ISSN: 2710-0588 DOI: 10.29556/FSE.202105_1(2).0004

Certificateless Privacy Protection Scheme based on Fog Computing in V2G Network

Baoyi Wang*, Jiawei Ling, Shaomin Zhang

North China Electric Power University, Hebei 071000, China.

Abstract

With large-scale electric vehicles connected to the power grid, the security and operating efficiency of V2G networks are facing severe challenges. Aiming at the shortcomings of the existing V2G privacy protection schemes, this study proposes a certificateless privacy protection scheme based on fog computing in V2G network. This scheme applies the elliptic curve certificateless public key signcryption algorithm to the V2G network, avoiding the bilinear pairing operation. At the same time, we introduce the fog calculation model into the charging and discharging data transmission process to design a new V2G network architecture, and used data aggregation technology, which can effectively improve the calculation efficiency. This study compares the security and computational overhead with other existing V2G privacy protection scheme. Compared with other schemes, the security and computational efficiency of the scheme proposed in this article are better.

Keywords

V2G; Fog Computing; Elliptic Curve; Certificateless Public Key Signcryption; Data Aggregation.

1. Introduction

Smart Grid (SG) supports and encourages the access of new energy power generation systems (such as wind power, tidal energy, solar power generation systems, etc.), but the discontinuity and randomness of the new energy sources themselves will cause fluctuations in the power grid, requiring other The auxiliary system of the new energy system is used as a compensation for the new energy system to smooth the fluctuations caused to the grid and ensure the stability of the grid voltage and frequency [1]. According to the characteristics of electric vehicles with mobile distributed energy storage, V2G technology (Vehicle to Grid) provides a brand-new service for smart grids: Under the unified dispatch and control of the grid, the EV completes the two-way information flow and communication with the grid. The interaction and exchange of power flow, using a large amount of stored energy as a buffer for the grid and new energy, optimizes the balance between energy supply and demand in the smart grid [2] [21]. In addition, because electric vehicles (EV) have lower operating costs and are more environmentally friendly than traditional fuel vehicles, the number of electric vehicles on the road has increased exponentially. The "Automotive Outlook" shows that by 2030, the global sales of electric vehicles may reach 23 million, and the number of vehicles in possession exceeds 130 million.

Due to the uncertainty of charging and discharging behaviors, such as charging and discharging time, location, and power amount, the disorderly access of a large number of electric vehicles poses a threat to the security of the power grid. Generally, the service information accessed by electric vehicles in the V2G network (such as battery status, payment records, the real identity of electric vehicle users, and the current location of electric vehicles, etc.) is uploaded and shared to the cloud by the grid control center [5-8], therefore, The following security issues need to be considered in V2G: (1) If the personal information of users accessing the V2G network is leaked [15], the attacker may infer the user's lifestyle and daily behavior from the information. The three-party collection is used for some commercial purposes (for example, based on such information to speculate on user preferences, and then promote the corresponding car products or push advertisements, etc.), and in particular, it may be blackmailed by criminals. (2) If the user's permission data is leaked[19], criminals can impersonate the user to perform illegal operations. The attacker may pretend to be a legitimate user to obtain financial benefits or cause the charging process to be interrupted (free charging or obtaining real users) Ancillary service rewards). (3) If the location privacy of electric vehicles connected to the V2G network to participate in charging and discharging activities is leaked [22], the location information may be outlined by criminals to outline the movement trajectory of the electric vehicle [3], and the user's personal and property security will be being threatened. (4) If the integrity of the data generated in the V2G network is damaged [17], the power grid control center will make wrong decisions based on the data, which will affect the dispatch and operation of the entire power grid. Therefore, in order to enable users to enjoy safe charging and discharging services in a V2G environment, choosing a suitable and efficient security strategy mechanism is an urgent problem to be solved.

In addition, due to the extremely large information flow between electric vehicles and cloud servers in the V2G network, the control center in the traditional power grid system is facing heavy computing tasks, and there are problems of transmission delay and degradation of service quality [11][13]. Fortunately, a new technology called fog computing can solve the above problems. Fog computing refers to the use of fog equipment between the control center and terminal equipment to provide data storage, computing and network services. In other words, it can process part of the work in advance instead of handing over all the work to the control center. As an extension of cloud computing, fog computing has network edge computing capabilities, which can not only provide low latency and location awareness, but also improve network service quality [12][23][24].

