Scientific Research Publishing

Journal of Computer and Communications, 2019, 7, 20-30
https://www.scirp.org/journal/jcc
ISSN Online: 2327-5227
ISSN Print: 2327-5219

Replay Attack and Defense of Electric Vehicle Charging on GB/T 27930-2015 Communication Protocol

Yafei Li, Yong Wang, Min Wu, Haiming Li

College of Information and Technology, Shanghai University of Electric, Shanghai, China
Email: 1156668369@qq.com

How to cite this paper: Li, Y.F., Wang, Y., Wu, M. and Li, H.M. (2019) Replay Attack and Defense of Electric Vehicle Charging on GB/T 27930-2015 Communication Protocol. *Journal of Computer and Communications*, **7**, 20-30.
https://doi.org/10.4236/jcc.2019.712003

Received: September 30, 2019
Accepted: December 6, 2019
Published: December 9, 2019

Abstract

The GB/T 27930-2015 protocol is the communication protocol between the non-vehicle-mounted charger and the battery management system (BMS) stipulated by the state. However, as the protocol adopts the way of broadcast communication and plaintext to transmit data, the data frame does not contain the source address and the destination address, making the Electric Vehicle (EV) vulnerable to replay attack in the charging process. In order to verify the security problems of the protocol, this paper uses 27,655 message data in the complete charging process provided by Shanghai Thaisen electric company, and analyzes these actual data frames one by one with the program written by C++. In order to enhance the security of the protocol, Rivest-Shamir-Adleman (RSA) digital signature and adding random numbers are proposed to resist replay attack. Under the experimental environment of Eclipse, the normal charging of electric vehicles, RSA digital signature and random number defense are simulated. Experimental results show that RSA digital signature cannot resist replay attack, and adding random numbers can effectively enhance the ability of EV to resist replay attack during charging.

Keywords

EV Charging, GB/T 27930-2015, Replay Attack, RSA Digital Signature, Adding Random Numbers

1. Introduction

In order to ensure the safety of the charging process, at the end of 2015 China announced the communication protocol between the electric vehicle conductive charger and BMS (GB/T 27930-2015). The agreement clearly stipulates that BMS adopts the CAN communication protocol for specification, and specifies the

process of specific charging and content of communication message. Since the protocol is based on the CAN bus protocol, some security vulnerabilities of the CAN protocol also exist in the protocol, which makes the electric vehicle face a series of security problems in the process of charging .

With the application of information technology in the field of electric vehicle charging, some vulnerabilities in the protocol may cause communication security problems, for example: the attacker maliciously attacks the charging pile, so that the charging pile stops charging the electric vehicle; some users may tamper with the charging data to reduce billing, and bring damage to the interests of the operating company [1]; personal privacy information such as payment password, location, charging account, etc. were stolen by hackers.

In view of the above problems, at present, there are four aspects on the security of charging protocols both here and abroad: CAN bus anomaly detection, data encryption transmission and authentication, firewall technology, security framework research.

In the research of anomaly detection, Zhang Zijian, Zhang Yue *et al.* [2] analyzed the existing anomaly detection system for CAN bus, and proposed a new CAN bus anomaly detection algorithm, which can detect abnormal frames in the bus and design. It can access the abnormality detection system of the CAN bus, and the system can verify the effectiveness of the proposed algorithm. Yu He, Qin Guihe *et al.* [3] proposed an on-board CAN bus network anomaly detection method based on information entropy and message relative distance. This method can be used for detection and attacks such as flooding and replay of the on-board CAN bus network.

In theresearch of data encryption transmission and security authentication, Zhao Xiang, Liu Zhihong, etc. [4] chose embedded system, improved the encryption method of one-time and one secret, simplified the encryption algorithm by using key pool technology, and increased the difficulty of cracking electric vehicle charging data. Zhao Bing and Yan *et al.* [5] designed a control method for electric vehicle charging piles with safety protection effect by using the national secret SM1 encryption algorithm to ensure the integrity and confidentiality of data transmission.

