ISSN: 2688-8645

Research on Information Security of Communication Network between Electric Vehicle and Charge Point

Wen Shao [1, 2, a], Yanyan Han [1, 2, b], Yihong Qin [1, 2, c], Kexun He [1, 2, d], Baizheng Wang [1, 2, e]

[1]CATARC Software Evaluation (Tianjin) Co., Ltd, Tianjin 300300, China

[2]CATARC Automotive Test Center (Tianjin) Co., Ltd, Tianjin 300300, China

[a] shaowen@catarc.ac.cn, [b] hanyanyan@catarc.ac.cn, [c] qinyihong@catarc.ac.cn, [d] hekexun@catarc.ac.cn, [e] wangbaizheng@catarc.ac.cn

Abstract

In view of the information security issues in the communication network between electric vehicles and charging piles, this study analyzes the information security risks existing in the communication network between electric vehicles and charging piles, expounds the charging process between electric vehicles and charging piles, and assesses the risks existing in the charging piles.

Keywords

Electric Vehicle; Charging Pile; Communication Network; Information Safety.

1. Introduction

In recent years, energy conservation and emission reduction have become a major concern in the world today. In the "Action Plan for Achieving Carbon Peak by 2030" released in 2021, it was clearly pointed out that nine specific tasks need to be carried out, including green and low-carbon transformation actions for energy, energy conservation, carbon reduction, and efficiency enhancement actions for transportation. Among them, energy conservation, carbon reduction, and efficiency enhancement actions account for a relatively large proportion. Therefore, China not only needs to expand the application of new energy in the field of transportation, but also needs to vigorously promote the low-carbon transformation of transportation tools. After the introduction of new energy vehicles and supporting charging piles, the market share of traditional fuel vehicles has been reduced to a certain extent[1]. Vigorously promoting the development of new energy vehicles and charging piles is an important way to achieve energy conservation, carbon reduction, and efficiency enhancement in China. For electric vehicles, there is a very close relationship between their development and charging and replacement facilities. In this context, people are also constantly improving the charging and replacement facilities for electric vehicles. Up to now, the charging and replacement facilities on China's highways and urban roads have developed to a certain scale, and with strong policy support, electric vehicles and their supporting industries have also ushered in new development opportunities. In the process of the development of the electric vehicle industry, its information security is also facing corresponding threats, the most important of which is the information security issue of the communication network between the electric vehicle and the charging pile. Due to the lack of corresponding requirements and standards for the information security of communication networks between electric vehicles and charging piles in China, both electric vehicle enterprises and charging pile enterprises are facing communication network information security issues. Based on this situation, this study analyzes the basic composition of electric vehicle communication networks, the functions of

ISSN: 2688-8645

communication protocols, the vulnerability of protocols, and the information security risks faced in practical application scenarios during the charging process.

2. Overview of Communication Network between Electric Vehicle Charging Piles

2.1. Requirements for Communication Protocol

After connecting the battery pack to the charging pile, in order to ensure charging efficiency and safety, the control unit of the charger monitoring system inside the charging pile needs to communicate with the battery management system accordingly[2]. In general, the communication protocol between the charger control unit and the electric vehicle BMS requires strict compliance with the following:

(1) The communication between the electric vehicle BMS and the charger control unit shall be achieved through a controller area network bus communication protocol to make it compatible with the network of the road vehicle control system.

(2) The physical layer, data link layer, and application layer of the CAN communication protocol between the electric vehicle BMS and the charger control unit comply with the provisions of "GB/T27930-2015, Communication Protocol between Offboard Conductive Charger and Battery Management System for Electric Vehicles".

(3) When charging a tram, both the onboard BMS and the charger control unit need to operate simultaneously to detect parameters such as voltage, current, and battery temperature in the tram battery[3]. At this point, the on-board BMS can select the optimal charging scheme through the charging control algorithm in the charger control unit, thereby improving the charging efficiency and safety of electric vehicles.

Taking minimizing the peak valley difference as the optimization objective and taking the decision quantity x obtained by adding free variables as the control object, the optimization objective function can be obtained:

$$\min Cx \quad s.t\begin{cases} Ax \le B \\ Aeq \bullet x = Beq \end{cases} \tag{1}$$

In Equation (1), $Aeq = (1,\ldots,1,0,0)$, $Beq = z(5) \times 2$, $z(5)$ Indicates the amount of charging power required by the car.

