Abstract—Vehicle-to-grid (V2G) as an essential network component of smart grid, provides services by periodically collecting the charging status of a battery vehicle (BV). A BV is normally associated with a default interest group (e.g., power grid operator). When the BV accesses its default charging or communication point, it works in the home mode. The BV may move around and temporarily access other aggregators, and then it works in the visiting mode. In this paper, we first identify that, for an aggregator, BVs have different security challenges when they work in different modes. Then, we propose an aggregated-proofs based privacy-preserving authentication scheme (AP3A) to achieve simultaneous identification and secure identification for different working mode BVs. In AP3A, BVs are differentiated into either home or visiting mode, and multiple BVs can be simultaneously authenticated by an aggregator to conserve communication resources. In addition, the aggregated pseudo-status variation is presented to realize that multiple BVs’ power status can be collected as a whole without revealing any individual privacy. We perform comprehensive analysis on the proposed scheme, including attack analysis, security analysis, and performance analysis. It is shown that AP3A can resist major attacks for security protection and privacy preservation, and can be an efficient authentication approach for V2G networks.

Index Terms—Authentication, privacy, security, smart grid, vehicle-to-grid (V2G).

I. INTRODUCTION

THE SMART GRID is converting the traditional power grid into more efficient and reliable networks, which is featured by real-time and two-way communications of electricity and information [1], [2]. Vehicle-to-grid (V2G) as an essential network component of smart grid [3]–[5], also receives featured by real-time and two-way communications of engineering, Beihang University, Beijing 100191, China (e-mail: liuhongler@ee.buaa.edu.cn; ninghuansheng@buaa.edu.cn).

Y. Zhang is with the Simula Research Laboratory, Norway; and Department of Informatics, University of Oslo, Oslo N-0373, Norway (e-mail: yanzhang@simula.no).

L. T. Yang is with the School of Computer Science and Technology, Huazhong University of Science and Technology, Wuhan, China, and also with the Department of Computer Science, St. Francis Xavier University, Antigonish B2G 2W5, Canada (e-mail: ltyang@stfx.ca).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2012.2212730

However, communication may suffer from data leakage, therefore, security becomes a significant issue in V2G networks [9], [10].

In V2G networks, a BV is normally associated with a default interest group. Here, an interest group is a generic term and can represent a power grid operator or an organization. In daily usage, the BV may move around in different sub-areas which belong to different groups. During the BV’s interactions with different groups, it may have different security/privacy requirements and authentication implementation. In this paper, we will identify and address a new security challenge in V2G networks due to BVs’ movement around different sub-areas with different group attributes.

Fig. 1 shows two working modes: home mode and visiting mode. The aggregator serves as the default charging and communication access point for the white BVs. We say that the white BVs work in the home mode when they access the aggregator. The black BVs move from other sub-areas and temporarily access the aggregator, and they work in the visiting mode. In this scenario, the BVs confront different security requirements in different working modes. For instance, the home mode BVs and the aggregator may perform more convenient authentication mode than those belonging to different groups. Therefore, a universal authentication scheme is not suitable for BVs, and we need to design different authentication protocols for BVs in different modes.

During the interaction between BVs and an aggregator, the aggregator can monitor the BVs to capture the charging status. The process of data acquisition may confront the abuse of privacy [11]. For instance, it is possible to correlate a BV’s identity information with its detailed power status. It becomes critical to realize anonymous data transmission for privacy consideration. Furthermore, it has been shown that most BVs are averagely in the parking status 95% of a whole day [12]. This indicates that an aggregator may have several BVs at one time. Therefore, it is possible for an aggregator to simultaneously authenticate several BVs during their stay in the parking lots. It is envi-
sioned that the aggregated authentication can conserve system resources compared with the one-by-one authentication scheme.

Based on aforementioned requirements, we will focus on the privacy preservation authentication: 1) to differentiate the working modes, and to design a new authentication scheme for different groups. The technical details in authenticating different modes will be further presented in Section IV-C; 2) to consider a simultaneous identification and authentication scheme to effectively authenticate multiple BVs at the same time; 3) to periodically collect power status data without compromising individual privacy, here the power status refers to a BV’s energy related status information (e.g., charging efficiency, and battery saturation status). It is observed that working modes differentiation or its security consideration has not been studied yet in the context of V2G networks. For simultaneous authentication, we are inspired by coexistence-proof which was studied in radio frequency identification (RFID) [13], [14]. In RFID systems, coexistence-proof is mainly introduced to simultaneously scan multiple tags by a reader. It is noteworthy that the coexistence-proof technique cannot be trivially applied in V2G networks. Traditional coexistence-proofs schemes usually require an entity as a proof initiator which acts as central role during the communications. As the proof initiator, it needs to link, distribute, and collect messages from other generic entities. In decentralized V2G networks, it is very difficult to appoint a BV to act as such entity. Hence, a new mechanism is needed since all BVs are equivalent. For this reason, we will present simultaneous existence of multiple BVs as a whole group to be verified by an aggregator. Following this, the established aggregated-proofs can realize the multiple-to-single authentication for both the home and the visiting BVs.

In particular, an aggregated-proofs based privacy-preserving authentication scheme (AP3A) is proposed in the V2G networks. We have proved that the proposed AP3A scheme can achieve the following security requirements. 1) \textit{Data confidentiality, integrity, and availability:} The exchanged messages between BVs and aggregators should be protected against unauthorized access and modification. The communication channels should be ensured reliable for legal entities. 2) \textit{Mutual authentication:} BVs and an aggregator should pass each other’s verification so that any illegal BV cannot access the networks to steal power resources, and any illegal aggregator cannot acquire the BV’s power status data. 3) \textit{Dynamic participation:} BVs can dynamically join and leave the networks without influencing ongoing communications. 4) \textit{Forward and backward security:} Attackers cannot correlate two communication sessions, and also cannot derive the previous or subsequent interrogations according to the current session. 5) \textit{Privacy preservation:} Aggregators or attackers cannot correlate a BV’s real identity with its private power information (e.g., state of charge). In summary, we have three major contributions in this work.

- We identify the necessity in differentiating BVs’ home and visiting modes in V2G networks, and consequently propose different authentication schemes for different modes. Multiple BVs can simultaneously access and be authenticated by an aggregator with dynamic participation and session unlinkability.
- We present anonymous aggregated-proofs to realize the geographically dispersed BVs’ power status to be collected as a group without revealing any individual privacy.
- We introduce a virtual battery vehicle concept for privacy consideration, which is an independent component to enhance message randomization and to realize distributed non-distinguishable identifications.

The remainder of the paper is organized as follows. Section II introduces the related work. Section III describes the system model, and Section IV introduces the proposed AP3A scheme. Section V further discusses the attack analysis. The security analysis and performance analysis are presented in Sections VI and VII respectively. Finally, Section VIII draws a conclusion.

### II. RELATED WORK

Towards the security solutions in V2G networks: Yang et al. [15] identified privacy-preserving issues and proposed a secure communication architecture with blind signature to achieve privacy-preserving for BV monitoring and rewarding. The protocol focuses on the privacy-preserving communication and precise reward architecture for V2G networks. Guo et al. [16] proposed an interesting batch authentication protocol to address the multiple responses from a batch of vehicles. The proposed protocol introduces the concept of interval time for an aggregator authenticating multiple vehicles, and applies the modified digital signature algorithm (DSA) to establish batch verification. The protocol focuses on multiple BVs’ batch authentication for V2G networks. Vaidya et al. [17] proposed a multi-domain network architecture for V2G networks. The protocol incorporates a comprehensive hybrid public key infrastructures (PKI) model which integrates hierarchical and peer-to-peer cross-certifications.

Towards the general security researches in smart grid: He et al. [18] considered the secure service provision in smart grid, and established a communications procedure among the electric utility, consumers, and service providers. Metke et al. [19] discussed the main security technologies for smart grid, including PKI algorithm and the trusted computing. Li et al. [20] proposed a one-time signature scheme based multicast authentication scheme, which effectively reduces both storage cost and signature size. Efthymiou et al. [21] proposed a privacy solution for anonymizing the high-frequency metering data by a pseudonymous identifier. Qiu et al. [22] proposed an energy efficient security algorithm for power grid wide area monitoring system by encryption-decryption based code optimization techniques. Chen et al. [23] applied the hierarchical Petri net (PN) model to analyze cyber-physical attacks on smart grid. Zhang et al. [24] built a distributed intrusion detection system, which uses the support vector machine and artificial immune system to detect malicious data and cyber-attacks. Son et al. [25] proposed a voucher scheme for securely trading the authority on the power usage for the collaborative customer community. Wu et al. [26] proposed a key management scheme which combines symmetric key encryption and elliptic curve cryptography (ECC) to realize scalability and fault-tolerance. Fouda et al. [27] proposed a lightweight message authentication scheme, in which the shared session key is established with Diffie-Hellman...
exchange protocol, and the mutual authentication is achieved by the shared session key and hash-based authentication code. Lu et al. [28] proposed an aggregation scheme to achieve privacy preservation, which applies a super-increasing sequence to structure multi-dimensional data and encrypt the structured data by the homomorphic Paillier algorithm.

