Advances in Computer, Signals and Systems (2023)
Clausius Scientific Press, Canada

DOI: 10.23977/acss.2023.070215
ISSN 2371-8838 Vol. 7 Num. 2

A Conditional Privacy-Preserving Authentication Scheme for Electricity Transaction in V2G Network

Baoyi Wang[a,*], Xue Guo[b], Shaomin Zhang[c]

School of Control and Computer Engineering, North China Electric Power University, Baoding, Hebei, 071003, China
[a]wangbaoyi@126.com, [b]guoxue7620@163.com, [c]zhangshaomin@126.com
[*]Corresponding author

Keywords: V2G, electricity transaction, authentication, conditional privacy

Abstract: The charging/discharging behavior of Electric Vehicle (EV) will naturally generate two-way electricity transactions between EV user and charging operator. Before electricity transaction, EV and Vehicle to Grid (V2G) network need to be mutually authenticated. However, wireless communication technology is usually adopted in V2G network, which easily leaks the privacy of EV user. Therefore, a conditional privacy-preserving authentication and key agreement scheme for electricity transaction in V2G network is proposed. In this scheme, the anonymity of EV user is guaranteed, and the true identity of EV user can be tracked when a transaction dispute occurs, which guarantees conditional privacy.

1. Introduction

Power grid and EV are connected in V2G network to realize the bidirectional transmission of electrical energy and data [1]. EV is used as distributed energy storage device in V2G network [2]. EV user can buy electrical energy from power grid to charge EV at low valley time, and sell electrical energy stored by EV to power grid at peak time, so as to mitigate the influence of renewable energy on power grid and realize the effect of “shaving peak and filling valley”. To conduct electricity transaction, EV and V2G network must first authenticate each other. EV user uses mobile device to send electricity transaction request to Multi-functional Aggregator (MAG). MAG authenticates the EV user. If the authentication is successful, MAG forwards the electricity transaction request to Charging Operator (CO). CO authenticates MAG and sends the electricity transaction request result along the reverse path. The electricity transaction request/request result contain many private information of EV user [3], such as EV user's identity (usually mobile phone number), location, license plate number, bank card number, etc. Since wireless communication technology is commonly adopted in V2G network, attacker can easily intercept, modify, and reuse sensitive information of EV user. After obtaining the sensitive information, attacker can analyze the workplace, home address, and living habit of EV user [4], which seriously violates the privacy of EV user. Therefore, secure mutual authentication and key agreement must be ensured between EV user and MAG and between MAG and CO to provide secure communication and protect the privacy of EV user.

In recent years, many authentication and key agreement schemes have been studied in V2G network to solve privacy issues. An authentication scheme based on hash function and elliptic curve cryptography for dynamic charging of EV is proposed in the literature [5]. User's anonymity and untraceability are guaranteed in this scheme. However, when EV user registers, the EV user does not provide real identity to trusted third party. If EV user conducts illegal operation, EV user cannot be tracked. Conditional privacy cannot be ensured in this scheme. A bilinear pairing-based group authentication protocol for V2G network is proposed in the literature [6]. Conditional privacy is guaranteed in this scheme. However, time-consuming pairing operation is used in this scheme, which leads to higher computing overhead compared to pairing-free schemes. A privacy-preserving signcryption-based authentication key agreement scheme for V2G network is designed in the literature [7]. In this scheme, charging station does not verify the identity of EV and directly forwards message to power service provider, which leads to a denial-of-service attack on the charging station easily. Therefore, in order to assure that our proposed scheme is resistant to denial-of-service attack, each entity should be authenticated before communicating. Meanwhile, in [7], only identity is considered for EV's registration, without considering password and biometric characteristic, which does not satisfy three-factor security.

To sum up, these existing V2G network authentication schemes do not simultaneously consider whether to provide conditional privacy, the level of computing efficiency, whether to resist denial-of-service attack and whether to provide three-factor security. Therefore, an authentication and key agreement scheme for electricity transaction that solves all above problems is needed.

2. Related Technology

2.1. Fuzzy Extractor

The fuzzy extractor algorithm [8] is used to generate and reconstruct biometric key. The algorithm contains two subalgorithms: Gen (·) and Rep (·).

