Privacy Protection Strategy of Vehicle-to-Grid Network Based on Consortium Blockchain and Attribute-based Signature

Guochen Wei* and Yonghong Ma

School of Electrical and Electronic Engineering, North China Electric Power University, Beijing, China

*Corresponding author email: 1182201219@ncepu.edu.cn

Abstract. V2G (vehicle-to-grid) is an integral part of the smart grid. To deploy a V2G network on a large scale, it is necessary to solve network security and trustworthiness and privacy protection of electric vehicle users (EV). Therefore, this paper proposes a privacy protection strategy for V2G networks based on consortium blockchain and attribute-based signature and designs an overall implementation scheme including system initialization, EV registration, anonymous authentication, optimized scheduling, local services, block construction and consensus mechanism. The strategy also uses the K-anonymity to protect the privacy of the EV's geographic location, making it well compatible with charging and discharging services. Finally, security and performance analysis proved the feasibility of design scheme.

Keywords: V2G; Privacy protection; Attribute-based signature; Consortium blockchain.

1. Introduction

As a new type of controllable load, electric vehicles can deliver energy to grid through battery discharge, realizing the bidirectional flow of energy between the electric vehicle and the grid [1]. This technology is called V2G (vehicle-to-grid). To deploy V2G networks on a large scale, it is also necessary to solve the problem about network security and EV’s privacy protection. The emerging technology blockchain provides a new method for solving these problems. Blockchain is an open, transparent, and decentralized database technology that deeply integrates distributed data storage, P2P transmission, consensus mechanism, encryption algorithm, etc [2]. At present, the research of blockchain technology in power energy is still in its infancy [3]. However, it is difficult to guarantee the privacy information of V2G users due to the disclosure of transaction data by conventional blockchain technology for maximum transparency, so most of the current research still has great defects in this aspect.

To this end, this paper proposes a privacy protection strategy for V2G networks. First, the strategy adopts the consortium blockchain to form a semi-centralized energy trading system, which satisfy the security, credibility, and scalability requirements of large-scale deployment for V2G networks [4-6]. Secondly, the strategy also uses the attribute signature [7-9] and the K-anonymity algorithm [10] to satisfy EV's identity and location privacy protection requirements. Finally, this paper verifies the feasibility of the proposed scheme through security analysis and simulation experiments.

2. V2G Network Privacy Protection Scheme

The architecture of a V2G network is shown in Figure 1, including four entities: central aggregator (CAG), local aggregator (LAG), a single EV and trusted third agency (TA). CAG and LAG belong to network operators, a single EV belongs to private users, and TA belongs to some independent organizations, such as regional transmission organizations or independent system operators. The flow
of information and energy in the network represented by thick dashed and thick solid lines, respectively. Besides, CAG is responsible for the overall monitoring and scheduling of the network, and is the only entity that can directly communicate with electricity market. In addition, in order to reduce the burden of CAG and meet the needs of EVs in different locations, LAG is deployed for each area to provide direct interaction for the local EV. TA, as a neutral third party, can be shared by multiple V2G networks, is responsible for generating system public parameters, assigning public and private keys to each entity.

2.1. System Initialization
By entering the security parameters $\lambda$, TA performs the following operations to generate system public parameters $\text{params}$:

1) TA selects a bilinear pair $e : G \times G \rightarrow G_1$ and defines three hash functions $H_1 : \{0,1\}^* \rightarrow \{0,1\}^k$, $H_2 : \{0,1\}^* \rightarrow G$, and $H_3 : \{0,1\}^* \times G_1 \rightarrow Z^*$ at the same time. Where $G$ and $G_1$ is a group with order $p$, and $p$ is a large prime number. $g$ is a generator of $G$ and $G_1$.

2) TA defines $\Lambda$ as the user's attribute space, and a random number $d$ is defined as the upper limit of the threshold predicate $\Gamma$ allowed by the system. $\Lambda$ contains all possible attributes of EV, and each attribute is coded as different elements.

3) In order to generate and verify the attribute signature, TA chooses a random number $\alpha \in Z_p$ as the master private key, and selects two vectors $\tilde{\alpha} = (\alpha_0, \alpha_1, \ldots, \alpha_l) \in Z_p^{l+1}$, $\tilde{U} = (u_0, u_1, \ldots, u_k)$, calculate $Z = e(g, g)^{\alpha_l}$, $\tilde{h} = g^{\tilde{\alpha}} = (h_0, h_1, \ldots, h_l)$. It should be known that $l = 2d + 1$, $u_0, u_1, \ldots, u_k \leftarrow G$.

