Research on A Cross-Domain Authentication Scheme Based on Consortium Blockchain in V2G Networks of Smart Grid

Donglan Liu*

State Grid Shandong Electric Power Research Institute

Jinan 250003, PR China

*e-mail: liudonglan2006@126.com

Dong Li

State Grid Shandong Electric Power Company

Jinan 250001, PR China

Xin Liu

State Grid Shandong Electric Power Research Institute

Jinan 250003, PR China

Lei Ma

State Grid Shandong Electric Power Research Institute

Jinan 250003, PR China

Hao Yu

State Grid Shandong Electric Power Research Institute

Jinan 250003, PR China

Hao Zhang

State Grid Shandong Electric Power Research Institute

Jinan 250003, PR China

***Abstract*—As an important part of the smart grid, the Vehicle-to-Grid (V2G) can provide various auxiliary services for the power grid and promote the use of renewable resources. However, there are various kinds of attacks in the V2G network. Based on consortium blockchain, this paper proposes a cross-domain authentication scheme for the security threat in the V2G network. This paper designs the trust model and the system architecture, and describes the scheme in detail. The signature and authentication of the scheme adopt the SM9 identity-based cryptographic algorithm. This scheme utilizes the fact that block chain technology is not easy to tamper with. It uses a hash algorithm to verify the certificate, reducing the number of public key algorithm signatures and verifications, making the solution efficient and scalable. The introduction of block chain technology provides new ideas and methods for solving the security problems in the Smart Grid.**

Keywords—Smart Grid; Vehicle-to-Grid; Consortium Blockchain; Cross-domain Authentication

I. INTRODUCTION

As an important part of smart grid, the Vehicle-to-Grid (V2G) has become a hot topic. The V2G technology not only solves the problem of charging pressure caused by the large-scale development of electric vehicles, but also can connect electric vehicles as mobile and distributed energy storage units to power grid. It is used to cut peak and fill valley, emergency security, rotating standby and so on. It can improve the power supply flexibility, reliability and energy utilization ratio of power grid. At the same time, it can postpone the investment in the construction of the power grid. As a new network component of smart grid, the V2G has attracted more and more attention [1, 2]. Because the V2G network satisfies real-time two-way communication, the interaction between electric vehicles and power grids may face various challenges of unsafe factors [3, 4]. Therefore, a safe and efficient authentication protocol has become a vital part of V2G network.

The existing authentication schemes for V2G networks mainly focus on privacy protection for users' identities. In the year 2011, Yang et al. firstly used anonym technology to achieve the anonymous authentication of V2G networks [5]. After that, several similar methods, i.e. using anonym technology, have been put forward [6, 7]. However, the anonym has to be termly changed, resulting in high cost of system. Later, methods based on group signature, blind signature and signcryption for the anonymous authentication of V2G networks have been developed [8-10]. Nevertheless, these methods either need complex communication and calculation or need high administrative expenses or have limitations, making them difficult to be widely used in real society, especially in huge group authentication environment. Given that cars can be moved in V2G networks, Vaidya et al. developed multi-domain network architecture for V2G [11]. This architecture contains one comprehensive mixed public key infrastructure model, which is suited for point-to-point cross-domain authentication. Also, it includes the certificate management for intra- and inter-domain to achieve access control. Then, privacy protection contained cross-domain authentication schemes for V2G were consecutively developed [12, 13].

All above methods are designed using centralization model of control center. However, with the increase of machine quantities, the convergence effect will lead to jam of the authentication server. As a result, signalling data storm will form and the authentication time delay will sharply increase. Block chain technology is de-centered, traceable, transparent, tamper, anonymous and consistant, making it identical with the theory of smart power grids [14]. The smart power grids and block chains are both built on web of things, and they both are intelligent, de-centered and self-governed. Besides, the reason bolck chains are introduced is to automatically read smart electric meters based on its characterization. Therefore, with the combination of artificial intelligence, the energy consumption can be intelligent in the future, thus bring convenience for peoples' life and work. The introduction of block chains can play an important role in decentration and dependability [15, 16]. Recently, the investigation on the application of block chains are attracting

This research was financially supported by the State Grid Shandong Electric Power Company (No. 52062617002V).

