Scientific Research Publishing

Int. J. Communications, Network and System Sciences, 2017, 10, 316-323
http://www.scirp.org/journal/ijcns
ISSN Online: 1913-3723
ISSN Print: 1913-3715

An Anonymous Authentication Scheme for Vehicle-to-Grid Networks

Zhongwei Sun

School of Electrical and Electronic Engineering, North China Electric Power University, Beijing, China
Email: zwsun@ncepu.edu.cn

How to cite this paper: Sun, Z.W. (2017) An Anonymous Authentication Scheme for Vehicle-to-Grid Networks. *Int. J. Communications, Network and System Sciences*, **10**, 316-323.
https://doi.org/10.4236/ijcns.2017.108B034

Received: August 7, 2017
Accepted: August 11, 2017
Published: August 14, 2017

Abstract

Vehicle to grid technology allows bidirectional energy exchange between electric vehicles and the power grid for achieving many known benefits. However, V2G networks suffer from certain security threats, such as EV's privacy and authentication problem. In this paper, we propose an anonymous group authentication scheme for V2G communications. This scheme realizes dynamic joining and revocation of EVs, and greatly reduces the overhead of EV revocation. Through the theoretical analysis, this scheme can ensure identity privacy of EV user and security of data transmission in the process of charging and discharging.

Keywords

Electric Vehicles, Vehicle to Grid, Group Signature, Anonymity Authentication

1. Introduction

Depletion of fossil fuel reserves and prominence of environment problem gives a wakeup call for finding the alternative energy sources for these sectors. Because the traditional power grid has the feature of high cost, easy to cause waste and unreliable system, and with the increasing user demand for electricity diversity, traditional power grid has already can't meet the development needs of the future [1]. However, smart grid can meet this Long-term demand. Smart grid support and encourage integration of new energy power generation system (such as wind energy, tidal power, solar power generation system), but because of the discontinuity and randomness, new energy will cause the fluctuation of power grid, so in order to smooth the fluctuations and ensure the stability of power grid voltage and frequency, smart grid need other auxiliary system as a compensation of new energy system. Vehicle to grid can be used as a buffer of new energy.

Vehicle to grid technology allows bidirectional energy exchange between electric vehicles and the power grid under the unified dispatch and control of power grid, and it is an integral part of the smart Grid. The core idea of V2G is using the storage energy of a large number of EV as a buffer of power Grid and new energy. When the power load is high, EV will feedback the surplus electricity to the power grid, and when the load is low, a large number of EV battery pack can be used to store excess power grid electricity. In this way, the V2G technology not only can be used as a buffer of new energy, but also play the role of peak shifting. Advantages of V2G: 1) using EV as a power grid buffer, and providing ancillary services for power grid, such as peak shaving, spinning reserve, reactive power compensation, etc., 2) providing EV owners with an extra income, and offsetting part of the cost to buy electric cars, which is conducive to the popularization of clean vehicles, 3) increasing power grid stability and reliability, and reducing the power system operating costs [2].

The V2G communications infrastructure can facilitate better power load management, and hence improve energy efficiency and reliability. However, the infrastructure may suffer from severe security attacks and vulnerabilities. In the literature, there are only a few studies on privacy and security issues in V2G networks, although several studies have been performed to enhance security and preserve privacy in the smart grid in general. H. R. Tseng *et al.* [3] noticed the privacy concerns created by EV owners' identity information leakage. They utilized a restrictive partially blind signature to protect the identities of the owners. The protocol has been proven to preserve identity and location privacy, and to achieve data confidentiality and integrity. Yang *et al.* [4] identified the emerging privacy issues in V2G networks, and secure communication architecture was built to achieve privacy-preserving EV monitoring, in which an ID-based blind signature was introduced to enhance anonymity. References [3] and [4] based on the blind signature to ensure the safety of the electric car users' privacy information, but blind signature algorithm is very complex, and it will bring huge delays to identity verification in V2G network. Miao He *et al.* [5] propose a privacy-preserving multi-quality charging (PMQC) scheme to evaluate the EV's attributes, and authenticate its service eligibility and generate its bill without revealing the EV's private information. This scheme reduces the delays of identity verification in references [3] and [4]. Hong Liu [6] distributes EVs into home mode and visiting mode, discusses the privacy security requirement of EVs in these two models, and designs security authentication scheme for each model. Guo *et al.* [7] proposed an authentication protocol to deal with multiple responses from a batch of vehicles. The proposed scheme introduced the concept of interval time for an aggregator verifying multiple vehicles, and the aggregator broadcasts a signed confirmation message to inform multiple vehicles using only one signature. The batch verification scheme employs a modified digital signature algorithm. Reference [8] distributed EVs into: charging, fully-charged (FC), and discharging, proposed a battery status-aware authentication scheme (BASA) to address the issue for V2G networks. References [7] [8] introduced batch authentication, which greatly reduces authentication delays of V2G. Because of pure anonymous, pseudonym technology is not a very good way to solve the security problem of vehicle privacy, and the above solutions are based on mixed scheme of anonymous technology and encryption technology, which will also bring great communication delay and computational over-head to LAG, so they are not suitable for V2G networks with a large number of users.