4) For the pre-registration of CAG and LAG, TA selects a random number $s$ and calculates $Q = s \cdot g$ as a public parameter. Then, based on the real identities $ID_{CAG}$ and $ID_{LAG}$, TA generate private keys $sk_{CAG} = sH_2(ID_{CAG})$, $sk_{LAG} = sH_3(ID_{LAG})$ and corresponding public keys $pk_{CAG} = H_2(ID_{CAG})$, $pk_{LAG} = H_3(ID_{LAG})$, send them back to the corresponding LAG and CAG. In the end, all aggregators save their private keys after receiving the public-private key pair and publish their public keys.

5) TA securely saves the master private key $\alpha$ and announces all public parameters:

$$\text{params} = (g, G, G_1, e, p, H_1, H_2, H_3, Z, Q, \tilde{h}, \tilde{U})$$

2.2. EV Registration
To join V2G network, EV chooses a random number $\beta$ as the user's private key $sk_{EV}$ and calculate $pk_{EV} = g^{\beta}$ as its public key. After that, EV securely saves the private key, sends real identity $ID_{EV}$ and
After receiving EV’s registration information, TA generates an attribute private key for it. First, TA selects the attribute set $\Omega$ belonging to the EV from $\Lambda$. Then, TA randomly selects parameters $a_1, \ldots, a_{d-1} \in \mathbb{Z}_p$ and defines:

$$q(w) = \sum_{i=1}^{d-1} a_i w^i + \alpha$$  \hspace{2cm} (1)

For each attribute $w \in \Omega$, TA randomly selects the index $r_w \in \mathbb{Z}_p$ and calculates:

$$\begin{cases} D_{w,1} = (g^{q(w)}) \cdot h_0^{r_w}, & D_{w,2} = g^{r_w} \\ K_{w,i} = (h_i^{w} \cdot h_{i+1})^{r_w} & \forall i \in [1, l-1] \end{cases}$$  \hspace{2cm} (2)

The attribute private key of EV is:

$$sk_\Omega = \{D_{w,1}, D_{w,2}, \{K_{w,i}\}_{i \in [1, l-1]}\}_{w \in \Omega}$$

In addition, to protect the privacy of users in the payment phase and prevent collision attacks, TA also prepares multiple random pseudonyms for EV as follows:

$$\{PS_{EV,i}, \ldots, PS_{EV,n}\}$$

Finally, TA sends attribute private key and the pseudonyms back to the EV that submitted the registration information. An EV receiving all above information indicates that the registration is completed.

### 2.3. Anonymous Authentication and Optimized Scheduling

After registration, EV can use its attribute private key to anonymously complete message authentication under different predicates $\Gamma$. We can assuming that the predicate specified by CAG in a period of time is $t_{\Gamma, S}$, any signature that can’t match $t_{\Gamma, S}$ will not be recognized by CAG, here $t = 3, S = \{Type; City; Serving-period\}$.

To protect location privacy, EV also need to hide its real location information before sending the transaction request. This paper uses K-anonymity algorithm to realize the protection of geographic location. According to this algorithm, EV pre-selection strategy $\Psi$ determines the size of cloaking area, which means EV needs to make a compromise between privacy protection and accurate service. The specific operation of EV hiding the real location information is as follows:

1) The EV determines the cloaking area $A_{\Psi}$ according to $\Psi$ and its real location $(x, y)$.

2) EV selects the center of the cloaking area $(x', y')$ as its cloaking position. Since all the EVs located in the same cloaking area $A_{\Psi}$ are selecting same $(x', y')$, the attacker will not be able to identify EVs in the same area.

After that, EV needs to send a transaction request to CAG. The transaction request includes two parts: transaction information $m$ and attribute signature $\sigma$. The transaction information contains different parts: ① the cloaking location $(x', y')$ generated by EV; ② the amount of electricity $B$ that EV wants to buy or sell; ③ the estimated time of arrival and departure $(t_a, t_b)$; ④ the timestamp $T$ used to prevent delay attacks.

