Aggregated-Proofs Based Privacy-Preserving Authentication for V2G Networks in the Smart Grid

Hong Liu, *Student Member, IEEE*, Huansheng Ning, *Member, IEEE*, Yan Zhang, *Senior Member, IEEE*, and Laurence T. Yang, *Member, IEEE*

***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 great attention in both industry and academia. In V2G networks, communication technologies are needed to provide supporting services by periodically collecting the charging status of a battery vehicle (BV) to realize efficient power scheduling [6]–[8].

Manuscript received December 07, 2011; revised April 21, 2012; accepted July 31, 2012. Date of publication October 22, 2012; date of current version December 28, 2012. This work was jointly funded by National Natural Science Foundation of China (NSFC) and Civil Aviation Administration of China (CAAC) (61079019). Paper no. TSG-00674-2011.

H. Liu and H. Ning are with the School of Electronic and Information 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

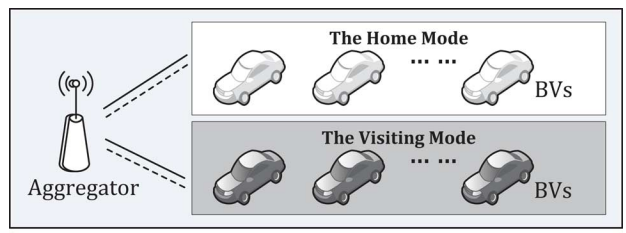


Fig. 1. Two working modes in V2G networks.

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. Thereafter, 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) 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) 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) Dynamic participation:* BVs can dynamically join and leave the networks without influencing ongoing communications. *4) 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) 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 nondistinctive 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 (BVs), 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 charing 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 bill 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 BV_hs, home local aggregator LAG_h, and home virtual battery vehicle VBV_h of the same group, and the home mode is launched by LAG_h; *out-group* entities to include the visiting battery vehicles BV_vs, visiting local aggregator LAG_v, and visiting virtual battery vehicle VBV_v of different groups, and the visiting mode is launched by LAG_v. In Fig. 2, LAG_1 and LAG_2 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 $\{LAG_{1h}, LAG_{1v}\}$ are used for LAG_1 when it provides services for BV_hs and BV_vs, respectively. For instance, a specific battery vehicle BV_a moves from the range of LAG_1 to the range of LAG_2, and it may act as BV_{ha} for LAG_1 in the home mode. When it moves to the range of LAG_2, it may act as BV_{va} for LAG_2 in the visiting mode.

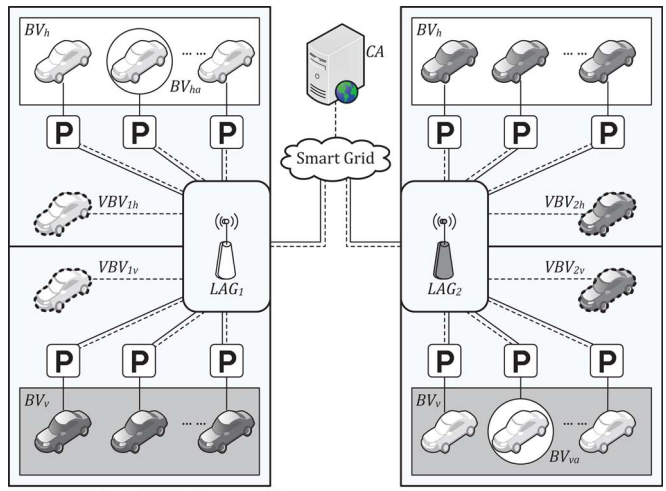


Fig. 2. The home and visiting modes based V2G network architecture.

Towards the introduced VBV, it is embedded into a LAG to provide support to enhance message randomization and to realize distributed nondistinctive identification. Similarly, VBV has the variants $\{VBV_h, VBV_v\}$ 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 $\{VBV_h, VBV_v\}$ 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 BVs 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 BV_{hi} (i.e., $\{BV_{h1}, \ldots, BV_{hI}\}$) simultaneously access LAG_h to perform power services (e.g., charging). LAG_h collects the BVs' power status data with the assistance of VBV_h to provide information services for smart grid, meantime periodically uploads the aggregated data to CA for bill services. Similarly, BV_{vj} (i.e., $\{BV_{v1}, \ldots, BV_{vJ}\}$), LAG_v and VBV_v participate in the visiting mode. $\{BV, LAG\}$ have their own real identifiers $\{ID_{BV}, ID_{LAG}\}$, pseudo-identity flags $\{F_{BV}, F_{LAG}\}$, and group identifiers $\{gid, Gid\}$. Besides, LAG has a pseudonym PID_{LAG}. The in-group key k_{hi} is allocated to $\{BV_{hi}, LAG_h\}$, and the out-group key k_{vj} is allocated to $\{gp_{vj}, GP_v\}$. 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 $z = f_0(x \oplus y)$. $f_0(.)$ is assigned to $\{BV, LAG\}$.
2) $f_1 : \{0,1\}^* \times \mathbb{R}^* \rightarrow \{0,1\}^*$, that satieties $k' = f_1(k, x)$, which as a collision-resistant function is applied for key updating. $f_1(.)$ 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 Δx. $f_2(.)$ is assigned to $\{BV, CA\}$.

TABLE I
Notations

Notation	Description
BV	The battery vehicle [15], including battery electric vehicles, fuel cell vehicles, plug-in hybrid electric vehicles, etc.
LAG	The local aggregator.
CA	The central authority.
BV_{hi}, BV_{vj}	The the i-th home BV, and the j-th visiting BV.
VBV_h, VBV_v	The home/visiting virtual battery vehicle.
LAG_h, LAG_v	The home/visiting local aggregator.
ID, PID	The real identifier, and pseudonym.
sid	The pseudo session identifier.
F	The pseudo identity flag with built-in timestamp.
gp, GP	The group attribution of BV, LAG.
gid, Gid	The pseudo group identifier of gp, GP.
r	The pseudorandom number.
k_{hi}	The in-group key of BV_{hi} and LAG_h.
k_{vj}	The out-group key of gp_{vj} and GP_v.
ST, PST	The real-status, and pseudo-status.
ΔST, ΔPST	The real-status variation, and pseudo-status variation.
$E_k(.)$	The symmetric key encryption by k.
$H_k(.)$	The keyed hash message authentication code (HMAC) function
M^{ℓ}	The locally derived value M.

4) $\{f_3, F\} : \mathbb{R}^* \times \{0,1\}^* \times \{0,1\}^* \rightarrow \{0,1\}^*$, that satiety 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 $\{f_3(.), F(.)\}$ are applied to obtain the aggregated power status data. $f_3(.)$ is assigned to $\{BV, CA\}$, and $F(.)$ is assigned to $\{LAG, CA\}$.

In system initialization, the symmetric keys (e.g., in-group key k_{hi}, and out-group k_{vj}) of $\{LAG_h, BV_{hi}\}$ and $\{LAG_v, BV_{vj}\}$ are distributed according to the Diffie-Hellman (DH) key agreement scheme. We take k_{hi} as an example to introduce the key distribution procedure.