(1) Gen (·): Gen (·) is a probabilistic generation algorithm. When user inputs biometric characteristic BIO_i, the algorithm generates a randomly extracted string of length l as the biometric key $b_i \in \{0,1\}^l$, and a public parameter α_i as the auxiliary string. In other words, Gen $(BIO_i)=(b_i, \alpha_i)$.

(2) Rep (·): Rep (·) is a deterministic reconstruction algorithm. The algorithm reconstructs the biometric key b_i based on the biometric characteristic BIO_i^* and the corresponding auxiliary string α_i, i.e., Rep $(BIO_i^*,\alpha_i) = b_i$. The hamming distance between BIO_i and BIO_i^* is less than defined fault tolerance threshold t.

2.2. Elliptic Curve Cryptography and ECDL Problem

$p>3$ is a large prime number. F_p is a finite field of order large prime q. An elliptic curve E [9] over F_p is defined as $y^2 = (x^3 + ax + b) mod\ p$, among it, $a, b \in F_p$ and $4a^3 + 27b^2 \neq 0$.

Elliptic Curve Discrete Logarithm (ECDL) problem [9]: Given a generator P of a finite cyclic group G with order of large prime q and (P, aP) for unknown $a \in Z_q^*$, it is difficult to compute a.

3. The Design Idea of the Scheme

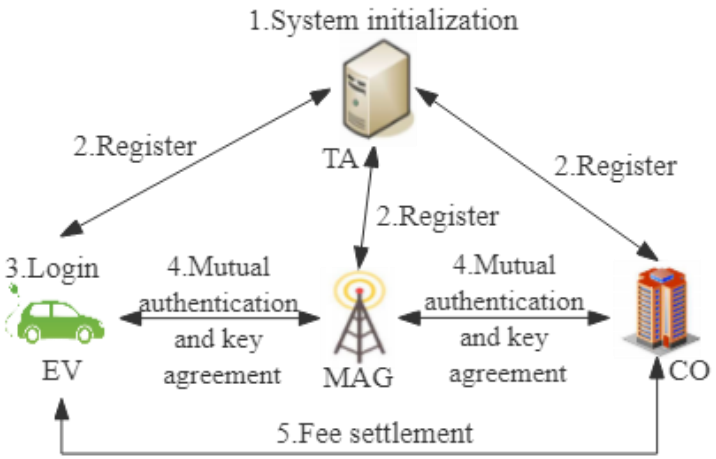

Figure 1: The process diagram of the scheme

The process diagram of the scheme is shown in Figure 1. In this paper, EV and EV user represent the same type of entity. Each entity is described as follows: (1) EV plays both charging and discharging roles in electricity transaction. (2) MAG acts as a communication intermediary to transmit identity authentication data between EV and CO through wireless communication technology and is responsible for electrical energy conversion. (3) CO sends control command, computes electricity transaction fee, etc., according to charging and discharging transaction requirements of EV. (4) Trusted Authority (TA) is responsible for managing the basic information of charging/discharging infrastructure and EV user, initializing system and publishing system parameter.

First, TA initializes the system and generates public parameter and master public/private keys. Second, EV user, MAG and CO register with TA, respectively. TA generates pseudo-identity set and private key set for EV user, and identities and private keys for MAG and CO. Third, EV user enters identity, password, and biometric characteristic into the mobile device to complete the login. Fourth, after successful login, EV user and MAG, as well as MAG and CO authenticate with each other and generate a consistent session key. Fifth, EV user and CO settle electricity bill after EV's charging and discharging are completed.

4. The Implementation of the Scheme

4.1. System Initialization

(1) TA selects a cyclic group G of order q based on elliptic curve E, where P is a generator of G.

(2) TA selects a one-way hash function: h(·)：$\{0,1\}^* \rightarrow Z_q^*$, fuzzy extractor generation function Gen (·) and reconstruction function Rep (·).

(3) TA selects master private key s$\in Z_q^*$ and computes master public key $P_{pub} = sP$. TA publishes system parameters *params* = $\{q, G, P, P_{pub}, h(\cdot), Gen(\cdot), Rep(\cdot)\}$, and secretly stores s.

