iJETRM
International Journal of Engineering Technology Research & Management

V2G PRIVACY PROTECTION AND SECURITY RESEARCH BASED ON BLOCKCHAIN AND SM2

Zhang Nan
First Author (Department of computer, North China Electric Power University, China)

ABSTRACT
With the global energy and environmental problems becoming more and more serious today, the importance of power grid as one of the main energy systems is beyond doubt, and the V2G technology to reduce the pressure of power grid has become the focus of discussion. V2G technology refers to the electric vehicle (EV) through the access to the grid to achieve two-way exchange of power and information, and through the charging and discharging of the tram to achieve the "peak shaving and valley filling" of the grid. However, when users exchange information with the power grid, they are faced with the security risk of privacy leakage. Therefore, it is particularly important to ensure the safe and efficient access of electric vehicles to the power grid and reliable communication. In this paper, aiming at the privacy protection problem in the process of V2G communication, the following research is carried out by combining the blockchain technology, ring signature technology and encryption algorithm:
First of all, aiming at the registration of electric vehicles and the mutual authentication between electric vehicles and charging piles, we propose a method to store the relevant messages of electric vehicles on the blockchain. The encryption algorithm of the blockchain itself can ensure the security and anonymity of user information, and the charging pile can verify the effectiveness of tram identity by visiting the blockchain. In order to solve the problem of user privacy information, power grid privacy information and EV privacy information leakage in the process of mutual authentication between electric vehicle users and charging points, and avoid the shortcomings of the previous methods in the process of authentication and encryption. The tram can prove the legitimacy of its identity to the charging point without disclosing any information related to its real identity.
Then, we propose a method of combining ring signature algorithm and encryption algorithm SM2 to ensure the data security when transmitting charge and discharge information to power grid control center. Ring signature makes the user requirements hidden in a series of users. Even if the attacker intercepts and decrypts the message, it is impossible to determine which EV vehicle sent it, so as to ensure the security of transmission. Ring signature and session key k_s encryption are used in the information transmission of tram and charging pile, while ring signature and SM2 encryption are used in the transmission process of charging pile to power grid control center, which ensures the confidentiality, authenticity and integrity of information.
To sum up, we propose a new V2G privacy protection scheme based on blockchain and encryption algorithm, which solves the privacy protection problem of electric vehicle charging and discharging from two aspects of identity information privacy and data information privacy. The correctness, non repudiation, unforgeability, anonymity and confidentiality of the scheme are proved in theory. The test of related technologies shows that the scheme can meet the security and feasibility of electric vehicle communication.

Keywords:
V2G; Ring signature; Privacy protection; Blockchain; Encryption algorithm

iJETRM
International Journal of Engineering Technology Research & Management

INTRODUCTION

With the depletion of fossil fuels and the aggravation of global warming, encouraging people to use clean energy will reduce the degree of environmental pollution and operating costs. As an important part of the new energy industry, electric vehicles have been strongly supported by governments all over the world. The government has constantly issued various preferential policies to accelerate the development of electric vehicle industry. When large-scale electric vehicles are connected to the power grid, their charging and discharging behavior has a great impact on the operation of the power grid. On the one hand, we need to pay attention to some adverse effects brought by the large-scale access of electric vehicles to the power grid, such as aggravating the peak valley difference of the power grid, affecting the power quality, and reducing the reliability and economy of the distribution network; On the other hand, it can make full use of the charging load characteristics and mobile energy storage characteristics of electric vehicles to provide auxiliary services for the optimal operation of the power grid, such as balancing the grid voltage, reducing the impact of large randomness and strong volatility of renewable energy output on the power grid, and bringing certain economic benefits to the power grid and vehicle owners. As a new type of controllable load, about 90% of electric vehicles are idle in a day. The grid connected electric vehicle is not only a random load, but also a mobile energy storage unit. The electric vehicle can not only obtain electric energy from the grid, but also feedback the energy to the grid under the incentive mechanism, realizing the two-way interaction between the electric vehicle and the grid (V2G). At present, V2G (vehicle to grid) technology is gradually attracting people's attention. Through V2G technology, not only the economy of power grid is improved, but also the benefits are created for the owners of electric vehicles. At the same time, it makes a great contribution to alleviate the global climate problem.

