Research and Application of Information Security Technology in New Energy Vehicle Based on Mobile Internet

Dongdong Hou¹,²,³,*, Yubing Han¹,², Jianhui Ma¹,²,³, b and Kun Guo¹,²,³, c

¹Qilu University of Technology (Shandong Academy of Sciences), Jinan, China
²Institute of Automation Shandong Academy of Sciences, Jinan, China
³Shandong Provincial Key Laboratory of Automotive Electronic Technology, Jinan, China

*Corresponding author e-mail: sdmcu@163.com, *sd_dsp@163.com,
³majianlong@aliyun.com, ⁴kingssgk@163.com

Abstract. With the development of artificial intelligence, automobile access to mobile internet has become a trend of development. Because the CAN bus of automobile adopts the data transmission mode of open code broadcast, there is a great risk to the information security in the vehicle. In view of this situation, the author develops a data encryption transmission protocol based on OBD, optimizes the bus topology of automobile electronic zero, and designs a comprehensive body control system starting with the research of CAN bus security. The system effectively integrates the current ECU nodes of the new energy vehicle body and reduces the bus load rate of the vehicle body. By combining with the encryption service specification, the system can better realize the security protection of the information inside the vehicle, and has a broad market prospect.

1. Introduction
With the development of social intelligence, it is a trend to monitor the automobile by mobile internet with mobile phone, iPad and other smart devices. Automobile ECU communicates with CAN bus, and can bus is connected to mobile Internet through OBD (On-Board Diagnostic interface). It uses clear code broadcast data transmission mode, which is a great risk to the information security in the vehicle. Therefore, through the analysis and research of various intrusion modes of CAN bus, the author puts forward the specification of encryption service protocol for developing OBD interface, which is suitable for the design of new energy vehicle integrated body control system. The system provides the OBD interface gateway to physically isolate the information inside and outside the vehicle. The gateway communicates with the in-vehicle bus through the encryption service protocol to reduce the risk of ECU intrusion in the vehicle.

2. Research on CAN bus security
Based on the hidden security characteristics of CAN bus, the inherent weaknesses of CAN bus physical layer, data link layer, application protocol and carrier monitoring / collision avoidance mechanism, vehicle-borne network structure and CAN protocol are discussed respectively. Based on the current CAN bus network security, the information security of new energy vehicles is studied.
Based on the findings of the current data survey, the following CAN bus security vulnerabilities have been identified.

2.1. **Broadcasting characteristics**

When receiving the paper, we assume that the corresponding authors grant us the copyright to use the paper for the book or journal in question. Should authors use tables or figures from other Publications, they must ask the corresponding publishers to grant them the right to publish this material in their paper.

According to the physical layer and logical link layer of CAN bus, once the can message is sent, it is broadcast to all nodes on the bus. The malicious components on the network can easily peek into the communication or data packet of the node on the network. Based on this feature, it is possible to observe bus packets and reverse engineering and inject new packets to enable vehicles to perform various wrong operations by using a simple USB-to-CAN device.

2.2. **Lack of sufficient bus protection**

In order to ensure real-time performance of CAN bus, the maximum payload of each message in standard CAN protocol is only 8 bytes, and the message on can bus can be read by any node without necessary security protection mechanism. And there is no message authentication code or digital signature protection, in particular: each message is sent on the bus in the form of broadcast, and the message on the bus lacks confidentiality; any node can impersonate other nodes to send messages to the nodes performing important functions in the system. The bus protocol has no rules on the identity of the sender. When malicious nodes always send high priority messages on the bus, can bus have no related policies to ensure other messages sent on time. Any malicious node connected to the CAN bus can make false messages, which can result the failure of vehicle function.

2.3. **Weak authentication**

The use of password in firmware modification of ECU belongs to weak authentication technology. There are still a considerable number of cars (including traditional and new energy vehicles) that use simple weak authentication when upgrading ECU firmware, such as using frame numbers or vehicle registration information to verify. But the frame number is not confidential information, most of the vehicle operators posted in the lower windscreen, registration information can also be obtained through the dealer.