978-1-5386-8549-5/18/$31.00 ©2018 IEEE

more and more attentions [17-19]. In this study, based on the block chain technology and SM9 digital signature algorithm, the high-powered cross-domain scheme in V2G has been put forward.

II. V2G Network Architecture

In V2G network architecture, the moving electromobile will provide power for the grid when the electric power is unbalanced. The geographic areas have been divided and each area has one certificate authority (CA). This model is used to analyze the procedure of buliding and transferring of trust relationship intra- and inter- the management domain of CA. Assuming such a scene that electromobile UA of Shanxi province belongs to management domain A, when it tried to join up the grid in Shandong province, it has to do authentication in management domain B of Shandong province. The grid of Shanxi and Shandong provinces belongs to A and B, respectively. In this paper, the cross-domain mode can be presented as Figure 1.

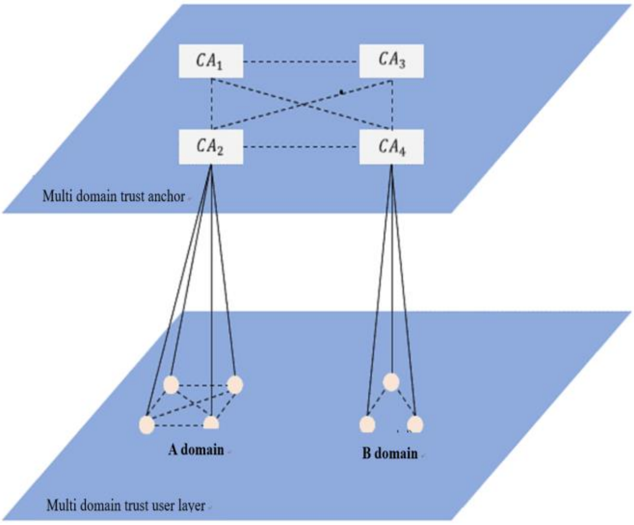

Fig. 1. The cross-domain mode for V2G

In Fig.1., the CA of different regions are represented by rectangle, while the intra-domain users are represented by solid round. In order to achieve cross-domain authentication, CAs of different domains can join the league chain after permission and become the Vaildating Peer (VP). In this paper, the root of league chain CA is credible. It creates certificate for VP and writes Hash data into blockchain, thus can be used as credential for domains. If one domain does not need to cross domains anymore, or the domain is not credible anymore, its permission for joining league chain can be cancelled. Figure 1 shows 4 CAs in different domains, named as CA1, CA2, CA3 and CA4, and they are regarded as VPs.

III. Design of Authentication Protocol Based on Consortium Chain

In this part, a V2G cross-domain authentication protocol in smart power grids based on consortium chain has been designed. This protocol has a basic assumption that domains in league chain are all credible due to the designed Identity access mechanism. Domain A and B were used as examples.

The digital signature scheme used for the protocol design is National secret standard SM9, and related parameters can be referred in [20]. SM9 is a novel public key cryptography technology developed from traditional PKI, based on bilinear pairings and elliptic curves. It has superiority in identity authentication, anti-denity, integrity, security, etc, thus providing a new thought to achieve application security. The meanings of some symbols are listed in Table 1.