Design background

V2G network is a double-edged sword. On the one hand, it can make users get benefits and improve the operation efficiency of smart grid; On the other hand, when V2G network collects, communicates and shares vehicle data, it also makes it easy for criminals to obtain users' privacy. The data in V2G network mainly involves the vehicle's identity, location, charging and discharging time, transaction bill and other information. The adversary can use these data to infer the user's privacy. The leakage of vehicle users' privacy not only affects the normal operation of V2G network, but also may cause serious harm to users' property and life. Generally, the following security and privacy issues need to be considered in V2G network: user privacy in V2G network is easy to be leaked in the process of vehicle charging / discharging, battery management, data communication, data management and communication protocol. Charge / discharge is the most basic service in V2G network. When carrying out the service, the vehicle must provide its valid identity to the charging point or local aggregator. Only after the identity is authenticated can the vehicle communicate with the power supply service provider and obtain the corresponding service. However, data will be continuously monitored by V2G network in charge / discharge service, which may expose sensitive information such as location and time of vehicle charge / discharge. The attacker can also analyze the action track of the vehicle by analyzing the battery status information of the vehicle, so as to infer the activity law of the vehicle owner. Data management is to collect, aggregate, store and publish these data. However, the database manager may become an attacker inside the system to attack the database to gain benefits. Therefore, how to defend against attackers inside the system is also a problem worthy of study in V2G network privacy protection.

We propose a method to store electric vehicle information on the blockchain for mutual authentication between the vehicle and the charging point. The encryption algorithm of the blockchain itself can ensure the security and anonymity of user information. In order to solve the problem of user privacy information, power grid privacy information and ev privacy information leakage in the process of mutual authentication between electric vehicle users

iJETRM
International Journal of Engineering Technology Research & Management

and charging points, and avoid the shortcomings of the previous methods in the process of authentication and encryption. Then, we propose a method of combining ring signature and SM2 to ensure the data security when transmitting charge and discharge information to the grid control center. Ring signature makes the user requirements hidden in a series of users. Even if the attacker intercepts and decrypts the message, it is impossible to determine which EV vehicle sent it, so as to ensure the security of transmission. To sum up, we solve the privacy protection problem of electric vehicle charging and discharging from two aspects of identity information privacy and data information privacy. The correctness, non repudiation, unforgeability, anonymity and confidentiality of the scheme are proved in theory, and the feasibility and effectiveness of the scheme are proved by experiments.The overall model of the system is shown in Figure 1

Design innovations

- We use the new technology of blockchain to store the information of electric vehicles in the blockchain to ensure its unchangeability. On this basis, we also carry out mutual authentication between the tram and the charging pile under the premise of anonymity.
- The ring signature technology is used to hide the tram with real demand. Even if the attacker intercepts the ring signature information, the tram with real signature cannot be found. In addition, the encryption algorithm is applied in the transmission process to ensure the security of the information.
- On the one hand, the ring signature process verifies the authenticity of the message, on the other hand, if the information is no longer complete, the signature will be destroyed, so it also verifies the integrity of the information.
- In the process of information transmission between charging point and EV, the session key k_s is updated regularly, which is combined with ring signature to ensure the security of information in this process.