The remainder of paper is organized as follows: section II introduces security threats and requirement of V2G communication. Section III presents an anonymous group signature authentication scheme. Section IV shows the security analysis of our scheme. Finally, section V makes a conclusion.

2. Security Threats and Requirements of V2G Communication

V2G should follow a fundamental principle: V2G cannot reduce or damage the security of smart grid. Lu *et al.* [9] divided the threat of SG into three categories: 1) availability of communication network; 2) integrity of communication data; 3) confidentiality of communication data. These security threats are also exist in V2G. Here we present some specific V2G security threat scenarios and serious consequences.

- When V2G communication network is under attack and data have been tampered, security control center will make wrong decision, which will influence the stability of power grid and charging/discharging plan of EVs. If a wide range of communication networks are subject to this type of attack, it will lead to the entire power system run under the conditions of fault data, and bring serious threat to the safety of power grid.
- When V2G communications network is under distributed denial of service attack (DDOS), related data information will be delayed, blocked, or even damaged. PEV/PHEV charge and discharge cannot be reasonably arranged so as to adapt to the current network conditions, which is likely to aggravate the load on the grid. Users can’t get the vehicle energy state, the state power load and billing information etc. in time, and thus they cannot make full use of time-sharing electricity to charge and discharge EVs.
- Data privacy of V2G in the process of communication include: the vehicle’s location information, the user’s identity, battery type, the user’s payment information, ST process information, etc. Regardless of the privacy protection would be likely to lead to leakage of users’ personal identity and electric car location information. A malicious attacker can also deduce user’s habits (activities range of the user, and, driving path and distance information) by basing on a lot of user data, such as charging time, charging locations and charging amount information [10].
- When malicious terminal connected to the electricity grid in the form of V2G, the data of DSO can be tapped, forged and damaged, so it is needed to firstly verify identity in DSO communication network, which requires au-

thentication protocol which has efficient design and can resist various attacks to meet the needs of real-time and security of V2G communication network.

3. An Anonymous Group Authentication Scheme for V2G

Boneh's group signature has advantages of short signature and save communication bandwidth [11], here we take the group signature as cryptography foundation of the proposed scheme.

3.1. System Model

The system model is described in **Figure 1**. There are five kinds of entities involved in the architecture, including trusted authority (TA), central aggregator (CAG), local aggregator (LAG), charging/discharging station (ST), electric vehicles (EV). TA is responsible for assignment of public/private key, certificate of EV, and tracing of signature. CAG divide the recharge area into a number of LAG subsets. LAG carries out register of EV, distribute group for EV, and generates group public key and private key of group member. ST can directly monitor and communicate with each EV and send the collected monitoring data to LAG, and then provides charging or discharging service for EV.

3.2. Authentication Scheme

Boneh's [11] group signature has advantages of short signature and save communication bandwidth, so we make the group signature as cryptography foundation of this scheme.

1) System initialization

a) CAG divides itself into a number of subsets, like LAG1, LAG2, ···, and announces them in the public.

b) EV sends its identity information $\mathrm{ID}_{\mathrm{EV}}$ to TA. TA generates public/private key pair for every entity (EV, ST, LAG, and CAG). EV's public/private key pair: $pk_{EV} = H(ID_{EV})$, $sk_{EV} = s \cdot H(ID_{EV})$. LAG's public/private key pair:

