Journal of Artificial Intelligence Practice (2022)
Clausius Scientific Press, Canada

DOI: 10.23977/jaip.2022.050105
ISSN 2371-8412 Vol. 5 Num. 1

Lightweight Privacy-preserving Authentication Scheme in V2G that Resists Desynchronization Attack

Baoyi Wang[a,*], Xining Duan[b] and Shaomin Zhang[c]

School of Control and Computer Engineering, North China Electric Power University, China
a. wangbaoyiqj@126.com, b. 18730271008@163.com, c. zhangshaomin@126.com
**corresponding author*

Keywords: privacy protection, electric vehicle, authentication scheme

Abstract: Electric vehicles play an important role in the energy Internet, however, there is a privacy leakage problem. The use of anonymous authentication and key agreement protocols can protect the privacy of users in the process of vehicle network communication and guarantee the safe and efficient operation of the grid. In this paper, we design an anonymous authentication and key negotiation scheme under the V2G networks, which uses one-way hash function design, low computation cost and strong security of the scheme. The scheme in this paper is proven secure by Proverif tool. This scheme is resistant to desynchronization attack while remaining lightweight in terms of computational overhead and communication overhead.

1. Introduction

Electric vehicles do not produce greenhouse gases and are of great significance in terms of environmental protection and energy conservation, and electric vehicle charging and discharging are important development scenarios for the development of the energy Internet. Electric vehicles via V2G (Vehicle-to-Grid) [1] network can make the electric energy flow in both directions between the grid and electric vehicles, but expose the privacy information of electric vehicle users when performing charging and discharging. The literature [2] introduces the privacy information and problems exposed in V2G, if no effective privacy protection mechanism is adopted, attackers may be able to analyze the collected privacy information and the privacy issues such as work information, home address and economic status of EV users are inferred, interfering with the normal life of users. attackers can also disrupt the normal operation of the V2G network by forging illegal users, thus endangering the entire power system. It can be seen that protecting the privacy issues of EV users can contribute to the development of the energy Internet. Anonymous authentication technology [2], as a key technology to guarantee real-time access to data, is widely applied in V2G networks and has become a current research hotspot.

Aiming at the privacy protection problem in V2G, many scholars have studied and achieved fruitful results. In the literature [3], in order to solve the privacy protection problem in the incentive mechanism in V2G networks, identity privacy is protected using ID-based restricted blind signature technique, which achieves that the real identity of EV users cannot be connected with the certificate identity, but there are security risks in this approach. The literature [4] proposes a traceable privacy-preserving communication and exact reward scheme using unforgeability and restricted formal definitions to enhance the scheme of [3], while adding traceability to obtain the true location for finding the electric vehicle in case of theft. The authentication protocols designed in the literature [5] using bilinear pairs guarantee the confidentiality of the communication and prevent from being traced, but the schemes are computationally intensive. The literature [6] proposes a lightweight privacy-preserving authentication scheme in energy Internet-based V2G networks that can effectively protect user identity and location privacy and prove key security through security. The literature [7] analyzes the literature [6] in detail and finds the problems such as no session key authentication, unsynchronized biometric information and inability to resist replay attacks, and then improves it to keep the protocol lightweight while ensuring security. To address the lack of security in lightweight authentication protocols, the literature [8] uses Chebyshev polynomials instead of traditional hyperbolic and elliptic curve operations to reduce the computation while ensuring the security of the process, but the computation is still high compared to lightweight protocols.

In this paper, we propose a lightweight anonymous authentication and key negotiation protocol for security and privacy issues in electric vehicle charging and discharging in V2G. The protocol guarantees the security of session keys, user anonymity, forward security and resistance to desynchronization attacks while ensuring lightweight, protecting the user's private information and resisting illegal users. In this paper, the security of the protocol is guaranteed by strict security proofs. The comparison results show that this scheme has low computational consumption and low communication overhead and is suitable for V2G networks.

The rest of the paper is as follows. The second part introduces the Adversary Model of scheme. The third part establishes the electric vehicles authentication scheme. The fourth part gives the simulation experimental results. The fifth part is the summary of this paper.