TABLE I. Meanings of Symbols

Symbols	Meanings
G_1, G_2	The rank is an additive cyclic group of prime N.
G_T	The rank is a multiplication cyclic group of prime N.
e	The bilinear map of $G_1 \times G_2 \to G_T$
P_1	The generator of group G_1
P_2	The generator of group G_2
$H_1(\ )$, $H_2(\ )$	A cryptographic function derived from a cryptographic hash function

Before electromobile U_A connecting with computers, it registers personal information in the authentication server in the home location of A, and obtains corresponding public and private key paris PK_A and SK_A. The identity information ID_A, public key PK_A, timestamp t_A, validity T (designed as bit string $m_A=ID_A||PK_A||t_A||T$) and the signature on m_A of U_A will be sent to regional management center R_A. The certificate authority CA$_A$ is also included in R_A. R_A will check the legality of U_A and calculate the signature public key $P_{pub\text{-}s\mathrm{A}}$ and signature private keyds_A for users. The process is shown as algorithm 1.

TABLE II. Algorithm for Calculating Public and Private Key of User Signature

Algorithm 1: Algorithm for calculating public and private key of user signature

```
Input: $(N, P_2, ID_A, H_1)$;
Output: $(P_{pub\text{-}s\mathrm{A}}, ds_A, hid)$;
1: generating random numbers, $ks \in [1, N\text{-}1]$;
2: calculate the element, $P_{pub\text{-}s\mathrm{A}}=[ks]P_2$ in group $G_T$;
3: select the function identifier $hid$, calculate the element $t_1=H_1(ID_A||hid, N)+ks$ finite field $F_N$;
4: if $t_1=0$ then back to step 1; otherwise, go to step 5;
5: calculate $t_2=ks \cdot t_1^{-1} \bmod N$;
6: calculate $ds_A=[t_2]P_1$;
7: end.
```

The regional management center R_A send the blockchain certificate of U_A ($BCert_{U_A-CA_A}$) the signature public key $P_{pub\text{-}s\mathrm{A}}$ and signature private keyds_A to U_A. Simultaneously, the identify information and $BCert_{U_A-CA_A}$ will be reserved in block chain and database. When the user U_A accesses the Grid, the regional management center R_A searches the data of Hash($BCert_{U_A-CA_A}$), and U_A will be allowed to accesses the Grid unless the searching result is *'issue'*.

Before U_A accesses the Grid in area B, it firstly sends application to visit the authentication server S_B in area B. After receiving the application, S_B will send random number M and timestamp t_B to U_A. By signing on M, $BCert_{U_A-CA_A}$ and t_B, U_A will obtain the value (h, S). The calculating process is listed in algorithm 2.

TABLE III. USER SIGNATURE ALGORITHM

```
Algorithm 2: User signature algorithm
Input: ($M$, $t_B$, $P_{pub\text{-}s\mathrm{A}}$, $BCert_{U_A-CA_A}$, $ds_A$);
Output: ($h$, $S$);
1: calculate the element $g=e(P_1, P_{pub\text{-}s\mathrm{A}})$ in group $G_T$;
2: generating random numbers $r \in [1, N\text{-}1]$;
3: calculate the element $w=g^r$ in group $G_T$, then convert the data type of $w$ to a bit string;
4: calculate the integer $h=H_2(M||t_B|| BCert_{U_A-CA_A} ||w, N)$;
5: calculate the integer $l=(r\text{-}h) \bmod N$, if $l$=0 then back to step 2; otherwise, go to step 6;
6: calculate $S=[l]\ ds_A$;
7: end.
```

The user U_A in area A responds to the request of certificate server S_B in area B and sends $P_{pub\text{-}s}$A, random number M, $BCert_{U_A-CA_A}$, t_B and (h, S) to S_B. Then, S_B checks the validity of M and verifies the correctness of (h, S) by using algorithm 3.