For the charger control unit, it is mainly connected to the electric vehicle BMS through the CAN bus to form a corresponding communication network. The network topology is shown in Figure 1.

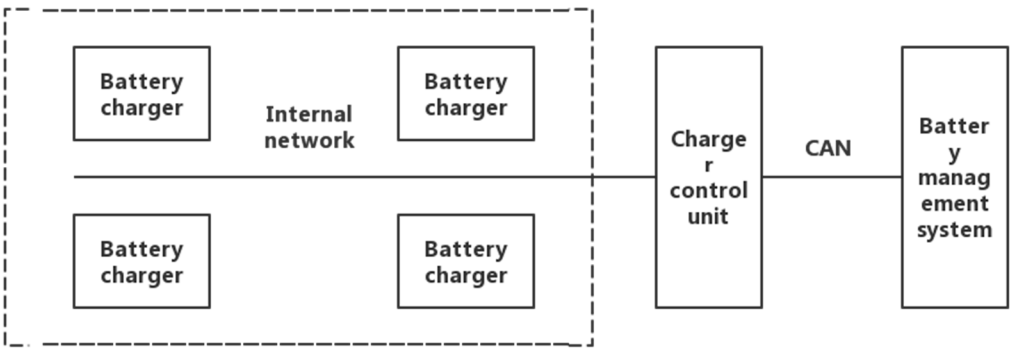

Figure 1. Network topology between charger and BMS

ISSN: 2688-8645

2.2. Overall Charging Process

During the entire charging process, it mainly involves the completion of physical connection, low-voltage auxiliary power on, charging handshake stage, charging parameter configuration stage, charging stage, and charging end stage. In each stage, if the charger and BMS fail to receive a message within a specified time period, it will be determined as a timeout, and the definition standard for timeout is generally 5 seconds. When a timeout condition is detected during the charging process, the BMS or charger will automatically send an incorrect warranty message, which will stop charging and enter the corresponding processing state. At this time, the physical connection can be reconnected and powered on. In general, if a fault occurs, different handling methods can be taken based on the type of fault. If the fault occurs after the end of charging, the charging will be directly ended after the end of charging[4].

Generally, electric vehicle charging piles are divided into public charging piles and household charging piles, where the power of the household charging pile is:

$$P_n^t = \begin{cases} P_n^{home}, t_{start} \le t \le t_{start} + T_{charge} \& 0 < SOC_{start} < SOC_{home} \\ 0, \text{ 其余时间} \end{cases} \ldots\ldots \quad (2)$$

$$T_{charge} = \min\{T_{dwel}, \frac{(1 - soc_{start})\ C_n}{\eta_n}\} \ldots\ldots \quad (3)$$

SOC_{home} --the set home charging SOC threshold;

SOC_{start} -- the actual SOC value at the start time of stay, i.e., the end time of the journey;

P_n^{home} --Charging power of auxiliary home charging pile;

t_{start} --Vehicle dwell time;

T_{charge} --Actual charging duration;

C_n --Calculate the total battery capacity;

η_n --Charging efficiency of charging pile;

If the current in the public charging pile is DC, the instantaneous power is:

$$P_n^t = \{P_n^{fast}, t_{start} \le t \le T_{charge}^{fast} \& \quad (4)$$

$$T_{charge}^{slow} = \min\left\{T_{dwel}, \frac{(0.9 - soc_{start})\ C_n}{\eta_n}\right\} \quad (5)$$

$$T_{charge}^{slow} = \min\left\{T_{dwel} - T_{charge}^{fast}, \frac{(1 - 0.9)\ C_n}{2\eta_n}\right\} = \min\left\{T_{dwel} - T_{charge}^{fast}, \frac{0.05 C_n}{2\eta_n}\right\} \quad (6)$$

k--Charging power linear decline rate parameter;

T_{charge}^{fast}--Fast charging duration of the first stage;

T_{charge}^{slow}--Fast charge duration for the second stage to slow down the rate;

3. CAN Bus and Information Security Status

3.1. CAN Bus

CAN bus belongs to a communication bus, which is mainly used to achieve communication between various electronic controller units (ECUs) in a vehicle. For ECU, its main purpose is to control the driving state of the vehicle and connect various functions on the vehicle. Generally speaking, the ECU and various vehicle sensors collect and exchange data through CAN bus. By analyzing the data, the formal state of the vehicle can be determined, and then the vehicle can

ISSN: 2688-8645

be controlled through the actuator. The function of the CAN bus is to provide a communication network for communication between ECUs. The CAN bus is a common part of various ECUs. Due to the relatively large number of sensors in the ECU, it is necessary to identify the information in the sensors in a specific way.