In the research of firewall technology, Tang Liang *et al.* [6] designed a vehicle-like gateway similar to the firewall function for the information security problem faced in the current vehicle network, which is used to filter the threat packets of traditional Ethernet. Xiao Peng, Li Yuanyuan, etc. [7] proposed a firewall technology for the security of in-vehicle information systems, which can prevent external network attacks to a certain extent.

In the research of security framework, Petit J and Schmidt R [8] adopted a privacy impact assessment method to design a privacy protection system based on privacy enhancement technologies such as anonymous certificates. Fazouane M and Kopp H *et al.* [9] outlined the method for verifying the privacy attributes of the POPCORN privacy protection protocol mentioned in the ISO15118 standard, pointing out its problems and providing corresponding improvement

measures.

The above four aspects of research have solved the security problem of GB/T 27930-2015 communication protocol to a certain extent, but in terms of data encryption transmission and security authentication, such as Zhao Bing and Wei Wei, the national secret SM1 encryption algorithm can be used to prevent data frames from being illegally intercepted or tampered with, but not against replay attacks.

In view of the current problems, this paper uses a total of 27,655 message data in the complete charging process provided by Shanghai Titanium Electric Co., Ltd., and uses the program written in C++ to parse these actual data frames into Chinese characters one by one and save them for analysis of GB/T 27930-2015 communication protocol security; then use JAVA program to simulate three charging modes of electric car charging, input "0" is normal charging mode, input "1" is for replay attack and try to defend with RSA signature Entering "2" is an attempt to defend against replay attacks by adding random numbers. By comparing experimental results, adding random number is selected as an effective defense to against replay attack, thereby ensuring information security during charging and communication of electric vehicles.

The first part of the paper gives a brief introduction to the protocol and charging process. The second part analyzes the provided message data. The third part proposes two anti-replay attack algorithms. The fourth part simulates three charging processes of electric vehicles to choose an algorithm that is effective to against replay attacks.

2. Description of the Problems

2.1. Introduction to GB/T 27930-2015

The GB/T 27930-2015 agreement specifies the definition of the physical layer, data link layer and application layer of the controller area network (Controller Area Network, CAN for short) between the charger and the BMS. It is the SAE on the CAN bus (US) (The Institute of Automotive Engineers) based on the J1939 agreement to expand development [10], summarized as follows:

1) Physical layer

The physical layer selected for this protocol shall comply with the physical layer provisions of ISO 11898-1:2003 and SAE J1939-11:2006; the communication between the charger and the BMS shall be performed using a CAN interface separately from the energy train control system; The communication speed between the machine and the BMS is 250 kbit/s, and it can be 50 kbit/s in a dedicated place with a bad communication environment.

2) Data link layer

The protocol uses a 29-bit identifier of the CAN extended frame. Each CAN data frame consists of one protocol data unit (PDU). Each PDU consists of seven parts: priority, reserved bits, data pages, PDU format, PDU specific, source address and data field, as shown in **Figure 1**.

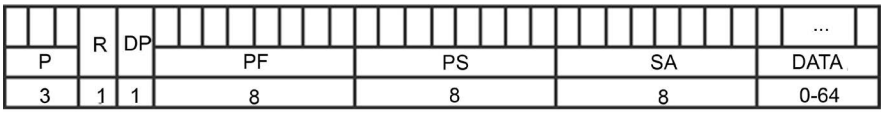

Figure 1. PDU.

In this protocol, the addresses of the charger and BMS are fixed in the program code of the ECU and cannot be modified. The address of the charger is 86 (56H) and the address of the BMS is 244 (F4H).

3) Application layer

The application layer directly serves the user based on the physical layer and the data link layer, and uses the parameters and parameter group defined methods to transmit data by using periodic transmission and event-driven methods. Each node uses PGN to identify the transmitted data, which can be passed. "Request PGN" to actively obtain the parameter set of the remaining nodes [11].