TABLE IV. SIGNATURE VERIFICATION ALGORITHM

```
Algorithm 3: Signature verification algorithm
Input: ($M$, $t_B$, $ID_A$, $P_{pub\text{-}s\mathrm{A}}$, $BCert_{U_A-CA_A}$, $hid$, ($h$, $S$));
Output: ($\circ$, $\perp$);
1: checkout $h \in [1, N\text{-}1]$ whether it is true or not; If not, the verification will
   not pass, then output $\perp$ and go to step 11; Otherwise, go to step 2;
2: convert the data type of S to the point on the elliptic curve, then checkout
   $S \in G_1$ whether it is true or not; If not, output $\perp$ and go to step 11;
   Otherwise, go to step 3;
3: calculate the element $g=e(P_1, P_{pub\text{-}s\mathrm{A}})$ in group $G_T$;
4: calculate the element $t=g^h$ in group $G_T$;
5: calculate $h_1=H_1(ID_A||hid, N)$;
6: calculate the element $P=[h_1]\ P_2+P_{pub\text{-}s\mathrm{A}}$ in group $G_2$;
7: calculate the element $u=e(S, P)$ in group $G_T$;
8: calculate the element $w' = u \cdot t$ in group $G_T$; then convert the data type of $w'$ to a bit string;
9: calculate the integer $h_2=H_2(M||t_B||w', N)$;
10: checkout $h_2$= $h$ whether it is true or not; If true then output $\circ$; otherwise, output $\perp$;
11: end.
```

When the output $\circ$ is received, S_B will send to S_A the application to obtain $BCert_{CA_A}$ in CA_A, which is the trust anchor in area A, and it send the random number n. When the request and the random number n is received by S_A, we will send to the $BCert_{CA_A}$ in CA_A and random number n to S_B. After S_B received the message, algorithm 4 was used to generate cross-domain blockchain certificate for user U_A.

TABLE V. CROSS-DOMAIN CERTIFICATE GENERATION ALGORITHM

```
Algorithm 4: Cross-domain certificate generation algorithm
Input: ($n$, $BCert_{CA_A}$, $BCert_{U_A-CA_A}$);
Output: ($\circ$, $\perp$);
1: verify that the random number $n$ is valid or not; If it fails, output
   $\perp$; Otherwise, go to step 2;
2: query the value of Hash( $BCert_{CA_A}$ ) on the blockchain;
3: (1) If there is no query result, then the A domain authentication
       server provides an incorrect trust anchor $CA_A$ blockchain
       certificate, authentication failed, and output $\perp$, go to step 7;
   (2) If the query result is issue and revoke, then the blockchain
       certificate of A domain trust anchor $CA_A$ has been revoked,
       authentication failed, and output $\perp$, go to step 7;
   (3) If the query result is issue, then the blockchain of A domain
       trust anchor $CA_A$ is published state, authentication success,
       and output $\circ$, go to step 4;
4: send the certificate $BCert_{CA_A}$ of user $U_A$ to the B domain trust anchor $CA_B$;
5: $CA_B$ analysis $BCert_{CA_A}$, generate the cross-domain blockchain
   certificate $BCert_{U_A-CA_A\square CA_B}$ of $U_A$, and send to $S_B$, write it into
   the blockchain;
6: send the domain-block chain certificate $BCert_{U_A-CA_A\square CA_B}$ to user $U_A$;
7: end.
```

Similarly, algorithm 4 can be used to realize reverse authentication of domain A to domain B, so as to realize bidirectional authentication. When the A domain user U_A enters the B domain again after leaving the B domain, it needs to be authenticated again. If the blockchain certificate $BCert_{U_A-CA_A\square CA_B}$ is valid at this time, the user U_A will send to the cross-domain blockchain certificate $BCert_{U_A-CA_A\square CA_B}$ to the B domain authentication server S_B directly, and the S_B will do hash operation, and query the blockchain to verify the validity of the certificate.

IV. SAFETY AND EFFICIENCY ANALYSIS

A. Safety Analysis

In each trust domain, the authentication of users and authentication server is realized by the original authentication method in the domain. Under the multi-domain consortium blockchain framework, the authentication server can obtain the root CA blockchain certificate by the request. After the Hash operation, the stored trust credentials in the blockchain can be queried to determine the trust relationship and realize the authentication of the server of the user and the other domain. The scheme can authenticate the local user and the other domain server, authenticate the domain server and the other domain user, and realize the two-way entity authentication between the two domain users.