LAG_h generates a random number $\gamma^1_{LAG_h}$, and transmits it to BV_{hi}. Upon receiving the query, BV_{hi} generates random numbers $\{\gamma^1_{BV_{hi}}, \gamma^2_{BV_{hi}}\}$ from $\mathbb{Z}^*_q$, and computes $\{X_{BV_{hi}}, Y_{BV_{hi}}\}$ by its pseudonym, where $\mathbb{Z}^*_q$ is a multiplicative group, p is a large prime, and g is a primitive root of q.

$$X_{BV_{hi}} = g^{\gamma^1_{BV_{hi}}} \pmod p$$
$$Y_{BV_{hi}} = H(\gamma^2_{BV_{hi}} \| PID_{BV_{hi}}) \oplus g^{\gamma^1_{LAG_h}\gamma^2_{BV_{hi}}}$$

BV_{hi} transmits $X_{BV_{hi}} \| Y_{BV_{hi}} \| \gamma^2_{BV_{hi}} \| PID_{BV_{hi}}$ to LAG_h, and LAG_h re-computes $H(\gamma^2_{BV_{hi}} \| PID_{BV_{hi}})$ by the received $\{\gamma^2_{BV_{hi}}, PID_{BV_{hi}}\}$, and derives $g^{\gamma^1_{LAG_h}\gamma^2_{BV_{hi}}}$ by an XOR operation. Thereafter, LAG_h locally computes $(g^{\gamma^2_{BV_{hi}}})^{\gamma^1_{LAG_h}}$, and compares whether the derived $g^{\gamma^1_{LAG_h}\gamma^2_{BV_{hi}}}$ equals the locally computed $(g^{\gamma^2_{BV_{hi}}})^{\gamma^1_{LAG_h}}$. If it holds, LAG_h will generate a random number $\gamma^2_{LAG_h}$, and computes $\{X_{LAG_h}, Y_{LAG_h}\}$

$$X_{LAG_h} = g^{\gamma^1_{LAG_h}} \pmod p$$
$$Y_{LAG_h} = H(\gamma^2_{LAG_h} \| PID_{LAG_h}) \oplus g^{\gamma^2_{BV_{hi}}\gamma^2_{LAG_h}}$$

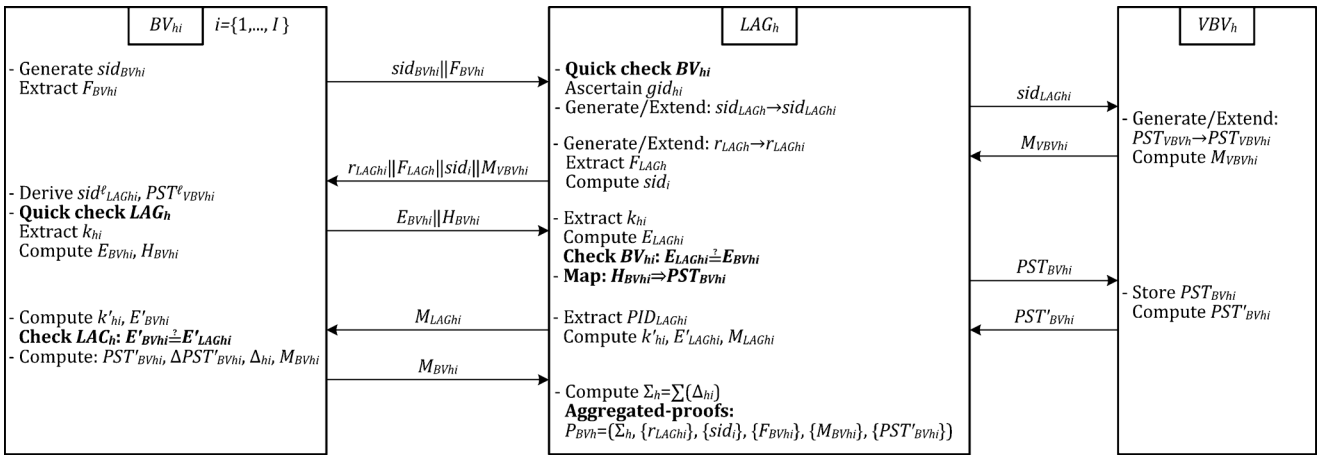


Fig. 3. The home mode of AP3A: The interaction among BV_{hi}, LAG_h and VBV_h.

LAG_h transmits $X_{LAG_h}\|Y_{LAG_h}\|\gamma^2_{LAG_h}\|PID_{LAG_h}$ to BV_{hi}, and BV_{hi} computes $H(\gamma^2_{LAG_h}\|PID_{LAG_h})$ by the received $\{\gamma^2_{LAG_h}, PID_{LAG_h}\}$, and derives $g^{\gamma^2_{BV_{hi}}\gamma^2_{LAG_h}}$ by an XOR operation. BV_{hi} locally computes $(g^{\gamma^2_{BV_{hi}}})^{\gamma^2_{LAG_h}}$, and compares whether the derived $g^{\gamma^2_{BV_{hi}}\gamma^2_{LAG_h}}$ equals the locally computed $(g^{\gamma^2_{BV_{hi}}})^{\gamma^2_{LAG_h}}$. If it holds, BV_{hi} and LAG_h will establish mutual authentication, and obtain k_{hi} as follows.

$$\begin{aligned} k_{hi} &= (X_{BV_{hi}})^{\gamma^1_{LAG_h}} = (X_{LAG_h})^{\gamma^1_{BV_{hi}}} \\ &= g^{\gamma^1_{BV_{hi}}\gamma^1_{LAG_h}} \pmod p. \end{aligned}$$

Similarly, the out-group key k_{vj} 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 $i = \{1, \ldots, I\}$ and $j = \{1, \ldots, J\}$, which are regarded as a whole entity during the following specifications.

A. Authenticating Home BVs

Fig. 3 shows the interaction among BV_{hi}, LAG_h, and VBV_h in the home mode, in which the in-group vehicles $\{BV_{h1}, .., BV_{hI}\}$ 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_{hi} and Activation of VBV_{hi}: BV_{hi} generates a session identifier $sid_{BV_{hi}}$, and extracts the corresponding identity flag $F_{BV_{hi}}$. BV_{hi} transmits the cascaded value $sid_{BV_{hi}}\|F_{BV_{hi}}$ to LAG_h to initiate a new session. Upon receiving the query, LAG_h performs the quick check on BV_{hi} by checking whether the received $sid_{BV_{hi}}$ and $F_{BV_{hi}}$ repeatedly emerge within an unacceptable time interval. The probability that $sid_{BV_{hi}}\|F_{BV_{hi}}$ repeatedly emerge is negligible. If so, LAG_h will refuse the query and eliminate the suspicious BV from the protocol. Otherwise, LAG_h will extract BV_{hi}'s group attribution via $F_{BV_{hi}}$ to ascertain the group identifier gid_{hi}, which makes LAG_h know that BV_{hi} under its jurisdiction, and the home mode is launched. Here, LAG cannot correlate $F_{BV_{hi}}$ with BV_{hi}'s real identifier $ID_{BV_{hi}}$ for privacy consideration.

Thereafter, LAG_h generates a session identifier sid_{LAG_h}, extends sid_{LAG_h} into $sid_{LAG_{hi}}$ for BV_{hi}, and transmits $sid_{LAG_{hi}}$ to VBV_h. The extension approach is based on the Hamming distance $d \in \mathbb{N}^*$. Thereafter, VBV_h generates a pseudo-status PST_{VBV_h}, extends PST_{VBV_h} into a series of pseudo-status values $PST_{VBV_{hi}}$. VBV_h continues to compute $M_{VBV_{hi}}$, and replies $M_{VBV_{hi}}$ to LAG_h.

$$M_{VBV_{hi}} = sid_{LAG_{hi}} \oplus PST_{VBV_{hi}}.$$

2) LAG_h Authenticating BV_{hi} and Real-to-Pseudo Status Mapping: Upon receiving VBV_h's response, LAG_h generates a pseudo-random number r_{LAG_h}, extends r_{LAG_h} into $r_{LAG_{hi}}$ for BV_{hi}, extracts the corresponding identity flag F_{LAG_h}, and computes a combined session identifier sid_i.

$$sid_i = f_0(sid_{BV_{hi}} \oplus sid_{LAG_{hi}})$$

LAG_h transmits $r_{LAG_{hi}}\|F_{LAG_h}\|sid_i\|M_{VBV_{hi}}$ to BV_{hi}, then BV_{hi} locally derives $sid^\ell_{LAG_{hi}}$ and $PST^\ell_{VBV_{hi}}$.

$$\begin{aligned} sid^\ell_{LAG_{hi}} &= f_0^{-1}(sid_i) \oplus sid_{BV_{hi}} \\ PST^\ell_{VBV_{hi}} &= M_{VBV_{hi}} \oplus sid^\ell_{LAG_{hi}} \end{aligned}$$