Different from existing security protocols in V2G and smart grid, we will identify and solve a new security challenge in V2G networks due to BVs’ movement. We also observe that BVs may work in different modes within an aggregator’s range. Thus, a universal authentication scheme is not suitable for all BVs in an aggregator. We need to design different authentication protocols for BVs that work in different modes (i.e., the home and visiting modes). It is observed that BVs’ working modes are not differentiated in the literature. As a result, distinct security challenges for different groups have not been studied yet in the previous studies.

III. SYSTEM MODEL

A. Network Model

Fig. 2 illustrates the V2G network architecture with the home and visiting modes BVs. The V2G network architecture mainly includes three real entities and one virtual entity: battery vehicles (BV s), local aggregators (LAGs), central authority (CA), and virtual battery vehicles (VBVs). Both real and viral entities participate in power transmission and information communication: the solid line is for power transmission, and the dashed line is for information communication. A BV is owned by an individual owner, and is normally associated with a preferred power grid operator. LAGs are granted by a power grid operator to collect BVs’ power status data for power scheduling. CA as a trusted third party belongs to an independent institution. VBV as a virtual entity provides ancillary authentication function for its attached LAG. In the network architecture, BVs can simultaneously access LAG to obtain charging services, LAG can directly communicate with the smart grid on behalf of the geographically dispersed BVs to obtain power status data. CA can derive the uploaded aggregated-proofs to achieve further billing services (e.g., payment for charging).

Assume that there are two groups in the V2G networks, and we designate in-group entities to include the home battery vehicles BVHs, home local aggregator LAG1, and home virtual battery vehicle VBVh of the same group, and the home mode is launched by LAG1; out-group entities to include the visiting battery vehicles BVVs, visiting local aggregator LAG2, and visiting virtual battery vehicle VBVv of different groups, and the visiting mode is launched by LAG2. In Fig. 2, LAG1 and LAG2 represent the aggregators of two different groups, and BVs can work as the home mode BVs and the visiting mode BVs for an in-group aggregator and an out-group aggregator. For the sake of illustration, we use two denotations for the same LAG. For instance, the denotations \{LAG1h, LAG1v\} are used for LAG1 when it provides services for BVHs and BVVs, respectively. For instance, a specific battery vehicle VBVh moves from the range of LAG1 to the range of LAG2, and it may act as BVHv for LAG2 in the home mode. When it moves to the range of LAG2, it may act as BVVv for LAG2 in the visiting mode.

Towards the introduced VBV, it is embedded into a LAG to provide support to enhance message randomization and to realize distributed non-distinguishable identification. Similarly, VBV has the variants \{VBVh, VBVv\} for the home and visiting modes, and the detailed working mode is determined by the group attributes of the interactive BVs and LAG. It means that \{VBVh, VBVv\} may coexist in a single LAG during the interactions of the in-group and out-group entities. We introduce the concept of VBV mainly due to privacy consideration. VBV communicates with LAG and VBV is also under CA’s jurisdiction. For this reason, LAG cannot obtain the VBV’s private algorithms (e.g., pseudo-random status generation, and Hamming distance based extension). In addition, VBV plays different roles in different access modes to deal with diverse security requirements. In the home mode, VBV performs the necessary pseudo-status storage and re-computation for the additional data inquiry. In the visiting mode, VBV will not store a BV’s pseudo-status data for privacy consideration (e.g., individual or group interest privacy). In the networks, VBV is self-triggered upon receiving BVs’ access challenges, and it may be in three phases, including the pre-trigger phase, trigger phase, and post-trigger phase.

- **Pre-trigger phase**: Upon LAG receiving a BV’s challenge, VBV is in the pre-trigger phase and is ready to launch its functions;
- **Trigger phase**: Upon LAG forwarding the BV’s session identifier, VBV is in the trigger phase. Then, VBV invokes its private algorithms and performs corresponding operations in different working modes;
- **Post-trigger phase**: Upon LAG transmitting the multiple BVs’ aggregated-proofs to CA, VBV is in the post-trigger phase and is ready for the next round challenge.

The communication between BVs, LAG, and CA is not limited to a specific communication technology. It can be based
on either traditional computer networks or wireless communications. For instance, the interface between HVs and LAG can use radio frequency identification (RFID).

B. Trust and Attack Model

Trust relationships among the entities are as follows. CA is the only entity trusted by all the other entities. LAG and VBV have inherent mutual trust, and no other direct trust relationships exist among BV, LAG, and VBV. Generally, BVs are rational and sensitive [29]. Being rational means that a BV’s behavior would be never based on experience or emotion, and misbehavior may only occur for selfish interests. Being sensitive means that a BV is reluctant to disclosure its sensitive data, but has strong interests in others’ privacy. Meanwhile, LAG that is granted by a power grid operator, is assumed to be honest but curious. Being honest means that LAG always appropriately follows the protocol procedure. Being curious means that LAG may attempt to obtain BVs’ private information (e.g., state of charge) [15].

Suppose that the communication channels between BVs and LAG are exposed to an attacker, which has the following capabilities. The attacker may: 1) corrupt the aggregator and the virtual battery vehicle, and impersonate as a legal entity to forward and modify the intercepted messages in the current session; 2) eavesdrop and record the exchanged messages in the former sessions, and replay the messages in the ongoing communication; 3) perform tracking and traffic analysis to monitor and estimate user privacy. The attacker cannot: 1) obtain pre-shared secrets, and distort the built-in timestamp of the exchanged messages; 2) extract the real identifier via the intercepted messages, and generate the consistent pseudonyms; 3) acquire the pseudo-random generation algorithm of the virtual battery vehicle.

IV. PROPOSED AUTHENTICATION SCHEME: AP3A

The proposed AP3A with the home mode and the visiting mode is designed for the in-group and out-group entities. In the home mode, multiple BVhi (i.e., \{BVhi1, . . . , BVhiν\}) simultaneously access LAG to perform power services (e.g., charging). LAGhi collects the BVs’ power status data with the assistance of VBVhi to provide information services for smart grid, meantime periodically uploads the aggregated data to CA for bill services. Similarly, BVvj (i.e., \{BVvj1, . . . , BVvjυ\}), LAGvj and VBVvj participate in the visiting mode. \{BV, LAG\} have their own real identifiers \{IDBV, IDLAG\}, pseudo-identity flags \{FIDBV, FLLAG\}, and group identifiers \{gid, Gid\}. Besides, LAG has a pseudonym P IDLAG. The in-group key khi is allocated to \{BVhi, LAGhi\}, and the out-group key kvj is allocated to \{BVvj, G PVvj\}. The detailed notations are introduced in Table I. The defined arithmetic functions are presented as follows:

1) \(f_0 : \mathbb{R} \times \mathbb{R} \rightarrow \mathbb{R}\), that is an XOR based function satieties \(z = f_0(x \oplus y)\); \(f_0(\cdot)\) is assigned to \{BV, LAG\}.

2) \(f_1 : \{0, 1\}^* \times \{0, 1\}^* \rightarrow \{0, 1\}^*\), that satieties \(k' = f_1(k, x)\), which as a collision-resistant function is applied for key updating. \(f_1(\cdot)\) is assigned to \{BV, LAG, CA\}.

3) \(f_2 : \mathbb{R} \rightarrow \mathbb{R}\), that satieties \(\Delta x = f_2(x)\), which as a nonreversible function is applied to distort \(x\) into \(\Delta x\). \(f_2(\cdot)\) is assigned to \{BV, CA\}.