At present, many security solutions have been proposed for V2G networks. Literature [14] uses identity-based restricted partial blind signature technology to achieve anonymous authentication between electric vehicles and the power grid. These schemes have the ability to track repeated applications for licenses, but the authentication process is more complicated. When providing services, it may even cause serious network congestion. Aiming at the problem of low access efficiency in V2G networks, literature [16] proposed a secure V2G network data sharing scheme based on membership. This scheme uses an encryption mechanism based on ciphertext policy attributes and combines fog computing to save system resources. However, this solution only discusses the secure data sharing solution from the grid control center CC to the EV user, and does not address the privacy protection solution from the EV user to the CC end. Literature [17] proposed a friendly privacy protection architecture for electric vehicles. This architecture includes an infrastructure anonymizer. The anonymizer generates a pseudonym for each vehicle to act as an interface between electric vehicles and aggregators. The pseudonym is used to replace the real ID in order to achieve the purpose of protecting one's own privacy, but this scheme cannot satisfy the non-repudiation, and it does not mention the establishment of a trusted institution to ensure the mapping from the pseudonym to the real ID. The V2G privacy protection scheme based on bilinear pairing proposed by literature [4] and literature [18] can meet the mutual authentication of communication parties and the privacy protection of EV information, but the method based on bilinear pairing has to be relatively expensive in terms of computational cost. Relatively high. Literature [20] proposed a lightweight authentication protocol for V2G to overcome the large amount of calculation using bilinear pair signcryption, but this scheme cannot prevent counterfeiting attacks and forward secrecy, and identity authentication is not Make a proof of correctness. In addition, most of the above documents adopt centralized cloud computing management methods for data transmission and processing, making the computing resources of edge devices not effectively used, and with the full deployment of smart grids in the future, the scale of data in V2G networks will continue to increase. At this time, the bandwidth resources supported by cloud computing technology will not be able to meet the needs of low-latency transmission, and will increase the risk of leaking user privacy data.

Aiming at the privacy problems in the charging and discharging phase of electric vehicles and the problems of transmission delay and service quality degradation in the grid control center facing heavy computing tasks, this paper proposes a V2G certificate-free privacy protection scheme based on fog computing. This scheme applies the elliptic curve certificateless signcryption algorithm to the charging and discharging service data transmission process and designs a new V2G network architecture, which avoids bilinear pairing calculations, uses the characteristics of elliptic curve calculations, speeds up signcryption, and guarantees It also effectively reduces the computing overhead and time of the EV user side. Secondly, we introduce the fog computing model into the V2G network, expand the network computing from the center of the grid to the edge of the network, and fully tap the local computing power, and in the fog computing model Data processing is supplemented by data aggregation technology, which can more effectively improve the quality of charging and discharging services and reduce the computational overhead of the grid control center.

2. V2G network security model of the proposed scheme

2.1. Design goals

The design goals of the charging and discharging scheme proposed in this article mainly include the following three aspects:

(1) Ensure that the communication between entities in the V2G network is secure, and the privacy of electric vehicles and their users is protected.

(2) The correctness, integrity, and confidentiality of the messages delivered during the interaction of each entity in the V2G network are guaranteed.

(3) The communication between the entities in the V2G network is efficient, and at the same time, the cost of the solution calculation is relatively low.

2.2. System model

This paper constructs a fog computing V2G network architecture suitable for smart grid data collection, processing and transmission. It consists of three levels: user layer (electric vehicle EV), fog layer, and cloud layer. In the constructed system model, the coverage area of the cloud server is divided into multiple sub-areas, each area is assigned 1 fog device, and there are multiple electric vehicle EVs in the coverage area of each fog device (each EV passes through the charging pile CP Connect with V2G system).

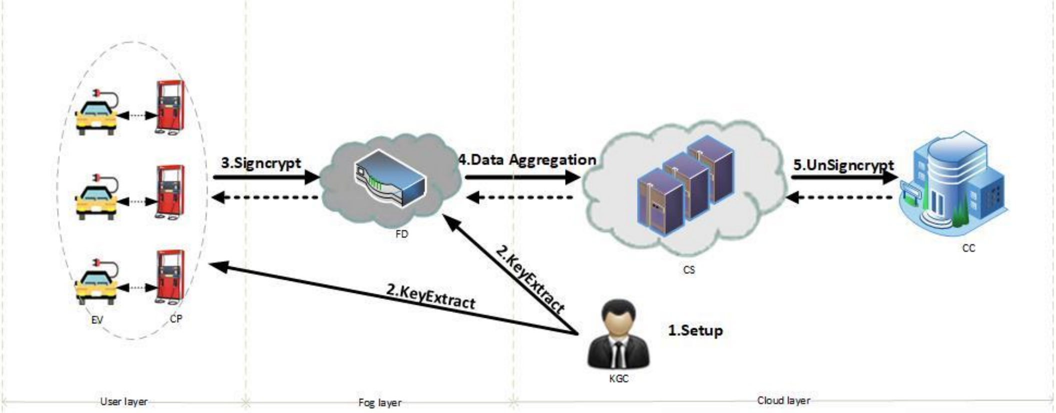

Figure 1. System model diagram

ISSN: 2710-0588 DOI: 10.29556/FSE.202105_1(2).0004

It can be seen from Figure 1 that the system model mainly includes the following six entities: Key Generation Center (KGC), Control Center (CC), Cloud Server (CS), fog device (FD), charging pile (CP), electric vehicle (EV).

(1) Key Generation Center (KGC): KGC is a completely trusted entity. It initializes the system and is mainly responsible for generating various types of keys and sending them to various entities. It has relatively powerful computing capabilities.

(2) Control Center (CC): CC is the operation center that controls the entire power grid, and is a trusted entity with a large number of information services. The power grid control center receives the aggregated data from the fog device, first verifies the aggregated ciphertext of each fog device in batches at high speed, and then decrypts to obtain the plaintext of the charging and discharging information of each electric vehicle. According to the registered user's credit status, pre-stored funds, and the amount of power required to be charged, it is determined whether to allow charging/discharging, and downloading allow charging/discharging instructions and prohibiting charging/discharging instructions.