2.2. Security Analysis of GB/T 27930-2015

The protocol was developed on the basis of SAE J1939, and J1939 is based on CAN2.0B, which re-specifies the 29-bit ID of the arbitration field. The other parts are identical, so some of the CAN protocols may pose a security threat. The characteristics also exist in the GB/T 27930-2015 agreement:

1) A broadcast protocol without an authentication scheme. The non-vehicle charger and the BMS transmit data through two CAN buses, which is equivalent to two CAN nodes communicating with each other. The attacker may access the CAN bus through the physical connection, receive the messages that the two CAN nodes communicate with each other, and then replaying into the CAN bus network at any time interferes with the normal charging process of the electric vehicle.

2) Plain text transmission. The data transmitted between the off-board charger and the BMS lacks encryption and authentication mechanisms, and there is no anomaly detection system. At present, the main research is to ensure data integrity and confidentiality by adopting encryption and identity authentication methods, but it is difficult to simultaneously consider the availability.

3) Support multi-master work mode. That is, any CAN node connected to the CAN bus can transmit data to the CAN bus at any time, and the transmitted data frame does not include source address and destination address information.

2.3. Charging Process

The normal charging process consists of six phases: physical connection completion, low voltage auxiliary power-on, charging handshake phase, charging parameter configuration phase, charging phase, and charging termination phase [12]. During the entire charging process, if the charger and the BMS do not receive the message within a certain period of time or the message is inaccurate, it

can be determined as a timeout. The general timeout period is 5 s. When it exceeds 5 s, the BMS or charger will send an error message and become an error processing state.

2.4. Process of Replay Attacks

Replay Attacks, also known as Replay Attacks, also known as replay attacks, replay attacks, or fresh attacks, refer to the use of interception or other means to steal packets sent by the client to the server, and then maliciously re-encrypt the stolen data repeatedly sent to the server [13]. In the normal charging process, a third-party attacker can access the CAN bus as a CAN node on the bus, and can use the broadcast feature of the protocol to receive the data frame between the BMS and the charging post on the bus, and then arbitrarily in the future. Repeatedly sending messages to the bus in one time interferes with the normal charging process of the electric vehicle, causing the electric vehicle to stop when it is overcharged or not fully charged. The process of replay attack is shown in Figure 2.

3. Experiment of Message Parsing

3.1. Experimental Content and Process

Shanghai Titanium Electric Co., Ltd. provided a total of 27,655 message data in the process of complete charging. Firstly, the actual data frame was parsed one by one through the program written in C++ language, and the file chuyuan.csv to be parsed was stored in the same directory as the application. Next, enter the complete file name "chuyuan.csv", and follow the prompts to start parsing the message:

The analysis is completed.

The parsed content will be automatically saved to Target-[chuyuan.csv].log in the same directory. Some data analysis is shown.

3.2. Analysis of Results

The program written in C++ parses the actual message in the charging process

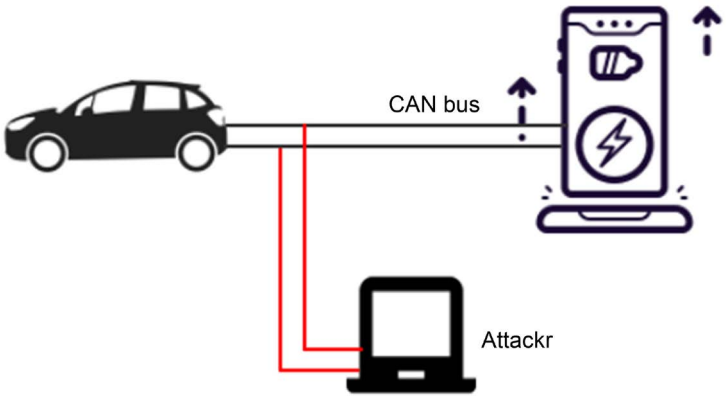

Figure 2. Process of replay attacks.

into Chinese and saves it as a file. After detailed analysis, it can be concluded that there are some security vulnerabilities in the GB/T 27930-2015 protocol: data transmission through plaintext, no encryption And authentication, and the destination address is not included in the data frame, which makes the electric car extremely vulnerable to replay attacks during charging.

