Research on Intelligent Networking Automotive Technology and Information Security Based on CAN Bus

Chen Chen, Boxin Zhang, Min Liu, Wei Shi, Jing Zhang, Lingcai Shen
Tianjin Cadake Data Co., Ltd., Tianjin, 300393

Abstract: With the advancement of information technology, the role of vehicles in people's lives is no longer just a means of transportation. It is also a carrier of mobile communication equipment. The emergence of the Internet has provided a new direction for the development and upgrading of automobiles. Modern information technology and Internet technology are combined with traditional vehicles to realize the intelligent advancement of automobiles. The ultimate goal of developing smart cars is to achieve driverless driving. With the research and development of intelligent networked vehicles, the problems in vehicle information security are gradually increasing. Based on CAN bus, this paper studies intelligent networking automotive technology and vehicle information security issues, and contributes to the development of intelligent networked vehicles.

1. The significance of CAN bus vehicle information security research
With the development and progress of the Internet information technology in the era, the automobile gradually integrated the Internet technology into the automobile manufacturing technology, and realized the initial intelligent development of the automobile. The "Network Security Law of the People's Republic of China" was promulgated on November 7, 2016. In this law, the intelligent information of smart car network is included, clearly indicating that network operators including automobile manufacturing and vehicle networking operations need to comply with the "Network Security Law of the People's Republic of China", which stipulates that "the performance of network security protection obligations shall be in accordance with the provisions of laws, administrative regulations and the mandatory requirements of national standards, and adopt technical measures and other necessary measures to ensure network security and stable operation, effectively respond to cybersecurity incidents, prevent network illegal criminal activities, and maintain the integrity, confidentiality and availability of network data [1]." The attention to vehicle network information is gradually increasing, and the state has begun to pay attention to the safety of vehicle network information.

The problem of car information security is a noteworthy issue. It is more dangerous than ordinary network information. It is no longer a shallow hazard. It directly rises to the issue of personal life safety. Once there is a problem with vehicle information, not only does it cause immeasurable personal injury to the driver, but it also causes immeasurable damage to pedestrians on the road. The damage caused by this problem is fatal [2]. Moreover, the detection method and defense method of the car's CAN network are different from the computer network information security detection. Studying the information security of the car CAN network can not only ensure the safety of drivers and pedestrians, but also promotes the smarter development of smart cars. Therefore, researching the problem of vehicle network safety information is a necessary task to achieve vehicle unmanned driving.
2. Key technologies for intelligent connected cars

2.1 Intelligent Networked Car Overview

In the definition, the primary form of the smart car is to drive the car with the most advanced driving assistance system, which can help the driver to complete certain driving operation tasks and improve the safety performance of the driving vehicle. The primary form of a smart car includes a system radar and advanced sensing, control and execution devices such as cameras, which enable the car to be safely controlled in a dangerous state when it is ready to drive. The real-time information exchange is realized by the external information sensing system and the vehicle information terminal installed in the automobile, and then the driver's own decision is made according to the driver's intention, and the driver is led to reach the final destination. The core of the intelligent networked car is the environment-aware system of the smart car. The ultimate goal of the intelligent network car is to develop a high-performance smart car, in order to achieve the purpose of driverlessness and liberate the hands of the driver, realize the safety of intelligent connected cars and ensure the safety of drivers and pedestrians.

2.2 The key technology of intelligent connected cars

Whether in a narrow sense or in a broad sense, the connection point of smart car networking is CAN network. The information security of CAN network is the core issue of intelligent car networking information security. After understanding the concept of smart car and connected car, specifically to introduce the key technologies of smart car networking, the general can be summarized as 12 key technologies: Environmental awareness technology, wireless communication technology, intelligent interconnection technology, vehicle network technology, advanced driver assistance technology, information fusion thermal technology, information security and privacy protection technology, human-machine interface technology, also known as HMI, high-precision map and positioning technology, heterogeneous 12 key technologies such as key technologies for network convergence, key technologies for traffic big data processing and analysis, key technologies for traffic cloud computing and cloud storage.

(1) Environmental awareness technology. The environment-aware technology contains more content, which can be divided into the state perception of the vehicle itself, the perception of the pedestrians on the road, and the perception of the traffic conditions of the driving route. The perception of the traffic signs set on the road, as well as the perception of the traffic signals through the intersections, and finally the perception of the vehicles around the driving vehicles. Under the complicated traffic conditions, the single environmental sensor cannot complete the complex road condition perception. It is necessary to integrate multiple sensors to facilitate the driving decision of intelligent connected cars to achieve complex road conditions.

(2) Wireless communication technology. The value of wireless communication technology refers to the use of 4G/5G technology to connect the car to the Internet to realize long-distance wireless communication. The specific embodiment of wireless communication technology is that it can transmit images, voice and data information and real-time road conditions to the driver of the vehicle in real time, and can also be used under high-speed driving conditions.

(3) Intelligent interconnection technology. It means that when driving on the road, if it is blocked or can be interconnected by means of intelligence, the mutual transmission of surrounding information can be realized.

(4) Vehicle network technology. The vehicle network technology includes three kinds of network buses, such as CAN, LIN and MOST bus. These network buses are convenient to use, have high transmission frequency, and have narrow bandwidth.

(5) Advanced driving assistance technology. This technology is a specific manifestation of all key application technologies. The maturity and usage of this technology is the embodiment of the intelligent networking technology.
(6) Information fusion technology. Mainly through the use of computer technology, the information and data perceived or received by the car are analyzed and processed to improve the accuracy of intelligent connected car information.