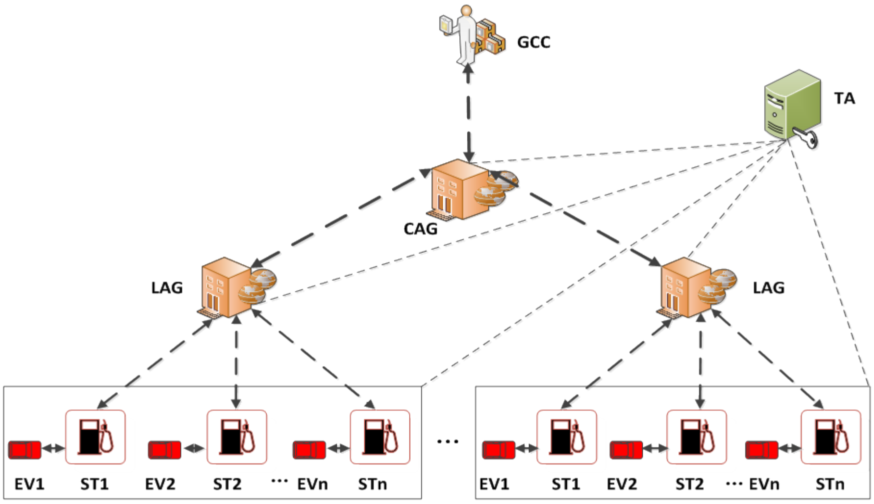


Figure 1. Centralized V2G model.

$pk_{LAG} = H\left(ID_{LAG}\right)$, $sk_{LAG} = s \cdot H\left(ID_{LAG}\right)$. S is the system key, which is only known by TA.

c) TA issues certificate $permit$ to EV, where $permit = sign_{sk_{TA}}\left(ID_{EV} \,\|\, pk_{EV}\right)$.

2) EV joins the group

EV complete register at LAG, LAG distributes a group for EV, and generates group public key and private key of group member. More specifically, when EV wants to join to V2G network via ST, EV sends message "$\mathrm{ID} \,\|\, pk_{EV} \,\|\, permit \,\|\, t$" to LAG, t is a timestamp. After verifying the validity of the certificate, LAG generate generates group public key and private key of group member according to the following steps.

a) LAG selects a generator: $g_2 \in G_2$, and set $g_1 = \varphi\left(g_2\right)$, φ is a calculation homomorphic mapping of g_1 to g_2.

b) LAG selects $\gamma \in Z_p{}^*$ at random, and sets $w = g_2{}^{\gamma}$, and announces w.

c) EV_i selects $x_i \in Z_p{}^*$ as its secret at random, and then sends this x_i to TA after encrypting it with its private key. TA computes: $A_i = g_1{}^{\frac{1}{\gamma + x_i}}$, ($\gamma + x_i \neq 0$), and sends $\left(A_i, x_i\right)$ secretly to LAG.

The group public key is $\mathrm{gpk} = \left(g_1, g_2, w\right)$, each EV_i's private key is $\mathrm{gsk}\left(i\right) = \left(A_i, x_i\right)$. The revocation token corresponding to a EV_i's key $\left(A_i, x_i\right)$ is $\mathrm{grt}\left(i\right) = A_i$. No party is allowed to possess γ, it is only known to LAG.

3) Signature computing

EV computes group signature of message M through the following steps:

a) Picking a random nonce $r \in Z_p$, and computing $\left(\hat{u}, \hat{v}\right) = H_0\left(gpk, M, r\right) \in G_2{}^2$;

b) Computing $u = \varphi\left(\hat{u}\right), v = \varphi\left(\hat{v}\right)$;

c) Selecting $\alpha \in Z_p$ at random, and compute $T_1 = u^{\alpha}, T_2 = A_i v^{\alpha}$;

d) Setting $\delta = x_i \alpha$;

e) Picking blinding values: $r_\alpha, r_x, r_\delta \in Z_p$, and compute R_1, R_2, R_3, where

$$R_1 = u^{r_\alpha}, \quad R_2 = e\left(T_2, g_2\right)^{r_x} \cdot e\left(v, w\right)^{-r_\alpha} \cdot e\left(v, g_2\right)^{-r_\delta}, \quad R_3 = T_1^{r_x} \cdot u^{-r_\delta};$$

f) Computing a challenge value $c = H\left(gpk, M, r, T_1, T_2, R_1, R_2, R_3\right) \in Z_p$;

g) Computing $S_\alpha = r_\alpha + c\alpha, S_x = r_x + cx_i, S_\delta = r_\delta + c\delta \in Z_p$;

h) Outputting signature $\delta = \left(r, T_1, T_2, c, S_\alpha, S_x, S_\delta\right)$, and EV sends $gpk \,\|\, \delta \,\|\, M$ to ST.