In the electric vehicle charging pile, the CAN data frame contains a single protocol data unit. Generally speaking, this data unit is mainly composed of priority, reserved bits, data pages, PDU format, specific PDU format, source address, and data domain. The core of data communication between the charger control unit and the electric vehicle BMS is the application layer. The application protocol messages in the charging parameter configuration phase are detailed in Table 1.

Table 1. Charging Parameter Configuration Phase Message

Message code	Message description	PGN(DEC)	PGN(HEX)	preemption	Data length/byte	Message period/ms	source address
BCP	Charging parameters of traction battery	1536	000600H	7	13	500	BMS charger
CTS	Charging point sends time synchronization information	1792	000700H	6	7	500	Charger - BMS
CML	Maximum output capacity of charging pile	2048	000800H	6	8	250	Charger - BMS
BRO	Battery charging ready state	2304	000900H	4	1	250	BMS charger
CRO	Charge Point Output Ready Status	2560	000A00H	4	1	250	Charger - BMS

3.2. Information Security Status of CAN Bus

As for the CAN bus, it is mainly connected to the ECU in various control systems of the vehicle. Attackers can directly attack the ECU through the CAN bus. Due to the lack of corresponding security definitions for the CAN bus, when the CAN sends corresponding malicious messages, the ECU in the vehicle control system will be threatened, seriously endangering the personal safety of drivers. As for the CAN bus communication protocol, it has certain vulnerabilities and is vulnerable to attacks by attackers, resulting in the information security risks of the CAN communication network being ignored. Therefore, it is necessary to study the information security risks of the communication network between electric vehicles and charging piles [5].

4. Threat of Real Vehicle and Pile Communication

In electric vehicles, the ECU in the control system is directly connected to the CAN communication network, or connected through a gateway. When an attacker accesses the CAN bus, they can attack components in the vehicle's internal control system. Through a large amount of analysis, it is found that public charging piles are the main way for attackers to invade the CAN communication network of electric vehicles. For CAN bus, it has many characteristics such as more working modes, protocol priorities, and the use of non-destructive bus arbitration technology. Under the influence of these characteristics, the CAN bus can achieve point-to-point transmission of messages, with relatively short data transmission time, and relatively strong data robustness and anti-interference. Among the characteristics of these CAN buses, the most relevant feature to information security is the multi master working mode. Based on the multi master working mode of the CAN bus, each ECU only needs to be responsible for sending and receiving their message to the bus. Therefore, when multiple ECUs simultaneously receive and

ISSN: 2688-8645

receive message messages, message conflicts will occur, so it is necessary to introduce the arbitration mechanism of the CAN bus. The arbitration mechanism of the CAN bus is based on the priority of the protocol. The purpose of arbitration is to prioritize the protocols on the CAN bus to determine which message can first occupy the CAN bus for communication when a data packet conflict occurs. For the CAN communication network between electric vehicles and charging piles, attackers can discard, read, and modify arbitrary information sent to the charging CAN communication network, conduct deception attacks between the on-board BMS system and the charger control unit, and also conduct flooding, replay, and other attacks.