The process for EV to send a transaction request to CAG is as follows:

1) EV packaging $m = \{B \| T \| (x', y') \| (t_a, t_b)\}$, select the attribute subset $S_t \subset \{\Omega \cap S\}$ that satisfies both the predicate and its own attributes, and the number of elements in the subset $|S_t| = t$. After that, EV selects a vector of coefficients $\bar{b} = (b_1, \ldots, b_t) \in \mathbb{Z}_p^t$, defines:
\[ \mu_S(y) = \sum_{i=1}^{l} b_i y^{i-1} = \prod_{w \in S} (y - w) \]  

(3)

2) For each attribute \( w \in S \), EV uses \( sk_\alpha \) to calculate:

\[
\begin{align*}
\Delta^i_j(x) &= \prod_{j=1}^{l} \frac{x - j}{i - j} \\
D_{w,1} &= D_{w,1} \prod_{i=1}^{l} K_{w,j}^{k_{w_i}} \\
D_1 &= \prod_{w \in S} D'_{w,1} \Delta^0 \ (0), \quad D_2 = \prod_{w \in S} D'_{w,1} \Delta^0 \ (0)
\end{align*}
\]  

(4)

3) EV calculate \( M = H_i(m, \Gamma) \in \{0,1\}^k \), parsed \( M \in \{0,1\}^k \) into a string \( (m_1, m_2, \ldots, m_k) \) and randomly selected \( s_1, s_2 \in Z_p \) at the same time, calculate:

\[
\begin{align*}
\sigma_1 &= D_1 \cdot (h_0 \prod_{i=1}^{l} h_{i}^{b_i})^{s_2} \cdot (u_0 \prod_{j=1}^{k} u_j^{m_j})^{s_1} \\
\sigma_2 &= D_2 \cdot g^{s_2}, \quad \sigma_3 = g^{s_1}
\end{align*}
\]  

(5)

\( \sigma = (\sigma_1, \sigma_2, \sigma_3) \) is the attribute signature generated by EV. EV will send \( (m, \sigma) \) to CAG. After CAG receives \( (m, \sigma) \), it verifies the attribute signature by checking whether equation (6) holds:

\[ \frac{e(g, \sigma_1)}{e(h_0 \prod_{i=1}^{l} h_{i}^{b_i}, \sigma_2) \cdot e(u_0 \prod_{j=1}^{k} u_j^{m_j}, \sigma_3)} = Z \]  

(6)

If it is established, the verification is successful, and then CAG extracts the necessary information from \( m \) and executes the optimal scheduling algorithm. The scheduling strategy finally returns the recommended LAG location \( \{L_1\} \) as result.

In addition, CAG uses its own \( sk_{CAG} \) to sign on \( m \) as the certification of EV transactions. CAG chooses \( g_1 \in G \) and a random integer \( k \in Z^* \), calculate:

\[
\begin{align*}
r &= e(g_1, g)^k \\
v &= H_3(m, r) \\
u &= v \cdot sk_{CAG} + k \cdot g_1
\end{align*}
\]  

(7)

In the end, CAG packages the scheduling results and transaction certification as \( \{L_1, (u, v)\} \) and sends them to the EV.

2.4. Local Charging and Discharging Service

After receiving \( \{L_1, (u, v)\} \), the EV chooses a LAG according to its own preference. At the parking pot, EV sends \( \{L_1, (u, v)\} \) to LAG, and LAG calculate:

\[ r = e(u, g) \cdot e(H_3(ID_{CAG}), -Q)^v \]  

(8)

According to equation (8), LAG obtain the value of \( r \), then it verifies whether \( v = H_3(m, r) \) is established, and if it is established, the signature verification is passed. LAG will read \( m \) to complete
the service and returns a signal to EV. After obtaining LAG’s signal, EV selects an address from pseudonyms as the wallet address and sends it to LAG. LAG extracts the latest data belonging to the wallet address from the memory pool and submits it to EV. EV need to check the integrity of the relevant data of this wallet address. In the end, EV and LAG begin to conduct energy flow and complete the transfer. LAG generates a new transaction record data and sends the data to EV as a transaction receipt.

2.5. Block construction and consensus process
LAG adds all transaction data to the local memory pool. Thereafter, in order to record all transactions and maintain a verifiable shared ledger, all LAGs need to perform the following two steps under the cooperation of CAG:
1) Block construction: LAG collects all local transaction records within a certain period of time and then signs it with its own private key. After that, LAG organizes transaction records into blocks and tries to find a valid proof of data work.
2) Consensus process: CAG broadcasts block data, timestamp and proof of work to other LAGs for verification and review. After LAG audits the block data, the result and signature information are broadcast on the network. Each LAG compares its audit results with the results of other LAGs, and then sends the comparison conclusion signature back to CAG. CAG compare the received conclusions. If more than a certain percentage (about one-third) of LAG agrees to the block data, CAG will send records including the currently reviewed block data and corresponding signatures to all authorized LAGs in the alliance blockchain.