In this scheme, the user's certificate file in each domain is hashed, and the hash value of the certificate is stored in the blockchain. Hash functions are unidirectional and collision-resistant, enabling any blockchain node to store trust credentials anonymously and securely. The existence and ownership of the certificate file are proved by storing the hash value of the file on the blockchain, and by submitting the hash value of the file to the time information and validity period in the blockchain.

In this scheme, both signature and authentication adopt the national secret standard SM9 cryptography algorithm, which is based on the elliptic curve discrete logarithm problem to design an identification cryptography algorithm. The algorithm satisfies the requirements of authentication, non-repudiation, integrity and confidentiality. It also satisfies the identity-based adaptive selection message attack with unforgeable security [20]. The intensity of the algorithm achieved by SM9 on the standard selected reference curve is equivalent to the RSA-3072 bit security intensity. According to the evaluation, the complexity of cracking the system is theoretically equivalent to the amount of calculated by 250 billion computers for one billion years [21].

In this scheme, the random number is passed along with the message, which is stored in the query server. Before verifying the feedback information, the random number is validated. The validation technology is the same as the original server to prevent replay attack. This agreement sets the validity period, checking whether the information is in the validity period before authentication, which can prevent denial of service attacks.

B. Efficiency Analysis

This scheme is based on distributed alliance chain. The increase of alliance members will not lead to the increase of the number of public key algorithms used by two parties in cross-domain authentication. In this paper, the Hash algorithm is used to store the Hash value of the certificate in the blockchain for searching. The calculation speed of the Hash algorithm is far higher than that of the public key algorithm, and the speed is even more than dozens of times. Therefore, even in the multi domain alliance environment, the implementation of cross domain authentication is quite impressive. SM9 algorithm used in the scheme is a public key system. Because of its ease of use and high security, it is very suitable for secure interactive communication of mass users. With the increase of the number of user equipment, the practicability of this scheme will not be reduced.

V. CONCLUSION

Based on consortium blockchain and the SM9 identity-based cryptographic algorithm, this paper proposes a cross-domain authentication scheme for the security threat in the V2G network of smart grid. Under the premise of not changing the PKI authentication model, the scheme adds the licensed domain into the consortium blockchain and realizes the cross-domain authentication between multiple domains. The scheme has survivability and unforgettable security under adaptive selection message attack, and it can resist replay attack and denial of service attack, making the solution efficient and scalable.

ACKNOWLEDGMENT

This research was financially supported by the State Grid Shandong Electric Power Company (No. 52062617002V). Meanwhile, the authors wish to acknowledge the anonymous reviewers and all co-workers for their helpful comments.

REFERENCES

[1] M. Yilmaz and P. T. Krein. Review of the Impact of Vehicle-to-Grid Technologies on Distribution Systems and Utility Interfaces. IEEE Transactions on Power Electronics, Vol. 28, No. 12, 2013, pp. 5673-5689.

[2] Liu, K. T. Chau, D. Wu, and S. Gao. Opportunities and Challenges of Vehicle-to-Home, Vehicle-to-Vehicle, and Vehicle-to-Grid Technologies. Proceedings of the IEEE, [online] http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=6571224.

[3] J. Liu, Y. Xiao, S. Li, W. Liang, and C. Chen. Cyber Security and Privacy Issues in Smart Grids. IEEE Commun. Surveys Tuts. Vol. 14, No. 4, 2012, pp. 981-997.

[4] H. Chaudhry and T. Bohn. Security Concerns of a Plug-in Vehicle. Innovative Smart Grid Technologies (ISGT), 2012 IEEE PES. IEEE, 2012, pp. 1-6.