### Table I: NOTATIONS

<table>
<thead>
<tr>
<th>Notation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>BV</td>
<td>The battery vehicle [15], including battery electric vehicles, fuel cell vehicles, plug-in hybrid electric vehicles, etc.</td>
</tr>
<tr>
<td>LAG</td>
<td>The local aggregator.</td>
</tr>
<tr>
<td>CA</td>
<td>The central authority.</td>
</tr>
<tr>
<td>BVhi, BVvj</td>
<td>The i-th home BV and the j-th visiting BV.</td>
</tr>
<tr>
<td>VBVhi, VBVvj</td>
<td>The home/visiting virtual battery vehicle.</td>
</tr>
<tr>
<td>LAGhi, LAGvj</td>
<td>The home/visiting local aggregator.</td>
</tr>
<tr>
<td>ID, PID</td>
<td>The real identifier, and pseudonym,</td>
</tr>
<tr>
<td>gid</td>
<td>The pseudo session identifier.</td>
</tr>
<tr>
<td>gp, GP</td>
<td>The group attribution of BV, LAG.</td>
</tr>
<tr>
<td>gid, Gid</td>
<td>The pseudo group identifier of gp, GP.</td>
</tr>
<tr>
<td>r</td>
<td>The pseudorandom number.</td>
</tr>
<tr>
<td>khi, kvj</td>
<td>The in-group key of BVhi and LAGhi, and the out-group key of gpvj, G PVvj.</td>
</tr>
<tr>
<td>ST, PST</td>
<td>The real-status, and pseudo-status.</td>
</tr>
<tr>
<td>E_k(\cdot)</td>
<td>The symmetric key encryption by k.</td>
</tr>
<tr>
<td>H_k(\cdot)</td>
<td>The keyed hash message authentication code (HMAC) function</td>
</tr>
<tr>
<td>M^e</td>
<td>The locally derived value M.</td>
</tr>
</tbody>
</table>

4) \(\{f_3, F\} : \mathbb{R}^* \times \{0, 1\}^* \times \{0, 1\}^* \rightarrow \{0, 1\}^*\), that satieties the functional relation as that,

\[
\prod_{n=1}^{N} f_3(x_n \oplus y_n \oplus z_n) = F(\sum_{n=1}^{N} x_n) \oplus \sum_{n=1}^{N} y_n \oplus \sum_{n=1}^{N} z_n).
\]

The pairwise functions \(\{f_3(\cdot), F(\cdot)\}\) are applied to obtain the aggregated power status data. \(f_3(\cdot)\) is assigned to \{BV, CA\}, and \(F(\cdot)\) is assigned to \{LAG, CA\}.

In system initialization, the symmetric keys (e.g., in-group key khi, and out-group key kvj) of \{LAGhi, BVhi\} and \{LAGvj, BVvj\} are distributed according to the Diffie-Hellman (DH) key agreement scheme. We take khi as an example to introduce the key distribution procedure.

LAGhi generates a random number \(\gamma_1 \in \mathbb{Z}_q^\\ast\), and transmits it to BVhi. Upon receiving the query, BVhi generates random numbers \(\gamma_2, \gamma_3 \in \mathbb{Z}_q^\\ast\) from \(\mathbb{Z}_q^\\ast\), and computes \(X_{BVhi}, Y_{BVhi}\) by its pseudonym, where \(\mathbb{Z}_q^\\ast\) is a multiplicative group, \(p\) is a large prime, and \(q\) is a primitive root of \(q\).

\[
X_{BVhi} = g^{\gamma_2 vhi} \mod q
\]
\[
Y_{BVhi} = H(\gamma_1 vhi, ||PID_{BVhi}||) \oplus g^{\gamma_2 vhi} \oplus \gamma_3 vhi.
\]

BVhi transmits \(X_{BVhi}, Y_{BVhi}, \gamma_2, \gamma_3, PID_{BVhi}\) to LAGhi, and LAGhi re-computes \(H(\gamma_1 vhi, ||PID_{BVhi}||)\) by the received \(\gamma_2, \gamma_3, PID_{BVhi}\), and derives \(g^{\gamma_2 vhi} \gamma_3 vhi\) by an XOR operation. Thereafter, LAGhi locally computes \((g^{\gamma_2 vhi})^{\gamma_1 vhi}\) of \(LAGhi\), and compares whether the derived \(g^{\gamma_1 vhi} vhi\) equals the locally computed \((g^{\gamma_2 vhi})^{\gamma_1 vhi}\). If it holds, LAGhi will generate a random number \(\gamma_2^{LAGhi}\), and computes \(X_{LAGhi}, Y_{LAGhi}\).

\[
X_{LAGhi} = g^{\gamma_2^{LAGhi}} \mod p
\]
\[
Y_{LAGhi} = H(\gamma_1^{LAGhi}, PID_{LAGhi}) \oplus g^{\gamma_2^{LAGhi}} \oplus \gamma_3^{LAGhi}.
\]
LAG_h transmits $X_{LAG_h} \parallel Y_{LAG_h} \parallel \gamma^2_{LAG_h} \parallel PID_{LAG_h}$ to BV_h, and BV_h computes $I(X_{LAG_h} \parallel Y_{LAG_h} \parallel \gamma^2_{LAG_h} \parallel PID_{LAG_h})$ by the received $\{\gamma^2_{LAG_h} \parallel PID_{LAG_h}\}$, and derives $g^{\gamma^2_{LAG_h} \parallel \gamma^2_{LAG_h}}$ by an XOR operation. BV_h locally computes $(g^{\gamma^2_{LAG_h}})^{\gamma^2_{LAG_h}}$, and compares whether the derived $(g^{\gamma^2_{LAG_h}})^{\gamma^2_{LAG_h}}$ equals the locally computed $(g^{\gamma^2_{LAG_h}})^{\gamma^2_{LAG_h}}$. If it holds, BV_h and LAG_h will establish mutual authentication, and obtain $k_{hi}$ as follows.

$$k_{hi} = (X_{LAG_h})^{\gamma^2_{LAG_h}} = (X_{LAG_h})^{\gamma^2_{LAG_h}} \mod p$$

Similarly, the out-group key $k_{ij}$ can be obtained according to the DH key agreement and mutual authentication. In the following authentication, we consider the multiple BVs $\{BV_{hi}, BV_{vj}\}$ for $i \in \{1, \ldots, I\}$ and $j \in \{1, \ldots, J\}$, which are regarded as a whole during the following specifications.

### A. Authenticating Home BVs

Fig. 3 shows the interaction among BV_h, LAG_h, and VBV_h in the home mode, in which the in-group vehicles $\{BV_{hi}, \ldots, BV_{hl}\}$ simultaneously access the in-group LAG_h, and LAG_h can provide the distributed power services and other advanced data inquiry services.

1) **Query Challenge of BV_h and Activation of LAG_h**: BV_h generates a session identifier $sid_{BV_h}$, and extracts the corresponding identity flag $F_{BV_h}$. BV_h transmits the cascaded value $sid_{BV_h} \parallel F_{BV_h}$ to LAG_h to initiate a new session. Upon receiving the query, LAG_h performs the quick check on BV_h by checking whether the received $sid_{BV_h}$ has the correct timestamp. If it does not hold, LAG_h will refuse the query and eliminate the suspicious BV from the protocol. Otherwise, the protocol will continue. LAG_h extracts the corresponding in-group key $k_{hi}$, performs the symmetric key encryption to obtain $E_{BV_h}$, and computes HMAC function to obtain $\Sigma_{hi}$, in which BV_h’s real-status $ST_{BV_h}$ is wrapped by BV_h’s pseudo-status $ST_{BV_h}$.

$$M_{BV_h} = sid_{LAG_h} \oplus PST_{BV_h}$$

**2) LAG_h Authenticating BV_h and Real-to-Pseudo Status Mapping**: Upon receiving BV_h’s response, LAG_h generates a pseudo-random number $r_{LAG_h}$, extends $r_{LAG_h}$ into $r_{LAG_h}$, for BV_h, extracts the corresponding identity flag $F_{LAG_h}$, and computes a combined session identifier $sid_{d}$,

$$sid_{d} = f_{0}(sid_{BV_h} \oplus sid_{LAG_h})$$

LAG_h transmits $r_{LAG_h} \parallel F_{LAG_h} \parallel sid_{d} \parallel M_{BV_h}$ to BV_h, then BV_h locally derives $sid_{d_{LAG_h}} \parallel PST_{BV_h}$,

$$sid_{d_{LAG_h}} = f_{0}^{-1}(sid_{d}) \oplus sid_{BV_h}$$

$$PST_{BV_h} = M_{BV_h} \parallel sid_{d_{LAG_h}}$$

BV_h performs the quick check on LAG_h by checking whether the received $F_{LAG_h}$ has the correct timestamp. If it does not hold, BV_h will terminate the protocol. Otherwise, the protocol will continue. BV_h extracts the corresponding in-group key $k_{hi}$, performs the symmetric key encryption to obtain $E_{BV_h}$, and computes HMAC function to obtain $H_{BV_h}$, in which BV_h’s real-status $ST_{BV_h}$ is wrapped by BV_h’s pseudo-status $ST_{BV_h}$.

$$F_{BV_h} = F_{k_{hi}}((sid_{d_{LAG_h}} \parallel r_{LAG_h}) \parallel F_{BV_h})$$

$$H_{BV_h} = H_{k_{hi}}(PST_{BV_h} \parallel ST_{BV_h})$$

BV_h transmits $E_{BV_h} \parallel H_{BV_h}$ to LAG_h, thereinto $E_{BV_h}$ is used for authentication, and $H_{BV_h}$ is used for real-to-pseudo status mapping. Upon receiving the message, LAG_h extracts $k_{hi}$ to compute $E_{LAG_h}$.

$$E_{LAG_h} = E_{k_{hi}}((sid_{d_{LAG_h}} \parallel r_{LAG_h}) \parallel F_{BV_h})$$

LAG_h verifies BV_h by checking whether the computed $E_{LAG_h}$ equals the received $E_{BV_h}$. If it does not hold, LAG_h
will regard the suspicious BV as an illegal vehicle and eliminate it from the protocol. Otherwise, $LAG_h$ will perform status mapping from $H_{BV_h}$ (including the real-status $ST_{BV_h}$) into the pseudo-status $PST_{BV_h}$ to realize further anonymous data transmission.