(3) Cloud server (CS): CS is a trusted entity used to store encrypted data. The cloud server forwards the aggregated data sent by the fog node to the power grid control center through a secure channel.

(4) Fog device (FD): FD is a trusted entity deployed in charging stations and is a key part of fog computing. It is located in the middle layer between the EV user layer and the cloud layer where the grid control center is located, and is committed to fully tapping local computing capabilities . FD interacts with the electric vehicle EVs within its coverage area, and will help the grid control center complete the heavy EV identity verification and data aggregation operations of charging and discharging information. This operation not only saves cloud computing resources, but also enables EV users to realize charging and discharging services with lower latency.

(5) Charging Pile (CP): As a medium connecting electric vehicles and charging stations, CP is responsible for collecting the identity of electric vehicle users and charging/discharging information (such as actual charging power, charging/discharging time, charging/discharging process Real-time battery status information, etc.). Complete the ring signcryption of the identity of the electric vehicle user and the charging/discharging information and forward it to the fog device FD. According to the control command of the control center to allow and prohibit charging/discharging, and the battery status of the electric vehicle, the electric vehicle can be charged/charged Discharge control.

(6) Electric vehicle (EV): EV refers to a car driven by electric energy stored in a battery.

3. Proposed scheme

3.1. Setup

KGC is a fully trusted entity that guides the entire V2G system by running a setup algorithm.

(1) Choose a safety parameter k, G_q is a cyclic group on an elliptic curve with a large prime q (q > 2^k), and P, f, e, and g are generators of the group G_q.

(2) Choose a s $\in Z_q^*$ as the private key, and calculate the public key $P_{Pub} = s \cdot P$ of KGC.

(3) Design 5 hash functions: $H: \{0,1\}^* \times G_q \to Z_q^*$, $H_1: \{0,1\}^* \times G_q \times \{0,1\}^* \to Z_q^*$, $H_2: G_q^2 \times \{0,1\}^* \times \{0,1\}^* \to Z_q^*$, $H_3: \{0,1\}^* \times G_q^2 \times \{0,1\}^* \times G_q \times \{0,1\}^* \to Z_q^*$, $H_4: \{0,1\}^* \times G_q \times \{0,1\}^* \times G_q \times \{0,1\}^* \to Z_q^*$.

(4) KGC publishes the system parameter $params = \{q, G_q, P, f, e, g, P_{Pub}, H, H_1, H_2, H_3, H_4\}$ and saves its own private key s in the tamper-proof device.

ISSN: 2710-0588 DOI: 10.29556/FSE.202105_1(2).0004

3.2. KeyGeneration

The key generation process for electric vehicles and fog equipment is as follows:

3.2.1. Key generation for electric vehicles

(1) The EV user randomly selects the secret value $x_{EV} \in Z_q^*$, calculates the public parameter $X_{EV} = x_{EV}P$; and sends the identity ID_{EV} and the public parameter X_{EV} to KGC.

(2) According to the identity ID_{EV} and public parameters X_{EV} sent by the EV, KGC randomly selects the secret value $r_{EV} \in Z_q^*$, calculates $Y_{EV} = r_{EV}P$ and $y_{EV} = r_{EV} + sH_1(ID_{EV}, X_{EV}, Y_{EV})$ and returns y_{EV} and Y_{EV} to the user ID_{EV} through a secure channel;

(3) The EV user ID_{EV} verifies whether the equation $y_{EV}\mathrm{P} = Y_{EV} + Pu_{KGC}H_1(ID_{EV}, X_{EV}, Y_{EV})$ is established, and judges the validity of y_{EV} and Y_{EV}; if the above equation is established, the public and private keys of ID_{EV} are $PuK_{EV} =< X_{EV}, Y_{EV} >$ and $PrK_{EV} =< x_{EV}, y_{EV} >$ respectively, publish their own public key PuK_{EV} and keep the private key secretly PrK_{EV}.

3.2.2. Key generation for fog device

Similar to the user key generation, the fog device FD generates key pair details as follows:

(1) Assuming that the identity of the fog device FD is ID_{FD}, the secret value $x_{FD} \in Z_q^*$ is randomly selected, and the public parameter $X_{FD} = x_{FD}P$ is calculated; and the identity ID_{FD} and the public parameter X_{FD} are sent to KGC.

(2) According to the identity ID_{FD} and the public parameter X_{FD} sent by the FD, KGC randomly selects the secret value $r_{FD} \in Z_q^*$, calculates $Y_{FD} = r_{FD}P$ and $y_{FD} = r_{FD} + sH_1(ID_{FD}, X_{FD}, Y_{FD})$, and returns y_{FD} and Y_{FD} to the ID_{FD} through a secure channel;

(3) The fog device ID_{FD} verifies whether the equation $y_{FD}\mathrm{P} = Y_{FD} + Pu_{KGC}H_1(ID_{FD}, X_{FD}, Y_{FD})$ is established, and judges the validity of y_{FD} and Y_{FD}; if the above equation is established, the public and private keys of ID_{FD} are $PuK_{FD} =< X_{FD}, Y_{FD} >$ and $PrK_{FD} =< x_{FD}, y_{FD} >$ respectively, and publish their own public key PuK_{FD} and keep the private key secretly PrK_{FD}.