2. Adversary Model

In the registration phase, each participant communicates in a secure channel, and in the user login and authentication phases, each participant communicates using a public channel with security risks. In this case, the Dolev-Yao threat model (DY model) is used in this paper. The following assumptions are made.

- An attacker can eavesdrop on messages on the public channel without the knowledge of each participant.
- The attacker can intercept and store messages on the public channel.
- The attacker can forge messages.
- An attacker can send messages.
- An attacker can participate in the operation of the protocol as a legitimate entity.

3. Scheme Design

3.1. Design Ideas

Before electric vehicles are charging or discharging, the V2G network is secured by mutual verification between charging stations and the grid. The charging service provider is responsible for building the charging stations, and each charging station is registered with the charging service provider. Each electric vehicle is first registered with the charging service provider. Since EVs use public open networks when communicating, they are vulnerable to receive attacks, such as replay attacks, counterfeit attacks, man-in-the-middle attacks and de-synchronization attacks, which lead to user privacy leakage and also affect the stable operation of the power grid. Therefore, before charging and discharging, anonymous authentication is conducted between EVs and charging stations and charging service providers in a three-way process to create a secure session key.

3.2. Scheme model

Charging Service Provider (CSP): In order to facilitate the management and control of electric energy of electric vehicles, the electric vehicle charging business is managed separately, making the charging service provider an independent unit of electricity consumption. Users can charge directly from the charging service provider, which builds charging stations and charging piles. The charging stations are dispatched in such a way that the settlement of electricity charges is settled separately in the power trading center.

Charging Station: The charging stations are widely distributed and each station has a box transformer and several charging piles. The charging piles are equipped with a power conversion unit, a communication unit and a meter (for measuring the electric vehicle charging power of the customer and for settlement with the customer).

Electric Vehicles (EV): Electric vehicles, including pure electric drive and plug-in hybrid vehicles, play an important role in the energy Internet. Each electric vehicle is equipped with a computing unit with limited computing power.

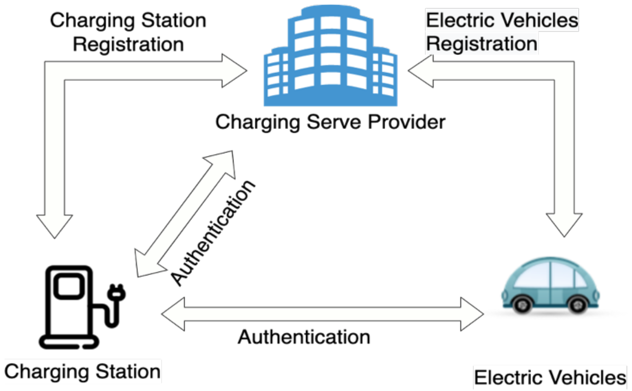


Figure 1: Electric vehicle certification schematic.

4. Scheme Implementation

4.1. Registration Stage

Step1: User U_i set their own identity ID_i and password PW_i and then U_i Generate a random number a_i and calculate: $A_i = h(ID_i \parallel PW_i \parallel a_i)$, where $h()$ is the collision-resistant hash function set by the CSP. Then the$\{ID_i, A_i\}$ is send to the CSP.

Step2: The CSP receives the registration request from the user and selects MSK as the master key and generates two random numbers b_i and K_{GU}. The CSP set the synchronization parameters: $NU_i = NU_{i0} = 0$. CSP generates a random pseudo-identity for the user: MID_i and then calculate: $B_i = h(ID_i \parallel MSK \parallel b_i)$, $C_i = B_i \oplus A_i$, and $D_i = h(B_i \parallel A_i) mod\, n_0$, where n_0 is an integer ($2^4 \leq n_0 \leq 2^8$). CSP stores $\{ID_i,\ MID_i,\ b_i,\ K_{GU},\ NU_i\}$ into memory and stores:

$\{MID_i,\ C_i,\ D_i,\ K_{GU},\ NU_{i0}, h()\}$ into the smart card, and then sends the smart card to the user.

