Advances in Computer, Signals and Systems (2020) 4: 13-18
Clausius Scientific Press, Canada

DOI: 10.23977/acss.2020.040103
ISSN 2371-8838

Research on Anonymous Authentication of Vehicle to Grid Users Based on Group Signature

Shaomin Zhang[a,*], Fang Xie[b] and Baoyi Wang[c]

[1]*Department of Control and Computer, North China Electric Power University, HuaDian Road, BaoDing, China*

zhangshaomin@126.com, xiefang223@163.com,wangbaoyi@126.com

Keywords: V2G, Group Signature, Privacy Protection, Anonymous Authentication, Complete Subtree Method

Abstract: In order to solve the problem that the privacy information of the vehicle to grid user is leaked, which endangers the safety of users' lives and properties. In this paper, a V2G user anonymous authentication scheme based on group signature is proposed to realize the user anonymous authentication of vehicle to grid. In order to realize the anonymous authentication of the charging station to the EV, the scheme mainly adopts group signature algorithm to achieve anonymous authentication between the EV and the power grid. In the process of authentication, only the trusted center has the real identity of the user to ensure the anonymous interaction between electric vehicle and power grid. The aggregation unit records the EV information by combining a complete subtree method and Chinese remainder theorem, so that other members do not need to change the key in the process of EV revocation. According to the security analysis, this scheme can ensure the confidentiality, integrity, effectiveness and non-repudiation of information in V2G network. The performance analysis shows that this scheme can reduce the computing and communication costs of the vehicle to grid.

1. Introduction

In the process of bidirectional information flow exchange with the power grid, the privacy of users in the V2G network may be exposed to curious third parties or malicious attackers.Once the user's information is intercepted or tracked, a successful attack by the attacker may leak the user's private data, which may threatens the user's property security or life [4]. Therefore, in order to realize the safe, reliable and orderly connection of V2G and protect the privacy of users, the privacy protection of V2G becomes very important.

In order to realize the safe access of electric vehicles to the power grid, protect the privacy of users, researchers at home and abroad put forward many schemes. Literature [1] proposes a secure and efficient authentication scheme with privacy-preserving for V2G networks, the scheme uses bilinear pairing and the NNL framework, and time overheads during verification stage are

independent with the number of involved PEVs. Literature [2] and Literature [5] based on bilinear pairing technology and accumulator batch verification propose a mutual authentication scheme to protect EV's forwarding privacy and identity anonymity, the scheme can reduce communication and computing costs. Literature [3] proposes a privacy protection and lightweight key protocol, but the protocol can not withstand simulated attacks, as well as session key security and perfect forward secrecy. Literature [6] proposes a lightweight security and privacy protection V2G connection scheme by using BlueJay ultra-lightweight hybrid cryptography system, during the authentication, electric vehicles protect their private information by generating pseudonym identities, but the scheme is suitable for EV with limited capacities. Literature [7] proposes a privacy protection authentication scheme (AP3A) based on aggregation proof for V2G network of smart grid, which divides BV into home and visit mode, but the scheme only uses informal methods to analyze the security of its protocols. Literature [8] proposes an authentication protocol scheme based on group signature, which used a complete subtree method to achieve membership revocation. All of the above schemes are based on anonymous technology or encryption technology, and these schemes will cause a large amount of computing overhead in the communication process, so they can not solve the problem of user anonymous authentication of vehicle to grid.

The main contributions of this paper can be summarized as follows. Firstly, the group signature algorithm is used for anonymous authentication during the communication between electric vehicles and the power grid. Secondly, when the aggregation unit records the electric vehicle information, it uses the method of complete subtree and Chinese Remainder Theorem to reduce the communication and calculation costs of V2G.

2. Scheme Description

2.1 Scheme Design Idea

In order to protect the privacy of users, this paper proposes a V2G user anonymous authentication scheme based on group signature. The group signature method is used to achieve anonymous authentication during the charging and discharging process of electric vehicles, ensuring secure communication between electric vehicles and the power grid. In order to prevent users from cheating and damaging the security of the power grid, a trusted third party CA supervises electric vehicles. CA can verify the identity of electric vehicles. At the same time, the CA cannot obtain the communication information between the electric vehicle and the power grid, thereby ensuring that the user's information will not be stolen. The communication between the entities is anonymous to ensure the user’s security.