2.4. **No authentication domain**

The CAN data packet does not contain the authentication domain, which means that any electronic control unit in any network can send the data message to any other node without distinction. That is to say, any hijacked ECU can be used to control all other functional nodes on the bus.

2.5. **Fragile denial of service**

The CAN protocol is very vulnerable to denial of service attacks. In the priority-based arbitration mode, the denial of service attack can be carried out through the bus arbitration mechanism. If the attacker sends data with the highest priority, other ECU will not be able to use the bus. In addition to simple message flooding attacks, malicious error frame messages are sent, and ECU can be forced to disconnect from the bus according to the CAN bus protocol.

2.6. **Message leaks**

At present, mobile interconnect devices are all accessing the information inside the vehicle through the conventional OBD interface. Due to the uneven OBD products on the market, they use Bluetooth, wifi or mobile network to send the status information of the vehicle to the mobile phone, the driving computer or even the cloud. These products are designed with little assessment of information security risks and the use of third-party OBD software at will also buries potential security risks. OBD modules
typically store instructions for access control ECU. The APP software is also chaotic in managing
vehicle status information and does not use cryptographic service protocols.

3. Design of encryption service protocol specification based on OBD

At present, the research on CAN bus security is mainly focused on encryption authentication
algorithm, intrusion detection and security framework. In theory, based on security framework is the
most effective way of protection. But because there are many ECU nodes in automobile, most of them
use 16-bit single-chip microcomputer, the software design mode is mostly used in front and back
systems and the memory and program code space is limited. Therefore, the software design scheme
based on the security framework is not applicable. In addition, because the CAN bus is plaintext
transmission, there is the possibility of being cracked. So long as the monitor gets enough data. From
the analysis of the source of the problem, we can found that the outside system accesses the inside
information of the vehicle through the OBD interface. As long as the information in the vehicle is
accessed through OBD, the vehicle ECU must be in the corresponding diagnostic session mode first.
According to ISO14229 standard, automobile ECU supports three session modes according to
different levels of security protection: default session mode, extended session mode and programming
session mode. The default session mode can be switched directly to the extended session mode, but
cannot to the programming session mode. If you want to enter the programming session mode, you
must enter the extended session mode first. Similarly, programming session mode cannot enter
extended session mode directly, only can to the default session mode. ECU reset and S3 timer timeout
will cause ECU to enter default session mode, ECU session switching state machine as shown in
Figure 1.

![Figure 1. ECU session mode state machine.](image)

On the basis of diagnosing session mode, the author develops an encryption service protocol
specification based on OBD interface aiming at OBD technology and the analysis and research of
CAN bus security at home and abroad. Taking the new energy vehicle of Shandong New Energy
Automobile Co., Ltd as an example, the safety information inside the vehicle is classified and sorted
out. According to the classification of different protection levels, three safety levels are proposed:
general level, extended level and control level. Encryption uses random number seed and key
authentication and adds authentication maintenance time. The control level is the most strict security
level. It is proposed to implement authentication maintenance by using the random number seed and
the algorithm in the random selection encryption algorithm library. As long as one authentication fails within a specified time, the vehicle node will withdraw from the controlled mode and will not respond to the failed authentication request to ensure that the intruder cannot obtain enough data. In control-level mode, the single authentication process within the specified maintenance time is shown in Figure 2.

Figure 2. A single certification flow chart in the control level.

The main content of this part is to evaluate and classify the information inside the vehicle, classify the different access information into different security level management and design the generation method of random number seeds and the key algorithm database. Different algorithms are selected by random number operation and the authentication is maintained within the specified time. Finally, the load rate of the bus is evaluated and tested by the CAN bus development tool of VECTOR Company, and the appropriate maintenance authentication time is selected.