3) **Pseudo-Status Storage and Recomputing on $BV_h$:** $LAG_h$ transmits the pseudo-status $PST_{BV_h}$ to $BV_h$. $BV_h$ stores $PST_{BV_h}$, and computes the updated $PST'_{BV_h}$.

\[
PST'_{BV_h} = PST_{BV_h} \oplus M_{BV_h}.
\]

$BV_h$ replies $PST'_{BV_h}$ to $LAG_h$. The pseudo-status storage provides the following data inquiry services for $BV_h$: $BV_h$ can inquire its accessing data by providing the anonymized $PST'_{BV_h}$ without revealing any sensitive information.

4) **BV_h Authenticating $LAG_h$ and Aggregated-proofs Generation:** Upon receiving $PST'_{BV_h}$, $LAG_h$ extracts the pseudonym $PID_{LAG_h}$, updates $k'_{h_l}$, and computes $k'_{LAG_h}$, and $M_{LAG_h}$.

\[
k'_{h_l} = f_1(kh_l, \{r_{LAG_h}, \text{sid}_{BV_h}\})
\]

\[
E'_{LAG_h} = E_{k'_{LAG_h}}(M_{BV_h} | M_{LAG_h}) | PID_{LAG_h}.
\]

$LAG_h$ transmits $E'_{LAG_h}$ to $BV_h$ for authentication. $BV_h$ obtains the updated $k'_{h_l}$, and computes $k'_{BV_h}$.

\[
E'_{BV_h} = E_{k'_{BV_h}}(PST'_{BV_h} | PID_{LAG_h}).
\]

$BV_h$ verifies $LAG_h$ by checking whether the computed $E'_{BV_h}$ equals the received $E'_{LAG_h}$. If it holds, $BV_h$ will regard $LAG_h$ as a legal aggregator. Otherwise, protocol will terminate. When $BV_h$ has been fully charged or wants to quit the charging operation, it computes $PST'_{BV_h}$, $\Delta PST_{BV_h}$, $\Delta_h$, and $M_{BV_h}$, in which the real-status variation $\Delta ST_{BV_h}$ is wrapped with $\Delta PST_{BV_h}$.

\[
PST'_{BV_h} = f_0^{-1}(M_{LAG_h}) \oplus M_{BV_h}, \quad \Delta PST_{BV_h} = f_2(PST'_{BV_h}), \quad \Delta_h = \Delta ST_{BV_h} \oplus \Delta PST_{BV_h}, \quad M_{BV_h} = f_3(\text{sid}_h \oplus \Delta_h \oplus PST_{BV_h}).
\]

$BV_h$ transmits $M_{BV_h}$ to $LAG_h$ for the aggregated-proofs establishment. $LAG_h$ periodically computes the aggregated pseudo-status variation $\Sigma_h$. $LAG_h$ obtains the aggregated-proofs $PST_{BV_h}$, and periodically uploads $PST_{BV_h}$ to $CA$.

\[
\Sigma_h = \sum_{i=1}^{I} \{\Delta_{hi}\}
\]

\[
= \sum_{i=1}^{I} \{PST'_{BV_h_i} \oplus f^{-1}(\prod_{i=1}^{I} M_{BV_h_i}) \oplus \sum_{i=1}^{I} \{\text{sid}_i\}\}
\]

\[
PST_{BV_h} = \{\text{r}_{LAG_h}, \{\text{sid}_i\}, \{F_{BV_h_i}\}, \{M_{BV_h_i}\}, \{PST'_{BV_h_i}\}\}.
\]

Thereinto, the denotations $\{r_{LAG_h}\}$, $\{\text{sid}_i\}$, and $\{X_{BV_h}\}$ ($X \in \{F, M, PST\}$) represent $BV_{1}, \ldots, BV_{N}$'s corresponding values, and the relation of $\{f_0(\cdot), f_1(\cdot)\}$ is applied to obtain $\Sigma_h$ that is provided for power scheduling. Afterwards, $CA$ derives the real-status variation $\Delta ST_{BV_h}$ for billing purposes.

\[
\Delta ST_{BV_h} = f_2(PST'_{BV_h}), \oplus (PST'_{BV_h} \oplus f_0^{-1}(M_{BV_h})).
\]

B. **Authenticating Visiting BVs**

Fig. 4 shows the interaction among $BV_{e_1}$, $LAG_e$, and $VBV_{e}$ in the visiting mode, in which the out-group vehicles $\{BV_{e_1}, \ldots, BV_{e_d}\}$ are not under $LAG_e$'s default jurisdiction, and the out-group $I.AG_e$ only provides the basic power services without storing BVS' privacy data or providing additional data inquiry services. The limited authority is appointed for the visiting mode according to the practical applications.

1) **Query Challenge of $BV_{e_1}$ and Activation of $VBV_{e}$** $BV_{e_1}$ generates a session identifier $sid_{BV_{e_1}}$, extracts the corresponding identity flag $F_{BV_{e_1}}$, and transmits $sid_{BV_{e_1}} \oplus F_{BV_{e_1}}$ to $LAG_e$. Upon receiving the query, $LAG_e$ performs the quick check on $BV_{e_1}$ by checking whether the received $sid_{BV_{e_1}} \oplus F_{BV_{e_1}}$ and $F_{BV_{e_1}}$ repeatedly emerge within an unacceptable time interval. If so, $LAG_e$ will refuse the query and eliminate the
suspicious $BV$ from the protocol. Otherwise, $LAG_v$ will ascertain $HV_v$,’s group attribution via $f_{HV_v}$ and obtain the group identifiers $gid_{v}$. Thereby, $LAG_v$ knows that $BV_v$ belongs to the out-group vehicles, and the visiting mode is launched. $LAG_v$ forwards $sid_{BV_v}$ to $BV_v$. Upon receiving the message, $BV_v$ generates a pseudo-status $PST_{BV_v}$, extends $PST_{BV_v}$ into a series of pseudo-status values $PST_{BV_v}$, and computes $M_{BV_v}$.

$$M_{BV_v} = sid_{BV_v} \oplus PST_{BV_v}.$$  

2) Mutual Authentication Between $BV_v$ and $LAG_v$: When $LAG_v$ receives $PST_{BV_v} | M_{BV_v}$, it generates a pseudo-random number $r_{LAG_v}$, extends $r_{LAG_v}$ for $BV_v$. Thereafter, $LAG_v$ extracts $\{F_{LAG_v}, Gid_v, k_v\}$ to compute $F_v$, $k_v$, and $G_{LAG_v}$:

$$F_v = f_0(F_{BV_v} \oplus F_{LAG_v}),$$
$$k_v = f_1(k_v) \oplus r_{LAG_v},$$
$$G_{LAG_v} = H_{k_v}(Gid_v \oplus gid_{v}) \oplus PST_{BV_v}.$$  

$LAG_v$ transmits $r_{LAG_v} \oplus F_v \oplus G_{LAG_v} | M_{BV_v}$ to $BV_v$, and $BV_v$ locally derives $F^I_{LAG_v}$ and $PST^I_{BV_v}$:

$$F^I_{LAG_v} = f_0^{-1}(F_v) \oplus sid_{BV_v},$$
$$PST^I_{BV_v} = M_{BV_v} \oplus sid_{BV_v.$$  

$BV_v$ performs the quick check by the derived $F^I_{LAG_v}$, and further ascertains $LAG_v$’s group attribution to obtain the group identifier $Gid_v$. Thereafter, $BV_v$ extracts $\{Gid_v, k_v\}$, updates $k_v$, and computes $G_{BV_v}$:

$$k_v = f_1(k_v) \oplus r_{LAG_v},$$
$$G_{BV_v} = H_{k_v}(Gid_v \oplus gid_{v}) \oplus PST_{BV_v}.$$  

$BV_v$ verifies $LAG_v$ by comparing the received $G_{BV_v}$ equals the received $G_{LAG_v}$. If it does not hold, $BV_v$ will regard $LAG_v$ as an illegal aggregator, and terminate the protocol. Otherwise, $BV_v$ will compute $H_{BV_v}$ and $H_{BV_v}$, then transmits $H_{BV_v} \oplus H_{BV_v}$ to $LAG_v$:

$$H_{BV_v} = H_{G_{BV_v}}(r_{LAG_v} | (F_v \oplus sid_{BV_v})).$$
$$H_{BV_v} = H_{G_{BV_v}}(PST_{BV_v} \oplus ST_{BV_v}).$$  

