Research on Information Security Protection System of Intelligent Networked Vehicles under Computer Artificial Intelligence Technology

Yunhui Jia
China Auto Information, Technology Co., Ltd., Tianjin, China,
jiayunhui@catarc.ac.cn,
Corresponding author

Shilan Hu
China Auto Information Technology Co., Ltd., Tianjin, China
hushilan@catarc.ac.cn

Yuchen Ma
China Auto Information Technology Co., Ltd., Tianjin, China
mayuchen@catarc.ac.cn

Shunkai Wang
China Auto Information Technology Co., Ltd., Tianjin, China
wangshunkai@catarc.ac.cn

Zonghao Ma
China Auto Information Technology Co., Ltd., Tianjin, China
mazonghao@catarc.ac.cn

Hongyu Niu
China Auto Information Technology Co., Ltd., Tianjin, China
niuhongyu@catarc.ac.cn

ABSTRACT

In order to fully understand the information security risks faced by intelligent networked vehicles and improve the information security protection level of intelligent networked vehicles, it is necessary to start from the characteristics of intelligent networked vehicles architecture to comprehensively analyze the threats, challenges and potential risks they face. Intelligent networked vehicles are composed of multiple complex subsystems composed of multi-function, loose coupling and dynamic. The interaction security between the component systems is affected by the characteristics of the availability, reliability and information security of the subsystems. Traditional analysis methods cannot meet these needs. Therefore, the intelligent networked vehicle information security risk control system is designed and implemented, including information security protection system security, mobile application APP security and server security analysis platform. Through experiments, the ability of the information security protection prototype to resist DoS attacks and network SYN attacks is tested, which verifies the effectiveness of the proposed information security risk control system.

CCS CONCEPTS

• **Information systems** → Information systems applications; Computing platforms.

KEYWORDS

Computer, artificial intelligence, Internet of Vehicles, information security protection system

ICCSIE2022, September 23–25, 2022, Brisbane, QLD, Australia

ACM ISBN 978-1-4503-9741-4/22/09…$15.00
https://doi.org/10.1145/3558819.3565231

ACM Reference Format:
Yunhui Jia, Shilan Hu, Yuchen Ma, Shunkai Wang, Zonghao Ma, and Hongyu Niu. 2022. Research on Information Security Protection System of Intelligent Networked Vehicles under Computer Artificial Intelligence Technology. In *7th International Conference on Cyber Security and Information Engineering (ICCSIE2022), September 23–25, 2022, Brisbane, QLD, Australia.* ACM, New York, NY, USA, 6 pages. https://doi.org/10.1145/3558819.3565231

1 INTRODUCTION

In recent years, with the continuous improvement of the intelligence of automobiles, the possibility of various systems of the vehicle being attacked is increasing, and its security risks are also increasing. Therefore, the safety performance of automobiles has received extensive attention. In order to reduce the incidence of traffic accidents, most automobile companies are working on the research and development of safety protection systems for automobiles. Intelligent network technology has been applied in the field of intelligent transportation [1]. The intelligent networked system is an information infrastructure for communication and information exchange between vehicles and vehicles, vehicles and people, vehicles and roads, and vehicles and the cloud (platform), according to the agreed system architecture and its communication protocols and data exchange standards. The safe operation of an intelligent networked system depends on the security of the subsystems within the system and the interoperability of the subsystems. Therefore, designing a safe and reliable intelligent networked system architecture is crucial.

2 FEATURES OF ICV SYSTEM ARCHITECTURE

ICV involves many professional technical fields and application fields, and its industry has developed from the "three-span" "chip module + terminal + car company" in 2018 to the "new four-span" "chip module" in 2020 + terminal + car company + CA platform", and the industrialization process has been further accelerated [2]. The common intelligent networked vehicle system architecture layer is shown in Figure 1 (the picture is quoted from Network Architectures in Internet of Vehicles (IoV): Review, Protocols Analysis, Challenges and Issues: 5th International Conference, IOV 2018,