(7) Human-machine interface technology. The technology, also known as HMI technology, includes speech recognition and control, gesture recognition and control, and smart touch screen control. The ultimate goal is to meet the sense of use of car users.

The above is a partial introduction of the key technologies of intelligent networked vehicles. Different key technologies have different functions. The purpose of these key technologies is ultimately to achieve driverless driving of intelligent connected cars. All technical research is in order to improve the performance of the car and the safety of the service, the hands of the people are finally liberated and safe driving is achieved.

3. Car CAN bus information security

3.1 CAN bus vehicle information security problem

With the development of Internet technology, smart cars are gradually developing towards intelligent networking. Therefore, there are a variety of interfaces, which are convenient for the driver to operate, but also bring a variety of problems to the intelligent networked car. These interfaces become the entrance to the malicious network destruction information. Two aspects of the CAN bus vehicle information security issues are introduced.

(1) CAN bus refers to the controller LAN. The essential for intelligent car networking is the CAN bus network. The original purpose of the bus design is to realize the information exchange between the devices in the car. CAN bus has many aspects. Firstly, the bus has low cost, low price and high cost performance, and the use technology is easier to master than others; Secondly, the bus has a good use mechanism, can transmit data over long distances, and has the most advanced arbitration function. It can handle the received information very well; then, when transmitting information, if the sent information is destroyed, it can also be automatically resent. If there is an error sending, it can also close the sending information in time, while ensuring that other systems are not affected, and achieve multi-faceted work; finally, the bus is internationally certified. It is the only fieldbus that is internationally recognized. The connection mode of the CAN bus is a combination of multiple buses to realize the mutual transmission and sharing of the final information in the vehicle. When the CAN bus completes its work, it will realize the transmission of information by sending frames. The frames transmitted by the bus include data frames, remote frames, error frames, overload frames, and interval frames.

(2) There are many threats to CAN bus security, including threats such as car entertainment systems, vehicle T-BOX, App, Tsp cloud platform, physical interface, and vehicle OBD. Moreover, when the bus is designed, it is a closed bus network system, and does not take into account the security performance of the system. However, in the process of continuous development of Internet technology, the phenomenon that the bus is a closed system is changed. More and more ports are being accessed, which poses a new security threat to the network bus. In the context of such rapid development, the CAN bus is exposed to more and more problems, including security certification issues and security protection problems, security isolation problems, data encryption problems, message integrity issues, and the relatively fragile CAN bus issues are all issues that need to be resolved. The solution to these problems is to implement data encryption, achieve regional isolation, and set up access control, set up anomaly detection [3], install security chip, and add security protocols and other functions.

3.2 CAN bus information anomaly detection method

For the CAN bus, the way to attack the bus can be divided into two types, one is the physical connection attack method, and the other is the remote control connection supply. Specifically, it can be divided into three attack methods: replay, flooding, and traversal. By using these three attack technologies, you can clearly feel the impact on the information security of intelligent connected
vehicles when the bus is attacked [4]. At present, the commonly used CAN bus detection method is an anomaly detection method, and the ideal CAN bus information security solution can utilize methods such as identity verification, data encryption, and user message verification [5]. However, these methods are more difficult to use in the current CAN bus technology [6], and more mature CAN bus technology is needed as a support. The following describes the anomaly detection method in detail.

(1) Anomaly detection. The detection method is also one of the types of system intrusion detection. The main purpose of using the system is to prevent malicious intrusion of the intelligent connected car system. The intrusion detection system consists of two parts, one is a hardware device and the other is a software system, which together constitute a malicious intrusion system [7]. The detection process of a malicious intrusion system is implemented in four steps. The first step is the collection of information data, collect the information collected by the vehicle as the original data in the system; the second step is the preprocessing of the information data, the collected information is pre-processed to realize the separation and summary of the data, and the collected data is converted into a form of data that the system can accept. The third step is the analysis of the data. The country analyzes the data that has been separated and summarized, and concludes whether it caused malicious intrusion; the fourth step is to respond to the received data. If a malicious intrusion is caused, the anomaly detection system will respond to the information, or interrupt the transmission of the information or immediately respond to the alarm.

(2) Methods and classification of anomaly detection. According to the analysis method of detecting the data at the time of invasion, the detection method can be divided into two types. One is the misuse detection method, also known as the knowledge detection method, which is based on known intrusion conditions. One is anomaly detection, which is also a behavioral detection.

4. Conclusion
This paper describes the key technologies of connected smart cars and various problems faced by CAN bus and detection methods, and initially understands some problems affecting the security of intelligent networked systems, and proposes the corresponding available detection methods and solutions to contribute to the safe and unmanned driving of intelligent connected cars.

References:
[1] The People's Republic of China Cyber Security Law [N]. People's Daily, 2016-11-23 (014).
[2] Zeng Fan. Research and implementation of network intrusion detection system [D]. University of Electronic Science and Technology, 2018.
[3] Zhao Zhentang. Research on vehicle network anomaly detection technology [D]. Tianjin University of Technology, 2018.
[4] Yang Hong. Research on CAN bus attack and defense detection technology based on intelligent networked car [D]. Tianjin University of Technology, 2017.
[5] Yu He. Network information on automotive information security and CAN bus anomaly detection technology [D]. Jilin University, 2016.
[6] Wu Shangze, Qin Guihe, Dynamic Password Identity Authentication Method for Vehicle Controller LAN Bus[J]. Journal of Xi'an Jiaotong University, 2017(6): 97-102.
[7] Zhang Zijian, Zhang Yue, Wang Jian. An Anomaly Detection System Applied to CAN Bus[J]. Information Security & Communication Security, 2015(8): 92-96.