BV_{hi} 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_{hi} will terminate the protocol. Otherwise, the protocol will continue. BV_{hi} extracts the corresponding in-group key k_{hi}, performs the symmetric key encryption to obtain $E_{BV_{hi}}$, and computes HMAC function to obtain $H_{BV_{hi}}$, in which BV_{hi}'s real-status $ST_{BV_{hi}}$ is wrapped by VBV_h's pseudo-status $PST_{VBV_{hi}}$.

$$\begin{aligned} E_{BV_{hi}} &= E_{k_{hi}}((sid^\ell_{LAG_{hi}} \oplus r_{LAG_{hi}})\|F_{BV_{hi}}) \\ H_{BV_{hi}} &= H_{k_{hi}}(PST^\ell_{VBV_{hi}}\|ST_{BV_{hi}}) \end{aligned}$$

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

$$E_{LAG_{hi}} = E_{k_{hi}}((sid_{LAG_{hi}} \oplus r_{LAG_{hi}})\|F_{BV_{hi}})$$

LAG_h verifies BV_{hi} by checking whether the computed $E_{LAG_{hi}}$ equals the received $E_{BV_{hi}}$. If it does not hold, LAG_h

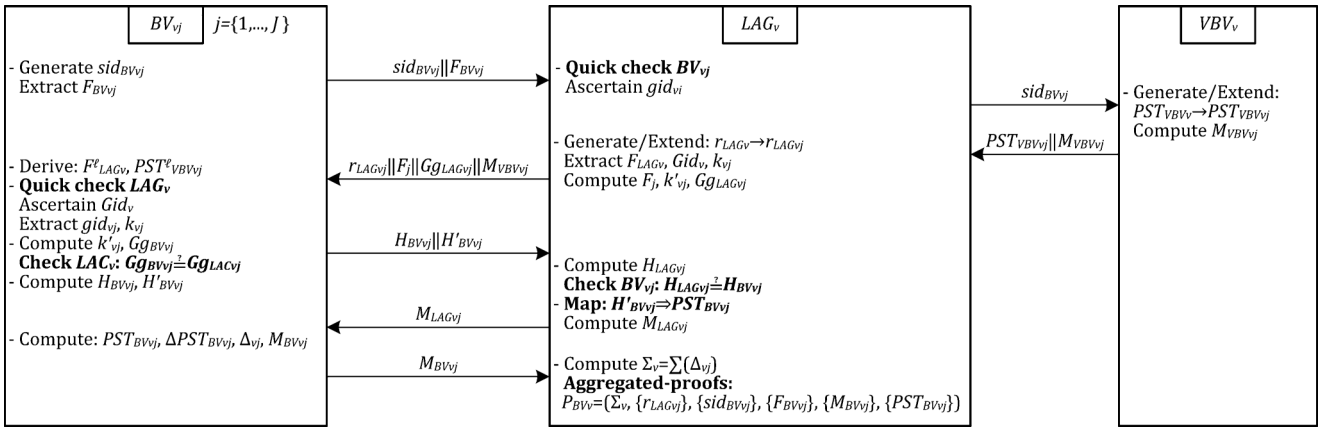


Fig. 4. The visiting mode of AP3A: The interaction among BV_{vj}, LAG_v and VBV_v.

will regard the suspicious BV as an illegal vehicle and eliminate it from the protocol. Otherwise, LAG_h will perform status mapping from $H_{BV_{hi}}$ (including the real-status $ST_{BV_{hi}}$) into the pseudo-status $PST_{BV_{hi}}$ to realize further anonymous data transmission.

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

$$PST'_{BV_{hi}} = PST_{BV_{hi}} \oplus M_{VBV_{hi}}$$

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

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

$$\begin{aligned} k'_{hi} &= f_1(k_{hi}\|(r_{LAG_{hi}} \oplus sid_{BV_{hi}})) \\ E'_{LAG_{hi}} &= E_{k'_{hi}}((M_{VBV_{hi}} \oplus sid_{LAG_{hi}})\|PID_{LAG_{hi}}) \\ M_{LAG_{hi}} &= f_0(M_{VBV_{hi}}\|PST'_{BV_{hi}}) \end{aligned}$$

LAG_h transmits $E'_{LAG_{hi}}\|M_{LAG_{hi}}$ to BV_{hi} for authentication. BV_{hi} obtains the updated k'_{hi}, and computes $E'_{BV_{hi}}$.

$$E'_{BV_{hi}} = E_{k'_{hi}}(PST^{\ell}_{VBV_{hi}}\|PID_{LAG_{hi}})$$

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

$$\begin{aligned} PST'_{BV_{hi}} &= f_0^{-1}(M_{LAG_{hi}}) \oplus M_{VBV_{hi}} \\ \Delta PST'_{BV_{hi}} &= f_2(PST'_{BV_{hi}}) \\ \Delta_{hi} &= \Delta ST_{BV_{hi}} \oplus \Delta PST'_{BV_{hi}} \\ M_{BV_{hi}} &= f_3(sid_i \oplus \Delta_{hi} \oplus PST'_{BV_{hi}}) \end{aligned}$$

BV_{hi} transmits $M_{BV_{hi}}$ to LAG_h for the aggregated-proofs establishment. LAG_h periodically computes the aggregated pseudo-status variation Σ_h. LAG_h obtains the aggregated-proofs P_{BV_h}, and periodically uploads P_{BV_h} to CA.

$$\begin{aligned} \Sigma_h &= \sum_{i=1}^{I}(\Delta_{hi}) \\ &= \sum_{i=1}^{I}(PST'_{BV_{hi}}) \oplus F^{-1}\left(\prod_{i=1}^{I} M_{BV_{hi}}\right) \\ &\quad \oplus \sum_{i=1}^{I}(sid_i) \\ P_{BV_h} &= (\Sigma_h, \{r_{LAG_{hi}}\}, \{sid_i\}, \{F_{BV_{hi}}\}, \{M_{BV_{hi}}\}, \\ &\quad \{PST'_{BV_{hi}}\}). \end{aligned}$$

Thereinto, the denotations $\{r_{LAG_{hi}}\}$, $\{sid_i\}$, and $\{X_{BV_{hi}}\}$ $(X \in \{F, M, PST'\})$ represent $\{BV_{h1}, \ldots, BV_{hI}\}$'s corresponding values, and the relation of $\{f_3(.), F(.)\}$ is applied to obtain Σ_h that is provided for power scheduling. Afterwards, CA derives the real-status variation $\Delta ST_{BV_{hi}}$ for billing purposes.

$$\begin{aligned} \Delta ST_{BV_{hi}} &= f_2(PST'_{BV_{hi}}) \oplus (PST'_{BV_{hi}} \oplus f_3^{-1}(M_{BV_{hi}}) \\ &\quad \oplus sid_i). \end{aligned}$$

B. Authenticating Visiting BVs

Fig. 4 shows the interaction among BV_{vj}, LAG_v, and VBV_v in the visiting mode, in which the out-group vehicles $\{BV_{v1}, \ldots, BV_{vJ}\}$ are not under LAG_v's default jurisdiction, and the out-group LAG_v 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_{vj} and Activation of VBV_v: BV_{vj} generates a session identifier $sid_{BV_{vj}}$, extracts the corresponding identity flag $F_{BV_{vj}}$, and transmits $sid_{BV_{vj}}\|F_{BV_{vj}}$ to LAG_v. Upon receiving the query, LAG_v performs the quick check on BV_{vj} by checking whether the received $sid_{BV_{vj}}$ and $F_{BV_{vj}}$ repeatedly emerge within an unacceptable time interval. If so, LAG_v will refuse the query and eliminate the

suspicious BV from the protocol. Otherwise, LAG_v will ascertain BV_{vj}'s group attribution via $F_{BV_{vj}}$ and obtain the group identifiers gid_{vj}. Thereby, LAG_v knows that BV_{vj} belongs to the out-group vehicles, and the visiting mode is launched. LAG_v forwards $sid_{BV_{vj}}$ to VBV_v. Upon receiving the message, VBV_v generates a pseudo-status PST_{VBV_v}, extends PST_{VBV_v} into a series of pseudo-status values $PST_{VBV_{vj}}$, and computes $M_{VBV_{vj}}$.

