ISSN: 1813-4890

Overview of Vehicle Network Technology and Security

Wen Shao[1,2,a], Baizheng Wang[1,2,b], Qiang Zhang[1,2,c], Kexun He[1,2,d], Xiong Zhao[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] wangbaizheng@catarc.ac.cn, [c] zhangqiang2021@catarc.ac.cn, [d] hekexun@catarc.ac.cn, [e] zhaoxiong@catarc.ac.cn

Abstract

With the continuous development of the Internet, the popularization of the Internet of Vehicles and cloud services, and the continuous improvement of the degree of computerization in the automotive field, a series of vehicle network security issues have followed. In view of the above problems, this paper mainly introduces the background, status quo, architecture and constraints faced by the design of network security technology of vehicle network. Combined with the characteristics of vehicle network structure, suggestions are put forward from three aspects: standard formulation, system functional security and information security.

Keywords

in-vehicle network; cybersecurity; intelligent and connected vehicle.

1. Introduction

In the next 10 years, the Internet will usher in a new transformation: from the "Internet of Things" to the "Internet of Everything" era. With the arrival of the Internet of Vehicles era, the intelligent network connected vehicle technology is playing a more and more important strategic role in the national socio-economic development. The intelligent network vehicle brings comfort and convenience for people's transportation, while the system complexity and external communication interface increase.

Safety has always been the eternal pursuit of people for automobiles. The safety problems of automobiles include both functional safety and information safety. The two are both interrelated and competitive in computing, network and other resources, which makes the network security problem of intelligent network connected vehicles more complex. A safe automotive electronic system must at least meet the confidentiality, integrity and availability requirements of the system. For ACPS, the authenticity and integrity of data is the most critical. However, in the face of information security threats, the existing vehicle network protocols lack of information security considerations at the beginning of design, so it is urgent to enhance information security. Among them, the vehicle network is the core of the internal network for building the whole intelligent network connected vehicle, and its protocol design and application are highly related to vehicle safety. It is a key field for the Internet of Vehicles to achieve the safety protection of this terminal node. Considering the balance of cost and performance, the current vehicle network has the requirements and characteristics of bandwidth limitation, strong real-time and deterministic delay, which lead to the traditional information security enhancement methods can not be directly used in the vehicle network environment.

This paper mainly summarizes the related research on the network security of intelligent network, and introduces the background, status quo, architecture of vehicle network and the constraints faced by the design of network security technology. Finally, according to the characteristics of the vehicle network structure, five research suggestions related to the safety of the intelligent network are put forward from three aspects: standard formulation, system function safety and information safety.

2. Background

2.1. Intelligent Connected Vehicle Network

Figure 1 shows the structure of the electronic system of the intelligent network interconnection vehicle from the network perspective[1]. The intelligent network interconnection vehicle is a heterogeneous distributed real-time system. The electronic control unit (ECU) is connected by controller area network (CAN) and local interconnection network(LIN). Information interaction between different networks is realized through gateways, The network architecture is heterogeneous, real-time, cost sensitive and has the following characteristics:

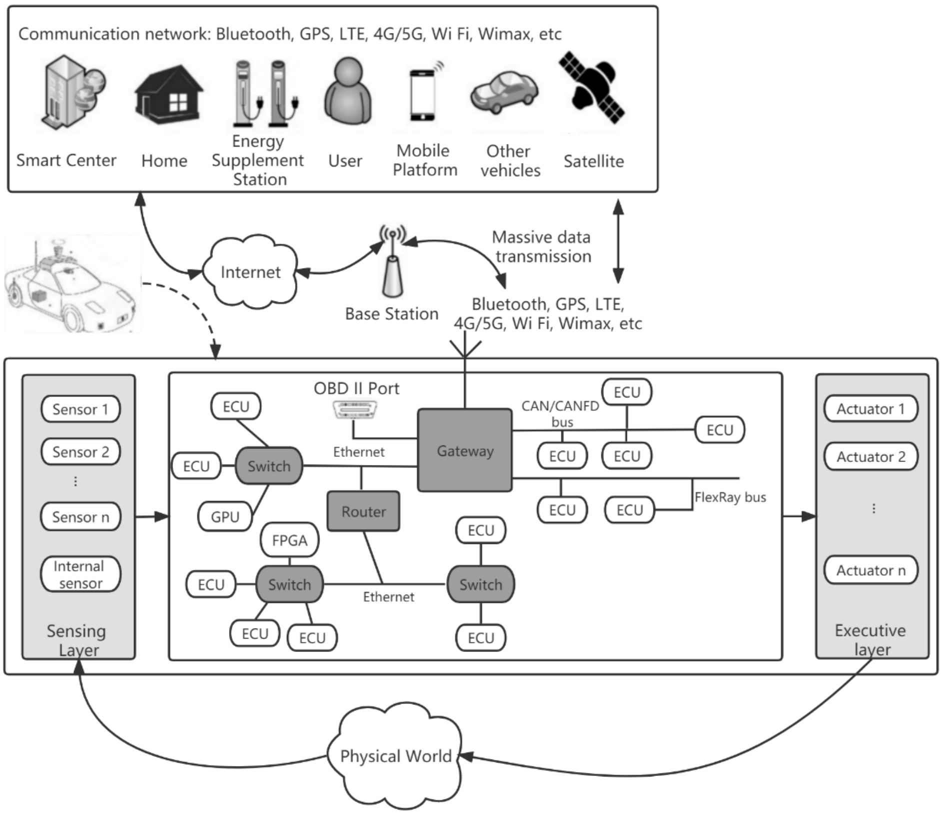

Figure 1. Structure Diagram of Intelligent Network Interconnection System

Rich external interfaces. With the development of vehicle to everything wireless communication technology (V2X), the intelligent networked vehicle has the characteristics of interconnection, that is, the vehicle will no longer be an independent electronic system, but a mobile terminal under the Internet of Vehicles architecture. In order to realize the information exchange between the vehicle and X (such as vehicle, road, people, cloud, etc.), it will be equipped with rich external communication interfaces (such as Bluetooth, GPS, 4G/5G, Wi Fi, etc.). At the same time, the increase of communication demand and the abundance of external interfaces will lead to the diversification of network attack entries and forms.

A large amount of real-time data. Automatic driving driven by IVI, e-cockpit, ADAS, AI and sensors (such as LiDAR, Radar, camera, etc.) will generate a lot of data, which needs to be transmitted and processed in real time. However, the existing vehicle network protocols cannot meet their bandwidth requirements, Ethernet can not provide deterministic delay guarantee. In order to meet the increasing bandwidth requirements of automobile functions, in recent years, high-speed on-board network protocols with deterministic delay characteristics have been developed rapidly, such as time sensitive on-board Ethernet, FlexRay, Ethernet TSN (time sensitive networking), in which FlexRay is applied to the drive by wire system, which makes use of its deterministic delay characteristics.

Heterogeneous network environment. For a long time, considering the balance of cost and performance, the automotive electronic system is in a state of coexistence of multiple network protocols. Different network protocols are applied to different functional domains (such as FlexRay for the backbone network, high-speed CAN for the power control and diagnostic system, and low-cost LIN for the vehicle body control). They will be interconnected through the gateway to build the overall vehicle network architecture. As shown in Figure 2, the vehicle network structure is heterogeneous, distributed and real-time. Its heterogeneity is not only reflected in the hardware platform, but also in the network.

Lack of information security protection mechanism. The traditional automobile is a relatively independent and closed individual, so the external network security threats were not considered at the beginning of the design of the on-board network, that is, the existing network protocols lack basic security mechanisms (such as authentication, encryption, access control, etc.). With the development of the Internet of Vehicles toward the "cloud management end" architecture, the intelligent network connected vehicles as terminal nodes, It is urgent to carry out research on network security enhancement technology of Internet of Vehicles terminal nodes to improve network security.

To sum up, in the intelligent network connected vehicle, the vehicle network needs to present three characteristics: high bandwidth (to meet the communication needs of large amounts of data), information security assurance and low delay (to ensure real-time communication and security)[2]. In order to avoid the excessive time cost caused by the ISO standard layer 7 protocol, the vehicle network is usually divided into three layers, namely, the application layer, the data link layer and the physical layer. The application layer directly accesses the data link layer.