Step3: U_i receives the smart card, calculate: $W_i = h(ID_i \parallel PW_i) \oplus a_i$ and add it to the smart card. At this time, the information in the smart card is $\{MID_i,\ C_i,\ D_i,\ K_{GU},\ NU_{i0},\ W_i, h()\}$.

Step4: The charging station CS_k set their own unique identity CID_k and send it to CSP.

Step5: The CSP generates random numbers K_{GS}, then set the synchronization parameter: $NC_k = NC_{k0} = 0$, store $\{CID_k,\ K_{GS}, NC_{k0}\}$ into memory and send $\{NC_k,\ K_{GS}\}$ to the charging station CS_k.

Step6: The charging station receives the message and stores $\{NC_k,\ K_{GS}\}$into the memory.

4.2. Login and Authentication Phase

The EV user needs to authenticate anonymously with the CSP and negotiate a security key before initiating a charging or discharging request. The main steps are as follows.

Step1: Electric Vehicle Users U_i enterID_i and passwordPW_i to activate the smart card, and then calculate: $a_i^* = W_i \oplus h(ID_i \parallel PW_i)$, $A_i^* = h(ID_i \parallel PW_i \parallel a_i^*)$, $B_i^* = C_i \oplus A_i^*$, $D_i^* = h(B_i^* \parallel A_i^*) mod\, n_0$,the electric car verifies whether D_i^* is equal to D_i. If it is not equal, the login request is rejected; if it is equal, the login is successful, then the following operation is performed.

Step2: Electric Vehicle UsersU_i generate a random numberR_1 and get the current timestampT_1, then calculate$MS_1 = (R_1 \parallel CID_k) \oplus h(\ MID_i \parallel B_i \parallel K_{GU})$, $V_1 = h(R_1 \parallel ID_i \parallel B_i)$. Then Electric Vehicle Users send MESSAGE1:$\{MID_i,\ MS_1,\ V_1,\ T_1\}$ to the charging station CS_k .

Step3: Charging station CS_k receive the message and firstly verify the validity of the timestamp: $|T_1 - T_1^*| \leq \Delta T$. Then generate a random number R_2 to obtain the current timestamp T_2. Then, the charging station CS_k calculates: $MS_2 = (R_2 \parallel MS_1 \parallel MID_i) \oplus h(K_{GS} \parallel CID_k \parallel NC_{k0})$ and $V_2 = h(R_2 \parallel K_{GS} \parallel V_1)$. Then MESSAGE2:$\{CID_k,\ MS_2,\ V_2,\ T_2\}$is sent to the CSP.

Step4: Receiving the charging stationCS_k message, the CSP firstly verifies the validity of the timestamp:$|T_2 - T_2^*| \leq \Delta T$. The CSP performs the operation: $(R_2 \parallel MS_1 \parallel MID_i) = MS_2 \oplus h(K_{GS} \parallel CID_k \parallel NC_k)$, to get the user's information $\{ID_i,\ MID_i,\ b_i,\ K_{GU},\ NU_i\ \}$, and then calculates: $B_i = h(ID_i \parallel MSK \parallel b_i)$ and $(R_1 \parallel CID_k) = MS_1 \oplus h(\ MID_i \parallel B_i \parallel K_{GU})$, $V_1 = h(R_1 \parallel ID_i \parallel B_i)$. Then calculate: $V_2^* = h(R_2 \parallel K_{GS} \parallel V_1)$, and verify that $V_2^* = V_2$ is valid, if not, the session is terminated and the ID_i number of failed login attempts: $fail_n = fail_n + 1$, and record the ID_i is recorded in the chain table $fail_{List}$ in the chain table.

If the equation holds, CSP generates a random number R_3 for the user U_i, randomly generates a new identity MID_i^{new} , get the current timestamp T_3 .Then calculate: $MID_i^{new*} = h(\ MID_i \parallel B_i) \oplus MID_i^{new}$, $SK = h(R_1 \parallel R_2 \parallel R_3 \parallel ID_i \parallel CID_k \parallel ID_{CSP})$, $MS_3 = SK \oplus h(R_2 \parallel K_{GS})$, $V_3 = h(SK \parallel CID_k \parallel R_2 \parallel NC_k$, $MS_4 = SK \oplus h(R_1 \parallel K_{GU} \parallel B_i)$, $V_4 = h(SK \parallel MID_i \parallel MID_i^{new} \parallel R_1 \parallel NU_i)$, $K_{GS} = h(K_{GS} \parallel CID_k)$, $NC_k = NC_k + 1$, $K_{GU} = h(K_{GU} \parallel B_i)$, $NU_i = NU_i + 1, MID_i = MID_i^{new}$. Then CSP send MESSAGE3: $\{MS_3,\ V_3,\ NC_k,\ T_3, MID_i^{new*}, MS_4\ , V_4, NU_i\}$ to the charging stationCS_k.