5. Charging Room Risk

The BMS of an electric vehicle can exchange information with an external charger control unit through a CAN charging bus cable. The man-in-the-middle attack mentioned above, or the attacker attacking any connected electric vehicle through a public charging pile by intruding into it, is a potential information security risk during the actual vehicle piling process. Based on this situation, it can be determined that the main information security risk of real vehicles and piles is the malicious exploitation of the vulnerability of the CAN bus communication protocol. According to the design of the physical layer and data link layer of the CAN bus, after sending a CAN message, the CAN bus will broadcast the message to all nodes on the bus. Malicious components on a bus network can easily listen to or steal data packets or messages from nodes on the network. Based on this feature, a CAN analyzer device can be used to capture data packets and messages from the CAN bus, reverse engineer the data packets and messages, and inject new packets. Observe whether the onboard BMS system or charger control unit has performed incorrect operations that are not expected by its functional design, such as modifying the message priority causing DoS attacks. This article mentions that if there are multiple nodes sending messages to the CAN bus at the same time, the priority of bus usage rights is determined through the bitwise arbitration mechanism of the message frame identifier. During the arbitration process, messages will not be lost. That is, after the arbitration is completed, if the message content that has obtained bus control rights has not been tampered with by the arbitration process, messages that have not yet been transmitted will continue to be sent on the bus. Take the charging parameter configuration stage as an example. After the charging handshake phase is completed, the charger control unit and the BMS enter the charging parameter configuration phase. At this stage, the charger sends a message about the maximum output capacity of the charger to the BMS, which determines whether charging can be performed based on the maximum output capacity of the charger. It is known that the smaller the ID value, the higher the priority of the message in the definition requirement of optimal CAN bus characteristic time. Messages with an ID of all 0 have the highest priority because they maintain the bus level at a significant length. According to the CAN standard, arbitration begins with the first bit of the basic ID and ends with the IDE bit of the standard frame or the RTR bit of the extended frame. This area is defined as the arbitration domain. In the real vehicle and pile scenario, the CAN protocol uses the extended frame standard, so it goes to the arbitration domain to the RTR bit. It can be analyzed that during the charging parameter configuration process in a real vehicle and pile environment, it is only necessary to set the P bit of the maliciously constructed PDU to binary 000 to 011 to set the message to the highest priority. Using this conclusion, attackers can intersperse their constructed malicious data packets between arbitrary periods of time and arbitrary messages in a real vehicle and pile environment, achieving the purpose of fuzzy testing and malicious attacks against the on-board BMS system or charger control unit, thereby further exploring the CAN communication network and achieving stronger destructive effects. Below are three risk assessments of information security during charging. (1) Sending too many high priority message messages overloads the recipient's resources, resulting in a DoS attack that destroys the availability of

ISSN: 2688-8645

real vehicles and piles. If malicious personnel use this method, it may cause the charging function of a large range of public charging piles to be paralyzed, which will have a significant social impact. Therefore, this risk level is determined as medium risk.

(2) Sending a fake message causes the receiver's buffer to overflow, thereby gaining control of the receiver. This attack has caused damage to the confidentiality, integrity, and availability of real vehicles and piles. If a malicious person uses this method to gain control of an electric vehicle or charging pile, it is highly likely to gain control of all electric vehicles and charging piles under the same model or brand, thereby endangering critical information infrastructure such as the Internet of Vehicles platform or smart grid platform, which will cause serious social impact. Therefore, this risk level is determined as high risk.

(3) In the parameter group (PG) definition of the CAN protocol, defining the same PG has an 8-bit data width. Considering the need to reserve some bytes or bits for future expansion, most PGs have reserved bits. Therefore, malicious data or confidential messages can be put into the PG through fragmentation to bypass detection tools or conceal transmission. If a malicious person uses this method, it may also require other conditions to trigger the use in parallel to cause significant social impact, so it is determined that this risk level is low.

6. Conclusion

Charging piles are the most common infrastructure for electric vehicles, and the threats faced by the information security of the communication network between electric vehicles and charging piles must be taken seriously. In this paper, the information security risks of the communication network between electric vehicles and charging piles are studied, and corresponding risk assessment conclusions are given based on the actual process of the actual vehicle pile, which has played a certain inspiration for the construction and standardization of the information security of the actual vehicle pile communication network.

Acknowledgments

National Key R&D Program of China: Research on Active Safety Protection System of Cheyun Platfor (No.2021-JCJQ-JJ-0480).

References

[1] Yi Xiaoshi,Qi Baochuan,Yi Zhengjun. Optimized Location of Charging Piles for New Energy Electric Vehicles[J]. Journal of Highway and Transportation Research and Development (English Edition), 2022,16(3).

[2] Liu Haitao,Lv Zhipeng,Song Zhenhao,Zhou Shan,Liu Wenlong,Fang Mu. Application of Blockchain Technology in Electric Vehicle Charging Piles Based on Electricity Internet of Things[J]. Wireless Communications and Mobile Computing,2022,2022.

[3] Zhang Chao,Zhao Yihang,Zhao Huiru,Wang Qiang. Research on Restrictive Factors and Planning of Charging Piles for Electric Vehicles in the Park Based on the Interpretative Structural Model[J]. Frontiers in Energy Research,2022.

[4] Housing Design For Ev Charging Pile: Sheet Metal Manufacturing Vs. Plastic Injection Molding[J]. M2 Presswire,2022.

[5] Liang Yingying,Fei Xiangyun,Li Jianlu,He Xiao,Gu He. Location of Electric Vehicle Charging Piles Based on Set Coverage Model[J]. World Electric Vehicle Journal,2022,13(5).