2.2. Classification of in-vehicle network

Figure 2 shows a typical vehicle network structure.According to different bandwidth and functional domains, SAE (Society of Automotive Engineers) divides network protocols into four categories: A, B, C, and D. Its representative protocols and main application fields are shown in the table below.

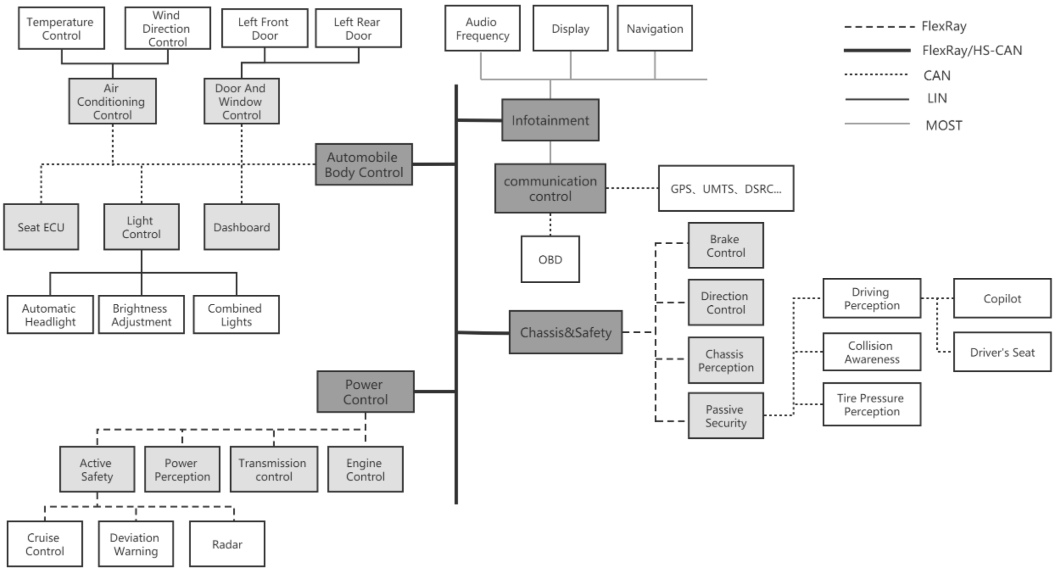

Figure 2. A typical vehicle network structure

Table.1 Classification of on-board network protocols

Type	*Representation Agreement*	*Application Area*
A	LIN	Vehicle body
B	Low speed CAN (SWC), CAN2.0, TTP/A	Body electronics, non diagnostic and safety critical data
C	High speed CAN (HSCAN), TTP/C, CAN-FD	Drives, mobile devices, diagnostics, remote control
D	FlexRay Safe-by-wire, Byte-flight MOST, IDB-1394, Ethernet	Power, chassis and other hard real-time and high reliability fields Security related real-time and reliable areas Multimedia (audio, video)

3. Analysis of information security of vehicle network

3.1. Severe information security threats

As the current vehicle network standard protocol, the vehicle mounted CAN lacked message authentication and data encryption mechanism at the beginning of design. As more consumer electronic products can be easily accessed, the intelligent network connected vehicle makes cars become intelligent mobile devices with wheels. The progressiveness of software and data services has gradually become the core competitiveness of cars. If the vehicle network security enhancement research and deployment are not carried out in time, it will be subject to malicious attacks from all aspects due to potential security vulnerabilities[3].

3.2. Vehicle network lacking information security guarantee

The existing vehicle network protocols, such as CAN and FlexRay, lack information security mechanism design at the beginning of design, which makes the vehicle network vulnerable to sniffing, forgery, modification and replay attacks. Its vulnerability is mainly reflected in the following three aspects[4].

Weak access control. The physical layer of the on-board network is twisted pair or coaxial cable, which is characterized by simple access and lack of abnormal access detection function. It is easy to be accessed illegally and cannot guarantee availability and integrity.

No data encryption guarantee. The internal message transmission is only coded according to the function and lacks encryption protection in information security, which easily leads to message theft and tampering, and cannot guarantee the authenticity of the message.