Design scheme

- Vehicle identity registration and writing to blockchain: The vehicle is registered in the trusted organization Ca and obtains the blockchain certificate. The certificate format is shown in Figure 1, including the user's public key, user ID, certificate validity and version number, CA organization number, etc. The certificate is automatically generated by Ca and recorded in the blockchain. Compared with the traditional digital certificate, this certificate does not need signature and signature algorithm module. In the traditional certificate, the digital signature is verified to determine whether the certificate has been tampered, so as to ensure that the identity and public key in the digital certificate are trustworthy. However, because the blockchain data is tamper resistant, CA automatically generates a blockchain certificate and stores the hash value of the certificate in the blockchain to replace the CA's signature process on the certificate. The charging point queries the hash value of the certificate in the blockchain to replace the signature verification process of the certificate, so as to achieve the purpose of vehicle identity verification.Blockchain certificate structure is shown in Figure 2.
  In order to ensure the security of communication, before the electric vehicle is connected to the power grid, it must be certified and registered by CA. the CA verifies the personal information submitted by the vehicle. If the identity is correct, a user's real id bid, a pseudo IDt^i and the corresponding public and private keys PK and SA are generated for the vehicle. At the same time, hash operation is performed on the block chain certificate to obtain hash (bcert), Then, hash (bcert), pseudo identity t^i, public and private keys PA and Sa of the vehicle's blockchain certificate are sent to the vehicle through the secure channel, and the blockchain certificate and hash (bcert) are stored in the blockchain. After that, the blockchain will verify the validity of the certificate. If the certificate is legal, a new block is generated and broadcast to the whole network. Then the message of successful

iJETRM
International Journal of Engineering Technology Research & Management

authentication is returned to the user. At this time, the user has successfully registered. If the certificate is illegal, the user registration fails, and the vehicle cannot access the blockchain.The flow chart of user registration is shown in Figure 3.

- Mutual certification of vehicle and charging point: After the vehicle is successfully registered on the Ca, the next step is mutual authentication between the vehicle and the charging point. After the authentication, the session key between the two will be generated. The authentication process is as follows:
  1. The vehicle sends a request to the charging point, and the charging point sends a random number R1 to the vehicle after receiving the request.
  2. After receiving the response from the charging point, the vehicle uses its private key SK to sign R1, and sends the hash value of its blockchain certificate hash (bcert), R1 and the signature of R1 to the charging point as information.
  3. After receiving the message, the charging point queries hash (bcert) on the blockchain. If the status of the blockchain certificate is normal, it obtains the public key PK of the vehicle in the blockchain certificate to decrypt and verify the signature of R1. If the verification is passed, the authentication is successful.
  4. After successful authentication, the charging point will generate a session key K_s, encrypt the random number R2 with the session key, encrypt the K_s with the vehicle public key PK, and send them to the vehicle.
  5. The vehicle gets K_s through its private key decryption, and checks the validity of R2, so as to complete the authentication of charging point. After authentication, they will get their session key K_s, which can be updated periodically by setting the effective duration of K_s.

- Ring signature process: Before establishing a connection with the charging point, the EV user must first select a user EVs to signcrypt the message M on behalf of the ring member, whose pseudo identity is t^i. Let's assume that there are n members in the ring, EV = {EV1, EV2,..., EVn}. We have the private key of EVs and the public key of all users. The user EVs should perform the following operations:
  1.Firstly, the following functions are defined, in which E_k is the symmetric encryption algorithm, k is the symmetric key corresponding to E_k, the encryption of x_i using public key P_i is expressed as y_i=$g_i(x_i)$, and the decryption of y_i using private key is the inverse function of the function:

$$C_{k,v}(y_1, y_2, \cdots y_n) = E_k(\mathrm{yn} \oplus E_k(y_{n-1} \oplus E_k(\cdots \oplus E_k(\mathrm{y1} \oplus \mathrm{v}) \cdots))) = \mathrm{v}$$

  2.The key of generating symmetric encryption algorithm is k = h(m), h is the hash algorithm, m is the message to be signed, where M =$m_i||t_i$,$m_i$is the information of charge and discharge, while t_i is the pseudo identity of the user, and M is a cascade of them.
  3.Randomly select a value v.
  4.Randomly select n-1 values $\{x_1, x_2, \cdots, x_{s-1}, x_{s+1}, \cdots, x_n\}$,and they are encrypted one by one by the known public key to get y_i=$g_i(x_i)$.
  5.令$C_{k,v}(y_1, y_2, \cdots y_n)$ =v,get the y_s that makes the equation hold.
  6.We can regard y_s as encrypted by public key P_s, and we have the private key corresponding to P_s, so we can decrypt y_s to get x_s.

iJETRM
International Journal of Engineering Technology Research & Management

7.Finally, we get the ring signature of information m, which is a 2n + 1 tuple, that is($P_1, \cdots, P_n$; v ; $x_1, \cdots, x_n$) .Through this signature, we can't know that P_s really owns the private key, because we can't see the difference.