Upon receiving the message, $LAG_v$ computes $H_{LAG_v}$, and verifies $BV_v$ by checking whether the computed $H_{LAG_v}$ equals the received $H_{BV_v}$. If it does not hold, $LAG_v$ will regard the suspicious $BV$ as an illegal vehicle and eliminate it from the protocol; otherwise, the protocol will continue.

$$H_{LAG_v} = H_{G_{LAG_v}}(r_{LAG_v} | (F_v \oplus sid_{BV_v})).$$  

3) Real-to-Pseudo Status Mapping and Aggregated-Proofs Generation: $LAG_v$ performs status mapping from the received $H_{BV_v}$ (including the real-status $ST_{BV_v}$) into the pseudo-status $PST_{BV_v}$. Thereafter, $LAG_v$ computes and transmits $M_{LAG_v}$ to $BV_v$.

$$M_{LAG_v} = f_0(M_{BV_v} \oplus PST_{BV_v}).$$  

In the case if $BV_v$ has been fully charged or wants to quit the charging operation, $HV_v$ will compute $PST_{BV_v} \oplus PST_{BV_v} \oplus \Delta_{j}$, and $M_{BV_v}$:

$$PST_{BV_v} = f_0^{-1}(M_{LAG_v}) \oplus M_{BV_v},$$
$$\Delta_{j} = f_2(PST_{BV_v}) \oplus \Delta_{j+1},$$
$$M_{BV_v} = f_2(sid_{BV_v} \oplus \Delta_{j} \oplus PST_{BV_v}).$$  

$BV_v$ transmits $M_{BV_v}$ to $LAG_v$ for the aggregated-proofs establishment, and $LAG_v$ periodically computes the aggregated pseudo-status variation $\Sigma_v$ to establish the aggregated-proofs $P_{BV_v}$, and then periodically uploads $P_{BV_v}$ to $CA$:

$$\Sigma_v = \sum_{j=0}^{J-1} \Delta_{j} = \sum_{j=0}^{J-1} (PST_{BV_v} \oplus F^{-1}(\prod_{j=0}^{J-1} M_{BV_v})) \oplus \Sigma_{v-1}.$$  

$P_{BV_v} = \{\Sigma_v, \{r_{LAG_v}\}, \{sid_{BV_v}\}, \{F_{BV_v}\}, \{M_{BV_v}\}, \{PST_{BV_v}\} \}$.

Thereinto, the denotations $\{r_{LAG_v}\}$ and $\{X_{BV_v}\}$ represent $\{sid, F, M, PST\}$, $X \in \{sid, F, M, PST\}$ represent $\{BV_v, \ldots, BV_v, \ldots\}$’s corresponding values. $CA$ further ascertains $BV_v$’s specific identity by $P_{BV_v}$, and derives the real-status variation $\Delta ST_{BV_v}$ for billing purposes.

$$\Delta ST_{BV_v} = f_0(PST_{BV_v}) \oplus (PST_{BV_v} \oplus f_0^{-1}(M_{BV_v}) \oplus sid_{BV_v}).$$

C. Requirements and Approaches for Authenticating BVs in Different Modes

In this section, we will clarify the privacy requirements to authenticate BVs in different modes, and present the approaches to satisfy the authentication differentiations.

1) Power Service Privilege: The home mode serves for in-group entities to provide the distributed power services and other data inquiry services. Thereby, $VB_v$ performs pseudo-status storage and recomputing to conduct to later data inquiry. $VB_v$ stores the pseudo-status $PST_{BV_v}$, and re-computes $PST_{BV_v} = PST_{BV_v} \oplus M_{BV_v}$, to realize pseudo-status inquiry within an allowable time interval. Hence, the home mode allows $VB_v$ to store $PST_{BV_v}$, for $VB_v$’s future retracing. The visiting mode serves for out-group entities to only provide the basic power services without storing a BV’s pseudo-status for privacy consideration.

2) Power Status Derivation: In a practical application, the in-group and out-group entities share different secrets and algorithms. It is necessary for the home mode to perform the reversible SKE algorithm by the in-group keys for mutual authentication, and for the visiting mode to apply the nonreversible HMAC function to avoid data inverse derivation.
Towards authentication operators, $BV_h$, performs the symmetric key encryption on $\{\text{sid}^t_{BVs,v}, F_BV_h, \}$ with the in-group key $k_{BVs,v}$ to obtain $E_{BVs,v}$, and on $\{PST^e_{BVs,v}, PID_{LAG_h}\}$ with the updated key $k'_{BVs,v}$ to obtain $E'_{BVs,v}$. The authentication operators are computed via symmetric key encryption. While $BVs_v$ applies HMAC function on $\{G_id_v, g_id_v, PST_{BVs,v}\}$ with the updated out-group key $k'_v$, and on $\{r_{LAG_v}, F_v, \text{sid}_{BVs,v}\}$ with the group identifier-based function $G_{BVs,v}$_. It realizes that $\{BV_h, LAG_h\}$ verify each other based on the reversible encryption algorithm, and $\{BV_{vs}, LAG_{vs}\}$ perform the verification via the nonreversible function, which conforms the two modes’ conditions.

3) Entity Group Attribution: The group attribution can recognize that whether the communicated entities belong to the same group, initiate the corresponding home or visiting mode, and extract the in-group or out-group keys for authentication.

In the home mode, $LAG_h$ can recognize that $BV_{h,i}$ belong to the in-group entities by the identity flag $F_{BVs,v}$, and the following authentication does not need to introduce any group identifier. Different from the home mode, the visiting mode performs the group attribution extraction with the purpose to ascertain the BVs’ general group information, rather than to obtain the detailed identity information. $BV_{vs}$ and $LAG_{vs}$ need extract each other’s group identifiers $\{G_id_v, g_id_v\}$ as the authentication operators, and ascertain the corresponding out-group keys $k_v$. $\{LAG_h, LAG_v\}$ can only know that the corresponding in-group $BV_{h,i}$ or out-group $BV_{vs}$ has accessed the networks, rather than acquaint $\{BV_{h,i}, BV_{vs}\}$’s specific identity. This process can enhance privacy preservation since there is no real identifiers leakage.

4) Entity Prior-Trust Degree: The home and visiting modes have different authentication demands. Particularly, $LAG_h$ first performs authentication on $BV_{h,i}$ in the home mode while $BV_{vs}$ first verifies $LAG_{vs}$ in the visiting mode. For $BV_{h,i}$, it knows that the accessed aggregator $LAG_h$ is its home aggregator, thereby $LAG_h$ has a strong demand to verify the unknown $BV_{h,i}$. For $BV_{vs}$, it knows that $LAG_v$ and itself belong to different groups, and it is a more vulnerable entity and has a stronger demand to authenticate $LAG_v$. Therefore, it is desirable for $BV_{vs}$ to first perform verification on $LAG_v$.

5) Entity Session Control: In the home mode, $BV_{h,v}$ and $LAG_h$ jointly work to monitor the active session in order to maximize $LAG_h$’s session control efficiency, which is convenient for the in-group aggregator to provide full services for its supervised BVs. Particularly, $\{BV_{h,v}, LAG_h\}$ generate session identifiers $\{\text{sid}^t_{BVs,v}, \text{sid}_{LAG_h}\}$, and $LAG_h$ extends $\text{sid}_{LAG_h}$ into $\text{sid}_{LAG_h}$. The re-computed session identifiers $\text{sid}_d = f_0(\text{sid}_{BVs,v} \oplus \text{sid}_{LAG_h})$ are obtained to ensure session freshness. Comparatively, in the visiting mode, only $BV_{vs}$ owns the initiative to generate and control session identifier $\text{sid}_{BVs,v}$, $LAG_v$ does not publish any session identifier to minimize the access privilege of the out-group BVs, and provides the basic power services.

V. ATTACK ANALYSIS

We perform attack analysis, including impersonation attack, replay attack, and denial of service (DoS) attack.

A. Impersonation Attack

Impersonation is a typical attack, in which an attacker forges a legal entity to obtain the access authority. For instance, an imitated vehicle $BV_a$ impersonates as an in-group vehicle $\overline{BV}_h$, (or an out-group vehicle $\overline{BV}_{v,a}$) to access $LAG_h$ (or $LAG_a$). If the aggregator cannot discern the suspicious vehicle, $\overline{BV}_a$ may perform power stealing or cheating. For another unusual instance, an imitated local aggregator serves as $LAG_h$ (or $LAG_a$) to collect $BV$s’ power status. If the $BV$s cannot recognize the suspicious aggregator, the sensitive data may be abused with malicious intentions.

1) HV Impersonation Attack: Suppose that $\overline{BV}_a$ disguises as $BV_v$ to cheat $LAG$ with the imitative messages.