2.2 Scheme Design Goal

The design goal of this scheme is to achieve anonymous authentication of V2G, which should meet the following objectives:

(1) The scheme can achieve reliable anonymous authentication between electric vehicles and entities, and ensure the anonymity of messages transmitted between entities.

(2) The scheme can realize the safe revocation of electric vehicles, and the revoked electric vehicles cannot communicate.

(3) The scheme can ensure that the communication between the electric vehicle and the power grid is efficient and does not generate huge overhead.

2.3 Scheme Model

This scheme mainly includes Grid Control Center(GCC), the Central Aggregator(CAG), the Local Aggregator(LAG), the Charging Station(CS), the Electric Vehicle(EV), and the trusted center(CA).CA is mainly responsible for the registration of various entities; EV obtains its own public and private key pairs through registration; CS provides charging and discharging services for EV; LAG makes the optimal charging strategy for EV; CAG issues power control commands to each LAG; GCC is responsible for unified dispatching and management of the entire power grid.

3 Scheme Realization

3.1 System Initialization

(1) CAG divides the LAG of each charging station into LAG_1, LAG_2... , LAG_n.

(2) The identity number of CA is ID_{CA},select the appropriate safety parameter k, Hash function H: $\{0,1\}^* \to \{0,1\}^k$,select the appropriate (n_c, e_c), e_c is a large prime number and e_c>4, Calculate dc to make $e_c d_c = 1 \bmod n_c$ .Select a large prime number P, determine the finite field GF(P), make p public, select elements $a, b \in GF(p)$, determine the elliptic curve on the finite field and group Z_q^* , and make a, b public. Select a large prime number q, the order of the base point G (x, y) is p, parameter h=|E1|/q , and make h public.

Randomly select $x_{CA} \in Z_q^*$ as the private key, public key $Y_{CA}=X_{CA}G$.Public parameter (k,H,n_c,e_c,a,b,p,q,G(x,y),c,h,Y_{CA}),and group private key is (d_c,X_{CA}),group public key is (e_c, Y_{CA}).

CA randomly generates identity identifiers for EV, CS, AGG and GCC, such as ID_{EV} and ID_{CS}, and generates their public-private key pairs,such as the key pairs of EV are denoted as PK_{EV} and SK_{EV}. The CA signs the certificate cer=sign (ID_{EV}||PK_{CA}) and sends it to the EV.

(3) The LAG selects the appropriate system safety parameter β and the maximum number of EVs that can be accommodated by the CS, constructs a complete binary tree T with the number of layers l=logN-1(N is the maximum number of EVs that can be accommodated), and generates the EV information record table, and the set of all EVs in the local aggregator is S_{LAG}.

Calculate $c \equiv y_1 P_1^{'} P_1 + y_2 P_2^{'} P_2 + ... + y_n P_n^{'} P_n (\bmod P)$ using the Chinese remaining theorem, and make c public.

3.2 Electric Vehicles Join the Power Grid

Assuming that EV_i applies to CAG to join the V2G network through the CS, then:

First, EV_i registers with its real identity and the real identity of the EV through CAG, and CAG issues the identity number ID_{EVi} for EV. The specific operation is as follows:

(1) EV_i computes ID_{EVi} and signature δ_{EVi} , and encrypts ID_{EVi} and δ_{EVi} with the public key of CAG, that is, Enc(ID_{EVi}||δ_{EVi})={C_1,C_2}.Send {C_1, C_2} to CAG,and request to join the grid.

(2) CAG receives the request from the EV, decrypts {C_1, C_2}to get the identity of the EV, and

then judges whether the EV is legal. If the EV law issues a certificate $cer_{Evi}=sign(ID_{EVi}||PK_{EVi})$ to the EV.

(3) CAG assigns the group LAG_l to which EV_i belongs, CA generates the key pairs of the group for EV, and the public and private key pairs $(PK_{EVi},SK_{EVi})$of group members.

EV_i encrypts its identity ID_{EVi} with the public key of LAG and sends it to LAG. LAG checks whether the information record of the EV_i exists in the database S_{LAG}. If not, it assigns a charging position to the EV with the number of ID_{xl}, and adds the information of the EV_i to the S_{LAG}, recalculates the c and publishes it, and calculatesthe corresponding to the path of the root node to the leaf nodes $L=(ID_{x1},ID_{x2},...,ID_{xl})$.