4) Signature verification

When receiving $gpk \,\|\, \delta \,\|\, M$, ST_i verifies the signiture according to the following steps:

a) Computing $\left(\hat{u}, \hat{v}\right) = H_0\left(gpk, M, r\right) \in G_2{}^2$;

b) Computing

$$R_1{}' = \frac{u^{S_\alpha}}{T_1^c},$$

$$R_2{}' = e\left(T_2, g_2\right)^{S_x} \cdot e\left(v, w\right)^{-S_\alpha} \cdot e\left(v, g_2\right)^{-S_\delta} \cdot \left(e\left(T_2, w\right) / e\left(g_1, g_2\right)\right)^c$$

$$R_3{}' = T_1^{S_x} u^{-S_\delta};$$

c) Checking if the challenge c is correct.

$$c' = H\left(gpk, M, r, T_1, T_2, R_1', R_2', R_3'\right).$$

If it is, the signature is verified, and ST_i makes revocation check, *i.e.* for each element $A_i \in RL$, ST_i checks whether A_i is encoded in $\left(T_1, T_2\right)$, by $e\left(T_2 / A_i, \hat{u}\right) = e\left(T_1, \hat{v}\right)$. If no element of RL is encoded in $\left(T_1, T_2\right)$, EV_i has not been revoked.

The overall process is shown in **Figure 2**.

3.3. Batch Authentication

Batch validation method can judge whether the signature collection contains invalid signature, thus reduce the verification time. When large-scale EVs connect to power grid, it is needed to use batch authentication to reduce verification time.

Let $\delta_i = (r_i, T_{i,1}, T_{i,2}, c_i, S_{i,\alpha}, S_{i,x}, S_{i,\delta})$, after ST received collection of messages M_i and signatures δ_i, it verifies the signature collection using batch authentication by

1) Computing $c_i = H\left(gpk, M_i, r_i, T_{i,1}, T_{i,2}, R_{i,1}, R_{i,2}, R_{i,3}\right)$;

2) Checking $u^{S_{i,\alpha}} = R_{i,1} \cdot T_{i,1}{}^{c_i}, T_{i,1}{}^{S_{i,x}} = R_{i,3} \cdot u^{S_{i,\delta}}$, If equality holds, continue. Otherwise, return "false";

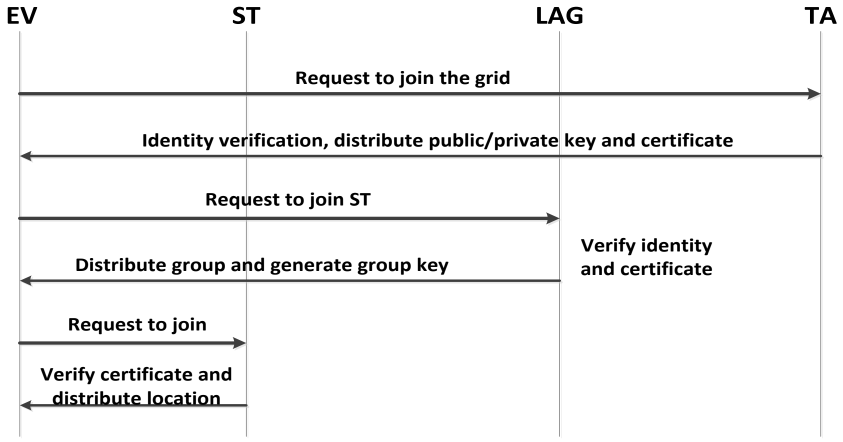
3) Select *n* numbers (the length is *b*): $\lambda_1, \lambda_2, \cdots, \lambda_n \in Z_p^*$, checking:

$$\prod_{i=1}^{n} R_{i,2}{}^{\lambda_i} = e(\prod_{i=1}^{n} (T_{i,2}{}^{S_{i,x}} v_i{}^{-S_{i,\alpha}} g_1{}^{-c_i}), g_2) e(\prod_{i=1}^{n} (v_i{}^{-S_{i,\alpha}} T_2{}^{c_i}, w)).$$

If it is, return "true". Otherwise, return "false".

4. Security Analysis

Firstly, LAG, TA or malicious EV cannot fake other entities to generate group signature, so this scheme has strong unforgeability. For example, suppose a malicious EV has forged a signature $\delta = (r, T_1, T_2, c, S_\alpha\ S_x\ S_\delta$. However, ST will compute c' and check whether c' is equal to c signature scheme. If the signature is forged, it cannot pass the verification process.