4. Anti-Replay Attack Algorithm

At present, in the research of electric vehicle charging protocol security, most of them propose some encryption and identity authentication algorithms for the characteristics of their plaintext transmission, such as RSA digital signature algorithm. In this paper, the algorithm is compared with the proposed random number algorithm, and the verification is carried out. The effectiveness of the algorithm and the RSA digital signature algorithm resist the failure of the replay attack and improve the information security during the charging process.

4.1. RSA Digital Signature Algorithm

Suppose A is the sender of the message and B is the receiver of the message. The RSA digital signature algorithm mainly includes the following two steps:

1) Signature algorithm

Beginning with A, the plaintext m is hashed using the MD5 algorithm to generate a 128-bit message digest h(m); then the message digest h(m) is encrypted by the SHA256 algorithm using the private key of the sender A, and the encrypted string is also encrypted. Is the signature S.

2) Verification signature algorithm

A sends the plaintext m and the signature S to B, because A's public key is shared between A and B, so B first uses the public key of A to decrypt the signature S with the SHA256 algorithm to obtain the decrypted 128-bit message. Abstract H(m); Then B sends the clear text m sent by A to the hash of the Message-digest algorithm 5 (MD5 algorithm) to get its own message digest h*(m); finally, the message digest h*(m) obtained by comparison B and the decrypted message digest H(m), if the two are the same, the verification is successful, indicating that the message has not been modified during the transmission process, otherwise the verification fails, indicating that the information has been tampered with or the signature is impersonated. The algorithm flow chart is shown in **Figure 3**.

4.2. Algorithm of Adding Random Numbers

This article attempts to defend against replay attacks by adding random numbers. The detailed steps are as follows:

1) Set the random number update rule. In this paper, the new Random function in JAVA is used to generate random numbers. This rule can set different random numbers for different messages, so that the random numbers requested by the message are fresh;

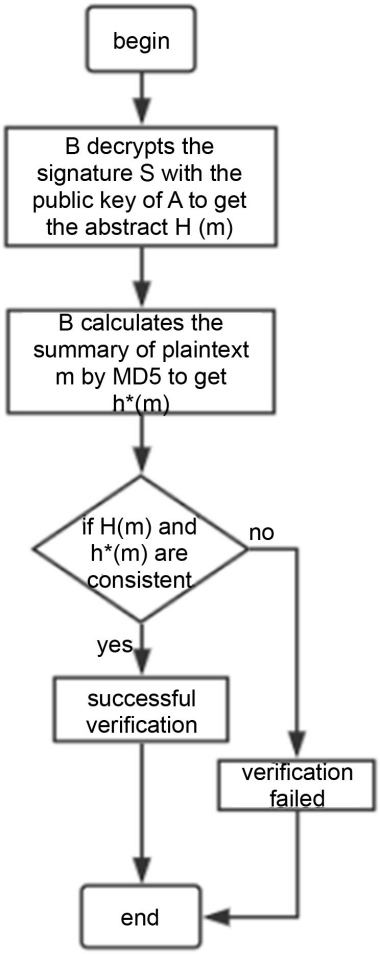

Figure 3. Verification signature algorithm flow chart.

2) When the sender and the receiver perform mutual transmission of messages, a corresponding random number is established for the message in advance;

3) The sender sends the generated random numbers to the receiver together when transmitting the data;

4) After receiving the message and the random numbers, the receiver detects whether the random number requested by the message has occurred in its own database. If it is detected that the random number is duplicated with the data carried by the previous data transmission, it is considered to have been attacked [14];

5) At the same time, the receiver establishes a corresponding index for each received random number and stores it in the database.

The flow chart of adding random numbers to resist the replay attack algorithm is shown in **Figure 4**.

5. Experiment Analysis

5.1. Environment of the Experiment

This experiment attempts to use the RSA digital signature algorithm and adding

random numbers algorithm to defend against replay attacks. By comparing the experimental results, we choose a method to effectively defend against replay attacks.

The three modes of the simulated electric vehicle charging process are available for the user to select, as shown in Table 1:

Table 1. Three charging modes.