The EV joins successfully. At this time, the signature keys of other EV users do not change. Only c in the group system parameters changes, but the number of group public keys does not change, and EV signed with LAG.

3.3 Electric Vehicle Revocation

When an EV wants to exit the group, the LAG needs to update the set S_{LAG} that does not contain the EV leaf node of the user, recalculate the c value, and publish it. Then, the withdrawal mark CRL_i of the EV is added to the revocation list CRL, and the length of the group center public key does not change throughout the process. For other legitimate EV users, there is no need to update their own keys.

3.4 Electric Vehicle Charging

After the EV is successfully joined in the CS_i, it will sign and send its charging request message m to the charging station,and m mainly includes the current remaining power of EV, EV identity information ID_{EVi} and the power to be charged. The specific process is as follows:

(1) CS_i checks its member information table to see whether the identity number ID_{EVi} corresponding to the EV_i is in its own group. If it exists, it proves that the EV is a legal user.

(2) EV signs the message m, selects a random number r, and calculates the equation:

$$c_i = H(t_i \| PK_{EV_i} \| c \| m)$$

$$s_{i1} = (c_i + SK_{EV_{i1}} x)/r$$

$$s_{i2} = (c_i + SK_{EV_{i1}} x)^{SK_{EVi2}}$$

Encrypt signature $\delta(m \| t_i)=(ID_{EVi},m,c_i,s_{i1},s_{i2},t_i)$ to CS.

(3) After receiving the message, the charging station CS_i decrypts it and verifies the difference $\Delta = t_{il} - t_i$ between time receiving time t_{il} and sending time t_i. If Δ is within the time difference allowed by the system, the sending time is valid. Next, verify the signature, Calculate $c_i G/s_{i1} + xPK_{EV_{i1}}/s_{i1}$ and compare with RG for equality, Calculate rs_{i1} and compare with $s_{i2}^{PK_{EVi2}} \bmod n_c$ for equality.If the results are equal, the signature is valid.

(4) After the above operation is completed, it is proved that the charging request information m of the electric vehicle is legal, then the charging station CS_i transmits electric energy to the EV according to m, and adds the charging information of the electric vehicle to the user information list, and then performs settlement.

4 Scheme Analysis

4.1 Security Analysis

This scheme has strong anonymity and unforgeability, can resist camouflage attacks, so that it can realize the safe communication between EVs and charging stations.

(1) Unforgeability: Assuming that EV user A has joined the grid, neither LAG nor other malicious EV can impersonate it to generate the corresponding group signature, so the scheme is unforgeable. Whether the attacker is a malicious EV user or LAG, the signature of EV can not be forged, and it is difficult to solve the elliptic curve discrete logarithm problem in the finite field.

(2) Anonymity: Except for the trusted center CA, it is computationally difficult for anyone to determine the identity of the signer based on the public information of the signature, which can guarantee the anonymity of the group signature. Other EV users cannot know which group member was generated during the group signature generation process. Only the CA can open the signature and identify the true identity of the signer.

(3) Anti-joint Attack: Assuming there are k EV users, even if k-1 users are united, it is computationally difficult to know the key of the k-th user. Other EV users only know the group public key, and calculating the group members' private keys is computationally difficult.

4.2 Performance Analysis

This paper proposes an anonymous authentication scheme for V2G users based on group signatures. In the process of communication between electric vehicles and the power grid, this scheme uses group signature algorithm to achieve anonymous authentication between the electric vehicle and the power grid. The core is group signature algorithm based on elliptic curves, and all of the EV can choose the same curve in a limited domain, which provides convenience for software and hardware implementation.In this scheme, the Chinese Remainder Theorem combine with complete subtree method are used to record member information, which reduces the computational cost of member revocation. TP, TM and TC are used to represent logarithm operation, power operation and point multiplication operation respectively, and N is used to represent the total number of EV. On the CPU with the main frequency of 3 GHz, the operation time TP = 4.5ms, the power operation time TM = 2.4ms, and the point multiplication operation time TC = 0.6ms.