$$M_{VBV_{vj}} = sid_{BV_{vj}} \oplus PST_{VBV_{vj}}.$$

2) Mutual Authentication Between BV_{vj} and lag_v: When LAG_v receives $PST_{VBV_{vj}} \| M_{VBV_{vj}}$, it generates a pseudo-random number r_{LAG_v}, extends r_{LAG_v} into $r_{LAG_{vj}}$ for BV_{vj}. Thereafter, LAG_v extracts $\{F_{LAG_v}, Gid_v, k_{vj}\}$ to compute F_j, k'_{vj}, and $Gg_{LAG_{vj}}$.

$$\begin{aligned} F_j &= f_0(F_{BV_{vj}} \oplus F_{LAG_v}) \\ k'_{vj} &= f_1(k_{vj} \| r_{LAG_{vj}}) \\ Gg_{LAG_{vj}} &= H_{k'_{vj}}((Gid_v \oplus gid_{vj}) \| PST_{VBV_{vj}}) \end{aligned}$$

LAG_v transmits $r_{LAG_{vj}} \| F_j \| Gg_{LAG_{vj}} \| M_{VBV_{vj}}$ to BV_{vj}, and BV_{vj} locally derives $F^{\ell}_{LAG_v}$ and $PST^{\ell}_{VBV_{vj}}$.

$$\begin{aligned} F^{\ell}_{LAG_v} &= f_0^{-1}(F_j) \oplus sid_{BV_{vj}} \\ PST^{\ell}_{VBV_{vj}} &= M_{VBV_{vj}} \oplus sid_{BV_{vj}} \end{aligned}$$

BV_{vj} performs the quick check by the derived $F^{\ell}_{LAG_v}$, and further ascertains LAG_v's group attribution to obtain the group identifier Gid_v. Thereafter, BV_{vj} extracts $\{gid_{vj}, k_{vj}\}$, updates k'_{vj}, and computes $Gg_{BV_{vj}}$.

$$\begin{aligned} k'_{vj} &= f_1(k_{vj} \| r_{LAG_{vj}}) \\ Gg_{BV_{vj}} &= H_{k'_{vj}}((Gid_v \oplus gid_{vj}) \| PST^{\ell}_{VBV_{vj}}) \end{aligned}$$

BV_{vj} verifies LAG_v by checking whether the computed $Gg_{BV_{vj}}$ equals the received $Gg_{LAG_{vj}}$. If it does not hold, BV_{vj} will regard LAG_v as an illegal aggregator, and terminate the protocol. Otherwise, BV_{vj} will compute $H_{BV_{vj}}$ and $H'_{BV_{vj}}$ then transmits $H_{BV_{vj}} \| H'_{BV_{vj}}$ to LAG_v.

$$\begin{aligned} H_{BV_{vj}} &= H_{Gg_{BV_{vj}}}(r_{LAG_{vj}} \| (F_j \oplus sid_{BV_{vj}})) \\ H'_{BV_{vj}} &= H_{Gg_{BV_{vj}}}(PST^{\ell}_{VBV_{vj}} \| ST_{BV_{vj}}) \end{aligned}$$

Upon receiving the message, LAG_v computes $H_{LAG_{vj}}$, and verifies BV_{vj} by checking whether the computed $H_{LAG_{vj}}$ equals the received $H_{BV_{vj}}$. 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.

$$H_{LAG_{vj}} = H_{Gg_{LAG_{vj}}}(r_{LAG_{vj}} \| (F_j \oplus sid_{BV_{vj}})).$$

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

$$M_{LAG_{vj}} = f_0(M_{VBV_{vj}} \oplus PST_{BV_{vj}})$$

In the case if BV_{vj} has been fully charged or wants to quit the charging operation, BV_{vj} will compute $PST_{BV_{vj}}$, $\Delta PST'_{BV_{vj}}$, Δ_{vj}, and $M_{BV_{vj}}$.

$$\begin{aligned} PST_{BV_{vj}} &= f_0^{-1}(M_{LAG_{vj}}) \oplus M_{VBV_{vj}} \\ \Delta PST_{BV_{vj}} &= f_2(PST_{BV_{vj}}) \\ \Delta_{vj} &= \Delta ST_{BV_{vj}} \oplus \Delta PST_{BV_{vj}} \\ M_{BV_{vj}} &= f_3(sid_{BV_{vj}} \oplus \Delta_{vj} \oplus PST_{BV_{vj}}) \end{aligned}$$

BV_{vj} transmits $M_{BV_{vj}}$ to LAG_v for the aggregated-proofs establishment, and LAG_v periodically computes the aggregated pseudo-status variation Σ_v to establish the aggregated-proofs P_{BV_v}, and then periodically uploads P_{BV_v} to CA.

$$\begin{aligned} \Sigma_v &= \sum_{j=1}^{J}(\Delta_{vj}) \\ &= \sum_{j=1}^{J}(PST_{BV_{vj}}) \oplus F^{-1}\left(\prod_{j=1}^{J} M_{BV_{vj}}\right) \\ &\quad \oplus \sum_{j=1}^{J}(sid_{BV_{vj}}) \\ P_{BV_v} &= \big(\Sigma_v, \{r_{LAG_{vj}}\}, \{sid_{BV_{vj}}\}, \{F_{BV_{vj}}\}, \\ &\quad \{M_{BV_{vj}}\}, \{PST_{BV_{vj}}\}\big). \end{aligned}$$

Thereinto, the denotations $\{r_{LAG_{vj}}\}$ and $\{X_{BV_{vj}}\}$ $(X \in \{sid, F, M, PST\})$ represent $\{BV_{1J}, \ldots, BV_{vJ}\}$'s corresponding values. CA further ascertains BV_{vj}'s specific identity by $F_{BV_{vj}}$, and derives the real-status variation $\Delta ST_{BV_{vj}}$ for billing purposes.

$$\begin{aligned} \Delta ST_{BV_{vj}} =& f_2(PST_{BV_{vj}}) \oplus (PST_{BV_{vj}} \oplus f_3^{-1}(M_{BV_{vj}}) \\ & \oplus sid_{BV_{vj}}). \end{aligned}$$

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, VBV_h performs pseudo-status storage and recomputing to conduce to later data inquiry. VBV_h stores the pseudo-status $PST_{BV_{hi}}$, and re-computes $PST'_{BV_{hi}} = PST_{BV_{hi}} \oplus M_{VBV_{hi}}$ to realize pseudo-status inquiry within an allowable time interval. Hence, the home mode allows VBV_h to store $PST_{BV_{hi}}$ for VBV_h's future retracing. The visiting mode serves for out-group entities to only provide the basic power services without allowing VBV_v to store 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_{hi} performs the symmetric key encryption on $\{sid^{\ell}_{LAG_{hi}}, r_{LAG_{hi}}, F_{BV_{hi}}\}$ with the in-group key k_{hi} to obtain $E_{BV_{hi}}$, and on $\{PST^{\ell}_{VBV_{hi}}, PID_{LAG_{hi}}\}$ with the updated key k'_{hi} to obtain $E'_{BV_{hi}}$. The authentication operators are computed via symmetric key encryption. While BV_{vj} applies HMAC function on $\{Gid_v, gid_{vj}, PST_{VBV_{vj}}\}$ with the updated out-group key k'_{vj}, and on $\{r_{LAG_{vj}}, F_j, sid_{BV_{vj}}\}$ with the group identifier-based key $Gg_{BV_{vj}}$. It realizes that $\{BV_{hi}, LAG_h\}$ verify each other based on the reversible encryption algorithm, and $\{BV_{vj}, LAG_v\}$ 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_{hi} belong to the in-group entities by the identity flag $F_{BV_{hi}}$, 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_{vj} and LAG_v need extract each other's group identifiers $\{Gid_v, gid_{vj}\}$ as the authentication operators, and ascertain the corresponding out-group keys k_{vj}. $\{LAG_h, LAG_v\}$ can only know that the corresponding in-group BV_{hi} or out-group BV_{vj} has accessed the networks, rather than acquaint $\{BV_{hi}, BV_{vj}\}$'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_{hi} in the home mode while BV_{vj} first verifies LAG_v in the visiting mode. For BV_{hi}, it knows that the accessed aggregator LAG_h is its home aggregator, thereby LAG_h has a strong demand to verify the unknown BV_{hi}. For BV_{vj}, 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_{vj} to first perform verification on LAG_v.