In the home mode, $\overline{BV}_{ha}$ impersonates $\overline{BV}_{h,a}$ to transmit a forged query $\text{sid}^t_{BVs,v} \| F_{BVs,v}$ to $LAG_h$. Suppose that $\overline{BV}_{ha}$ can pass the quick check, and $LAG_h$ considers that the query is from $BV_{h,a}$. $LAG_h$ generates and transmits $sid_{LAG_h}$ to $VBV_a$, and $VBV_a$ replies $MV_{BVs,v}$ to $LAG_h$. Subsequently, $LAG_h$ obtains $\{r_{LAG_h}, F_{LAG_h}, \text{sid}_{h,a}\}$, and transmits $r_{LAG_h}, F_{LAG_h}, \| \text{sid}_{h,a} \| MV_{BVs,v}$ to $\overline{BV}_{ha}$. Afterwards, $\overline{BV}_{ha}$ skips the quick check, and locally computes $E_{\overline{BVs,v}}$. Thereinto, $\overline{BV}_{ha}$ cannot obtain $BV_{h,a}$’s in-group key $k_{h,a}$. Upon receiving $E_{\overline{BVs,v}}, \| H_{\overline{BVs,v}}$ from $\overline{BV}_{ha}$, $LAG_h$ extracts $k_{h,a}$, and compute $E_{LAG_h}$ to verify $\overline{BV}_{h,a}$. It turns out that $LAG_h$ regards $\overline{BV}_{h,a}$ as an illegal home vehicle according to $E_{LAG_h} \neq E_{\overline{BVs,v}}$, in which $k_{h,a} \neq \overline{k}_{h,a}$.

In the visiting mode, $\overline{BV}_{va}$ impersonates $BV_v$ to transmit a forged query $\text{sid}^t_{BVs,v} \| F_{BVs,v}$ to $LAG_v$. Suppose that $\overline{F}_{BVs,v}$ has an acceptable timestamp, and $\overline{BV}_{va}$ could pass the quick check. Thereafter, $LAG_v$ considers that the query is from $BV_{v,a}$. $LAG_v$ generates and transmits $sid_{LAG_v}$ to $\overline{BV}_{va}$, and $\overline{BV}_{va}$ replies $MV_{BVs,v}$ to $LAG_v$. Upon receiving the message, $\overline{BV}_{va}$ computes the corresponding $PST_{BVs,v}$ and $MV_{BVs,v}$, and transmits $PST_{BVs,v}, \| MV_{BVs,v}$ to $LAG_v$. Then, $LAG_v$ obtains $\{r_{LAG_v}, F_{LAG_v}, G_id_v, \overline{k_v}\}$, and computes $G_{LAG_v}, LAG_v$ transmits $r_{LAG_v}, F_{LAG_v}, \| G_{LAG_v}, MV_{BVs,v}$, to $\overline{BV}_{va}$, and $\overline{H}_{\overline{BVs,v}} can locally compute $G_{\overline{BVs,v}}$. Skipping the quick check and authentication on $LG_{LAG_v}, \overline{BV}_{va}$ computes and transmits $\overline{H}_{\overline{BVs,v}}, \| H_{\overline{BVs,v}}$ to $LAG_v$. Thereafter, $LAG_v$ locally computes $H_{LAG_v}$ to verify $\overline{BV}_{va}$. It turns out that $LAG_a$ regards $\overline{BV}_{va}$ as an illegal visiting vehicle according to $H_{LAG_v} \neq H_{\overline{BVs,v}}$ and the inconsistencies of $\{G_{LAG_v}, G_{\overline{BVs,v}}\}$, in which $k_v \neq \overline{k}_{va}$ and $G_id_v \neq G_id_v$.  

2) LAG Impersonation Attack: Suppose that an attacker impersonates $\overline{LAG}$ to collect the power status of $BV_v$.

In the home mode, $\overline{LAG}$ impersonates a home aggregator $\overline{LAG}_h$ to receive $BV_{h,v}$’s query $\text{sid}_{BVs,v}, \| F_{BVs,v}$. Thereafter, $\overline{LAG}_h$ skips the quick check to generate and transmit $\text{sid}_{BVs,v}$ to $\overline{BV}_h$. After a series of operations, $BV_{h,a}$ receives $\overline{LAG}_h, \| F_{\overline{LAG}_h}, \| \text{sid}_{h,a} \| MV_{BVs,v}$, and performs the quick check on $LAG_h$. $\overline{BV}_{h,a}$ transmits $\overline{F}_{BVs,v}, \| \overline{H}_{\overline{BVs,v}}$ to $LAG_h$. Thereafter, $\overline{LAG}_h$ directly transmits the mapped pseudo-status $\overline{PST}_{BVs,v}$ to $\overline{BV}_h$. $\overline{BV}_h$ replies $PST_{BVs,v}$ to $LAG_h$. 

LIU et al. AGGREGATED-PROOFS BASED PRIVACY-PRESERVING AUTHENTICATION FOR V2G NETWORKS IN THE SMART GRID 1729
and LAGk further computes E′ \text{LAG}_{k}. \) Upon receiving
\( E′ \text{LAG}_{k}, M_{\text{LAG}} \), BVk computes E\text{BV}_{k}, to verify LAGk, in
which \( P_{\text{ST}} V_{\text{BVk}} = M_{\text{BVk}} \oplus \{f_{k}^{-1}(s_{\text{id}}) \oplus s_{\text{id}} \text{BV}_{k} \}. \) It
outturns that BVk regards LAGk as an illegal home aggrega-
tor according to E\text{BV}_{k}, \neq E′ \text{LAG}_{k}, in which k_{\text{h}} \neq k_{\text{h}} and
\( P_{\text{ID}} \text{LAG}_{k}, \neq P_{\text{ID}} \text{LAG}_{k}. \)

In the visiting mode, LAG impersonates a visiting aggrega-
tor to receive s_{\text{id}} \text{BV}_{k}. After passing the quick check, LAGk for-
wards s_{\text{id}} \text{BV}_{k} to BVk, thereafter BVk replies P_{\text{ST}} V_{\text{BV}}. LAG\text{f} further computes
\( G_{\text{LAG}} \) to transmit \( \hat{r}_{\text{LAG}}, F, \|G_{\text{LAG}} \| \) to BVk. BVk extracts \( \{ \hat{g}_{\text{id}}, k_{\text{v}} \}, \) computes
\( G_{\text{LAG}} \) to verify LAGk. It turns out that BVk regards LAGk as an illegal visiting aggregator according to
\( G_{\text{LAG}} \), in which k_{\text{h}} \neq k_{\text{h}} and g_{\text{id}} \neq \hat{g}_{\text{id}}. \)

B. Replay Attack

Replay attack means that an attacker eavesdrops a legal en-
identity’s messages during former sessions, and in another session
the attacker replays the intercepted messages to involve into the
current communication. For instance, an illegal vehicle BV\text{f}
replays BV’s query to challenge LAG, or an illegal aggrega-
tor LAGk replies LAG’s response to reply HV’s query.

1) BV Replay Attack: Suppose that an attacker BVk replies
BV’s outdated query to involve into the communication.

In the home mode, BV\text{h} ha intercepts BVk’s former mes-
sages to replay the outdated query s_{\text{id}} \text{BV}_{k}, F_{\text{old}} \text{BV}_{k} to LAGk. Upon re-
ceiving the query, LAGk performs the quick check on
\( \text{BV}_{\text{h}}. \) It turns out that \( s_{\text{id}} \text{BV}_{\text{h}}, F_{\text{old}} \text{BV}_{\text{h}} \) has aa wrong timestamp, thereby LAGk
may refuse BV\text{h}’s query. In a worse condition, the protocol
may continue, and LAGk creates a new s_{\text{id}} \text{LAG}_{k}. There-
after, \{ LAGk, BVk \} perform the corresponding operations to
transmit r_{\text{old}} \text{LAG}_{k}, H_{\text{old}} \text{LAG}_{k}, \| s_{\text{id}} \text{LAG}_{k} \| M_{\text{BV}_{\text{k}}} to BVk. Upon receiv-
ing the message, BVk skips the quick check and directly rep-
sponds with the formerly intercepted E_{\text{old}} \text{LAG}_{k}, H_{\text{old}} \text{LAG}_{k}. Upon receiv-
ing the message, LAGk extracts k_{\text{h}} to compute
\( E_{\text{old}} \text{LAG}_{k}, \) and verifys BV\text{h} by checking whether E_{\text{old}} \text{LAG}_{k}
eq E_{\text{old}} \text{LAG}_{k}. It turns out that LAGk regards BV\text{h} as an illegal
vehicle aggregating to \( \geq E_{\text{old}} \text{LAG}_{k}, \) in which
\( s_{\text{id}} \text{BV}_{\text{h}}, F_{\text{old}} \text{BV}_{\text{h}} \) are abnormal and eliminates BV\text{h} from
the protocol. In a worse condition, LAGk may ignore the
mistake, and \{ LAGk, BVk \} proceed with the operations to obtain
\( G_{\text{LAG}} \) and \( \text{LAG}_{k}. \) Then, LAGk transmits
\( r_{\text{LAG}}, F_{\text{LAG}}, H_{\text{LAG}} \text{LAG}_{k}, \| s_{\text{id}} \text{LAG}_{k} \| M_{\text{BV}_{\text{k}}} \) to BVk, and BVk repl-
s the intercepted \( H_{\text{old}} \text{LAG}_{k}, \| s_{\text{id}} \text{LAG}_{k} \| M_{\text{BV}_{\text{k}}} to LAGk. \) Afterwards,
LAGk computes the updated H_{\text{LAG}}, to verify BVk. It turns out that
LAGk regards BVk as an illegal visiting aggrega-
tor according to \( H_{\text{LAG}}, \neq H_{\text{old}} \text{LAG}_{k}, \) in which
\( G_{\text{LAG}}, \neq G_{\text{LAG}}, r_{\text{LAG}} \neq r_{\text{LAG}} \text{LAG}_{k}, \) and \( F_{\text{LAG}} \neq F_{\text{LAG}} \).