EV
ST
LAG
TA
Request to join the grid
Identity verification, distribute public/private key and certificate
Request to join ST
Verify identity and certificate
Distribute group and generate group key
Request to join
Verify certificate and distribute location

Figure 2. Vehicle to grid schematic diagram.

Secondly, it is not feasible for other entities to determine the vehicle status according to the result of group signature. Other group members only know group public key $\text{gpk} = (g_1, g_2, w)$, but they do not know private key $\text{gsk}(i) = (A_i, x_i)$ of each group member. Although everyone can verify each signature is generated by group member, they cannot confirm who is signer. And only LAG can open the signature to confirm the identity of the signer. So our scheme has strong anonymity, and it can ensure that the identity information of EV user cannot be leaked. So this scheme has the characteristics of anonymity.

Thirdly, due to the unforgeability of this group signature, only group members can generate valid group signature. Moreover, this scheme use Hash function, and it is not feasible that outside attackers want to get EV's private key through collecting common parameters to compute inverse operation of Hash function. So, our scheme can resist outside attack and protect data security of EV users.

5. Conclusion

This paper has proposed an anonymous group authentication scheme based on revocable group signature in view that EVs are frequently join and leave from ST, in which the signature scheme is dynamic, and EVs can dynamically join and withdraw. Algorithm overhead is essentially same with ordinary group signature algorithm. ST only need to add the vehicle information to revocation list RL when EV logs out ST, and other EVs can anonymously prove that they are not revocable group members. Besides, this scheme solves the problem that ST revocation management is complicated.

References

[1] Wang, X. (2011) The Bottleneck Problems and Countermeasures of Current EVs' Development. *Energy Technology Economy*, **23**, 1-5.

[2] Liu, X., Zhang, Q. and Cui, S. (2012) Vehicle to Grid Review. *Transactions of China Electro-Technical Society*, **27**, 121-127.

[3] Tseng, H.R. (2012) A Secure and Privacy-Preserving Communication Protocol for V2G Networks. *IEEE Wireless Communications and Networking Conference* (*WCNC*), Shanghai, 1-4 April 2012, 2706-2711. https://doi.org/10.1109/WCNC.2012.6214259

[4] Yang, Z., Yu, S., Lou, W. and Liu, C. (2012) P2: Privacy-Preserving Communication and Precise Reward Architecture for V2G Networks in Smart Grid. *IEEE Trans. Smart Grid*, **2**, 697-706. https://doi.org/10.1109/TSG.2011.2140343

[5] He, M., Zhang, K. and Shen, X.M. (2014) PMQC: A Privacy-Preserving Multi-Quality Charging Scheme in V2G Network. *IEEE Global Communications Conference*, Austin, 8-12 December 2014, 675-680. https://doi.org/10.1109/GLOCOM.2014.7036885

[6] Liu, H., Ning, H.S., Zhang, Y. and Yang, L.T. (2012) Aggregated-Proofs Based Privacy Preserving Authentication for V2G Networks in the Smart Grid. *IEEE Transactions on Smart Grid*, **3**, 1722-1733. https://doi.org/10.1109/TSG.2012.2212730

[7] Guo, H., Wu, Y., Bao, F., Chen, H. and Ma, M. (2012) UBAPV2G: A Unique Batch Authentication Protocol for Vehicle-to-Grid Communications. *IEEE Transactions*

on Smart Grid, **2**, 707-714. https://doi.org/10.1109/TSG.2011.2168243

[8] Liu, H., Ning, H.S., Zhang, Y. and Guizani, M. (2013) Battery Status-Aware Authentication Scheme for V2G Networks in Smart Grid. *IEEE Transactions on Smart Grid*, **4**, 99-110. https://doi.org/10.1109/TSG.2012.2224387

[9] Lu, Z., Lu, X. and Wang, W. (2010) Review and Evaluation of Security Threats on the Communication Networks in the Smart Grid. *IEEE Military Communications Conference*, Sa Jose Convention Center, CA, 31 October-3 November 2010, 1830-1835. https://doi.org/10.1109/MILCOM.2010.5679551

[10] McDaniel, P. (2009) McLaughlin S. Security and Privacy Challenges in the Smart Grid. *IEEE Security & Privacy Magazine*, **7**, 75-77. https://doi.org/10.1109/MSP.2009.76

[11] Boneh, D., Boyen, X. and Shacham, H. (2004) Short Group Signatures. *Proc. of Advances in Cryptology*, Vol. 3152, Springer-Verlag, Berlin, 41-55. https://doi.org/10.1007/978-3-540-28628-8_3