No message authentication mechanism. Messages are calibrated and filtered as received only through the message ID, and are vulnerable to DoS (denial of service), replay, forgery and other attacks. For example, the current CAN and FlexRay specifications only provide CRC (Cyclic Redundancy Check) codes for message integrity and error verification functions, lacking node authentication mechanisms.

3.3. Rich network security attack portals

This paper will summarize and classify the external interfaces that may be attacked by ICV from the perspective of network hierarchy, and divide different attacks into different levels according to the attack source. As shown in Figure 3, potential attackers often carry out network attacks at different levels on cars through these external interfaces. The characteristics of these cyber attacks are as follows[5].

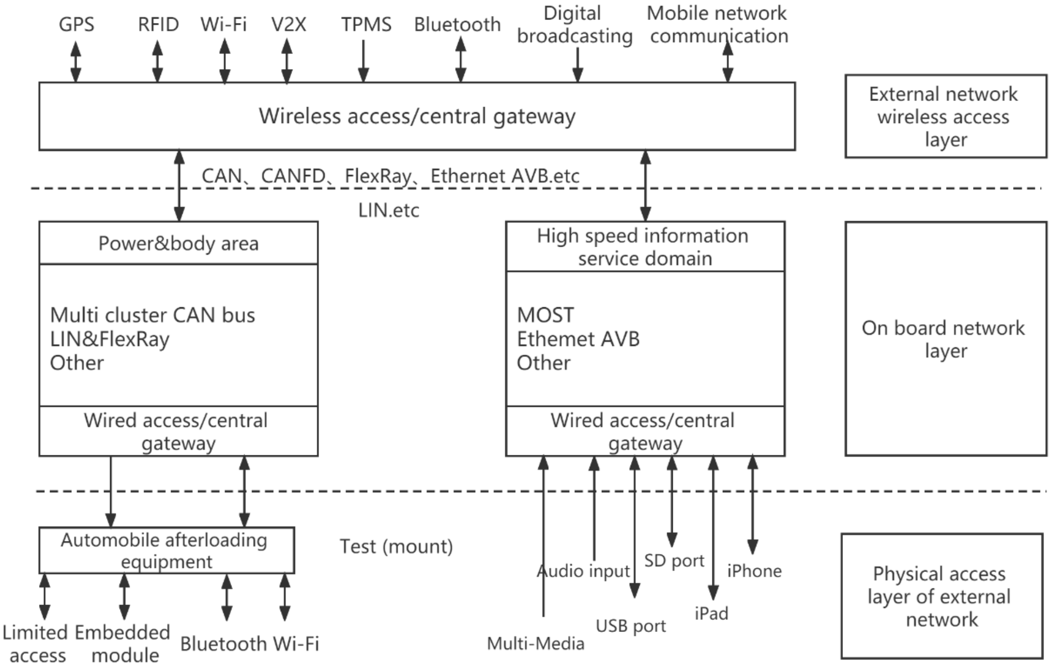
GPS
RFID
Wi-Fi
V2X
TPMS
Bluetooth
Digital broadcasting
Mobile network communication
Wireless access/central gateway
External network wireless access layer
CAN、CANFD、FlexRay、Ethernet AVB.etc
LIN.etc
Power&body area
Multi cluster CAN bus
LIN&FlexRay
Other
Wired access/central gateway
High speed information service domain
MOST
Ethemet AVB
Other
Wired access/central gateway
On board network layer
Automobile afterloading equipment
Test (mount)
Limited access
Embedded module
Bluetooth
Wi-Fi
Multi-Media
Audio input
USB port
SD port
iPad
iPhone
Physical access layer of external network

Figure 3. Description of external interface of on-board network.

Attacks from the sensor layer (physical layer). In the future, cars will be more equipped with a series of advanced sensors, such as laser radar, millimeter wave radar, camera and GPS, to collect information about the perception of the external environment, providing the ability to perceive the environment for automatic driving decisions. Therefore, attacking vehicles through the physical layer will become a new threat to vehicle network security. For example, Rouf et al. proposed an attack that interferes with the tire pressure monitoring system through the radio channel to disable the vehicle tire pressure monitoring system. Tao et al. proposed to attack the keyless starting system and start the target vehicle illegally by controlling the radio channel.

