Advances in Computer, Signals and Systems (2022)
Clausius Scientific Press, Canada

DOI: 10.23977/acss.2022.060105
ISSN 2371-8838 Vol. 6 Num. 1

A Privacy Preserving Scheme for Multicast Data Transmission of Electric Vehicles Based on Consortium Blockchain

Shaomin Zhang[a,*], Mingzuo Ma[b] and Baoyi Wang[c]

School of Control and Computer Engineering, North China Electric Power University, China
a. zhangshaomin@126.com, b. mamingzuo32@163.com, c. wangbaoyiqj@126.com
**corresponding author*

Keywords: electric vehicles, privacy preserving, signcryption, consortium blockchain.

Abstract: To ensure that charging service companies (CSC) can provide intelligent services to electric vehicle (EV) users, CSC needs to broadcast command information to massive electric vehicles (EVs). In the communication process, there are privacy and security issues in data transmission. Therefore, a lightweight privacy preserving scheme for multicast data transmission of electric vehicles based on consortium blockchain (CB) is proposed to solve the problems mentioned above. Our scheme designs the new lightweight certificateless multi-message and multi-receiver signcryption (CLMMSC) mechanism and CB mechanism, and can ensure the privacy of CSC broadcast command information.

1. Introduction

Traditional cars are speeding up the consumption of fossil fuels, and today society is faced with the problems of energy depletion and environmental deterioration. It has become a primary trend that the energy consumption form from fossil fuel to renewable energy. As one of the mainstream renewable energy applications, electric vehicles (EVs) have great potential in solving such problems. Therefore, Tesla, BMW, and other automobile companies are constantly studying electric vehicle (EV) technology, and are devoted to overcoming technical difficulties such as EV's data concentrator deployment, charge and discharge dispatching, and virtual network communication [1], to make EVs more secure and convenient to be used in our life.

With further research, we find that real-time data communication is crucial for EV and charging service companies (CSC). EV seeks intelligent service by uploading real-time power information to CSC, and CSC provides intelligent service for EV by broadcasting command information, to implement reasonable control and scheduling of EV [1]. In the actual deployment environment, EV users connect to the public network of the power grid (PG) through Vehicle-to-Grid (V2G) network and then conduct two-way communication and energy exchange with CSC [2]. At that time, the communication information between the two parties is vulnerable to leakage and tampering [3]. Therefore, the privacy preserving of real-time power information uploaded by EV users and command information broadcast by CSC is a problem that must be solved in the construction of EV communication networks.

With the rapid development of EVs, EVs may be widely distributed in urban and rural areas in

the future, and charging pile (CP) will also appear in large numbers in charging stations. When massive EVs are charged and discharged through CP, it will inevitably have a huge impact on the PG [4]. In addition, EV, CP, and other terminal devices have limited computing power and cannot quickly complete complex calculations [5]. Therefore, under the demand response strategy, we must design a lightweight multi-message and multi-receiver privacy preserving scheme to ensure CSC's secure and efficient broadcast command information.

Recently, with the improvement of data mining technology, the risk of the traditional centralized storage model is gradually increasing, which may encounter problems such as information leakage, single point failure, and data tampering [6]. Aim at the above problems. The PG urgently needs a secure, efficient, and distributed storage method to ensure the storage security of EV real-time power information and CSC command information [7].

In conclusion, to ensure the privacy and security of CSC broadcast command information, a privacy preserving scheme for multicast data transmission of electric vehicles based on consortium blockchain is proposed in this paper. This scheme ensures the privacy of data transmission and has high computing efficiency.

The rest of the paper is as follows: The second part introduces the basic knowledge required for the scheme. The third part introduces the scheme model in detai. The fourth part introduces the specific implementation process of the scheme. The fifth part analyzes the characteristic of the scheme. The sixth part is the summary of this paper.