8.The vehicle encrypts the 2n + 1 tuple and the message m with the session key K_s generated before and sends it to the charging point.

Charging point uses session key K_s decrypts the tuple and message, and then verifies the ring signature:

1.Through the public key $\{P_1, \cdots, P_n\}$ Accordingly, for $\{x_1, \cdots, x_n\}$ Encrypt to get $\{ y_1, y_2, \cdots, y_n\}$

2.Symmetric key for calculating E_k,k=hash(m)

3.Verify whether the equation $C_{k,v}(y_1, y_2, \cdots y_n) = v$ is true

If the charging point passes the verification, it proves that the ring signature is credible, so the tuple and information transmitted by EV users are encrypted by SM2 encryption algorithm and then transmitted to CC through aggregator LA. If the verification fails, it is rejected.

- Encryption algorithm SM2 encryption transmission: SM2 asymmetric encryption algorithm belongs to elliptic curve cryptosystem (ECC). Based on the elliptic curve discrete logarithm problem, the current SM2256bit encryption algorithm is quite secure, which is equivalent to rsa2048bit and above. It can be divided into public key and private key: if the public key is given to others, it can be disclosed within a certain range, and the private key is left to itself, which must be kept secret. The public key can be calculated from the private key; It is quite difficult to calculate the private key from the public key, which is impossible at present.
  Let the message to be sent be bit string m (including message M and ring signature tuple), and klen be the bit length of M. In order to encrypt plaintext m, the charge point, as the encryptor, should implement the following operation steps:
  1.The random number k ∈ [1, n-1] is generated by random number generator;
  2.Calculate the elliptic curve point C1 = [k] g = (x1, Y1), ([k] g represents k * g) to convert the data type of C1 into bit string;
  3.Calculate the elliptic curve point s = [H] Pb. If s is an infinite point, report an error and exit;
  4.Calculate the elliptic curve point [k] Pb = (X2, Y2), and convert the data types of coordinates x2 and Y2 into bit strings;
  5.Calculate t = KDF (x2 // Y2, klen), if t is all zero bit string, return A1;
  6.Calculate C2 = m ⊕ T;
  7.Calculate C3 = hash (x2 // m // Y2);
  8.Output ciphertext C = C1 ‖ C2 ‖ C3.
  After the message is sent to the power grid control center step by step, the control center decrypts the message:
  1. Take out the bit string C1 from C, convert the data type of C1 to the point on the elliptic curve, verify whether C1 meets the elliptic curve equation, if not, report an error and exit;
  2. Calculate the elliptic curve point s = [H] C1. If s is an infinite point, report an error and exit;
  3. Calculate [DB] C1 = (X2, Y2), and convert the data types of coordinates x2 and Y2 into bit strings;
  4. Calculate t = KDF (x2 // Y2, klen). If t is all zero bit string, error will be reported and exit;
  5. Take out the bit string C2 from C and calculate M '= C2 ⊕ t;

iJETRM
International Journal of Engineering Technology Research & Management

6. Calculate u = hash (x2 // m ′ // Y2), and take out the bit string C3 from C, if u= C3, it will report an error and exit;
7. Output plaintext M '.

- The control center processes information and generates bills: After the CC decrypts the message, it verifies the signature. On the one hand, it confirms that the message is sent by the legal EV user. On the other hand, it confirms that the integrity of the message is not damaged in the transmission process. The verification method is the same as that of the charging point. If the verification fails, the message will be discarded. Then, the control center obtains the message M of the user EV, and according to the cascade m=$m_i \| \| t_i$. Find out the corresponding (m_i, t_i), carry out the charge and discharge instruction according to the corresponding information and generate the bill M_i of user I, and then the control center will send M_i and t_i to the CA organization through the security channel. The organization will find out the user's real identity BID according to t_i and send the bill to the user, and the user can log on the relevant website to pay or collect the bill.