3.3. Signcryption

In this stage, each electric vehicle EV signcryptes the charge and discharge information, and then sends these signcryption messages to the fog device. The specific process is as follows:

(1) Randomly select the secret number a $\in Z_q^*$, and calculate $\mathrm{R} = g^a$;

(2) Calculate $h_1^{FD} = H_1(ID_{FD}, X_{FD}, Y_{FD})$, $\mathrm{V} = (X_{FD}Y_{FD}P_{Pub}^{h_1^{FD}})^a$ and $U = d(x_{EV} + y_{EV}) + af$ (where $d = H_4(ID_{EV}, m, X_{EV}, R)$, $f = H_4(ID_{EV}, m, Y_{EV}, R)$);

(3) Generate sign ciphertext $C = (m||U) \oplus H_3(V)$ and $S = a(x_{EV} + y_{EV} + h)^{-1}$;

(4) Send the sign ciphertext $\sigma = (h, S, C)$ to the fog device FD..

3.4. Data Aggregation

After receiving the ciphertext σ=(h,S,C), the fog device FD performs the following operations:

(1) Calculate $h_1^{EV} = H_1(ID_{EV}, X_{EV}, Y_{EV})$, $R' = (X_{EV}Y_{EV}P_{Pub}^{h_1^{EV}} g^h)^S$ and $\mathrm{V}' = \mathrm{R}'^{(x_{FD}+y_{FD})}$;

(2) Calculate $m||U = C \oplus H_3(V')$;

(3) Verify the equation $g^U = (X_{EV}Y_{EV}P_{Pub}^{h_1^{EV}})^{d'} R'^{f'}$ (where $d' = H_4(ID_{EV}, m, X_{EV}, R')$, $f' = H_4(ID_{EV}, m, Y_{EV}, R')$) and $h = H_2(ID_{EV}, R', C)$ is it true, if the equation is not true, discard the message ; If the equation holds, *FD_i(i=1,2,...,n)*aggregates the received *EV_j(j=1,...,l)* message m_{ij} as $C_i = f^{r_{FD}} \prod_{j=1}^{l} C_{ij}$, where

$$\begin{aligned} C_i = f^{r_{FD}} \prod_{j=1}^{l} C_{ij} = f^{r_{FD}} f^{\sum_{j=1}^{l} r_{FD}} g^{\sum_{j=1}^{l} \mathrm{m}_{ij}} h^{\sum_{j=1}^{l} r_{FD}} \\ = f^{r_{FD}+\sum_{j=1}^{l} r_{FD}} g^{\sum_{j=1}^{l} \mathrm{m}_{ij}} h^{\sum_{j=1}^{l} r_{FD}} = f^0 g^{\sum_{j=1}^{l} \mathrm{m}_{ij}} h^{\sum_{j=1}^{l} r_{FD}} = g^{\sum_{j=1}^{l} \mathrm{m}_{ij}} h^{\sum_{j=1}^{l} r_{FD}} \end{aligned} \quad (1)$$

FD_i obtains the current timestamp *t_i* and generates a signature for the aggregated data $\sigma_i = H(ID_{FDi}||C_i||t_i)^{PrK_{FD}}$. Finally, *FD_i* submits the message $\{ID_{FDi}, C_i, \sigma_i, t_i\}$ to the grid control center CC.

3.5. Decryption

When receiving the message reported by FD{FD$_1$, FD $_2$,..., FD $_n$}, CC authenticates ID_{FDi} and checks the timestamp $t_i(i=1,2,...,n)$, if one of them fails The message is discarded. Then CC performs batch verification $e(\prod_{i=1}^{n} \sigma_i , g) \overset{?}{=} \prod_{i=1}^{n} e(H(ID_{FDi}||C_i||t_i), PuK_{FD})$. If the equation does not hold, at least one message reported by FD$_i$(i=1,2,...,n) is invalid, and the grid control center CC can check $e(\sigma_i, g) \overset{?}{=} e(H\left(ID_{FDi}\middle||C_i\middle|\middle|t_i\right), PuK_{FD})(i = 1,2, \dots, n)$ An invalid message was found. On the contrary, the messages reported by FD$_i$(i=1,2,...,n) are all valid, and CC restores the plaintext information m and makes corresponding decisions.

4. Security analysis

4.1. Correctness

Theorem 1. The fog device FD can recover the original plaintext message from the ciphertext message $\sigma = (h, S, C)$, and can verify the legitimacy of the EV identity of the electric vehicle.