5) Entity Session Control: In the home mode, BV_{hi} 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, $\{BV_{hi}, LAG_h\}$ generate session identifiers $\{sid_{BV_{hi}}, sid_{LAG_h}\}$, and LAG_h extends sid_{LAG_h} into $sid_{LAG_{hi}}$. The re-computed session identifiers $sid_i = f_0(sid_{BV_{hi}} \oplus sid_{LAG_{hi}})$ are obtained to guarantee session freshness. Comparatively, in the visiting mode, only BV_{vj} owns the initiative to generate and control session identifier $sid_{BV_{vj}}$. 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 as a legal entity to obtain the access authority. For instance, an imitated vehicle $\widehat{BV}_{\alpha}$ impersonates as an in-group vehicle $\widehat{BV}_{h\alpha}$ (or an out-group vehicle $\widehat{BV}_{v\alpha}$) to access LAG_h (or LAG_v). If the aggregator cannot discern the suspicious vehicle, $\widehat{BV}_{\alpha}$ may perform power stealing or cheating. For another unfrequent instance, an imitated local aggregator serves as $\widehat{LAG}_h$ (or $\widehat{LAG}_v$) to collect BVs' power status. If the BVs cannot recognize the suspicious aggregator, the sensitive data may be abused with malicious intentions.

1) BV Impersonation Attack: Suppose that $\widehat{BV}_{\alpha}$ disguises as BV_{τ} to cheat LAG with the imitative messages.

In the home mode, $\widehat{BV}_{h\alpha}$ impersonates $BV_{h\tau}$ to transmit a forged query $\widehat{sid}_{\widehat{BV}_{h\alpha}} \| \hat{F}_{BV_{h\tau}}$ to LAG_h. Suppose that $\widehat{BV}_{h\alpha}$ can pass the quick check, and LAG_h considers that the query is from $BV_{h\tau}$. LAG_h generates and transmits $sid_{LAG_{h\tau}}$ to VBV_h, and VBV_h replies $M_{VBV_{h\tau}}$ to LAG_h. Subsequently, LAG_h obtains $\{r_{LAG_{h\tau}}, F_{LAG_h}, \widehat{sid}_{\tau}\}$, and transmits $r_{LAG_{h\tau}} \| F_{LAG_h} \| \widehat{sid}_{\tau} \| M_{VBV_{h\tau}}$ to $\widehat{BV}_{h\alpha}$. Afterwards, $\widehat{BV}_{h\alpha}$ skips the quick check, and locally computes $\hat{E}_{\widehat{BV}_{h\alpha}}$. Thereinto, $\widehat{BV}_{h\alpha}$ cannot obtain $BV_{h\tau}$'s in-group key $k_{h\tau}$. Upon receiving $\hat{E}_{\widehat{BV}_{h\alpha}} \| \hat{H}_{\widehat{BV}_{h\alpha}}$ from $\widehat{BV}_{h\alpha}$, LAG_h extracts $k_{h\tau}$, and compute $E_{LAG_{h\tau}}$ to verify $\widehat{BV}_{h\alpha}$. It turns out that LAG_h regards $\widehat{BV}_{h\alpha}$ as an illegal home vehicle according to $E_{LAG_{h\tau}} \neq \hat{E}_{\widehat{BV}_{h\alpha}}$, in which $k_{h\tau} \neq \hat{k}_{h\alpha}$.

In the visiting mode, $\widehat{BV}_{v\alpha}$ impersonates $BV_{v\tau}$ to transmit a forged query $\widehat{sid}_{\widehat{BV}_{v\alpha}} \| \hat{F}_{BV_{v\tau}}$ to LAG_v. Suppose that $\hat{F}_{BV_{v\tau}}$ has an acceptable timestamp, and $\widehat{BV}_{v\alpha}$ could pass the quick check. Thereafter, LAG_v considers that the query is from $BV_{v\tau}$ by the received $\hat{F}_{BV_{v\tau}}$, and forwards $\widehat{sid}_{\widehat{BV}_{v\alpha}}$ to VBV_v. Upon receiving the message, VBV_v computes the corresponding $PST_{VBV_{v\tau}}$ and $\hat{M}_{VBV_{v\tau}}$, and transmits $PST_{VBV_{v\tau}} \| \hat{M}_{VBV_{v\tau}}$ to LAG_v. Then, LAG_v obtains $\{r_{LAG_{v\tau}}, F_{LAG_v}, Gid_v, k_{v\tau}\}$, and computes $Gg_{LAG_{v\tau}}$. LAG_v transmits $r_{LAG_{v\tau}} \| \hat{F}_j \| \widehat{Gg}_{LAG_{v\tau}} \| \hat{M}_{VBV_{v\tau}}$ to $\widehat{BV}_{v\alpha}$, and $\widehat{BV}_{v\alpha}$ can locally compute $\widehat{Gg}_{\widehat{BV}_{v\alpha}}$. Skipping the quick check and authentication on $LAG_{v\tau}$, $\widehat{BV}_{v\alpha}$ computes and transmits $\hat{H}_{\widehat{BV}_{v\alpha}} \| \hat{H}'_{\widehat{BV}_{v\alpha}}$ to LAG_v. Thereafter, LAG_v locally computes $H_{LAG_{v\tau}}$ to verify $\widehat{BV}_{v\alpha}$. It turns out that LAG_v regards $\widehat{BV}_{v\alpha}$ as an illegal visiting vehicle according to $H_{LAG_{v\tau}} \neq \hat{H}_{\widehat{BV}_{v\alpha}}$ and the inconsistencies of $\{Gg_{LAG_{v\tau}}, \widehat{Gg}_{\widehat{BV}_{v\alpha}}\}$, in which $k_{v\tau} \neq \hat{k}_{v\alpha}$ and $gid_{v\tau} \neq \widehat{gid}_{v\alpha}$.

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

In the home mode, $\widehat{LAG}$ impersonates a home aggregator $\widehat{LAG}_h$ to receive $BV_{h\tau}$'s query $sid_{BV_{h\tau}} \| F_{BV_{h\tau}}$. Thereafter, $\widehat{LAG}_h$ skips the quick check to generate and transmit $\widehat{sid}_{\widehat{LAG}_{h\tau}}$ to $\widehat{VBV}_h$. After a series of operations, $BV_{h\tau}$ receives $\hat{r}_{\widehat{LAG}_{h\tau}} \| \hat{F}_{\widehat{LAG}_h} \| \widehat{sid}_{\tau} \| \hat{M}_{\widehat{VBV}_{h\tau}}$, and performs the quick check on $\widehat{LAG}_h$. $BV_{h\tau}$ transmits $\hat{E}_{BV_{h\tau}} \| \hat{H}_{BV_{h\tau}}$ to $\widehat{LAG}_h$. Thereafter, $\widehat{LAG}_h$ directly transmits the mapped pseudo-status $\widehat{PST}_{BV_{h\tau}}$ to $\widehat{VBV}_h$. $\widehat{VBV}_h$ replies $\widehat{PST}'_{BV_{h\tau}}$ to $\widehat{LAG}_h$,

and $\widehat{LAG}_h$ further computes $\hat{E}'_{\widehat{LAG}_{h\tau}}$. Upon receiving $\hat{E}'_{\widehat{LAG}_{h\tau}}\|\hat{M}_{\widehat{LAG}_{h\tau}}$, $BV_{h\tau}$ computes $E'_{BV_{h\tau}}$ to verify $\widehat{LAG}_h$, in which $\widehat{PST}^{\ell}_{VBV_{h\tau}} = \hat{M}_{\widehat{VBV}_{h\tau}} \oplus (f_0^{-1}(\widehat{sid}_\tau) \oplus sid_{BV_{h\tau}})$. It turns out that $BV_{h\tau}$ regards $\widehat{LAG}_h$ as an illegal home aggregator according to $\hat{E}'_{BV_{h\tau}} \neq \hat{E}'_{\widehat{LAG}_{h\tau}}$, in which $k_{h\tau} \neq \hat{k}_{h\alpha}$ and $PID_{LAG_{h\tau}} \neq \widehat{PID}_{\widehat{LAG}_{h\alpha}}$.