Safety analysis

- Anonymity: In the authentication process, the charging point obtains the vehicle's blockchain certificate by accessing the hash value book to verify the authenticity of the vehicle. In this process, we don't know the real identity of the vehicle, which prevents the attacker from obtaining vehicle information by camouflage charging pile and has anonymity. At the same time, in the ring signature, any member in the ring is indistinguishable and may act as signer on behalf of all members in the whole ring. Even if the attacker obtains the private key of all members, the probability of guessing the right signer is no more than one in N, so it has unconditional anonymity and protects the security of user information and vehicle information.
- Unforgeability: CA is trustworthy and only transfers the private key to the vehicle itself. In addition, no one can obtain the private key, so they can not forge their identity to participate in authentication and ring signature.
- Confidentiality: In the process of authentication, both sides confirm the authenticity of each other through mutual authentication, and generate a unique session key which is updated regularly, so the communication between the tram and the charging point is confidential. In the process of transmission, the encryption algorithm SM2 is used. Theoretically, the attacker can't obtain the decryption method of SM2 from pure mathematical method. Even if the attacker gets the plaintext of the message due to extreme circumstances such as information leakage, the attacker can't determine the specific identity of the user because the user uses the pseudo identity t^i.
- Non repudiation: After obtaining the charging and discharging message and the user's pseudo identity t^i, the grid sends the generated bill to the trusted authority Ca, and then the CA finds the user's real identity and ID and sends it to the user's account. Although the authentication and message transmission process has unconditional anonymity, the final bill is still non repudiation.
- Integrity: On the one hand, the authenticity of the message is verified by ring signature, on the other hand, if the information is no longer complete, the signature will be destroyed, so the integrity of the information is verified at the same time.

Practical application

iJETRM
International Journal of Engineering Technology Research & Management

The technology of vehicle to grid (V2G) is that under the unified dispatch and control of the power grid, the electric vehicle completes the interaction and exchange of two-way information flow and power flow with the power grid. Through the advanced information and communication technology, the isolated electric vehicles are connected with the power grid, so that the electric vehicles can participate in the demand side management, and the electric vehicles can provide auxiliary services for the power grid through the infrastructure. However, electric vehicle access to the power grid is a double-edged sword, which not only provides auxiliary services for the power grid, but also brings great challenges to the privacy security of V2G network. Therefore, in order to realize the safe, reliable and orderly access of electric vehicles to the power grid, and then complete the reliable communication between them, it is very important to ensure the security of information exchange between the power grid and V2G network. This paper studies the information security of authentication and information transmission in the process of V2G. On the one hand, the combination of blockchain technology and Ca mechanism enables users to complete mutual authentication with the charging pile without disclosing their real identity, thus realizing user anonymity; On the other hand, through ring signature and SM2 encryption, the security of the message sent by the charging point to the power grid center is realized. Finally, the power grid center can restore the user's real identity and generate the bill through Ca, which is non repudiation. This research has a good application prospect, which is conducive to the application of V2G technology in real life.