Proof. The ciphertext decryption process of the fog device is as follows:

(1) Calculation

$$\begin{gathered} \mathrm{V}' = (g^{x_{EV}} g^{r_{EV}} g^{sh_1^{EV}} g^h)^{S(x_{FD}+x_{FD})} \\ = g^{(x_{EV}+r_{EV}+sh_1^{EV}+\mathrm{h})\mathrm{a}(x_{EV}+y_{EV}+h)^{-1}(x_{FD}+y_{FD})} = g^{a(x_{FD}+x_{FD})} \\ \text{where, } h_1^{EV} = H_1(ID_{EV}, X_{EV}, Y_{EV}) \text{ and } y_{EV} = r_{EV} + sh_1^{EV}; \end{gathered} \tag{2}$$

(2) Calculation

$$\begin{gathered} \mathrm{V} = (g^{x_{FD}} g^{r_{FD}} g^{sh_1^{FD}})^a = g^{(x_{FD}+r_b+sh_1^{FD})a} = g^{a(x_{FD}+y_{FD})} \\ \text{where } h_1^{FD} = H_1(ID_{FD}, X_{FD}, Y_{FD}) \text{ and } y_{FD} = r_{FD} + sh_1^{FD}; \end{gathered} \tag{3}$$

(3) Therefore $\mathrm{m}||\mathrm{U} = (\mathrm{m}||\mathrm{U}) \oplus H_3(\mathrm{V}) \oplus H_3(\mathrm{V}')$, where $\mathrm{V} = \mathrm{V}'$.

Therefore, the fog device FD can restore the original communication message based on the EV public key of the electric vehicle, and at the same time verify the identity of the message sender EV. The certificate is complete.

Theorem 2. Fog device FD can verify the validity of the signature.

Proof. The verification process of the signature legality of the electric vehicle EV is as follows:

(1) Calculation

$$\begin{gathered} \mathrm{R}' = \left(X_{EV} Y_{EV} P_{Pub}^{h_1^{EV}} g^h\right)^S = \left(g^{x_{EV}} g^{r_{EV}} g^{sh_1^{EV}} g^h\right)^S \\ = g^{(x_{EV}+r_{EV}+sh_1^{EV}+h)a(x_{EV}+y_{EV}+h)^{-1}} = g^a = R \end{gathered} \tag{4}$$

(2) Calculation

$$\begin{gathered} g^U = g^{d(x_{EV}+y_{EV})+af} = g^{d(x_{EV}+y_{EV})} g^{af} = g^{d\left(x_{EV}+r_{EV}+sh_1^{EV}\right)} g^{af} \\ = \left(X_{EV} Y_{EV} P_{Pub}^{h_1^{EV}}\right)^d R^f = (X_{EV} Y_{EV} P_{Pub}^{h_1^{EV}})^{d'} R'^{f'} \end{gathered} \tag{5}$$

where $R' = R, d' = H_4(ID_{EV}, m, X_{EV}, R') = d, f' = H_4(ID_{EV}, m, Y_{EV}, R') = f$.

(3) The equation $g^U = (X_{EV} Y_{EV} P_{Pub}^{h_1^{EV}})^{d'} R'^{f'}$ and $h = H_2(ID_{EV}, R', C)$ is established.

Therefore, the fog device FD can verify the correctness of the signature, that is, the FD can complete the verification of the legality and integrity of the ciphertext σ. The certificate is complete.

4.2. Data integrity

Data integrity is an important attribute of V2G network security. It ensures that data is not destroyed or tampered with during transmission. In the first two sections, we proved the confidentiality and unforgeability between the EV user terminal and the fog device FD. At the same time, this solution can also ensure the integrity of the message data transmitted by the fog device to the grid control center CC. CC can detect Messages that have been tampered with. When the message$\{ID_{FNi}, C_i, \sigma_i, t_i\}$ reported by FD_i is received, CC can verify the integrity of the message, that is, the equation$e(\sigma_i, g) \overset{?}{=} e\left(H\left(ID_{FNi}\middle|\middle|C_i\middle|\middle|t_i\right), PuK_{FD}\right)(i = 1,2, \dots, n)$ is it true. Any tampering with the message will cause the equation to become invalid, because each part of $\{ID_{FNi}, C_i, \sigma_i, t_i\}$ involves integrity verification. Therefore, the CC can check the data integrity of the message reported by the FD.

4.3. Public verification

In the scheme of this article, when the signcryption sender EV and the ciphertext receiver FD have a dispute about the validity of the ciphertext and need to publicly verify the identity of the electric vehicle user, the receiver can send a ciphertext message $\sigma=(h,S,U,m)$ and ID_{EV} of the EV user are given to any third party. The third party does not need to send and receive any private information in ciphertext, and only needs to verify the equation $g^U = (X_{EV} Y_{EV} P_{Pub}^{h_1^S})^{d'} R'^{f'}$ and $h=H_2(ID_{EV},R',C)$ (where the parameters d', f', R'can be calculated from relevant public information) Whether If it is established, because the scheme in this paper is unforgeable, when the above equation is established, it means that the ciphertext is a legal ciphertext generated by the user ID_{EV}.

4.4. Non-repudiation

In the scheme of this article, it can be seen from the above that the scheme is unforgeable, that is, the ciphertext message is unforgeable. Therefore, if the electric vehicle EV user does generate the sign ciphertext, then the sender cannot deny it. ; At the same time, it can be known from the public verifiability that any third party can publicly verify the identity of the ciphertext sender.

4.5. Forward/backward security

In the solution in this paper, even if the attacker obtains the relevant parameters of the EV user or the fog device FD during the sending and receiving of a certain sign ciphertext, since the ciphertext generation parameters are randomly selected and have strong freshness, the attack If the attacker cannot know the previous ciphertext and related parameters, the attacker cannot know the plaintext message that has been sent; at the same time, the attacker cannot guess the sign ciphertext and related parameters that the sender is about to send, so he cannot know what to send in the future. Clear text message.