[5] Z. Yang, S. Yu, and C. Liu. P2: Privacy-preserving Communication and Precise Reward Architecture for V2G Networks in Smart grid. IEEE Trans. Smart Grid, Vol. 2, No. 4, 2011, pp. 697-706.

[6] Nicanfar, H.; Hosseininezhad, S.; TalebiFard, P.; Leung, V.C.M. Robust Privacy-preserving Authentication Scheme for Communication Between Electric Vehicle as Power Energy Storage and Power Stations. Proceedings of the IEEE INFOCOM, Turin, Italy, 14-19 April 2013; pp. 3429-3434.

[7] Asmaa Abdallah and Xuemin (Sherman) Shen Lightweight Authentication and Privacy-Preserving, IEEE Transactions on Vehicular Technology, Vol. 66, No. 3, 2017, pp.2615-2629.

[8] Braeken A. Efficient Anonym Smart Card Based Authentication Scheme Formulti-server Architecture. Int J Smart Home. 2015, 9(9), pp.177-184.

[9] A. Braeken Abdellah Touhafi. AAA - Autonomous Anonymous User Authentication and its Application in V2G. Concurrency and Computation: Practice and Experience 30(12), 2018.

[10] Saxena N, Choi BJ. Authentication Scheme for Flexible Charging and Discharging of Mobile Vehicles in the V2G Networks. IEEE Trans Inf Forensics Secur. 2016, 11(7), pp.1438-1452.

[11] B. Vaidya, D. Makrakis, and H. T. Mouftah. Security Mechanism for Multi-domain Vehicle-to-grid Infrastructure. in Proc. IEEE Global Telecommun. Conf. GLOBECOM 2011.

[12] CHEN Jie, ZHANG Yueyu, SU Wencong. An Anonymous Authentication Scheme for Plugin Electric Vehicles Joining to Charging/discharging Station in Vehicle-to-grid (V2G) Networks. China Communications, March 2015 pp.10-20.

[13] Binod Vaidya, Dimitrios Makrakis, Hussein T. Mouftah. Multi-domain Public key Infrastructure for Vehicle-to-Grid network. MILCOM 2015: 1572-1577.

[14] Tang Wenjian. Blockchain [M]. China Machine Press, 2016.

[15] Esther Mengelkamp, Benedikt Notheisen, Carolin Beer, David Dauer, Christof Weinhardt. A Blockchain-based Smart Grid: Towards Sustainable Local Energy Markets. Computer Science - Research and Development. Volume 33, Issue 1-2, 2018, pp 207-214.

[16] Jianbin Gao, Kwame Omono Asamoah, Emmanuel Boateng Sifah. GridMonitoring: Secured Sovereign Blockchain Based Monitoring on Smart Grid. IEEE Access (Volume: 6), 2018, pp. 9917-9925.

[17] RUIGUO YU, JIANRONG WANG, TIANYI XU, JIE GAO, YONGLI AN, GONG ZHANG, AND MEI YU. Authentication with Block-Chain Algorithm and Text Encryption Protocol in Calculation of Social Network. IEEE Access (Volume: 5) 09 November 2017, pp. 24944 -24951.

[18] Christopher Mann, Daniel Loebenberger. Two-factor Authentication for the Bitcoin Protocol. Int. J. Inf. Secur. (2017) 16, pp.213-226.

[19] ZHOU Zhicheng，LI Lixin* ，LI Zuohui. Efficient cross-domain authentication scheme based on blockchain technology[J]. Journal of Computer Applications[J], 2018, 38(2):316-320.

[20] Yuan Feng, Cheng Zhaohui. Overview on SM9 Identity-Based Cryptographic Algorithm[J]. Journal of Information Security Research, 2016, 2(11):1008-1027.

[21] Chen Zhaohui. A more secure and easy to use domestic cryptosystem -- SM9 algorithm. Infosec Spotlights，06, 2016, pp. 85-86.