Illegal access (data link layer). Due to the lack of data encryption and message verification mechanisms in the vehicle network, attackers can easily implement attacks once they can access network devices. The attack modes of the data link layer include frame injection, frame forgery, frame sniffing, pause and DoS attack. The availability of the network will be seriously threatened. For example, Cho and others have implemented DoS attacks on the data link layer of the on-board CAN, leading to the functional failure of the entire automotive electronic system.

Attacks from the interface (application layer). In recent years, there have been many reports of remote network attacks on cars by using vulnerabilities in external network interfaces and devices. Because such attacks do not have illegal access to nodes and obvious data frame exceptions, they are more difficult to detect. For such attacks, researchers at home and abroad mainly focus on the design of intrusion detection methods based on machine learning. At present, there are mainly problems such as excessive consumption of computing resources, lack of test data sets and model evaluation.

3.4. Information security under functional security

Functional safety is the premise for the development of intelligent networked vehicles. Traditional designs around vehicle safety include safety belts, passive safety (airbag), active safety (ABS, anti lock braking system), electronic stability program (ESP), ADAS, etc. Functional safety is to avoid unacceptable risks and safety damage caused by electrical and electronic system failure. The design of functional security enhancement should not only comply with the corresponding security standards (such as ISO 26262), but also face the constraints of computing and network resources, real-time, reliability and other aspects[6].

The following four points are summarized: challenges and constraints faced by information security design of vehicle network under functional security guarantee.

The constraints of computing, storage and communication bandwidth resources make the internal hardware resource constraints of the vehicle mainly include computing, storage, bandwidth and energy constraints.

Complex and heterogeneous software and hardware structure. The automobile is composed of a large number of heterogeneous and complex software and hardware components, which communicate with the gateway through heterogeneous vehicle network protocols. The complexity and heterogeneity of the system not only add uncertainties to the functional security and information security, but also add difficulties to the system functional security assurance testing and verification.

Considering the balance of cost and performance, the computing and storage resources of ECUs in ACPS are often limited. However, the high cost of deployment may lead to the low priority of network security deployment, and the vehicle network security design is subject to strict cost constraints, which also leads to the inability of traditional information network information security enhancement schemes to be deployed in the automotive environment.

The constraints of on-board network on functional safety design are mainly manifested as real-time message transmission, end-to-end delay boundary, and system task schedulability, which will affect the reliability and stability of the system. The current research on the schedulability analysis of vehicle network messages mainly focuses on exploring the upper bound of communication delay and satisfying deterministic delay analysis.

4. Analysis and summary

In recent years, the network security of intelligent network has attracted extensive attention from the industry and academia. One of the focuses is to develop algorithms and architectures with anti attack capability around the vehicle network. Combined with the development trend of intelligent network connected vehicles described above and the latest research progress in vehicle network security, this paper further proposes some open issues in the field of intelligent network connected vehicle network security[7].

4.1. How to improve intrusion detection accuracy and reduce response time

In view of the serious functional security threat caused by the untimely detection of malicious attacks on the vehicle network, it is one of the most urgent problems to be solved in the future research of vehicle network intrusion detection technology to improve the detection accuracy, reduce the false alarm rate, shorten the detection response time and improve the system robustness by using intrusion detection as an important means to enhance the security of the intelligent network connected to the vehicle.

4.2. How to achieve accurate network security testing and evaluation

Due to the increasing complexity of heterogeneous software and hardware components used in the future intelligent network connected vehicles, new attacks against the vehicle network will continue to emerge. The complexity of these new components and on-board systems not only brings more challenges to the development of efficient and adaptable on-board network security mechanisms, but also brings difficulties to the testing and verification of network security. For example, in order to verify an intrusion detection model and algorithm, it is necessary to simulate the vehicle network information flow under network attack in the real vehicle network environment. The acquisition and generation of test data will further affect the accuracy and effect of detection. How to achieve accurate vehicle network security test and evaluation is a problem that has not been effectively solved at present.