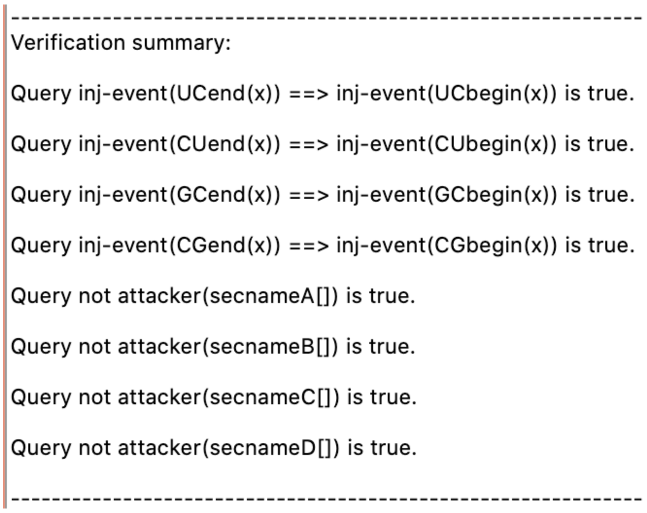
Step5: Charging station CS_k receive the message and firstly verify the validity of the timestamp: $|T_3 - T_3^*| \leq \Delta T$. Then charging station verify that the inequality holds:$1 \leq |NC_k - NC_{k0}| \leq N$, where N is the set integer, if the inequality does not hold, the session is terminated; conversely, let $K_{GS}^* = K_{GS}$ and perform$|NC_k - NC_{k0}|$ sub-operations: $K_{GS}^* = h(K_{GS}^* \parallel CID_k)$ .If it satisfies $N - 1 = 0$, then no hash operation is required. Charging stationCS_k computes:$SK = MS_3 \oplus h(R_2 \parallel KG_S)$, and $V_3^* = h(SK \parallel CID_k \parallel R_2 \parallel (NC_k - 1))$. Then, charging station verify:$V_3^* = V_3$.If not, terminate the session. Conversely, charging station CS_k updates parameters: $K_{GS} = K_{GS}^*$,$NU_{i0} = NU_{i0} + 1$ and gets the current timestamp T_4 .Charging station then send MESSAGE4:$\{MID_i^{new*}, MS_4\ , V_4, NU_i,\ T_4\}$ to the EV user U_i.

Step6: Electric Vehicle UsersU_i Receive the message and firstly verify the validity of the timestamp: $|T_4 - T_4^*| \leq \Delta T$ and verify that the inequality holds:$1 \leq |NU_i - NU_{i0}| \leq M$, where M is the set integer. If the inequality does not hold, the session is terminated. Conversely, let $K_{GU}^* = K_{GU}$ and perform$|NU_i - NU_{i0}|$ sub-operations: $K_{GU}^* = h(K_{GU}^* \parallel B_i)$, if it satisfies $M - 1 = 0$, then no hash operation is required.

Electric vehicle users U_i Calculation: $SK = MS_4 \oplus h(R_1 \parallel K_{GU} \parallel B_i)$, $MID_i^{new} = h(\ MID_i \parallel B_i) \oplus MID_i^{new*}$and $V_4 = h(K \parallel MID_i \parallel MID_i^{new} \parallel R_1 \parallel (NU_i - 1))$.Then user verifies: $V_4^* = V_4$.If not, terminate the session. Conversely, user update the parameters in the smart card:$K_{GU} = K_{GU}^*$,$NU_{i0} = NU_{i0} + 1$ and $MID_i = MID_i^*$.

