] M.H. Eiza, Q. Ni, Q. Shi. "Secure and Privacy-Aware Cloud-Assisted Video Reporting Service in 5G-Enabled Vehicular Networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 10, pp. 7868 – 7881, Oct 2016.

[17] M.H. Eiza, T. Owens, Q. Ni. "Secure and Robust Multi-Constrained QoS aware Routing Algorithm for VANETs," *IEEE Trans. Dependable and Secure Computing*, vol. 13, no 1, pp. 32 – 45, Jan 2016.

[18] M.H. Eiza, Q. Ni. "Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cybersecurity," *IEEE Veh. Technol. Magazine*, vol. 12, no 2, pp. 45 – 51, June 2017.

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

[20] 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.

[21] M.H. Eiza, Q. Shi, A.K. Marnerides and T. Owens, "Secure and Privacy-Aware Proxy Mobile IPv6 Protocol for Vehicle-to-Grid Networks," in *Proc. ICC*, IEEE, 2016.

[22] 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.

[23] 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.

[24] K.-S. Kong, W. Lee, Y.-H. Han, and M.-K. Shin, "Handover latency analysis of a network-based localized mobility management protocol," in *Proc. IEEE Int. Conf. Comm.*, pp. 5838–5843, May 2008.

[25] K.-S. Kong, W. Lee, Y.-H. Han, M.-K. Shin, and H. You, "Mobility management for all-IP mobile networks: Mobile IPv6 versus proxy mobile IPv6," *IEEE Wireless Comm.*, vol. 15, no. 2, pp. 36–45, Apr 2008.

[26] J.-H. Lee and T.-M. Chung, "Secure handover for proxy mobile IPv6 in next-generation communications: Scenarios and performance," *Wireless Commun. Mobile Comput.*, vol. 11, no. 2, pp. 176–186, Feb 2011.

[27] D. Kang, J. Jung, D. Lee, H. Kim, and D. Won, "Security analysis and enhanced user authentication in proxy mobile IPv6 networks," *PLoS ONE*, vol.12, no. 7, July 2017.

[28] M. Alizadeh, M. Zamani, S. Baharun, WH. Hassan and T. Khodadadi, "Security and Privacy criteria to evaluate Authentication Mechanisms in Proxy Mobile IPv6," *Jurnal Teknologi*, vol. 72, no. 5, pp. 27–30, 2015.

[29] S. Taha and X. Shen, "ALPP: Anonymous and Location Privacy Preserving Scheme for Mobile IPv6 Heterogeneous Networks," *Security and Communication Network*, vol. 6, no. 4, pp. 401-419, Apr 2013.

[30] 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 Feb 2018].

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

[32] M. Burrows, M. Abadi and R. Needham, "A logic of authentication," *ACM Trans. Computer Systems*, vol. 8, no.1, pp. 18-26, Feb 1990.

[33] OMNeT++ Community, OMNeT++ Network Simulator. [Online]. Available: http://www.omnetpp.org/ (Accessed: 05/20 2011).

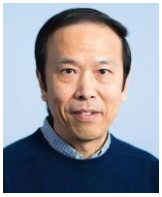
[34] German Aerospace Center – Institute of Transportation Systems, "Models/Electric – SUMO – Simulation of Urban Mobility," 29 Apr 2016. [Online]. Available: http://www.sumo.dlr.de/userdoc/Models/Electric.html. [Accessed 21 July 2016].

[35] Population UK, "Liverpool Population 2018," [Online]. Available: https://www.ukpopulation.org/liverpool-population/ [Accessed 28 Sept 2018].

[36] RAC Foundation, "Car ownership rates per local authority in England and Wales," 26 Dec 2012. [Online]. Available: https://www.racfoundation.org/assets/rac_foundation/content/downloadables/car%20ownership%20rates%20by%20local%20authority%20-%20december%202012.pdf [Accessed 28 Sept 2018].

[37] Crypto++ community, "Speed Comparisons of Popular Crypto Algorithms," 9 Dec 2017. [Online]. Available: https://www.cryptopp.com/benchmarks.html [Accessed 28 Sept 2018].

Mahmoud Hashem Eiza received his M.Sc. and Ph.D. degrees in electronic and computer engineering from Brunel University London, U.K. in 2010 and 2015, respectively. He is a lecturer in computing (computer and network security) at the School of Physical Sciences and Computing, University of Central Lancashire, U.K. His research interests include computer and network security, with specific interests in quality of service, security, and privacy in vehicular networks, smart grids, cloud computing, and the Internet of Things.



Qi Shi is a Professor in Computer Security and the Director of the PROTECT Research Centre in the Department of Computer Science at Liverpool John Moores University (LJMU), U.K. He received his PhD in Computing from the Dalian University of Technology, P.R. China, in 1989. He has many years research experience in several areas, e.g. computer networks and security, privacy-preserving data aggregation, cryptography, formal security models and cloud security. He has published over 200 papers in international conference proceedings and journals and served in several conference IPCs and journal editorial boards. He has also played a key role in many funded research and development projects related to his research topics.

Angelos K. Marnerides (M'07) received the M.Sc. and Ph.D. degrees in computer science from Lancaster University, U.K. He is a Lecturer in computer networking with the School of Computing and Communications, Lancaster University, U.K. His research interests include network resilience and security, malware/botnet detection, cloud computing, the smart grid, and the IoT. He has received significant funding for his research from public funding agencies (such as EPSRC, EC, Innovate U.K., GCHQ) and the industry (such as Fujitsu, Raytheon, BAE).

Thomas Owens obtained his PhD in Electrical and Electronic Engineering from Strathclyde University in 1986. He joined as a lecturer in the Department of Electronic and Electrical Engineering, Brunel University London, which was eventually absorbed into the College of Engineering, Design and Physical Sciences in which he was Reader Signals and Systems. He was the project coordinator of the IST FP5 project CONFLUENT, the IST FP6 Integrated Project INSTINCT, and the FP7 Support Action CHOICE. He has published more than 50 papers in refereed journals.

Qiang Ni (M'04–SM'08) received his Ph.D. degree in engineering from the Huazhong University of Science and Technology, China in 1999. He is currently a Professor and the Head of the Communication Systems Group, School of Computing and Communications, Lancaster University, Lancaster, U.K. His research interests include future generation communications and networking, including green communications and networking, cognitive radio network systems, heterogeneous networks, 5G and 6G, SDN, network security, energy harvesting, wireless information and power transfer, IoTs, big data analytics, vehicular networks and smart energy networks. He has authored or co-authored over 200 papers in these areas.