4.3. How to deal with unknown intelligent network connected network attacks

Considering the characteristics of long life cycle (about 20 years) of automobiles and dynamic changes of network environment, there are mainly three problems in the existing research. 1) Detection methods often correspond to specific attack models; 2) The robustness of the detection effect is not strong (there are many preconditions, lacking the perception of the vehicle state); 3) Lack of evaluation of detection response time and impact on functional safety assurance. Considering the key attributes of ACPS functional security, it is urgent to solve the above problems through the optimization of intrusion detection models and algorithms, so as to avoid the serious safety crisis of intelligent network interconnection function caused by network security problems.

4.4. How to balance network security enhancement and resource consumption

The limitation of computing and communication bandwidth in the intelligent network connected vehicle environment brings about a competition game between functional security and information security design on resources. The existing intrusion detection methods based on machine learning have the problem of large consumption of computing and bandwidth resources. How to reduce the computational complexity and the consumption of vehicle network communication bandwidth. Realizing the balance between network security enhancement and resource consumption is a problem to be further solved in the current research on information security enhancement of intelligent network connected vehicles.

4.5. How to formulate timely and effective information security standards for intelligent network connected vehicles

Standardization construction is an effective measure to effectively improve the collaborative efficiency of automobile product development and reduce the cost of development and maintenance. Similarly, the design of network security issues of intelligent connected vehicles also needs to follow a series of standards and guidelines. Currently, ISO 26262 and SAE J3061 for information security are aimed at vehicle functional safety. OSEK, AUTOSAR, Automotive SPICE, etc. are the functional safety standards, specifications and information safety guidelines for intelligent network connected vehicles.

However, as the legal and regulatory framework often lags behind the speed of technological development, the decentralized business ecosystem of automobiles and the global supply chain make it more difficult to comply with regulations, which will lead to more information security threats to automobiles in the future. At the same time, it will also bring challenges to the formulation of relevant standards. At present, the construction of standards for the network security of intelligent vehicles lags behind. For example, ISO is developing a new standard (Road Vehicles - Safety of Expected Functions ISO 21448), which focuses not on the safety of the system in case of failure, but on the safety of the system in normal operation (including the safety problems caused by information security hazards). At the same time, the National Information Security Standardization Technical Committee also proposed the white paper on the standardization of automotive electronic network security in 2018. Therefore, how to formulate timely and effective information security standards for intelligent network connected vehicles is an important problem to be solved in the future.

5. Conclusion

As the terminal node under the development of the Internet of Vehicles towards the "cloud management end" architecture, the intelligent network connected vehicle is facing an increasingly serious threat to information security. Under this background, this paper first introduces the status quo and classification of vehicle network protocols in intelligent network connected vehicles. Then it summarizes the current vehicle network security issues. Finally, the development and research of vehicle network security technology in the future are summarized and prospected.

Acknowledgements

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

References

[1] Guan T, Han Y, Kang N, et al. An overview of vehicular cybersecurity for intelligent connected vehicles[J]. Sustainability, 2022, 14(9): 5211.

[2] Kleberger P, Olovsson T, Jonsson E. Security aspects of the in-vehicle network in the connected car[C]//2011 IEEE Intelligent Vehicles Symposium (IV). IEEE, 2011: 528-533.

[3] Song H M, Kim H R, Kim H K. Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network[C]//2016 international conference on information networking (ICOIN). IEEE, 2016: 63-68.

[4] Ueda H, Kurachi R, Takada H, et al. Security authentication system for in-vehicle network[J]. SEI technical review, 2015, 81: 5-9.

[5] Craigen D, Diakun-Thibault N, Purse R. Defining cybersecurity[J]. Technology Innovation Management Review, 2014, 4(10).

[6] Martínez Torres J, Iglesias Comesaña C, García-Nieto P J. Machine learning techniques applied to cybersecurity[J]. International Journal of Machine Learning and Cybernetics, 2019, 10(10): 2823-2836.

[7] Xun Y, Liu J, Zhao J. Research on security threat of intelligent connected vehicle[J]. Chinese Journal on Internet of Things, 2019, 3(4): 72-81.