3. Security and Performance Analysis

3.1. Security Analysis

Theorem 1 (Correctness):
1) The correctness of the attribute signature in the transaction request:
For each \( w \in \mathcal{S} \), since the vector \( \bar{b} \) is orthogonal to \( \bar{X}^l_w = (1, w, w^2, ..., w^{l-1}) \), then the equation (9) holds:

\[
D'_{w,j} = D_{w,j} \cdot \prod_{i=1}^{l-1} K_{w,i}^{b_{i+1}} \\
= g^{q(w)} \cdot (h_0 \cdot h_1) \cdot \prod_{i=2}^{l} h_i^{b_i} e^{r_w} \\
= g^{q(w)} \cdot (h_0 \cdot \prod_{i=1}^{l} h_i^{b_i})^{r_w} 
\]

In addition, since \( (D_1, D_2) \) satisfies equation (10):

\[
e(D_1, g) = e(g, g)^{r_1} \cdot e(h_0 \cdot \prod_{i=1}^{l} h_i^{b_i}, D_2)
\]

Thus, the verification equation can be derived as equation (6).
2) The correctness of the ID signature in the transaction certification:
For verifier, the correctness of the value \( r \) in the equation (7) can be derived from the equation (8):

\[
r = e(u, g) \cdot e(Hz(ID_{cag}), -Q)^v \\
= e(v \cdot sk_{cag}, g) \cdot e(k \cdot g, g) \cdot e(Hz(ID_{cag}), -Q)^v \\
= e(Hz(ID_{cag}), v \cdot s \cdot g) \cdot e(Hz(ID_{cag}), -v \cdot Q) \cdot e(k \cdot g, g)
\]

(11)
Theorem 2 (Unforgeability):
In our scheme, the attribute private key generated by EV, and the transaction certification generated by CAG satisfy the unforgeability.
In order to provide an effective registration algorithm, this paper uses the attribute signature scheme of [7]. Since the generation method is the same as the scheme [7], the proof that the attribute signature cannot be forged is similar to [7]. In addition, for the ID signatures, this paper uses the signature scheme of [11], and the proof process is similar to [11]. The specific process is omitted due to page restrictions.

Theorem 3 (Anonymity):
The EV in our scheme has perfect anonymous privacy:
In authentication phase, the attribute subsets \( S_t \subset S, |S_t| = t \) and \( S'_t \subset S, |S'_t| = t \) used by different EVs under the predicate \( \Gamma_{t,s} \) are not same, because the attributes \( w \) and \( w' \) in the two subsets are random. However, a valid signature generated by any EV may also be generated by another EV. Since any pair \( (w, w') \) that satisfies equation (12) will result in the same signature. So the verifier cannot distinguish different EVs, and the anonymous privacy of EVs is satisfied.

\[
\sum_{w \in \text{SM}} \Delta^S_w(0) \cdot r_w + w = \sum_{w \in \text{SY}} \Delta^S_w(0) \cdot r_w + w'
\]  
(12)

3.2. Case study
Table 1 shows the theoretical computation overhead of each entity at different stages. the power computation cost is expressed as \( E \), the bilinear pairing computation cost is expressed as \( P \), and the scalar multiplication computation cost is expressed as \( M \). \( j \) represents the number of LAGs in the network, and \( * \) indicates that the entity is not involved in the step, small indicating that the calculation cost is small.

| procedure | TA | EV | CAG | LAG |
|-----------|----|----|-----|-----|
| System initialization | \((2j+1)M\) | * | * | * |
| EV registration | \((4d+1)E\) | Small | * | * |
| Anonymous authentication and optimized scheduling | * | \((4d+7)E\) | \((2d+2)E+1M+3P\) | * |
| Local charging and discharging service | * | Small | * | \(1E+1P\) |