Number	Charging mode
0	Normal charging, no encryption
1	Replay the attack and try to defend it with RSA digital signatures
2	Use random numbers to defend replay attacks
Other numbers	Exit this program

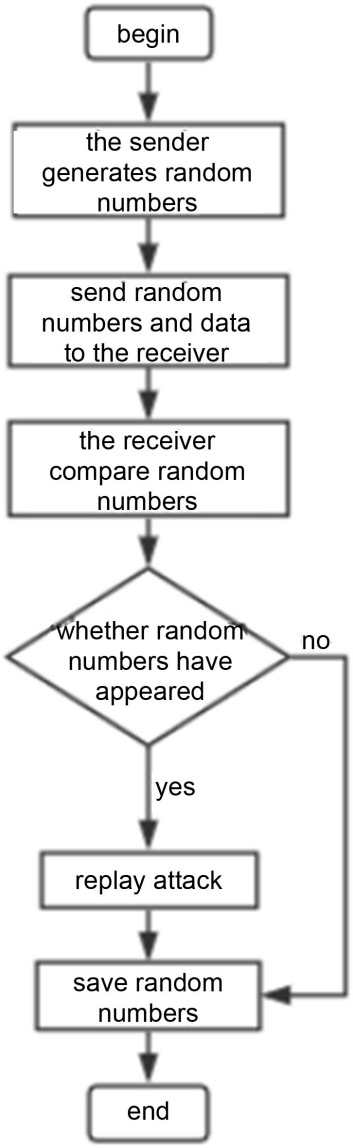

Figure 4. Algorithm of adding random numbers.

5.2. Algorithm Test

The normal charging process of an electric vehicle consists of six parts: physical connection completion, low voltage auxiliary power-on, charging handshake phase, charging parameter configuration phase, charging phase, and charging end phase [12]. In this paper, the program written by JAVA simulates the charging process of electric vehicle. When inputting "0", it enters the normal charging mode of electric vehicle. Through the analysis of CAN frame, it is mainly sent to the charging pile.

In the simulated attack process of this experiment, when the message sent by the charging pile to the electric vehicle shows that the current voltage is 45 V, a replay attack is implemented, that is, a third party continuously sends a charging pin to the charging pile to stop charging. The news forced the electric car to stop charging, and the result of the attack is shown.

When the electric car is subjected to a replay attack during charging, the charging process is stopped and the normal charging process is disturbed. Then RSA digital signature algorithm is often used to defend against replay attacks. The experimental results are shown. The test results show that the RSA digital signature algorithm is not able to withstand replay attacks, and the replay attack will still cause voltage drop. At 0 V, the charging process is stopped.

After applying the algorithm of adding random numbers to resist the replay attack to this experiment, a random number is added to each of the charging pile and BMS for CAN data transmission, and the replay attack is performed when the voltage reaches 40 V. The experimental result at the number "2" is shown. The experimental result shows that a random number is added to the message request sent by the BMS to the charging post. If the random number is duplicated with the previously stored random numbers in the database, then, it can be determined that the attack is replayed, and the charging pile does not execute the stop charging command issued by the attacker to ensure the safe charging process.

5.3. Experimental Results

The simulation experiment in this paper is based on the real data frame improved by Shanghai Titanium Electric Co., Ltd. and the charging process specified in GB/T 27930-2015. The experimental results show that after using the RSA digital signature algorithm, the voltage will be reduced to 0 V when it is increased to 50 V, and the charging process will be forced to stop like the replay attack. This algorithm cannot resist replay attacks; after adding the random number, the voltage value change during charging is consistent with the normal charging mode, which indicates that the algorithm can effectively resist the replay attack and ensure the information security during the charging process.

5.4. Further Work

By analyzing the security of GB/T 27930-2015 protocol, this paper focuses on finding an algorithm that can effectively resist replay attacks. Finally, the effec-

tive method to resist replay attacks is to add random numbers, but there are some limitations in this method. The limitations are mainly reflected in the following two aspects:

1) The generated random number must be additionally stored in the database, which will increase the overhead of the database;

2) The database should be queried for each message request, so that the algorithm runs at a low rate.

Based on the above analysis, the focus of further work is to compare with other anti-replay attack algorithms, and how to improve the efficiency of the algorithm and reduce the saving and query overhead.