2. Related Technology

2.1. Related Difficult Questions and Assumptions

Definition 1: Decision Diffie-Hellman (DDH) problem: Set the cyclic group of order q is G_q, whose generator is P, for any and unknown number $a,b \in Z_q^*$, known tuples $U_1 = (P, aP, bP, abP)$ and $U_2 = (P, aP, bP, \delta \in G)$, The goal of a DDH problem is judgment $\delta = abP$. For any probability-polynomial-time (PPT), the advantage of adversary A successfully solving DDH problems is negligible. The adversary of adversary A is expressed as :

$$Adv_A^{DDH}(k) = \left| \Pr\left[1 \leftarrow A(T_1)\right] - \Pr\left[1 \leftarrow A(T_2)\right] \right| \quad (1)$$

Definition 2: Discrete Logarithm (DL) problem: Set the cyclic group of order q is G_q, whose generator is P, for any and unknown number $a' \in Z_q^*$, known $(P, a'P) \in G$, The goal of a DDH problem is calculation a'. For any PPT, the advantage of adversary A successfully solving DL problems is negligible. The adversary of adversary A is expressed as :

$$Adv_A^{DL}(k) = \Pr\left[A(P, a'P) = a' \mid a' \in Z_q^* \right] \quad (2)$$

2.2. Certificateless Multi-message and Multi-receiver Signcryption (CLMMSC)

CLMMSC is a mechanism that broadcasts one or more messages to multiple authorized receivers after signcryption, and each receiver acquires the messages after unsigncryption with its private key [5]. CLMMSC solves the problem that multiple encryptions are required when using the traditional public key cryptography mechanism to distribute multiple messages, and realizes the sender's purpose to send messages to multiple receivers. CLMMSC is more suitable for broadcast communication than the traditional method.

2.3. Consortium Blockchain (CB)

CB is a secure, efficient, and distributed storage mechanism [6]. It is built on a certain number of pre-selected nodes, and its consensus algorithm is executed by these pre-selected nodes rather than all nodes in the network, which can significantly reduce network overhead. Besides being widely used in transactions, CB can store data and protect privacy [7]. Therefore, based on the security, high consensus efficiency, tamper-proof, and other CB characteristics, in our scheme, the CB is designed to implement CSC's secure, efficient, and distributed command information storage.

3. Scheme Design

3.1. Design Ideas

In this paper's EV privacy persevering scheme, when massive EVs are connected to CP, CSC needs to broadcast command information to provide intelligent service for EV users. The CSC generates ciphertext for multiple command informations through the signcryption algorithm and sends the ciphertext to the charging station gateway (CSS) through key generation center (KGC). After verifying the ciphertext's validity, the CSS sends the ciphertext to the CP for EV connections and CSS primary node. After that, the CSS primary node generates new blocks and achieves a consensus, publishing the new block to the CB. CP receives the ciphertext and obtains the EV user's command information through the unsigncryption algorithm. Finally, CP dispatches electric energy according to the control information and charges EV users according to the billing information. In this process, the attacker cannot decrypt the information received by the CP, all CP cannot know the information about other CP except their own, and only the CP authorized by CSC can decrypt. In this way, EV user's privacy is protected in our scheme, which is the design idea of our scheme.

3.2. Scheme Model

Combined with the privacy preserving framework in [8]. An EV privacy preserving framework is designed in this scheme composed of EV, CP, CSS, CB, KGC and CSC, as shown in Fig. 1.

3.3. Scheme Implementation Process

In our scheme, CSC can broadcast information to CSS or CP. In addition, CSS can also broadcast information to CP, and the three processes are similar. However, to describe the scheme implementation process, all entities in the framework are involved. We use the CSC broadcasting information to CP as an example. The implementation process of our privacy preserving scheme corresponding to Fig. 1 is as follows:

(1)KGC system initialization: During system initialization, KGC generates partial public keys, partial private keys, and pseudo-identities for EV, CSS, and CSC.

(2)CSC signcryption and broadcast command information: CSC selects the pseudo-identity of EV receivers and the information set to be signcryption, and then generates ciphertext for command informations through the signcryption algorithm, which is sent to CP through KGC and CSS.

(3)CSS verify ciphertext and reache a consensus: The CSS verifies the validity of the ciphertext. If the ciphertext is valid, the primary CSS node uses the PBFT algorithm to reach a consensus, publishes a new block to the CB, and sends the valid ciphertext to the CP.

(4)CP unsigncryption and processe command information: CP obtains the EV user's command information through the unsigncryption algorithm, rationally dispatches electric energy according to the control information, and charges EV users according to the bill information.