2) LAG Replay Attack: Suppose that an attacker LAGk re-
plays the intercepted messages to collect HV’s’ power status.
In the home mode, LAGk intercepts LAGk’s former mes-
sages. When \( \text{LAG}_{k} \) receives BV\text{h}’s query \( s_{\text{id}} \text{BV}_{\text{h}}, F_{\text{new}} \text{BV}_{\text{h}} \) in
another session, LAGk directly replies the formerly intercepted
\( r_{\text{old}} \text{LAG}_{k}, H_{\text{old}} \text{LAG}_{k}, \| s_{\text{id}} \text{LAG}_{k} \| M_{\text{LAG}} \) to BVk. Upon receiving the
outdated message, BVk derives the distorted \( s_{\text{id}} \text{LAG}_{k} \) by
\( P_{\text{ID}} \text{LAG}_{k}, \neq P_{\text{ID}} \text{LAG}_{k}. \) It turns out that BVk may ignore the mistake, and transmits
\( E_{\text{old}} \text{LAG}_{k}, \| s_{\text{id}} \text{LAG}_{k} \| M_{\text{LAG}} \) to LAGk. LAGk replies \( E_{\text{old}} \text{LAG}_{k}, \| s_{\text{id}} \text{LAG}_{k} \| M_{\text{LAG}} \)
without authenticating BVk. BVk computes \( E_{\text{old}} \text{LAG}_{k}, \) to verify LAGk, in which \( P_{\text{ST}} V_{\text{BVk}}, \neq M_{\text{LAG}} \text{LAG}_{k}. \) It turns out that BVk regards LAGk as an illegal aggrega-
tor according to \( E_{\text{old}} \text{LAG}_{k}, \neq E_{\text{old}} \text{LAG}_{k} \), and the inconsistencies of \( \{ k_{\text{h}}, k_{\text{v}} \} \) and \( \{ P_{\text{ID}} \text{LAG}_{k}, P_{\text{ID}} \text{LAG}_{k} \} \) in which \( s_{\text{id}} \text{LAG}_{k} \neq s_{\text{id}} \).

In the visiting mode, LAGk intercepts and replays
LAGk’s former messages. Upon receiving BV\text{v}’s query
\( s_{\text{id}} \text{BV}_{\text{v}}, F_{\text{old}} \text{BV}_{\text{v}} \) in another session, LAGk repl-
yes the outdated \( r_{\text{old}} \text{LAG}_{k}, \| s_{\text{id}} \text{LAG}_{k} \| M_{\text{LAG}} \). Thereafter,
BVv performs the quick check on LAGk by the distorted
\( P_{\text{ST}} V_{\text{BVv}}, = f_{k_{\text{t}}}^{-1}(s_{\text{id}}) \oplus s_{\text{id}} \text{BV}_{v}. \) The identity flag has wrong
time stamp so that HVv refuses LAGk. If HVv ignores the
mistake, it will compute \( G_{\text{LAG}} \) to verify LAGk. Here,
\( k_{\text{t}} = k_{\text{t}} \) and \( P_{\text{ID}} \text{LAG}_{k}, \neq P_{\text{ID}} \text{LAG}_{k}. \) It turns out that
BVv regards LAGk as an illegal visiting aggregator accord-
ing to \( G_{\text{LAG}} \) and the inconsistencies of \( \{ P_{\text{ST}} V_{\text{BVv}}, P_{\text{ST}} V_{\text{BVv}} \} \), in which \( s_{\text{id}} \text{LAG}_{k} \neq s_{\text{id}} \).

C. Denial of Service Attack

DoS attack may be caused by flooding data streams or jam-
mhing channels to interfere in the normal communication. An
attacker may disguise as legal a BV to transmit a huge number
of queries with false addresses. The purpose of the DoS attack
is not to capture a BV’s sensitive information, but rather to ensure
that a legal entity cannot establish communication.

In AP3A, the quick check mechanism is able to resist the
DoS attack. For instance, an attacker A may disguise as BV\text{h},
to consecutively challenge a legal LAGk. Upon receiving the
queries, LAGk performs the quick check on BV\text{h} by verifying
whether the received \( s_{\text{id}} \text{LAG}_{k} \) and \( \text{LAG}_{k} \) repeatedly emerged
within an unacceptable time interval. \( \text{LAG}_{k} \) can discern the il-
legal BV\text{h} according to the one-time-valid session identi-
vacy and Data Integrity

Data confidentiality and data integrity are achieved by the
anonymous aggregated-proofs. Towards the aggregated-proofs
\{P_{BV_A}, P_{BV_e}\}$, six parameters are included: \(\{\Sigma_h, \Sigma_v\}\) are the aggregated pseudo-status variations to provide information for power scheduling, the pseudo-random numbers \(\{r_{LAG_h}, r_{LAG_e}\}\) and the session identifiers \(\{sid_h, sid_{BV_h}\}\) are used to ensure data randomization and session freshness, the identity flags \(\{F_{BV_h}, F_{BV_e}\}\) are used to determine BV's group attributes, \(\{M_{BV_h}, M_{BV_e}\}\) and \(\{PST_{BV_h}, PST_{BV_e}\}\) are used to derive the detailed real-status for bill purposes. Meanwhile, \(\{BV_h, BV_e\}\) apply HMAC functions on the current real-status \(\{ST_{BV_h}, ST_{BV_e}\}\) to obtain \(\{H_{BV_h}, H_{BV_e}\}\), in which \(\{ST_{BV_h}, ST_{BV_e}\}\) have been wrapped with \(\{PST_{BV_h}, PST_{BV_e}\}\). Upon receiving the messages, \(\{LAG_h, LAG_e\}\) map their respective real-status-inbuilt values \(\{H_{BV_h}, H_{BV_e}\}\) into the pseudo-status \(\{PST_{BV_h}, PST_{BV_e}\}\) to realize anonymous data transmission. Particularly, the aggregated-proofs are established based on the distributed networks, which may reduce the dependency on the central authority. Meanwhile, \(LAG\) applies the primary authentication on multiple \(BV\)'s, and eliminates any suspicious \(BV\)'s from the protocol without influencing other ongoing authentications. Meanwhile, the identity flags with the timestamp are used for the quick check, which may terminate the malicious message challenges to alleviate the DoS attack, and to provide enhanced data availability.

### B. Mutual Authentication

Two round mutual authentications are performed to establish trusted relationships. In both the home and visiting modes, \(BV\) and \(LAG\) first perform the quick check based on the received session identifiers and identity flags. Thereafter, \(BV\)'s and \(LAG\) verify each other by SKE or HMAC algorithms. During the execution of the cryptographic algorithms, the in-group key \(k_{h,i}\) is assigned to \(BV_h\) and \(LAG_h\), and the out-group key \(k_{o,j}\) is assigned to \(gp_{e}\) and \(GP_e\). If and only if both mutual authentications succeed, \(BV\)'s will transmit the pseudo-status to \(LAG\) for the final aggregated-proofs establishment.