5. Performance evaluation

In this section, we use two recent V2G privacy protection schemes [18], [20] and two recent fog computing-based privacy protection schemes [23], [24] to evaluate the performance of the proposed scheme. In order to evaluate, the calculation cost is mainly considered. We tested [9] the time cost of citing encryption operations on the platform, and the test results are the same as [9]. Some data in this paper comes from this document. We give the specific time in Table 1.

In order to evaluate the computational cost of this scheme and other related schemes [23], [24], we assume that there are *n FDs* in the data aggregation scheme, and each *FD* contains *1 EV*. In the scheme of this paper, *EV* needs $2T_{e2}+T_{mp}+T_e$ to generate sign ciphertext σ. Therefore, the total computational cost of each *EV* is $2T_{e2}+Tmp+Te = 1.7968$ *ms*. Each *FD* needs $(m+1)Tp+2(m-1)Tm+mTmp$ to perform batch verification, $Te+mTm$ generates aggregated data, and *Tmp+Te* is used for the corresponding signature σi. Therefore, the total computational cost of each *FD* is $(T_p + 3T_m + T_{mp})\, l + T_p - 2T_m + 2T_e = (14.3065l + 14.3534)$ *ms*. In addition, CC needs $(n + 1)\ T_p + 2\ (n-1)T_m + nT_{mp}$ to perform batch verification. The total calculation cost of the grid control center is $(T_p + 3\ T_m + T_{mp})\ n + T_p - 3\ T_m + T_e) = 14.3065\ n + 14.0097ms$.

Table 1. Run time comparison table

Symbol	Description	Time(ms)
T_p	Bilinear pairing	13.6736
T_{e2}	Double exponentiation	0.4139
T_e	Exponentiation	0.3418
T_s	Scalar multiplication	0.2986
T_{mp}	Point mapping operation	0.6272
T_i	Cyclic group inverse operation	0.0256
T_m	Dot multiplication	0.0019