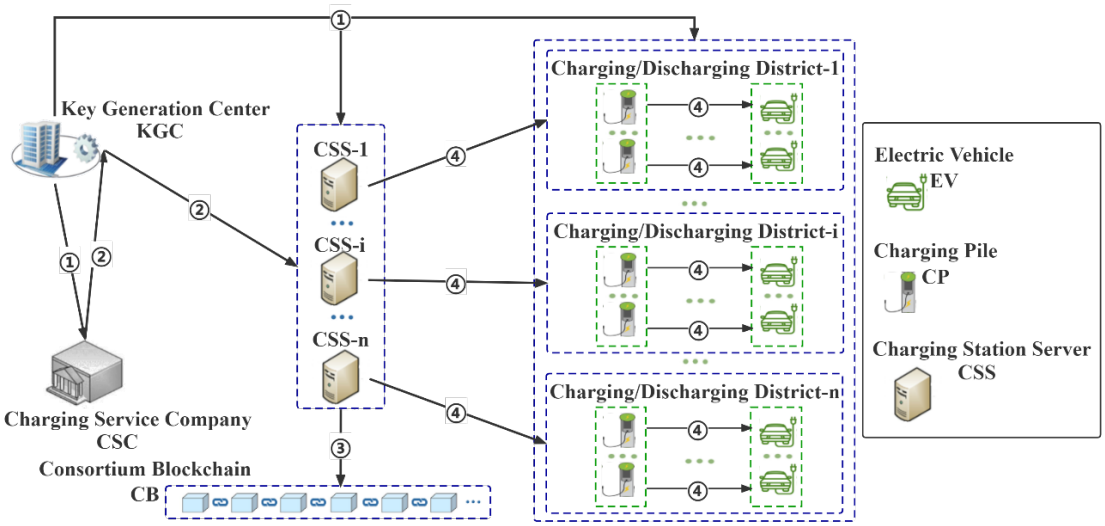

Figure 1: Privacy preserving framework of EV.

4. Scheme Implementation

4.1. KGC System Initialization

KGC generates private keys msk, public keys P_{pub}, and public parameters $Params$ for the system. After that, KGC generates the partial private key d_i, partial public key PR_i, and pseudo-identity f_i for the registered user and passes d_i, PR_i, f_i to the entity with the corresponding identity over a secure channel. Finally, KGC sends the pseudo-identity list f of all EV users to CSC, and then stores f in the internal database.

4.2. CSC Signcryption and Broadcast Command Information

CSC generates the ciphertext σ for broadcast informations $M_i = f_i \| m_i$ through the signcryption algorithm. f_i and m_i indicate pseudo-identity and command information of the receiving user. Then, CSC transmits σ and f_i to the KGC. The KGC decrypts the real identity of the EV through f_i, and delivers σ to the CSS where the EV user is located through the real identity.

4.3. CSS Verify Ciphertext and Reache a Consensus

After CSS receive the ciphertext σ, it verifies the σ validity. If σ is valid, CSS broadcasts σ to the CP for EV connections and stores the σ in the CB through the consensus mechanism; if not, it disables the σ. Our scheme sets the identity of all CSS_1 to $\{CSS_1, CSS_2, \ldots, CSS_n\}$, assuming CSS_1 is the selected primary node. It collects each secondary node's data set and generates a new block stored internally through the Merkle tree. Then, CSS_1 broadcasts the new block to all secondary nodes. After running the PBFT algorithm to reach a consensus, CSS_1 publishes the new block to the CB.

4.4. CP Unsigncryption and Processe Command Information

After the CP for EV connections receives the ciphertext σ, CP locates the corresponding ciphertext field, acquires $M_i' = f_i' \| m_i'$ though calculate, verifies the accuracy of the received information by judging $f_i' = f_i$, and provides intelligent services for EV through m_i'. Among them, command information mainly includes control information and billing information. CP rationally dispatches electric energy according to the control information and charges EV users according to the billing information.

5. Scheme Analysis

5.1. CLMMSC Analysis

The CLMMSC proposed in this scheme has the following characteristics:

(1)Anonymity of receiver and sender: In our scheme, the ciphertext does not need to contain the receiver's identity list, and only the receiver can restore the sender's identity information from the ciphertext, which ensures the anonymity of the receiver and the sender.

(2)Mutual authentication: CSC authenticates at the time of signcryption, while EV authenticates at the time of unsigncryption. Only EV and CSC can perform these procedures.

(3)Key escrow resilience: EV user’s complete private key comprises two parts of secret values. KGC only generates part of the private key. Even if KGC is attacked, the attacker cannot get all of the user’s complete private keys.