4.2. Registration

(1) The registration of CO

TA sets CO's identity ID_{CO}, selects random number $r_c \in Z_q^*$ and computes: $R_c = r_c P$, $h_c = h(ID_{CO}||R_c)$, $\mathrm{SK_c} = r_c + h_c s$. TA sends message $\{ID_{CO}, R_c, \mathrm{SK_c}\}$ to CO. CO verifies whether

equation $SK_cP = R_c + h_cP_{pub}$ holds. If it holds, CO accepts private key SK_c and calculates public key $PK_c = SK_cP$. CO stores $\{SK_c\}$ in the tamper-proof device and publishes $\{ID_{CO}, R_c, PK_c\}$. TA stores $\{ID_{CO}, R_c, PK_c\}$ in the database.

(2) The registration of MAG

The registration process of MAG is the same as the registration process of CO. MAG stores $\{SK_m\}$ in the tamper-proof device and publishes $\{ID_{MAG}, R_m, PK_m\}$. TA stores $\{ID_{MAG}, R_m, PK_m\}$ in the database.

(3) The registration of EV user

EV user EVU_i inputs identity ID_i and sends registration request $\{ID_i\}$ to TA. TA checks if EVU_i is registered. If EVU_i is not registered, TA selects n random numbers $x_i \in Z_q^*$ (i=1, 2,...,n) and computes: $PID_i^1 = x_iP$, $PID_i^2 = ID_i \oplus h(x_iP_{pub})$. EV user's pseudo-identity is $PID_i = (PID_i^1, PID_i^2)$. The private key corresponding to PID_i is $SK_i = x_i + s$. The pseudo-identity set of EVU_i is $LPID_{EVU} = \{PID_1, PID_2, \ldots, PID_n\}$. The private key set of EVU_i is $LSK_{EVU} = \{SK_1, SK_2, \ldots, SK_n\}$. TA stores $\{ID_i, LPID_{EVU}, LSK_{EVU}\}$ in the database. TA sends $\{LPID_{EVU}, LSK_{EVU}\}$ to EVU_i.

EVU_i inputs password PW_i and biometric characteristic BIO_i, chooses random number $r_e \in Z_q^*$ and computes: $\mathrm{Gen}(BIO_i) = (b_i, \alpha_i)$, $V_{login} = h(ID_i||PW_i||b_i)$, $W = r_e \oplus b_i$, $\alpha_i^* = \alpha_i \oplus h(ID_i||PW_i)$, $LPID_{EVU}^* = LPID_{EVU} \oplus h(ID_i||PW_i||b_i||r_e)$, $LSK_{EVU}^* = LSK_{EVU} \oplus h(ID_i||PW_i||b_i||r_e)$. EVU_i stores $\{W, \alpha_i^*, LPID_{EVU}^*, LSK_{EVU}^*, V_{login}\}$ in the mobile device.

4.3. Login

EVU_i inputs identity ID_i, password PW_i and biometric characteristic BIO_i. Mobile device computes: $\alpha_i = \alpha_i^* \oplus h(ID_i||PW_i)$, $b_i^* = Rep(BIO_i^*, \alpha_i)$, $V_{login}' = h(ID_i||PW_i||b_i^*)$. The mobile device compares whether V_{login}' and V_{login} are equal. If they are equal, EVU_i's login is successful. Mobile device computes: $r_e = W \oplus b_i^*$, $LPID_{EVU} = LPID_{EVU}^* \oplus h(ID_i||PW_i||b_i^*||r_e)$, $LSK_{EVU} = LSK_{EVU}^* \oplus h(ID_i||PW_i||b_i^*||r_e)$. Since mobile device is equipped with GPS function, the mobile device will automatically get the information of nearby charging stations.

4.4. Authentication and Key Agreement

(1) EVU_i →MAG: $\{PID_i, sig_{EVU}, c_1, t_1, R_1\}$

EVU_i chooses pseudo-identity PID_i and private key SK_i. By operating on the mobile device, electricity transaction request $request_i$ is generated. EVU_i chooses random number $r_1 \in Z_q^*$, generates current time t_1, and computes: $R_1 = r_1P$, $c_1 = request_i \oplus h(PID_i||SK_iPK_c)$, $sig_{EVU} = r_1h(PID_i||R_1||t_1) + SK_i$, where, c_1 is the ciphertext, and sig_{EVU} is the signature of EVU_i. EVU_i sends $\{PID_i, sig_{EVU}, c_1, t_1, R_1\}$ to MAG.