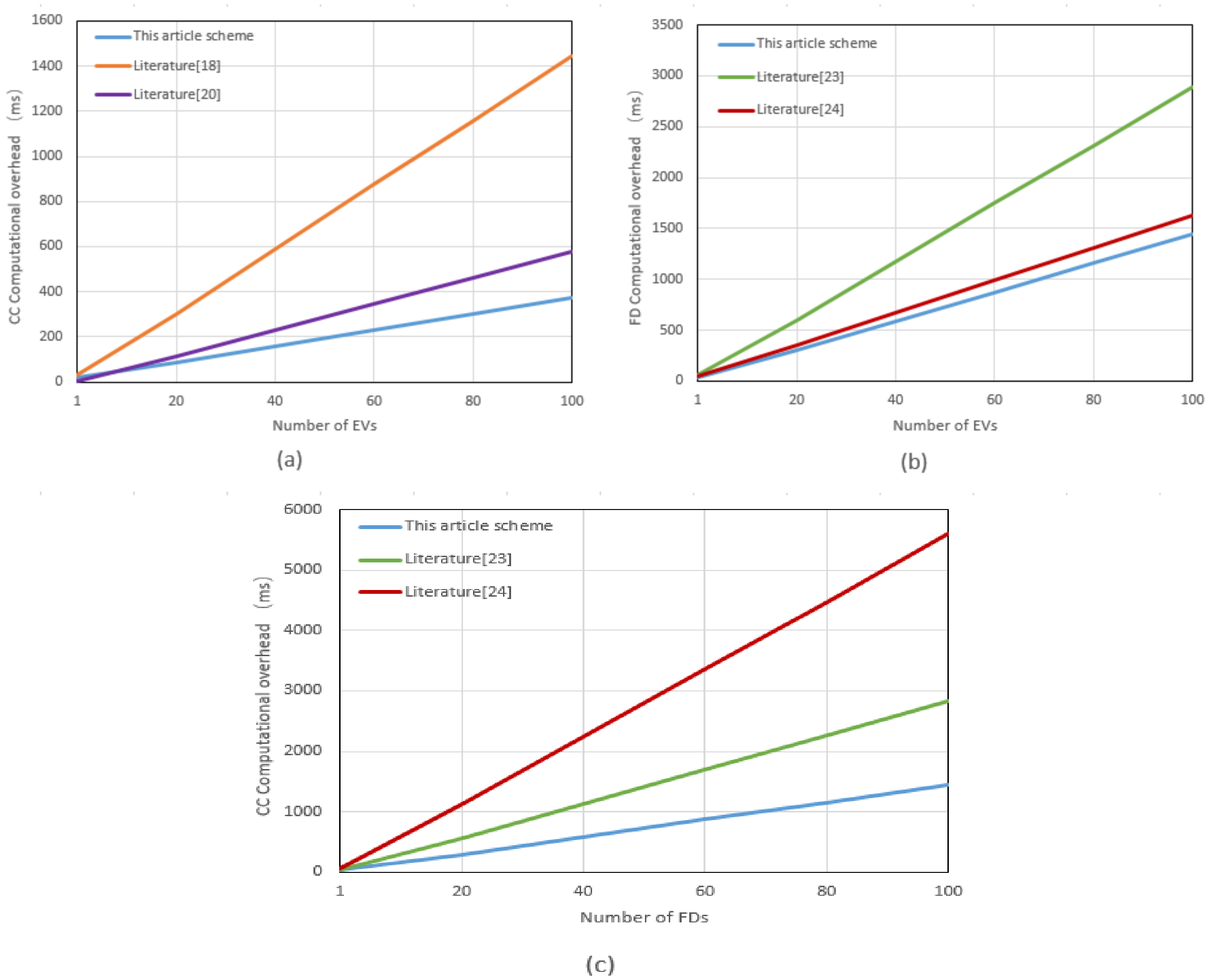

Figure 2. (a) Comparing with the calculation cost of traditional cloud computing literature control center. (b) Comparing with the calculation cost of fog equipment using fog calculation literature. (c) Comparing with the computational cost of using the fog computing literature control center

In the V2G privacy protection scheme [20], a lightweight encryption system is used, and the *EV* needs $T_s+3T_e+T_m$ to generate ciphertext *σ*. Therefore, the total computational cost of each EV is $T_s+3T_e+T_m= 1.3259$ *ms*. In addition, it takes $9lT_s+9lT_e =5.7636l$ *ms* for CC to verify the signature and recover the plaintext. As in the V2G network security scheme [18], because of the use of bilinear pairing operation, *EV* needs $3Ts+Tp$ to generate ciphertext σ. Therefore, the total computational cost of each *EV* is $3T_s+T_p = 14.5694\ ms$. In addition, it takes $(2l+11)T_s+(l+1)T_p=14.2708l+16.9582\ ms$ for CC to verify the signature and recover the plaintext. It can be seen from Figure 2.(a) that compared with the V2G data aggregation scheme that does not use fog computing [18] [20], with the increase of electric vehicle *EVs*, the calculation cost of the grid control center in this scheme is the lowest.

In the scheme using fog computing [23], *TD* (terminal device, in this case, electric vehicle *EV*) requires T_e+T_{e2} to generate ciphertext C, $T_{mp} + T_s$ to generate signature σ, and $2T_p + T_{mp}$ to verify the equation. Therefore, the total cost of TD is $T_e + T_{e2} + 2T_{mp} + T_s + 2T_p = 29.6559\ ms$. Each *FD* needs $(2T_p+T_{mp})\ l$ to verify all queries, $2T_p+lT_{mp}$ to verify the validity of the message, $2(l-1)T_m$ to aggregate the message, and $T_{mp} + T_s$ to create the signature. Therefore, the total cost of *FD* is $(2T_p + 2T_{mp} + 2T_m)\ l + 2T_p-2T_m + T_{mp} + T_s = 28.6054l + 28.2692\ ms$. CC needs $(2T_p + T_{mp} + T_e + T_i + T_m)n = 28.3437n\ ms$ to verify the message and restore the plaintext. In the same scheme that uses fog computing [24], *TD* (terminal device, in this case, electric vehicle *EV*) requires $2T_e + T_{e2} + T_{mp} + T_m = 1.7266\ ms$ to generate ciphertext and corresponding signature. FD requires $(3T_e + 3T_m + 2T_{mp} + T_p)\ l-2T_m + 2T_p$ for batch verification, and $(2l-1)T_m + 2T_e + T_{mp}$ generates aggregated ciphertext and corresponding signature. Therefore, the total computational cost of *FD* is $(3T_e+5T_m + 2T_{mp} + T_p)\ l-3T_m + 2T_p + 2T_e + T_{mp} = 15.9629l + 28.6523\ ms$. It takes $(4T_p + 2T_{mp} + 2T_m + T_i)n = 55.9782n\ ms$ for CC to verify the signature and recover the plaintext. It can be seen from the above analysis that the time cost of our scheme on *EV* encryption is in the middle, but only slightly higher than [24]. The time cost comparison results of the fog equipment *FD* side and the control center CC side are shown in Figure 2.(b) and Figure 2.(c), respectively. It can be seen from these two figures that our scheme spends the least time on *FD* and *CC* among the three schemes. As a V2G data aggregation solution, saving time in the aggregation part is very important. In summary, our scheme performs better than the four schemes compared.

6. Conclusion

In view of the shortcomings of the existing V2G privacy protection schemes and the problem of transmission delay and service quality degradation due to the heavy computing tasks of the grid control center, this paper proposes a V2G certificateless privacy protection scheme based on fog computing. This solution applies the elliptic curve certificateless public key signcryption algorithm to the V2G network, avoiding the bilinear pairing operation. At the same time, we introduce the fog calculation model into the charging and discharging data transmission process to design a new V2G network architecture. And supplemented by data aggregation technology, it can more effectively improve the quality of charging and discharging services and reduce the computational overhead of the grid control center. This paper proves the confidentiality and unforgeability of the proposed scheme based on the difficulty of discrete logarithm, and compares it with the existing privacy protection scheme in terms of computational overhead. Compared with other schemes, the proposed scheme is safe and computational Better efficiency. Therefore, this solution is more suitable for V2G networks. In the future, we will study the privacy protection of V2G networks under semi-trusted cloud and fog servers.