(4)Address analyticity: CP obtains the CSC's command information through the unsigncryption algorithm. CP verifies the information's legality again through pseudo-identity to ensure the accuracy of the received information.

(5)Public verifiability: The ciphertext validation in our scheme only relies on public parameters, without the receiver's private information. Therefore, entities with computing power in the EV privacy preserving framework can check ciphertext's validity.

5.2. CB Analysis

The CB proposed in this scheme has the following characteristics:

(1)Data storage without trusted third party management: The storage scheme of CB proposed in our paper adopts end-to-end communication between nodes, which can implement secure, efficient, and distributed power information storage without relying on trusted third party entities. Thus, this scheme solves the problem of the single point of failure and data integrity in a centralized storage method. Furthermore, this distributed storage system has good scalability and reliability.

(2)Data storage security verification: The scheme using the PBFT consensus algorithm, all data are verified publicly by CSS to ensure the data block’s validity. Moreover, the consensus algorithm only uses pre-selected nodes to reache a consensus, rather than all nodes in the whole blockchain network, which significantly reduces network overhead and improves consensus efficiency.

(3)Storing data against malicious tampering: The PBFT algorithm in this scheme can tolerate no more than $(n-1)/3$ CSS Byzantine nodes, where n is the number of CSS. If there are l malicious *CSSs* exist in the whole network, the data tampering attacks initiated by l *CSSs* can be resisted if the total number of *CSSs* meets $n > 3l+1$, and the validity of the data can be guaranteed. For example, if the probability of *CSSs* becomes a Byzantine node is $1/2$, and there are n *CSSs* in the whole network. At least control $(n-1)/3$ nodes to successfully tamper with the data block. Therefore, the probability of successful tampering is $1/2^{(n-1)/3}$. Assuming our

scheme has 100 *CSSs*, the successful tampering probability is almost negligible.

6. Conclusion

CSC needs to broadcast command information to massive EVs to ensure that CSC can provide intelligent services to EV users. However, when CSC broadcasts information to massive EVs, it may lead to several security issues, such as the privacy security problem of data transmission and data storage. Therefore, a lightweight privacy preserving scheme for multicast data transmission of electric vehicles based on consortium blockchain is proposed to ensure the privacy and security of two-way communication. Our scheme designs the new lightweight CLMMSC and CB mechanisms to solve the problem of data transmission and data storage.

References

[1] N. Chen, M. Wang, N. Zhang and X. Shen. Energy and Information Management of Electric Vehicular Network: A Survey[J]. IEEE Communications Surveys & Tutorials, VOL. 22, NO. 2, Pages: 967-997, Secondquarter 2020.

[2] W. Zhong, R. Yu, S. Xie, Y. Zhang and D. K. Y. Yau. On stability and robustness of demand response in V2G mobile energy networks[J]. IEEE Transactions on Smart Grid, VOL. 9, NO. 4, Pages: 3203-3212, July 2018.

[3] L. Gong, W. Cao, K. Liu, Y. Yu and J. Zhao. Demand responsive charging strategy of electric vehicles to mitigate the volatility of renewable energy sources[J]. Renewable Energy, VOL. 156, Pages: 665-676, August 2020.

[4] P. Gope and B. Sikdar. An efficient privacy-preserving authentication scheme for energy internet-based vehicle-to-grid communication[J]. IEEE Transactions on Smart Grid, VOL. 10, NO. 6, Pages: 6607-6618, November 2019.

[5] C. Peng, J. Chen, M. S. Obaidat, P. Vijayakumar and D. He. Efficient and provably secure multireceiver signcryption scheme for multicast communication in edge computing[J]. IEEE Internet of Things Journal, VOL. 7, NO. 7, Pages: 6056-6068, July 2020.

[6] Z. Su, Y. Wang, Q. Xu, M. Fei, Y. Tian and N. Zhang. A secure charging scheme for electric vehicles with smart communities in energy blockchain[J]. IEEE Internet of Things Journal, VOL. 6, NO. 3, Pages: 4601-4613, June 2019.

[7] R. Zhang, R. Xue, and L. Liu. Security and privacy on blockchain[J]. ACM Computing Surveys, VOL. 52, NO. 3, ART. NO. 51, July 2019.

[8] Z. Fu, P. Dong, Y. Ju. An intelligent electric vehicle charging system for new energy companies based on consortium blockchain[J]. Journal of Cleaner Production, VOL. 261, Art. NO. 121219, July 2020.