In the visiting mode, $\widehat{LAG}$ impersonates a visiting aggregator $\widehat{LAG}_v$ to receive $sid_{BV_{v\tau}}\|F_{BV_{v\tau}}$. After passing the quick check, $\widehat{LAG}_v$ forwards $sid_{BV_{v\tau}}$ to $\widehat{VBV}_v$, thereafter $\widehat{VBV}_v$ replies $\widehat{PST}_{\widehat{VBV}_{v\tau}}\|\hat{M}_{\widehat{VBV}_{v\tau}}$. $\widehat{LAG}_v$ further computes $\widehat{Gg}_{\widehat{LAG}_{v\tau}}$ to transmit $\hat{r}_{\widehat{LAG}_{v\tau}}\|\hat{F}_j\|\widehat{Gg}_{\widehat{LAG}_{v\tau}}\|\hat{M}_{\widehat{VBV}_{v\tau}}$ to $BV_{v\tau}$. $BV_{v\tau}$ extracts $\{gid_{v\tau}, k_{v\tau}\}$, computes $\widehat{Gg}_{BV_{v\tau}}$ to verify $\widehat{LAG}_v$. It turns out that $BV_{v\tau}$ regards $\widehat{LAG}_v$ as an illegal visiting aggregator according to $\widehat{Gg}_{BV_{v\tau}} \neq \widehat{Gg}_{\widehat{LAG}_{v\tau}}$, in which $k_{h\tau} \neq \hat{k}_{h\alpha}$, $Gid_v \neq \widehat{Gid}_v$, and $gid_{v\tau} \neq \widehat{gid}_{v\alpha}$.

B. Replay Attack

Replay attack means that an attacker eavesdrops a legal entity'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 $\widehat{BV}$ replays BV's query to challenge LAG, or an illegal aggregator $\widehat{LAG}$ replays LAG's response to reply BV's query.

1) BV Replay Attack: Suppose that an attacker $\widehat{BV}_\alpha$ replays BV_τ's outdated query to involve into the communication.

In the home mode, $\widehat{BV}_{h\alpha}$ intercepts $BV_{h\tau}$'s former messages to replay the outdated query $sid^{old}_{BV_{h\tau}}\|F^{old}_{BV_{h\tau}}$ to LAG_h. Upon receiving the query, LAG_h performs the quick check on $\widehat{BV}_{h\alpha}$. It turns out that $\{sid^{old}_{BV_{h\tau}}, F^{old}_{BV_{h\tau}}\}$ have repeatedly emerged, and $F^{old}_{BV_{h\tau}}$ has a wrong timestamp, thereby LAG_h may refuse $\widehat{BV}_{h\alpha}$'s query. In a worse condition, the protocol may continue, and LAG_h generates a new $sid^{new}_{LAG_{h\tau}}$. Thereafter, $\{LAG_h, VBV_h\}$ perform the corresponding operations to transmit $r^{new}_{LAG_{h\tau}}\|F^{new}_{LAG_h}\|sid^{new}_\tau\|M^{new}_{VBV_{h\tau}}$ to $\widehat{BV}_{h\alpha}$. Upon receiving the message, $\widehat{BV}_{h\alpha}$ skips the quick check and directly responds with the formerly intercepted $E^{old}_{BV_{h\tau}}\|H^{old}_{BV_{h\tau}}$. Upon receiving the message, LAG_h extracts $k_{h\tau}$ to compute $E^{new}_{LAG_{h\tau}}$, and verifies $\widehat{BV}_{h\alpha}$ by checking whether $E^{new}_{LAG_{h\tau}}$ equals $E^{old}_{BV_{h\tau}}$. It turns out that LAG_h regards $\widehat{BV}_{h\alpha}$ as an illegal home vehicle according to $E^{new}_{LAG_{h\tau}} \neq E^{old}_{BV_{h\tau}}$, in which $sid^{new}_{LAG_{h\tau}} \neq sid^{\ell old}_{LAG_{h\tau}}$, and $r^{new}_{LAG_{h\tau}} \neq r^{old}_{LAG_{h\tau}}$.

In the visiting mode, $\widehat{BV}_{v\alpha}$ transmits an outdated query $sid^{old}_{BV_{v\tau}}\|F^{old}_{BV_{v\tau}}$ to challenge LAG_v. LAG_v identifies that $\{sid^{old}_{BV_{v\tau}}, F^{old}_{BV_{v\tau}}\}$ are abnormal and eliminates $\widehat{BV}_{v\alpha}$ from the protocol. In a worse condition, LAG_v may ignore the mistake, and $\{LAG_v, VBV_v\}$ proceed with the operations to obtain $Gg^{new}_{LAG_{v\tau}}$. Then, LAG_v transmits $r^{new}_{LAG_{v\tau}}\|F^{new}_\tau\|Gg^{new}_{LAG_{v\tau}}\|M^{new}_{VBV_{v\tau}}$ to $\widehat{BV}_{v\alpha}$, and $\widehat{BV}_{v\alpha}$ replies the intercepted $H^{old}_{BV_{v\tau}}\|H'^{old}_{BV_{v\tau}}$ to LAG_v. Afterwards, LAG_v computes the updated $H^{new}_{LAG_{v\tau}}$ to verify $\widehat{BV}_{v\alpha}$. It turns out that LAG_v regards $\widehat{BV}_{v\alpha}$ as an illegal visiting vehicle according to $H^{new}_{LAG_{v\tau}} \neq H^{old}_{BV_{v\tau}}$, in which $Gg^{new}_{LAG_{v\tau}} \neq Gg^{old}_{BV_{v\tau}}$, $r^{new}_{LAG_{v\tau}} \neq r^{old}_{LAG_{v\tau}}$, and $F^{new}_\tau \neq F^{old}_\tau$.

2) LAG Replay Attack: Suppose that an attacker $\widehat{LAG}$ replays the intercepted messages to collect BVs' power status.

In the home mode, $\widehat{LAG}_h$ intercepts LAG_h's former messages. When $\widehat{LAG}_h$ receives $BV_{h\tau}$'s query $sid^{new}_{BV_{h\tau}}\|F^{new}_{BV_{h\tau}}$ in another session, $\widehat{LAG}_h$ directly replies the formerly intercepted $r^{old}_{\widehat{LAG}_{h\tau}}\|F^{old}_{LAG_h}\|sid^{old}_\tau\|M^{old}_{VBV_{h\tau}}$ to $BV_{h\tau}$. Upon receiving the outdated message, $BV_{h\tau}$ derives the distorted $sid^{\ell new}_{LAG_{h\tau}}$ by the inconsistent sid^{old}_τ. According to the quick check on $\widehat{LAG}_h$, it turns out that $F^{old}_{LAG_h}$ has a wrong timestamp that is beyond the acceptable time interval so that $BV_{h\tau}$ refuses $\widehat{LAG}_h$. In a worse condition, $BV_{h\tau}$ may ignore the mistake, and transmit $E^{new}_{BV_{h\tau}}\|H^{new}_{BV_{h\tau}}$ to $\widehat{LAG}_h$. $\widehat{LAG}_h$ replies $E'^{old}_{LAG_{h\tau}}\|M^{old}_{LAG_{h\tau}}$ without authenticating $BV_{h\tau}$. $BV_{h\tau}$ computes $E'^{new}_{BV_{h\tau}}$ to verify $\widehat{LAG}_h$, in which $PST^{\ell new}_{VBV_{h\tau}} \neq M^{old}_{VBV_{h\tau}} \oplus sid^{old}_{LAG_{h\tau}}$. It turns out that $BV_{h\tau}$ regards $\widehat{LAG}_h$ as an illegal aggregator according to $E'^{new}_{BV_{hi}} \neq E'^{old}_{LAG_{h\tau}}$ and the inconsistencies of $\{k'^{new}_{h\tau}, k'^{old}_{h\tau}\}$ and $\{PID^{new}_{LAG_{h\tau}}, PID^{old}_{LAG_{h\tau}}\}$, in which $sid^{new}_{BV_{h\tau}} \neq sid^{old}_{BV_{h\tau}}$.