Fig. 1: Overall system model

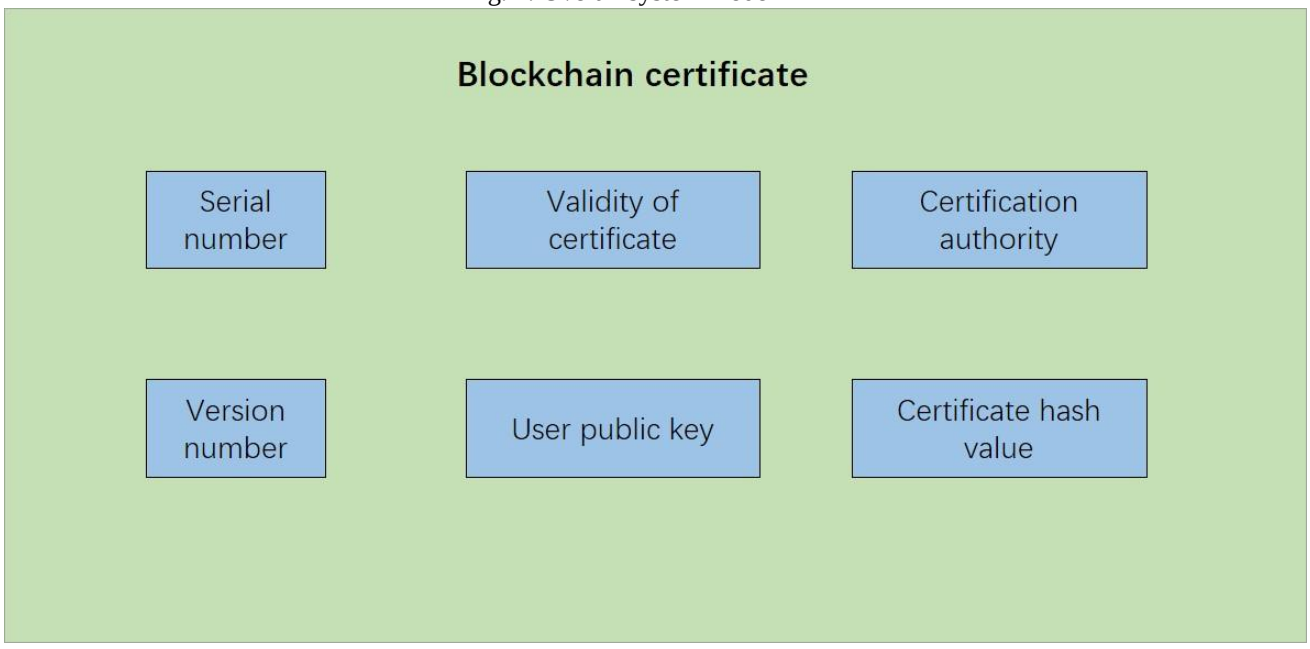

Fig. 2: Blockchain certificate structure

iJETRM
International Journal of Engineering Technology Research & Management

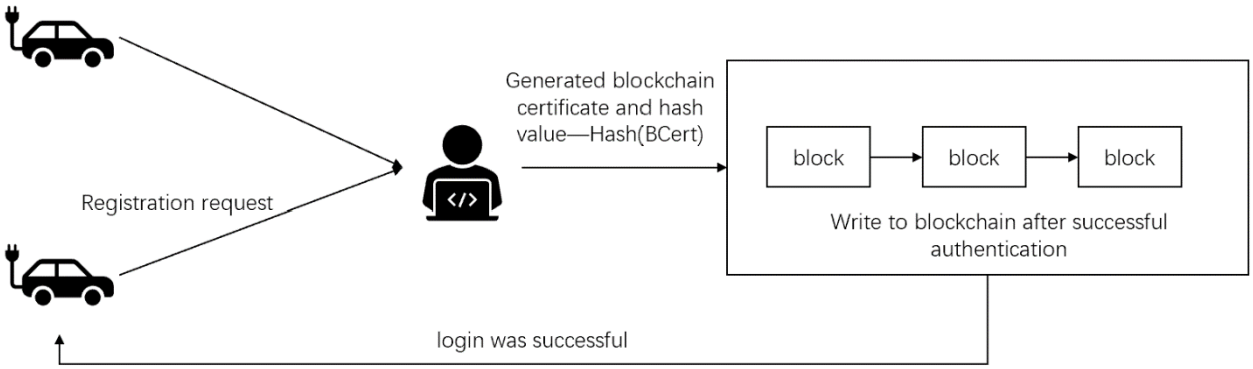

Fig. 3: User registration flow chart

METHODOLOGY

The method used in this paper is to use blockchain technology to complete the user registration, and realize the safe transmission of electric vehicle information through ring signature and SM2 encryption algorithm. With our scheme, we can realize the confidentiality, anonymity, non repudiation, non repudiation and integrity of V2G transmission process.