(2) MAG →CO: $\{PID_i, c_1, R_1, sig_{MAG}, t_3, R_2, T_1\}$

MAG generates current time t_2 and checks transmission delay $|t_2\text{-}t_1| \leq \triangle t$. MAG checks if the equation $sig_{EVU}P = R_1h(PID_i||R_1||t_1) + PID_i^1 + P_{pub}$ holds. If it holds, MAG verifies EVU_i successfully. MAG chooses random number $r_2 \in Z_q^*$ and computes: $R_2 = r_2P$, $T_1 = r_2R_1$, $sig_{MAG} = r_2 + SK_m$, where sig_{MAG} is the signature of MAG. MAG sends $\{PID_i, c_1, R_1, sig_{MAG}, t_3, R_2, T_1\}$ to CO, where t_3 is current time.

(3) CO →MAG: $\{R_3, T_2, sig_{CO}, VSK, c_2, t_5\}$

CO generates current time t_4 and checks transmission delay $|t_4\text{-}t_3| \leq \triangle t$. CO validates if the

equation $sig_{MAG}P = R_2 + PK_m$ holds. If it holds, CO verifies MAG successfully. CO decrypts with private key SK_c: $request_i = c_1 \oplus h(PID_i||SK_c(PID_i^1 + P_{pub}))$. CO generates electricity transaction request result $response_i$ according to $request_i$. CO chooses random number $r_3 \in Z_q^*$ and computes: $R_3 = r_3 P$, $T_2 = r_3 R_1$, $sig_{CO} = r_3 + SK_c$, $\mathrm{SK} = \mathrm{h}(PID_i||\mathrm{ID_{MAG}}||\mathrm{ID_{CO}}||\mathrm{r_3T_1})$, $\mathrm{VSK} = \mathrm{h}(\mathrm{SK}||\mathrm{ID_{CO}})$, $c_2 = response_i \oplus SK$, where sig_{CO} is the signature of CO, SK is session key, c_2 is the ciphertext. CO sends $\{R_3, T_2, sig_{CO}, VSK, c_2, t_5\}$ to MAG, where t_5 is current time.

(4) MAG → EVU_i: $\{sig_{MAG}, T_3, R_2, VSK, c_2, t_7\}$

MAG generates current time t_6 and checks transmission delay $|t_6\text{-}t_5| \leq \triangle t$. MAG checks if the equation $sig_{CO}P = R_3 + PK_c$ holds. If it holds, MAG verifies CO successfully. MAG computes: $\mathrm{SK} = \mathrm{h}(PID_i||\mathrm{ID_{MAG}}||\mathrm{ID_{CO}}||\mathrm{r_2T_2})$, $\mathrm{VSK}' = \mathrm{h}(\mathrm{SK}||\mathrm{ID_{CO}})$. If $\mathrm{VSK}' = \mathrm{VSK}$, MAG generates the same session key as CO. MAG decrypts with private key SK: $response_i = c_2 \oplus SK$. MAG performs corresponding operation according to $response_i$. MAG computes: $T_3 = r_2 R_3$. MAG sends $\{sig_{MAG}, T_3, R_2, VSK, c_2, t_7\}$ to EVU_i, where t_7 is current time.

(5) EVU_i generates session key and decrypts ciphertext

EVU_i generates current time t_8 and checks transmission delay $|t_8\text{-}t_7| \leq \triangle t$. EVU_i validates if the equation $sig_{MAG}P = R_2 + PK_m$ holds. If it holds, EVU_i verifies MAG successfully. EVU_i computes: $\mathrm{SK} = \mathrm{h}(PID_i||\mathrm{ID_{MAG}}||\mathrm{ID_{CO}}||\mathrm{r_1T_3})$, $\mathrm{VSK}'' = \mathrm{h}(\mathrm{SK}||\mathrm{ID_{CO}})$. If $\mathrm{VSK}'' = \mathrm{VSK}$, EVU_i generates the same session key as MAG. EVU_i, MAG and CO generate the same session key SK. EVU_i decrypts with private key SK: $response_i = c_2 \oplus SK$.