In the visiting mode, $\widehat{LAG}_v$ intercepts and replays LAG_v's former messages. Upon receiving $BV_{v\tau}$'s query $sid^{new}_{BV_{v\tau}}\|F^{new}_{BV_{v\tau}}$ in another session, $\widehat{LAG}_v$ replies the outdated $r^{old}_{LAG_{v\tau}}\|F^{old}_\tau\|Gg^{old}_{LAG_{v\tau}}\|M^{old}_{VBV_{v\tau}}$. Thereafter, $BV_{v\tau}$ performs the quick check on $\widehat{LAG}_v$ by the distorted $F^{\ell new}_{LAG_v} = f_0^{-1}(F^{old}_\tau) \oplus F^{new}_{BV_{v\tau}}$. The identity flag has wrong timestamp so that $BV_{v\tau}$ refuses $\widehat{LAG}_v$. If $BV_{v\tau}$ ignores the mistake, it will compute $Gg^{new}_{BV_{v\tau}}$ to verify LAG_v. Here, $k'^{old}_{v\tau} = k'^{new}_{v\tau} = f_1(k_{v\tau}\|r^{old}_{LAG_{v\tau}})$. It turns out that $BV_{v\tau}$ regards $\widehat{LAG}_v$ as an illegal visiting aggregator according to $Gg^{new}_{BV_{v\tau}} \neq Gg^{old}_{LAG_{v\tau}}$ and the inconsistencies of $\{PST^{\ell new}_{VBV_{v\tau}}, PST^{old}_{VBV_{v\tau}}\}$, in which $sid^{new}_{BV_{v\tau}} \neq sid^{old}_{BV_{v\tau}}$.

C. Denial of Service Attack

DoS attack may be caused by flooding data streams or jamming 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 $\mathcal{A}$ may disguise as $\widehat{BV}_{h\alpha}$ to consecutively challenge a legal LAG_h. Upon receiving the queries, LAG_h performs the quick check on $\widehat{BV}_{h\alpha}$ by verifying whether the received $\widehat{sid}_{\widehat{BV}_{h\alpha}}$ and $\hat{F}_{\widehat{BV}_{h\alpha}}$ repeatedly emerge within an unacceptable time interval. $\widehat{LAG}_h$ can discern the illegal $\widehat{BV}_{h\alpha}$ according to the one-time-valid session identifier $\widehat{sid}_{\widehat{BV}_{h\alpha}}$ and the incorrect timestamp in the identity flag $\hat{F}_{\widehat{BV}_{h\alpha}}$, and will eliminate it from the protocol without influencing other ongoing authentications. Thus, $\mathcal{A}$ cannot involve into the sessions to disturb the normal communication.

VI. Security Analysis

We perform security analysis that focuses on the security requirements for V2G networks, and present the main features.

A. Data Confidentiality and Data Integrity

Data confidentiality and data integrity are achieved by the anonymous aggregated-proofs. Towards the aggregated-proofs

$\{P_{BV_h}, P_{BV_v}\}$, six parameters are included: $\{\Sigma_h, \Sigma_v\}$ are the aggregated pseudo-status variations to provide information for power scheduling, the pseudo-random numbers $\{r_{LAG_{hi}}, r_{LAG_{vj}}\}$ and the session identifiers $\{sid_i, sid_{BV_{hi}}\}$ are used to guarantee data randomization and session freshness, the identity flags $\{F_{BV_{hi}}, F_{BV_{vj}}\}$ are used to determine BVs' group attributes, $\{M_{BV_{hi}}, M_{BV_{vj}}\}$ and $\{PST'_{BV_{hi}}, PST_{BV_{vj}}\}$ are used to derive the detailed real-status for bill purposes. Meanwhile, $\{BV_{hi}, BV_{vj}\}$ apply HMAC functions on the current real-status $\{ST_{BV_{hi}}, ST_{BV_{vj}}\}$ to obtain $\{H_{BV_{hi}}, H'_{BV_{vj}}\}$, in which $\{ST_{BV_{hi}}, ST_{BV_{vj}}\}$ have been wrapped with $\{PST_{VBV_{hi}}, PST_{VBV_{vj}}\}$. Upon receiving the messages, $\{LAG_h, LAG_v\}$ map their respective real-status-inbuilt values $\{H_{BV_{hi}}, H'_{BV_{vj}}\}$ into the pseudo-status $\{PST_{BV_{hi}}, PST_{BV_{vj}}\}$ 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 BVs, and eliminates any suspicious BVs 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, BVs and LAG first perform the quick check based on the received session identifiers and identity flags. Thereafter, BVs and LAG verify each other by SKE or HMAC algorithms. During the execution of the cryptographic algorithms, the in-group key k_{hi} is assigned to BV_{hi} and LAG_h, and the out-group key k_{vj} is assigned to gp_{vj} and GP_v. If and only if both mutual authentications succeed, BVs will transmit the pseudo-status to LAG for the final aggregated-proofs establishment.

C. Dynamic Participation

Suppose that $\{BV_{hi}, BV_{vj}\}$ have established communication with $\{LAG_h, LAG_v\}$. During the ongoing communications, newly joined in-group BV_{hn} (or out-group BV_{vn}) for $n = \{1, \ldots, N\}$, transmits $sid_{BV_{hn}} \| F_{BV_{hn}}$ (or $sid_{BV_{vn}} \| F_{BV_{vn}}$) to challenge LAG_h (or LAG_v). Upon receiving the new queries, the interactions of $BV_{hn,vn}$ and $LAG_{h,v}$ are performed in the corresponding home or visiting mode without interfering with the existing operations of $\{BV_{hi}, LAG_h\}$ (or $\{BV_{vj}, LAG_v\}$). When some BVs have fully charged or want to quit the charging operations, BV_{hi} (or BV_{vj}) immediately transmits $M_{BV_{hi}}$ (or $M_{BV_{vj}}$), and LAG_h (or LAG_v) periodically uploads the current aggregated pseudo-status along with other parameters to CA. Furthermore, even if only one BV (e.g., BV_{hm}) communicates with an aggregator LAG_h, the aggregated pseudo-status $\Sigma_h = \Delta_{hm} = PST'_{BV_{hm}} \oplus F^{-1}(M_{BV_{hm}}) \oplus sid_m$ cannot reveal BV_{hm}'s real-status. LAG_h knows nothing about the function $f_2(.)$, so that it cannot compute $\Delta PST'_{BV_{hm}}$ to derive the real-status variation $\Delta ST_{BV_{hm}}$.

D. Forward and Backward Unlinkability

Towards $\{BV_{hi}, LAG_h\}$, the session identifiers $\{sid_{BV_{hi}}, sid_{LAG_{hi}}\}$ are XORed as the combined session identifier sid_i, and the timestamp in the identity flags $\{F_{BV_{hi}}, F_{LAG_h}\}$ are dynamic to ensure the identity randomization. Towards $\{BV_{vj}, LAG_v\}$, the session identifier $sid_{BV_{hi}}$ and the combined identity flag F_j jointly guarantee the session freshness. Meanwhile, the home and visiting modes also introduce the extended pseudo-random numbers $\{r_{LAG_{hi}}, r_{LAG_{vj}}\}$ and pseudo-status $\{PST_{VBV_{hi}}, PST_{VBV_{vj}}\}$ 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 BVs 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, $\{LAG_h, LAG_v\}$ may attempt to correlate $\{BV_{h\tau_1}, BV_{v\tau_2}\}$'s specific identifiers with the detailed power status. In AP3A, privacy preservation is addressed by introducing anonymous aggregated-proofs, which realizes that multiple BVs' pseudo-status values are uploaded in a whole group without revealing any individual privacy. $\{LAG_h, LAG_v\}$ derive the aggregated pseudo-status variations in the form of $\{\Sigma_h, \Sigma_v\}$, and upload the aggregated-proofs $\{P_{BV_h}, P_{BV_v}\}$ to CA for power scheduling. $\{LAG_h, LAG_v\}$ can obtain the aggregated pseudo-status variation of multiple BVs 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 $\{F_{BV_{hi}}, F_{BV_{vj}}\}$ are appointed diverse access authorities for LAG and CA. Concretely, LAG can only ascertain BVs' group identifiers $\{gid_{hi}, gid_{vj}\}$ for launching a specific working mode, rather than obtaining the real identities. CA owns a full-authority on $\{F_{BV_{hi}}, F_{BV_{vj}}\}$, 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 gid, an in-group key k_h, an out-group key k_v, and two access lists of aggregators' identity flags and pseudonyms $\{L_{F_{LAG}}, L_{PID_{LAG}}\}$. LAG is assumed to be a hardware-unrestricted entity, which includes a pseudonym PID_{LAG}, in-group key set $\{k_{hi}\}$, and out-group key set $\{k_{vj}\}$. 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