CONCLUSION

The technology of vehicle to grid (V2G) is that under the unified dispatch and control of the power grid, the electric vehicle completes the interaction and exchange of two-way information flow and power flow with the power grid. Through the advanced communication technology, the isolated electric vehicles are connected with the power grid, so that the electric vehicles can participate in the demand management, and provide auxiliary services for the power grid through the infrastructure, so as to achieve the purpose of "cutting peak and filling valley". Of course, this technology not only provides auxiliary services for the power grid, but also brings great challenges to the privacy and security of V2G network. In this process, the leakage of user's personal information, charging and discharging information may cause huge losses, giving attackers an opportunity. Therefore, it is very important to realize the safe and efficient access of electric vehicles to the power grid and ensure the safety of information exchange between the power grid and trams. Therefore, this paper focuses on the privacy security of electric vehicles connected to the power grid. The main tasks are as follows:

Firstly, we propose a method to store the information of electric vehicles on the blockchain for mutual authentication between vehicles and charging piles. The encryption algorithm of blockchain can ensure the security and anonymity of user information. In order to solve the problem of user privacy information, power grid privacy information and ev privacy information leakage in the process of mutual authentication between electric vehicle users and charging points, and avoid the shortcomings of the previous methods in the process of authentication and encryption. Among them, anonymous authentication has the characteristics of proving the legitimacy of one's identity to the verifier under the condition that the verifier does not disclose any information related to one's real identity, so it has become a widely used technology in privacy protection system.

Then, we propose a method of combining ring signature and SM2 to ensure the data security when transmitting charge and discharge information to the grid control center. Ring signature makes the userrequirements hidden in a series of users. Even if the attacker intercepts and decrypts the message, it is impossible to determine which EV vehicle sent it, so as to ensure the security of transmission. Ring signature and session key k_s are used in the information transmission between tram and charging

point_ The ring signature and SM2 encryption are used in the transmission process of charging pile to CC of power grid control center, which ensures the confidentiality, authenticity and integrity of information. To sum up, we solve the privacy protection problem of electric vehicle charging and discharging from two aspects of identity information privacy and data information privacy. The correctness, non repudiation, unforgeability, anonymity and confidentiality of the scheme are proved in theory, and the feasibility and effectiveness of the scheme are proved by experiments.

This paper presents a privacy protection scheme for electric vehicles in the process of V2G, which plays a certain role in the research of V2G privacy protection, but also has the following shortcomings and problems:

- The security scheme given in this paper can not be integrated into a complete system, which needs further modification and improvement.
- The security model in this paper is based on the reliability of Ca organization, and does not consider the case that the trusted structure CA is broken.
- For the charging and discharging of electric vehicles, vehicle failure or theft may occur. We also need to study how to effectively deal with and identify the invalid nodes in the ring signature, and select the normal nodes to establish the ring signature, so as to further ensure the health and safety of communication.

ACKNOWLEDGEMENT

This research is supported by North China Electric Power University. We thank the teachers from North China Electric Power University for their insights and expertise, which greatly helped the research, although they may disagree with all the conclusions of this paper. We thank Mr. ZhangShaomin for his help in technical guidance. These comments have greatly improved the manuscript.

REFERENCES

[1] Xia Zhuoqun,FangZhenwei,GuKe,WangJing,TanJingjing,WangGuanghui. Effective charging identity authentication scheme based on fog computing in V2G networks[J]. Journal of Information Security and Applications,2021,58.

[2] BibakBijan,Tekiner-MoğulkoçHatice. A comprehensive analysis of Vehicle to Grid (V2G) systems and scholarly literature on the application of such systems[J]. Renewable Energy Focus,2021,36.

iJETRM
International Journal of Engineering Technology Research & Management

[3] Jafari Mina,KavousiFardAbdollah,NiknamTaher,Avatefipour Omid. Stochastic synergies of urban transportation system and smart grid in smart cities considering V2G and V2S concepts[J]. Energy,2021,215(PB).

[4] Liu Lijun,XieFeng,HuangZonglong,WangMengqi. Multi-Objective Coordinated Optimal Allocation of DG and EVCSs Based on the V2G Mode[J]. Processes,2020,9(1).

[5] ZhonghanHao,HaoZhonghan. Research on the Topology of Wireless V2G for Electric Vehicle[J]. Journal of Physics: Conference Series,2020,1678(1).

[6] YinghuiZhang,JianZou,Rui Guo. Efficient privacy-preserving authentication for V2G networks[J]. Peer-to-Peer Networking and Applications,2020(prepublish).