6. Conclusion

In this paper, a total of 27,655 pieces of message data in the complete charging process provided by Shanghai Titanium Electric Co., Ltd. are used to parse these actual data frames into Chinese characters and save them as files in a program written in C++. The GB/T 27930-2015 protocol is analyzed in detail. The existing security problem; for the vulnerabilities that electric vehicles are vulnerable to replay attacks during charging, try to use RSA digital signature algorithm and adding random numbers algorithm to resist, and deploy the corresponding programs based on the two algorithms to electric vehicles. During the charging communication process, it is verified by experiments that the RSA digital signature algorithm can not defend against replay attacks, and the random number algorithm is more effective against replay attacks, which increases the security of the electric vehicle charging process.

Fund

This paper was supported by the National Natural Science Foundation of China under Grant61772327, Qianxin Open Project of Big Data Collaborative Safety National Engineering Laboratory (QAX-201803) Shanghai Municipal Natural Science Foundation under Grant 16ZR1436300, Shanghai University of Electric Power, Department of Smart Grid Center under Grant A-0009-17-002-05, Shanghai.

Conflicts of Interest

The authors declare no conflicts of interest regarding the publication of this paper.

References

[1] Zhang, B.J. (2018) Research and Implementation of Information Security Protection Technology for Distributed Electric Vehicle Charging Piles. Harbin Institute of Technology, Harbin.

[2] Zhang, Z.J., Zhang, Y. and Wang, J. (2015) An Anomaly Detection System Applied to CAN Bus. *Information Security & Communication Security*, No. 8, 92-96.

[3] Yu, H., Qin, G.H., Sun, M.H., *et al.* (2016) Vehicle CAN Bus Network Security Problem and Anomaly Detection Method. *Journal of Jilin University*, **46**, 1246-1253.

[4] Zhao, X., Liu, Z.H., Chen, Y.M., *et al.* (2011) Data Communication Security Strategy for Electric Vehicle Charging Facilities. *Automation of Electric Power Systems*, **35**, 92-94.

[5] Zhao, B., Yan, W., Qi, F., *et al.* (2013) Electric Vehicle Charging Pile Control Device with Safety Protection Function. *Electrical Apparatus and Energy Efficiency Management Technology*, No. 16, 53-57.

[6] Tang, L., Li, Y.W., Shi, C., *et al.* (2017) Design and Implementation of Information Security Gateway for Electric Vehicles. *Computer Applied Software*, **34**, 277-283.

[7] Xiao, P., Li, Y.Y. and Li, X.H. (2009) Design and Implementation of Vehicle MOST Network Firewall. *Microcomputer Information*, No. 21, 60-62.

[8] Höfer, C., Petit, J., Schmidt, R., *et al.* (2013) POPCORN: Privacy-Preserving Charging for Emobility. In: *ACM Workshop on Security, Privacy & Dependability for Cyber Vehicles*, ACM, New York, 37-48. https://doi.org/10.1145/2517968.2517971

[9] Fazouaue, M., Kopp, H., Heijden, R.W.V.D., *et al.* (2015) Formal Verification of Privacy Properties in Electrical Vehicle Charging. In: *Engineering Secure Software and Systems*, Springer International Publishing, Berlin, 17-33. https://doi.org/10.1007/978-3-319-15618-7_2

[10] Yang, Z.X. (2018) Method for Consistency Detection of DC Charging Communication in Electric Vehicles. North China Electric Power University, Beijing.

[11] Wu, S.Y. and Shi, R.X. (2015) Research on Communication Protocol Detection System of Off-Board Charger and Battery Management System. *Passenger Car Technology and Research*, No. 4, 60-62.

[12] GB/T 27930-2015, Communication Protocol between Electric Vehicle Non-Vehicle Conductive Charger and Battery Management System.

[13] Chen, Y.Q. (2012) A Time-Based Radio Frequency Replay Attack Defense Scheme. *Modern Computer*, No. 3, 24-25.

[14] Xiao, B.B. and Xu, Y.M. (2017) Anti-Replay Attack Scheme Based on Double Verification. *Computer Engineering*, **43**, 115-125.