5. Simulation Experimental

Proverif is an automated authentication tool for security protocols that is widely used in research work on security protocols, and this paper uses this tool to experimentally demonstrate the security of this scheme. First, two public channels are defined: ch1 and ch2, then each basic variable in the protocol is defined, and then each entity is initialized. After initialization, the protocol flow is modeled according to the protocol flow and four values are used to verify the security of the negotiated keys. The simulation results under version Proverif 1.96 are shown in Fig2.



```
--------------------------------------------------------------
Verification summary:

Query inj-event(UCend(x)) ==> inj-event(UCbegin(x)) is true.

Query inj-event(CUend(x)) ==> inj-event(CUbegin(x)) is true.

Query inj-event(GCend(x)) ==> inj-event(GCbegin(x)) is true.

Query inj-event(CGend(x)) ==> inj-event(CGbegin(x)) is true.

Query not attacker(secnameA[]) is true.

Query not attacker(secnameB[]) is true.

Query not attacker(secnameC[]) is true.

Query not attacker(secnameD[]) is true.

--------------------------------------------------------------
```

Figure 2: Simulation experimental results of the protocol.

6. Conclusion

In this paper, a lightweight anonymous authentication and key negotiation protocol is designed in a

V2G network. The protocol guarantees the security of session keys, user anonymity, forward security and resistance to desynchronization attacks while ensuring lightweight, protecting the user's private information and resisting illegal users. In this paper, the security of the protocol is guaranteed by strict security proofs. The scheme has low computational consumption and low communication overhead and is suitable for V2G networks.

References

[1] Kempton, W., Tomić, J., 2005. vehicle-to-grid power fundamentals: Calculating capacity and net revenue. journal of power sources 144, 268 Journal of Power Sources 144, 268. -279. doi:10.1016/j.jpowsour.2004.12.025

[2] Han, W., Xiao, Y., 2016. privacy preservation for V2G networks in smart grid: a survey. computer Communications 91-92, 17-28. doi:10.1016/j.comcom.2016.06.006

[3] Z. Yang, S. Yu, W. Lou, and C. Liu, "P2: Privacy-preserving communi- cation and precise reward architecture for V2G networks in smart grid, " IEEE Trans. smart Grid, vol. 2, no. 4, pp. 697-706, Dec. 2011.

[4] H. Wang, B. Qin, Q. Wu, L. Xu, and J. Domingo-Ferrer, "TPP: Traceable privacy-preserving communication and precise reward for vehicle-to grid networks in smart grids," IEEE Trans. Inf. Forensics Secur., vol. 10, no. 11, pp. 2340-2351, Nov. 2015.

[5] Roman, L.F.A., Gondim, P.R.L., Lloret, J., 2019. pairing-based authentication protocol for V2G networks in smart grid. Ad Hoc Networks 90, 101745. doi:10.1016/j.adhoc.2018.08.015

[6] P. Gope and B. Sikdar, "An Efficient Privacy-Preserving Authentication Scheme for Energy Internet-Based Vehicle-to-Grid Communication," in IEEE Transactions on Smart Grid, vol. 10, no. 6, pp. 6607-6618, Nov. 2019, doi: 10.1109/TSG.2019.2908698.

[7] A. Irshad, M. Usman, S. A. Chaudhry, H. Naqvi and M. Shafiq, "A Provably Secure and Efficient Authenticated Key Agreement Scheme for Energy Internet- Based Vehicle-to-Grid Technology Framework," in IEEE Transactions on Industry Applications, vol. 56, no. 4, pp. 4425-4435, July-Aug. 2020, doi: 10.1109/TIA.2020.2966160.

[8] D. Abbasinezhad-Mood, A. Ostad-Sharif, S. M. Mazinani and M. Nikooghadam, "Provably Secure Escrow-Less Chebyshev Chaotic Map-Based Key Agreement Protocol for Vehicle to Grid Connections With Privacy Protection," in IEEE Transactions on Industrial Informatics, vol. 16, no. 12, pp. 7287-7294, Dec. 2020, doi: 10.1109/TII.2020.2974258.