Table 1: Comparison of time cost with other literature

Literature schemes	Pair operation	exponentiation	Point multiplication
scheme [5]	2*N	15*N	8*N+1
scheme [7]	0*N	16*N	1*N
Our scheme	0*N	7*N	17*N

From the above comparison, it can be seen that the cost of this scheme is lower than that in the literature [5] [7], and before the EV does not perform identity revocation, the EV does not need to update its own key and group private key to join the charging station for charging. When the EV wants to perform identity revocation, the length of the public key of the group center does not

change in the whole process. For other legitimate EV users, there is no need to update their own signature keys and have higher communication efficiency.

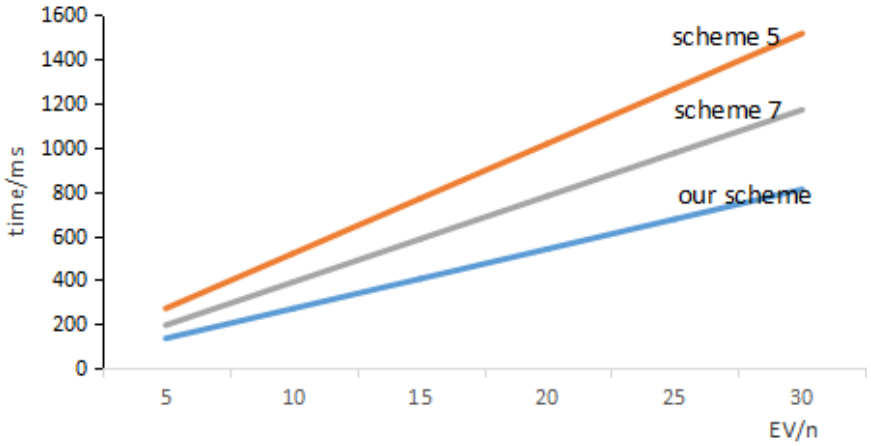

Figure 1: Comparison of time overhead

5 Conclusions

In this paper, a V2G user anonymous authentication scheme based on group signature is proposed to realize the user anonymous authentication of V2G. The scheme uses the combination of Chinese Remainder Theorem and complete subtree method when CAG records the information of EV, reducing the calculation cost of EV in the revocation process, improving the calculation efficiency, and improving the efficiency of the calculation. The security analysis and efficiency analysis are performed on it, the results show that the scheme can ensure the confidentiality, integrity, effectiveness and non repudiation of the certification of EVs in V2G network, can realize the safe transmission of V2G data and information, and reduce the time overhead.

References:

[1] Jie Chen,Yueyu Zhang,Wencong Su. An anonymous authentication scheme for plug-in electric vehicles joining to charging/discharging station in vehicle-to-Grid (V2G) networks[C]. China Communications ,2015,12(3):9-19.

[2] Neetesh Saxena,Bong Jun Choi. Authentication Scheme for Flexible Charging and Discharging of Mobile Vehicles in the V2G Networks[J]. IEEE Transactions on Information Forensics and Security,2016,11(7): 1438-1452.

[3] Shen Jian,Zhou Tianqi,Wei Fushan. Privacy-Preserving and Lightweight Key Agreement Protocol for V2G in the Social Internet of Things[J]. IEEE Internet of Things Journal,2018,5(7):2526-2536.

[4] Christophe Jouvray, Gloria Pellischek. Impact of a Smart Grid to the Electric Vehicle Ecosystem From a Privacy and Security Perspective[C]. 2013 World Electric Vehicle Symposium and Exhibition (EVS27),2013,1-10.

[5] Neetesh Saxena,Bong Jun Choi,Shinyoung Cho. Lightweight Privacy-Preserving Authentication Scheme for V2G Networks in the Smart Grid[C]. 2015 IEEE Trustcom/BigDataSE/ISPA,2015,604-611.

[6] Asmaa Abdallah,Xuemin (Sherman) Shen. Lightweight Authentication and Privacy-Preserving Scheme for V2G Connections[J]. IEEE Transactions on Vehicular Technology, 2017,66(3):2615-2629.

[7] Hong Liu ,Huansheng Ning et al. Aggregated-Proofs Based Privacy-Preserving Authentication for V2G Networks in the Smart Grid[J]. IEEE Transactions on Smart Grid,2012, 3(4):1722-1733.

[8] Xiaohan Yue,Bing Chen. An Efficient and Secure Anonymous Authentication Scheme for VANETs Based on the Framework of Group Signatures[J]. IEEE Access,2018,6:62584-62600.