TABLE II
THE COMPUTATION LOAD

	The Home Mode			The Visiting Mode		
	BV_{hi}	LAG_h	VBV_h	BV_{vj}	LAG_v	VBV_v
BLO	8	7	2	8	6	1
PRNG	1	1	1	1	1	1
SKE	2	2	–	–	–	–
HMAC	1	–	–	3	2	–
DAF	5	7	–	5	7	–

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 $\{sid_{LAG}, r_{LAG}, PST_{VBV}\}$ 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 executed 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 $\{LAG, VBV\}$ are estimated as $(82 + 26) = 108$ bytes in the home mode, and $(80 + 18) = 98$ 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

[1] H. Gharavi and R. Ghafurian, "Smart grid: The electric energy system of the future," *Proc. IEEE*, vol. 99, no. 6, pp. 917–921, 2011.

[2] Y. Zhang, R. Yu, M. Nekovee, Y. Liu, S. Xie, and S. Gjessing, "Cognitive machine-to-machine communications: Visions and potentials for the smart grid," *IEEE Netw. Mag.*, vol. 26, no. 3, pp. 6–13, 2012.

[3] C. Guille and G. Gross, "A conceptual framework for the vehicle-to-Grid (V2G) implementation," *Energy Policy*, vol. 37, no. 11, pp. 4379–4390, 2009.

[4] K. Clement-Nyns, E. Haesen, and J. Driesen, "The impact of vehicle-to-grid on the distribution grid," *Elec. Power Syst. Res.*, vol. 81, no. 1, pp. 185–192, 2011.

[5] C. D. White and K. M. Zhang, "Using vehicle-to-grid technology for frequency regulation and peak-load reduction," *J. Power Sources*, vol. 196, no. 8, pp. 3972–3980, 2011.

[6] H. Lund and W. Kempton, "Integration of renewable energy into the transport and electricity sectors through V2G," *Energy Policy*, vol. 36, no. 9, pp. 3578–3587, 2008.

[7] W. Kempton and J. Tomic, "Vehicle-to-Grid power implementation: From stabilizing the grid to supporting large-scale renewable energy," *J. Power Sources*, vol. 144, no. 1, pp. 280–294, 2005.

[8] W. Kempton and J. Tomic, "Vehicle-to-Grid power fundamentals: Calculating capacity and net revenue," *J. Power Sources*, vol. 144, no. 1, pp. 268–279, 2005.

[9] H. Khurana, M. Hadley, N. Lu, and D. A. Frincke, "Smart-grid security issues," *IEEE Security Privacy*, vol. 8, no. 1, pp. 81–85, 2010.

[10] A. G. Boulanger, A. C. Chu, S. Maxx, and D. L. Waltz, "Vehicle electrification: Status and issues," *Proc. IEEE*, vol. 99, no. 6, pp. 1116–1138, 2011.

[11] S. Han, S. Han, and K. Sezaki, "Development of an optimal vehicle-to-grid aggregator for frequency regulation," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 65–72, 2010.

[12] "Car prototype generates electricity, and cash" [Online]. Available: http://www.sciencedaily.com/releases/2007/12/071203133532.htm

[13] N. W. Lo and K. H. Yeh, "Anonymous coexistence proofs for RFID tags," *J. Inf. Sci. Eng.*, vol. 26, no. 4, pp. 1213–1230, 2010.

[14] J. S. Cho, S. S. Yeo, S. Hwang, S. Y. Rhee, and S. K. Kim, "Enhanced yoking proof protocols for RFID tags and tag groups," in *Proc. 22nd Int. Conf. Advanced Inf. Netw. Appl. Workshops (AINAW).*, Okinawa, Japan, Mar. 25–28, 2008, pp. 1591–1596.

[15] Z. Yang, S. Yu, W. Lou, and C. Liu, "P^2: Privacy-preserving communication and precise reward architecture for V2G networks in smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 697–706, 2012.

[16] H. Guo, Y. Wu, F. Bao, H. Chen, and M. Ma, "UBAPV2G: A unique batch authentication protocol for vehicle-to-grid communications," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 707–714, 2012.

[17] B. Vaidya, D. Makrakis, and H. T. Mouftah, "Security mechanism for multi-domain vehicle-to-grid infrastructure," in *Proc. 2011 IEEE Global Telecommun. Conf. (GLOBECOM 2011)*.

[18] D. He, C. Chen, S. Chan, Y. Zhang, J. Bu, and M. Guizani, "Secure service provision in smart grid communications," *IEEE Commun. Mag.*, vol. 50, no. 8, pp. 53–61, 2012.

[19] A. R. Metke and R. L. Ekl, "Security technology for smart grid networks," *IEEE Trans. Smart Grid*, vol. 1, no. 1, pp. 99–107, 2010.

[20] Q. Li and G. Cao, "Multicast authentication in the smart grid with one-time signature," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 686–696, 2012.

[21] C. Efthymiou and G. Kalogridis, "Smart grid privacy via anonymization of smart metering data," in *Proc. 1st IEEE Int. Conf. Smart Grid Commun. (SmartGridComm2010)*, Gaithersburg, MD, pp. 234–243.

[22] M. Qiu, W. Gao, M. Chen, J. W. Niu, and L. Zhang, "Energy efficient security algorithm for power grid wide area monitoring system," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 715–723, 2012.

[23] T. M. Chen, J. C. Sanchez-Aarnoutse, and J. Buford, "Petri net modeling of cyber-physical attacks on smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 741–749, 2012.

[24] Y. Zhang, L. Wang, W. Sun, R. C. Green, II, and M. Alam, "Distributed intrusion detection system in a multi-layer network architecture of smart grids," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 796–808, 2012.

[25] H. Son, T. Y. Kang, H. Kim, and J. H. Roh, "A secure framework for protecting customer collaboration in intelligent power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 759–769, 2012.

[26] D. Wu and C. Zhou, "Fault-tolerant and scalable key management for smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 375–381, 2011.

[27] M. M. Fouda, Z. M. Fadlullah, N. Kato, R. Lu, and X. Shen, "A lightweight message authentication scheme for smart grid communications," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 675–685, 2012.

[28] R. Lu, X. Liang, X. Li, X. Lin, and X. Shen, "EPPA: An efficient and privacy-preserving aggregation scheme for secure smart grid communications," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 9, pp. 1621–1631, 2012.

[29] D. He, J. Bu, S. Zhu, S. Chan, and C. Chen, "Distributed access control with privacy support in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 10, pp. 3472–3481, 2011.

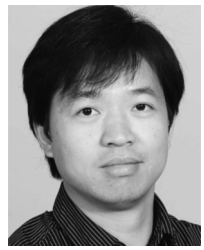
[30] Helion IP Core Products: Data Security Products [Online]. Available: http://www.heliontech.com/core.htm
[31] Advanced Security Products-Anti-Counterfeiting, Privacy Protection, Brand Protection, Protection Against Theft of Service or Content. Products: HMAC-SHA [Online]. Available: http://www.intrinsic-id.com/hmacsha.htm

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.