References

[1] Clement K, Haesen E, Driesen J. The Impact of Charging Plug-in Hybrid Electric Vehicles on the Distribution Grid[J]. IEEE Transactions on Power Systems, 2010, 25(1):371-380.

[2] Shuaib K , Barka E, Abdella JA, et al. Secure Plug-in Electric Vehicle PEV Charging in a Smart Grid Network[J]. Energies, 2017, 66(3):1-1.

[3] Wang H, Qin B, Wu Q, et al. TPP: Traceable Privacy-Preserving Communication and Precise Reward for Vehicle-to-Grid Networks in Smart Grids[J]. IEEE Transactions on Information Forensics & Security, 2015, 10(11):2340-2351.

[4] Abdallah A, Shen XM. Lightweight authentication and privacy-preserving scheme for V2G connections[J]. IEEE Transactions on Vehicular Technology, 2017, 66(3): 2615-2629.

[5] Kisung Park, Youngho Park, Ashok Kumar Das, et al. A Dynamic Privacy-Preserving Key Management Protocol for V2G in Socia l Internet of Things[J]. IEEE Access, 2019, 7: 76812-76832.

[6] Yixin Su, Gang Shen , Mingwu Zhang. A Novel Privacy-Preserving Authentication Scheme for V2G Networks[J]. IEEE Systems Journal, 2019, 1-9.

[7] Saxena N , Grijalva S , Chukwuka V , et al. Network Security and Privacy Challenges in Smart Vehicle-to-Grid[J]. IEEE Wireless Communications, 2017:2-12.

[8] Yasmine Harbi, Zibouda Aliouat, Allaoua Refoufi, et al. Enhanced authentication and key management scheme for securing data transmission in the internet of things[J]. Ad Hoc Networks, 2019,94.

[9] Wu F, Li X, Xu L, et al. Authentication Protocol for Distributed Cloud Computing: An Explanation of the Security Situations for Internet-of-Things-Enabled Devices[J]. IEEE Consumer Electronics Magazine, 2018, 7(6):38-44.

[10] Ullah I, Ul Amin N , Naeem M , et al. A Novel Provable Secured Signcryption Scheme PSSS:A Hyper-Elliptic Curve-Based Approach[J]. Mathematics, 2019, 7(8).

[11] Tao M, Ota K, Dong M. Foud: Integrating Fog and Cloud for 5G-Enabled V2G Networks[J]. IEEE Network, 2017, 31(2):8-13.

[12] Faruque M A A, Vatanparvar K. Energy Management-as-a-Service Over Fog Computing Platform[J]. IEEE Internet of Things Journal, 2015, 3(2):161-169.

[13] X. Li, S. Liu, F. Wu, S. Kumari, et al. Privacy Preserving Data Aggregation Scheme for Mobile Edge Computing Assisted IoT Applications[J]. IEEE Internet of Things Journal, 2019, 6(3): 4755-4763.

[14] Yang Z, Yu S, Lou W, et al. P2: Privacy-Preserving Communication and Precise Reward Architecture for V2G Networks in Smart Grid[J]. IEEE Transactions on Smart Grid, 2012, 2(4):697-706.

[15] Mahmoud Hashem Eiza, Qi Shi, Angelos K. Marneride. Efficient, Secure, and Privacy-Preserving PMIPv6 Protocol for V2G Networks[J].IEEE Transactions on Vehicular Technology,2019,68(1):19-33.

[16] G. Shen , Y. Su , M. Zhang. Secure and Membership-Based Data Sharing Scheme in V2G Networks[J]. IEEE Access, 2018, 6: 58450-58460.

[17] Rottondi C, Fontana S, Verticale G. A Privacy-Friendly Framework for Vehicle-to-Grid Interactions[J]. 2014.

[18] Luis F.A.Roman, Paulo R.L.Gondim, JaimeLloret. Pairing-based authentication protocol for V2G networks in smart grid[J]. Ad Hoc Networks, 2019, 90.

[19] Wan Z, Zhu W T, Wang G. PRAC: Efficient privacy protection for vehicle-to-grid communications in the smart grid[J]. Computers & Security, 2016, 62:246-256.

[20] Shen J, Zhou T, Wei F, et al. Privacy-Preserving and Lightweight Key Agreement Protocol for V2G in the Social Internet of Things[J]. IEEE Internet of Things Journal, 2017:1-1.

[21] Han, Wenlin, Xiao, Yang. Privacy preservation for V2G networks in smart grid: A survey[J]. Computer Communications, 2016, 91-92: 17-28.

[22] Ying B, Nayak A. Anonymous and Lightweight Authentication for Secure Vehicular Networks[J]. IEEE Transactions on Vehicular Technology, 2017:1-1.

[23] Wang, Huaqun, Zhiwei, et al. Anonymous and secure aggregation scheme in fog-based public cloud computing[J]. Future Generations Computer Systems Fgcs, 2018.

[24] Wang Z. An Identity-Based Data Aggregation Protocol for the Smart Grid[J]. IEEE Transactions on Industrial Informatics, 2017, 13(5):1-1.