(6) Fee settlement

When EV is charged and discharged at the specified location, EVU_i and CO use the session key SK to complete security payment.

5. Security Analysis

(1) Conditional privacy: During authentication and key agreement, EV user uses pseudo-identity to communicate with other entities. The anonymity of EV user is guaranteed when EV user performs legitimate operation. When EV user performs illegal operation, TA can trace the real identity of EV based on pseudo-identity: $ID_i = PID_i^2 \oplus h(PID_i^1 s)$. Therefore, conditional privacy is ensured in our scheme.

(2) Three-factor security: The three authentication factors are identity ID_i, password PW_i and biometric characteristic BIO_i. When EV user logs in, mobile device computes: $V_{login} = h(ID_i||PW_i||b_i)$. The biometric key b_i can be derived from biometric characteristic BIO_i. Without the correct ID_i, PW_i, and b_i, attacker cannot complete login and authentication process. Therefore, three-factor security is ensured in our scheme.

(3) Resistance to denial-of-service attack: EV user and MAG, as well as MAG and CO, authenticate each other before communicating. This authentication process can effectively prevent entities (such as EV user, MAG, and CO) from receiving a large number of fake packets sent by attacker, thus preventing entities from being subjected to denial-of-service attack.

6. Conclusion

To ensure secure communication during electricity transaction in V2G network, an authentication and key agreement scheme is proposed. Conditional privacy, three-factor security and resistance to denial-of-service attack are theoretically proved. In this scheme, elliptic curve cryptography is used without adopting time-consuming pairing operation, which brings a higher computing efficiency compared to pairing-free schemes.

References

[1] S. Aggarwal, N. Kumar, and P. Gope. An Efficient Blockchain-Based Authentication Scheme for Energy-Trading in V2G Networks [J]. IEEE Transactions on Industrial Informatics, VOL. 17, NO. 10, Pages: 6971-6980, OCT 2021.

[2] Q. Yang, D. Li, and D. An, et al. Towards Incentive for Electrical Vehicles Demand Response With Location Privacy Guaranteeing in Microgrids [J]. IEEE Transactions on Dependable and Secure Computing, VOL. 19, NO. 1, Pages: 131-148, 2022.

[3] S. M. Danish, K. Zhang, and H. -A. Jacobsen, et al. BlockEV: Efficient and Secure Charging Station Selection for Electric Vehicles [J]. IEEE Transactions on Intelligent Transportation Systems, VOL. 22, NO. 7, Pages: 4194-4211, JUL 2021.

[4] Z. Wan, T. Zhang, W. Liu, M. Wang, and L. Zhu. Decentralized Privacy-Preserving Fair Exchange Scheme for V2G Based on Blockchain [J]. IEEE Transactions on Dependable and Secure Computing, VOL. 19, NO. 4, Pages: 2442–2456, JUL 2022.

[5] P. R. Babu, R. Amin, and A. G. Reddy, et al. Robust Authentication Protocol for Dynamic Charging System of Electric Vehicles [J]. IEEE Transactions on Vehicular Technology, VOL. 70, NO. 11, Pages: 11338-11351, NOV 2021.

[6] L. F.A. Roman, P. R.L. Gondim, and J. Lloret. Pairing-based Authentication Protocol for V2G Networks in Smart Grid [J]. Ad Hoc Networks, VOL. 90, 2018.

[7] S. Ahmed, S. Shamshad, and Z. Ghaffar, et al. Signcryption Based Authenticated and Key Exchange Protocol for EI-Based V2G Environment [J]. IEEE Transactions on Smart Grid, VOL. 12, NO. 6, Pages: 5290-5298, NOV 2021.

[8] R. Vinoth, L. J. Deborah, P. Vijayakumar and N. Kumar. Secure Multifactor Authenticated Key Agreement Scheme for Industrial IoT [J]. IEEE Internet of Things Journal, VOL. 8, NO. 5, Pages: 3801-3811, MAR 2021.

[9] N. B. Gayathri, G. Thumbur, and P. Rajesh Kumar, et al. Efficient and Secure Pairing-Free Certificateless Aggregate Signature Scheme for Healthcare Wireless Medical Sensor Networks[J]. IEEE Internet of Things Journal, VOL. 6, NO. 5, Pages: 9064-9075, OCT 2019.