In order to test the actual computational cost of the scheme, this paper implement a comprehensive simulation in a computer under the development framework Charm [12]. The configuration is Intel Core i7-8750H CPU @ 2.20GHz and 8.00 GB RAM, and the operating system is Ubuntu 14.04 on VMware Workstation Player (1GB RAM).
Figures 3 and 4 respectively show the average computation time of EV and CAG in the anonymous authentication phase and the average calculation time of LAG in the local service phase. The calculation process is performed on three different elliptic curves: SS512, MNT159 and MNT224. Comparing the three curves used in the experiment, it can be seen that: SS512 has the best computational performance, while MNT224 has higher computational overhead.
Taking the average computation time of the SS512 curve in Figure 4 as an example, a LAG can process about 50 user transactions simultaneously in one second. Assuming that the number of LAGs in the network is about 200, the entire network can process about 10,000 transactions simultaneously in one second. In addition, for CAG, which is responsible for overall scheduling, this simulation experiment uses only a laptop computer with a common configuration. In practice, CAG can use a higher hardware configuration to further improve its computational efficiency. Considering that only one CAG needs to be deployed in each network, the increase in computational efficiency is reasonable and obvious. Based on the above analysis, it can be seen that the network under this scheme can better handle the simultaneous access of large-scale EVs.

4. Conclusion
In order to deploy V2G on a large scale, must solve the problems of network security and privacy protection of EVs. This article proposes a privacy protection strategy for V2G networks based on consortium blockchain and attribute signatures. Security and performance analysis verify the feasibility of the design scheme. To this end, this paper proposes a privacy protection strategy for V2G networks. The strategy adopts the consortium blockchain to form a semi-centralized energy trading system, which
satisfy the security, credibility, and scalability requirements of large-scale deployment for V2G networks and uses attribute signature and K-anonymity algorithm to satisfy EV's identity and location privacy protection requirements. The next step of our work will be: ①Hiding the real data of on-chain transactions to prevent data analysis attacks, and design the on-chain transaction data protection scheme; ②Deeply analyses the influence of different property settings on the application performance of the V2G network and proposes targeted optimization scheduling strategies and personalized charging/discharging services.

Acknowledgments
This work was supported by State Grid Information and Communication Industry Group Corporation, entitled” Research and development of special quantum secret communication key distribution equipment suitable for electric overhead environment”, under Grant SGITG-201802SQHF-FF10

References
[1] CHEN Zhong, LIU Yi, CHEN Xuan, et al. Charging and discharging scheduling strategy for electric vehicles considering mobile energy storage characteristics[J].Automation of Electric Power Systems,2020,44(02):77-88.
[2] ZHAO Yuehao, PENG Ke, XU Bingyin, et al. Status and prospect of energy blockchain application engineering[J]. Automation of Electric Power Systems, 2019, 43(07):20-30+76.
[3] WANG Haoran, CHEN Sijie, YAN Zheng, et al. Blockchain-based charging right transaction for electric vehicle charging stations: mechanism, model and method[J]. Chinese Journal of Electrical Engineering, 2020,40(02):425-436.
[4] LI Z, KANG J, YU R, et al. Consortium Blockchain for Secure Energy Trading in Industrial Internet of Things[J]. IEEE Transactions on Industrial Informatics. vol. 14, no. 8, pp. 3690-3700, Aug. 2018, DOI: 10.1109/TII. 2017.2786307.
[5] GAI K, WU Y,ZHU L, et al. Privacy-Preserving Energy Trading Using Consortium Blockchain in Smart Grid[J]. IEEE Transactions on Industrial Informatics, vol. 15, no. 6, pp. 3548-3558, June 2019, DOI: 10.1109/TII.2019.2893433.
[6] JIN Zhigang, WU Ruocian, LI Gen, et al. Electric vehicle charging transaction model based on alliance blockchain[J]. Power System Technology, 2019, 43(12).
[7] HERRANZ J,LAGUILLAUMIE F,LIBERT B, et al. Short attribute-based signatures for threshold predicates[C]. Proc. Cryptogr. Track RSA Conf., in Lecture Notes in Computer Science, San Francisco, CA, USA, 2012, P. 51–67.
[8] LI J,KIM K. Hidden attribute-based signatures without anonymity revocation[J]. Information Sciences, 2010, 180(9):1681-1689.
[9] LI J,AU M,SUSILO W, et al. Attribute-based signature and its applications[J]. In ASIACCS’10, ACM Press, pp. 60–69, 2010.
[10] LI D, YANG Q, AN D, et al. On Location Privacy-Preserving Online Double Auction for Electric Vehicles in Microgrids[J]. IEEE Internet of Things Journal, 2018, PP:1-1.
[11] HESS F. Efficient identity-based signature schemes based on pairings[J]. Proc. SAC’02, vol. 2595 of LNCS. 2003. p. 310–324.
[12] AKINYELE J, et al. Charm: A framework for rapidly prototyping cryptosystems[J]. J. Cryptograph. Eng., vol. 3, no. 2, pp. 111–128, 2013