4. Design of network topology for new energy vehicles
First of all, we have a comprehensive understanding of the domestic new energy vehicles, and then we focus on the trial production and testing of the integrated body control system based on a new energy automobile company in Shandong. According to the current survey results, the new energy vehicle ECU node network structure is shown in Figure 3.
According to the field investigation of the new energy vehicle factory, it is found that TPMS / PEPS and BCM, account for more than 85% of the total amount of information in the vehicle in the information in the vehicle that the new energy vehicle connects to the mobile interconnection through smart devices such as mobile phone, the three nodes. And the key function to control the ignition of the vehicle is accomplished by the PEPS node. Although the application of encryption service protocol based on OBD to the current new energy vehicle can play a protective role, it will increase the amount of software code for the combination instrument, DVD / radio, tire pressure monitoring system, body controller and keyless access node. The software design complexity of this ECU and the hardware cost and bus load ratio of the nodes are also increased. Therefore, our team integrate TPMS / PEPS and BCM node functions and develop an integrated auto body control system made use of the development experience in traditional automobile, The system realizes the functions of TPMS / peps and BCM and integrates the OBD gateway. The gateway is physically isolated from the outside world and the encryption service protocol specification is realized on the gateway software so that it can realize double protection. The network topology of integrated body control system is shown in Figure 4.

Figure 3. The ECU node network of old new energy vehicle.

Figure 4. The ECU node network with integrated body controller system.
5. Design of integrated body control system
In order to reduce the possibility of external invasion of new energy vehicle, the author combines the previous development experience of the traditional automobile body node, integrates the functions of the components of the new energy vehicle and tailors the hardware circuit and software module. An integrated body control system for new energy vehicles is designed. The system integrates body controller (BCM), keyless access system (PEPS), Tire pressure monitoring system (TPMS) and OBD gateway, and communicates with external mobile interconnected devices through this gateway. The encryption service specification developed by the subject is implemented in the OBD gateway and the high priority packets of the external intrusion are filtered to prevent the blocking of the bus in the vehicle and play a better protective role. The overall function block diagram of integrated body control system is shown in Figure 5.

Figure 5. The block diagram of the integrated body control system.

6. Conclusion
Based on the research of automobile CAN bus, the encryption service protocol specification based on OBD is developed which is used as the security protection standard for the introduction of mobile interconnection to new energy vehicles. Using this specification, the integrated body control system of new energy vehicle is designed which effectively integrates the current ECU node of new energy vehicle body and reduces the cost of hardware and software of ECU node and the load rate of in-vehicle bus. According to combining with the encryption service specification, this system can better realize the safety protection of the information inside the car. The market industrialization prospect is broad.

Acknowledgments
This work was supported by Shandong province key research and development plan (public welfare special project) in 2017, China (Grant No. 2017GGX10145), Youth doctoral cooperation fund of Qilu Industrial University (Shandong Academy of Sciences) (Grant No. 2017BSHZ006) and the Innovation Program of the Shandong Academy of Sciences.
References

[1] Niu Zhongjun and Zhou Rongxuan. Research and Design of Safety CAN Bus Software for Construction Vehicle. Journal of Jilin University(Information Science Edition)(2017), Vol(4), p465-474.

[2] Yalian Yang, Baolin Chen, Lin Su and Datong Qin. Research and Development of Hybrid Electric Vehicles CAN-Bus Data Monitor and Diagnostic System through OBD-II and Android-Based Smartphones. Advances in Mechanical Engineering (2013), p1-9.

[3] Jianhui Ma, Zhixue Wang, Yanqiang Li and Liangjie Yu. Analysis and Design of Automotive Body Control Module. Proceedings of the FISITA 2012 World Automotive Congress, p25-32.

[4] Hou Dongdong, Hu Dairong and Guokun. The Design of TPMS Hand-Held Diagnostic Instrument. Sensors. Measurement and Intelligent Materials II. Part 1(2013), p 82-85.

[5] Hou Dongdong, Hu Dairong and Liu Yuanyang. Design of a Direct TPMS System Based on SP37. Advances in Mechatronics and Control Engineering Part2(2013), p 1022-1026.