### C. Dynamic Participation

Suppose that \(\{BV_{h,i}, BV_{e,j}\}\) have established communication with \(\{LAG_h, LAG_e\}\). During the ongoing communications, newly joined in-group \(BV_{h,n}\) (or out-group \(BV_{e,n}\)) for \(n = 1, \ldots, N\), transmits \(sid_{BV_{h,n}} F_{BV_{h,n}}\) (or \(sid_{BV_{e,n}} \parallel F_{BV_{e,n}}\)) to challenge \(LAG_h\) (or \(LAG_e\)). Upon receiving the new queries, the interactions of \(BV_{h,n} - n\) and \(LAG_h, LAG_e\) are performed in the corresponding home or visiting mode without interfering with the existing operations of \(\{BV_{h,i}, LAG_h\}\) (or \(\{BV_{e,j}, LAG_e\}\)). When some \(BV\)'s have fully charged or want to quit the charging operations, \(BV_{h,i}\) (or \(BV_{e,j}\)) immediately transmits \(M_{BV_{h,i}}\) (or \(M_{BV_{e,j}}\)), and \(LAG_h\) (or \(LAG_e\)) periodically uploads the current aggregated pseudo-status along with other parameters to \(CA\). Furthermore, even if only one \(BV\) (e.g., \(BV_{h,m}\)) communicates with an aggregator \(LAG_h\), the aggregated pseudo-status \(\Sigma_h = D_{h,m} = \Delta PST_{BV_{h,m}} \in F^{-1}(M_{BV_{h,m}}) \ominus \delta m\) cannot reveal \(BV_{h,m}\)'s real-status. \(LAG_h\) knows nothing about the function \(f_\Sigma(\cdot)\), so that it cannot compute \(DPS_{BV_{h,m}}\) to derive the real-status variation \(\Delta ST_{BV_{h,m}}\).

### D. Forward and Backward Unlinkability

Towards \(\{BV_{h,i}, LAG_h\}\), the session identifiers \(\{sid_{BV_{h,i}}, sid_{LAG_h}\}\) are XORed as the combined session identifier \(sid_i\), and the timestamp in the identity flags \(\{F_{BV_{h,i}}, F_{LAG_h}\}\) are dynamic to ensure the identity randomization. Towards \(\{BV_{e,j}, LAG_e\}\), the session identifier \(sid_{BV_{e,j}}\), and the combined identity flag \(f_\Sigma\) jointly guarantee the session freshness. Meanwhile, the home and visiting modes also introduce the extended pseudo-random numbers \(\{r_{LAG_h}, r_{LAG_e}\}\) and pseudo-status \(\{PST_{BV_{h,i}}, PST_{BV_{e,j}}\}\) to make the communication unlinkable, and the nonreversible HMAC function assists to provide forward and backward security. The attacker regards the previous sessions as random even if both \(BV\)'s and \(LAG\) have been corrupted, and regards the subsequent sessions as random even if the attacker can intercept the current exchanged messages. The current security compromises cannot correlate with the previous and subsequent interactions due to the introduced pseudo-random values (e.g., session identifier).

### E. Privacy Preservation

Towards the privacy, \(\{LAG_h, LAG_e\}\) may attempt to correlate \(\{BV_{h,i}, BV_{e,j}\}\)'s specific identifiers with the detailed power status. In AP3A, privacy preservation is addressed by introducing anonymous aggregated-proofs, which realizes that multiple \(BV\)'s pseudo-status values are uploaded in a whole group without revealing any individual privacy. \(\{LAG_h, LAG_e\}\) derive the aggregated pseudo-status variations in the form of \(\{\Sigma_h, \Sigma_v\}\), and upload the aggregated-proofs \(\{P_{BV_h}, P_{BV_e}\}\) to \(CA\) for power scheduling. \(\{LAG_h, LAG_e\}\) can obtain the aggregated pseudo-status variation of multiple \(BV\)'s without revealing an individual \(BV\)'s real-status, and the relative values reflect the power demands to offer service for power management (e.g., real-time scheduling). Furthermore, the pseudo-identity flags \(\{F_{BV_{h,i}}, F_{BV_{e,j}}\}\) are appointed diverse access authorities for \(LAG\) and \(CA\). Concretely, \(LAG\) can only ascertain \(BV\)'s group identifiers \(\{g\text{id}_{h,i}, g\text{id}_{e,j}\}\) for launching a specific working mode, rather than obtaining the real identities. \(CA\) owns a full-authority on \(\{F_{BV_{h,i}}, F_{BV_{e,j}}\}\), by which it can derive the real identities for billing purposes. Such authority separation mechanism may provide auxiliary support for privacy consideration.

### VII. Performance Analysis

The storage requirement of a \(BV\) includes a real identifier \(ID_{BV}\), a pseudo-identity flag \(F_{BV}\), a group identifier \(g\text{id}\), an in-group key \(k_{h,i}\), an out-group key \(k_{o,j}\), and two access lists of aggregators’ identity flags and pseudonyms \(\{I_{LAG_h}, I_{PDP_{LAG}}\}\). \(LAG\) is assumed to be a hardware-unrestricted entity, which includes a pseudonym \(P\text{ID}_{LAG}\), in-group key set \(\{k_{h,i}\}\), and out-group key set \(\{k_{o,j}\}\). Meanwhile, \(BV\) has additional components: metering device, control and communication module, and the hardware cost is moderate [3], [15].

The computation load mainly consists of the bitwise logical operation (BLO), pseudo-random number generation (PRNG), symmetric key encryption (SKE), keyed hash message authentication code (HMAC), and other defined arithmetic functions (DAF). The computation loads of the home and
visiting modes are presented in Table II. Both modes have comparable computation loads, and the main distinction is on SKE and HMAC operations due to the practical applications. In AP3A, lightweight and flexible encryption algorithms may be recommended. For instance, AES 128-bit keysize encryption [30], needs less than 5 K logic gates for tiny solution, less than 9.5 K logic gates for standard solution, and less than 27 K logic gates for fast solution. HMAC-SHA-256 [31] needs less than 30 K logic gates. Meanwhile, the extension approach on \{sid_{LAG}, r_{LAG}, PST_{V BV}\} is based on the pre-defined Hamming distance, and avoid performing the PRNG operation for each BV to alleviate redundant calculations.

The communication overhead depends on the data packets during the protocol execution. The authentication scheme completes via 4 rounds for the home mode, and 3 rounds for the visiting mode. Thereinto, the pseudo-status storage and recomputing phase does not execute in the visiting mode. Suppose that: 1) the session identifier, identity flag, and pseudo-random number are 16-bit length; 2) the pseudo-status and its variant are 64-bit length; 3) the encrypted SKE and HMAC values are 128-bit length. Thus, the communication overheads of \{BV, LAG\} and \{LAG, V BV\} are estimated as (82 + 26) \times 108 bytes in the home mode, and (80 + 18) \times 98 bytes in the visiting mode, respectively. The communication overhead is lightweight for the current communication environment.

VIII. CONCLUSION

In this paper, we have identified a new security challenge for authenticating different group BVs, and proposed an authentication scheme AP3A with the home and visiting modes in V2G networks. The proposed scheme applies anonymous aggregated-proofs to achieve an aggregator simultaneous authenticating BVs without compromising individual privacy. Besides the accredited privacy preservation, other essential features include mutual authentication, dynamic participation, and session unlinkability. Security analysis and performance analysis indicated that AP3A can perform securely and efficiently for V2G networks.

REFERENCES


Hong Liu (S’10) is currently working toward a Ph.D. degree at the School of Electronic and Information Engineering, Beihang University, China. She focuses on the security and privacy issues in radio frequency identification, vehicle-to-grid, and wireless machine-to-machine networks. Her research interests include authentication protocol design, and security formal modeling and analysis.

Huansheng Ning (M’10) received a B.S. degree from Anhui University, China, in 1996 and the Ph.D. degree from Beihang University, China, in 2001. Now he is an Associate Professor in School of Electronic and Information Engineering, Beihang University. His current research focuses on Internet of Things, aviation security, electromagnetic sensing, and computing. He has published more than 30 papers in journals, international conferences/workshops.

Yan Zhang (M’05-SM’10) received a Ph.D. degree from Nanyang Technological University, Singapore. From August 2006, he has been working with Simula Research Laboratory, Norway. He is currently Senior Research Scientist at Simula Research Laboratory. He is an adjunct Associate Professor at the University of Oslo, Norway. He is a Regional Editor, Associate Editor, on the Editorial Board, or Guest Editor of a number of international journals. He is currently serving the Book Series Editor for the book series on “Wireless Networks and Mobile Communications” (Auerbach Publications, CRC Press, Taylor & Francis Group). He serves as organizing committee chairs for many international conferences. His research interests include resource, mobility, spectrum, energy, data, and security management in wireless communications and networking.

Laurence T. Yang (M’97) received a B.E degree in computer science from Tsinghua University, China, and a Ph.D. degree in computer science from the University of Victoria, Canada. He is a Professor in Computer Science and the Director of the Parallel and Distributed Computing Laboratory, and Embedded and Ubiquitous Computing Laboratory at St. Francis Xavier University, Canada. His research interests include high-performance computing and networking, embedded system, and ubiquitous/pervasive computing and intelligence. His research is supported by the National Sciences and Engineering Research Council, and the Canada Foundation for Innovation.