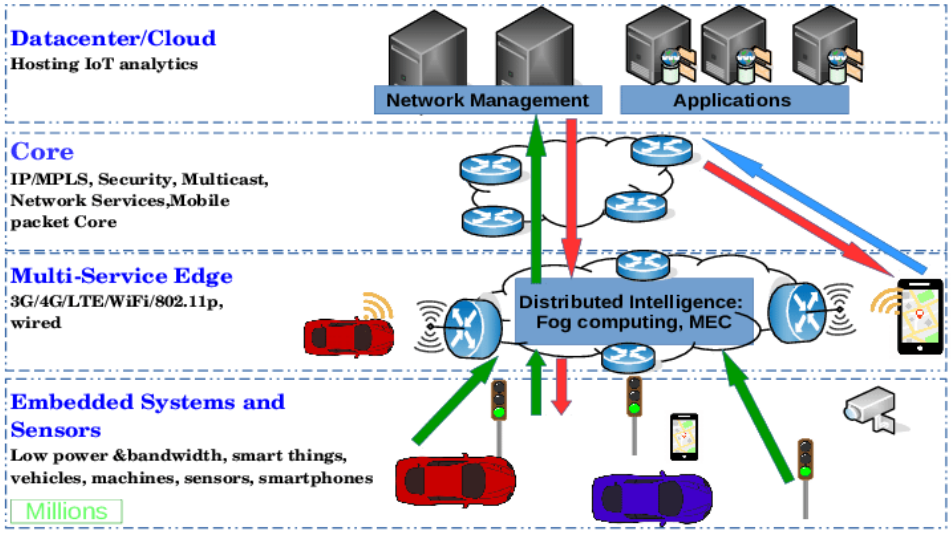

Figure 1: ICV system architecture layering

Table 1: Layered composition of functions of intelligent networked vehicle system

Layered	Classification	Composition
Perception layer	Intelligent Transportation Facilities	Traffic lights, roadside units, traffic control centers, etc.
	Vehicle external connection equipment	WiFi, Bluetooth, vehicle terminal, etc.
	Vehicle external sensor	Radar, ultrasonic sensors, cameras, etc.
Decision-making level	Intelligent driving system	Sensor fusion algorithm, decision algorithm, operating system, computing platform and other software and hardware
Control layer	System electronic control unit	Electronic control unit software, hardware, etc.
Executive layer	Vehicle execution system	Engine/motor, steering motor, etc.

Paris, France, November 20–22, 2018, Proceedings). At the physical level, the ICV system architecture can be divided into four layers: traffic equipment layer, vehicle intelligent system and external interface layer, vehicle network control layer and vehicle component execution layer. From the functional point of view, the intelligent networked vehicle system is divided into perception layer, decision-making layer, control layer and execution layer. The equipment or components involved in each layer are shown in Table 1. Each layer coordinates and divides labor with each other, and its interaction security extremely important.

3 SECURITY THREATS OF CONNECTED VEHICLE INFORMATION INTERACTION SYSTEM

The vehicle information interaction system is composed of information security protection (telematic information processor) and IVI (vehicle infotainment system). Its schematic diagram is shown in Figure 2 (the picture is quoted from Design and Implementation of Roadside Intelligent Information Interaction System Based on Edge Computing). It mainly provides External communication, remote control, information collection, positioning anti-theft and audio-visual entertainment and other functions [3]. Due to its system complexity, diversity of external interfaces, and readable and writable CAN bus information, it is more likely to be exploited by attackers, resulting in information leakage and even affecting the safe driving of vehicles.

The threats faced by the vehicle information interaction system include hardware security threats, communication protocol and interface security threats, operating system security threats, application software security threats and data security threats.

3.1 Hardware Security Threats

When making information security protection and IVI, auto parts manufacturers reserve some debugging ports on the device PCB, such as JTAG, UART, USB and other debugging ports, for the convenience of debugging. Usually, the information of these debugging ports is not encrypted [4]. Interface, you can log into the system, and even obtain root permissions, which leads to the risk of leakage of user data in the system, and more serious is to control the vehicle power system by tampering with the internal files of the system.

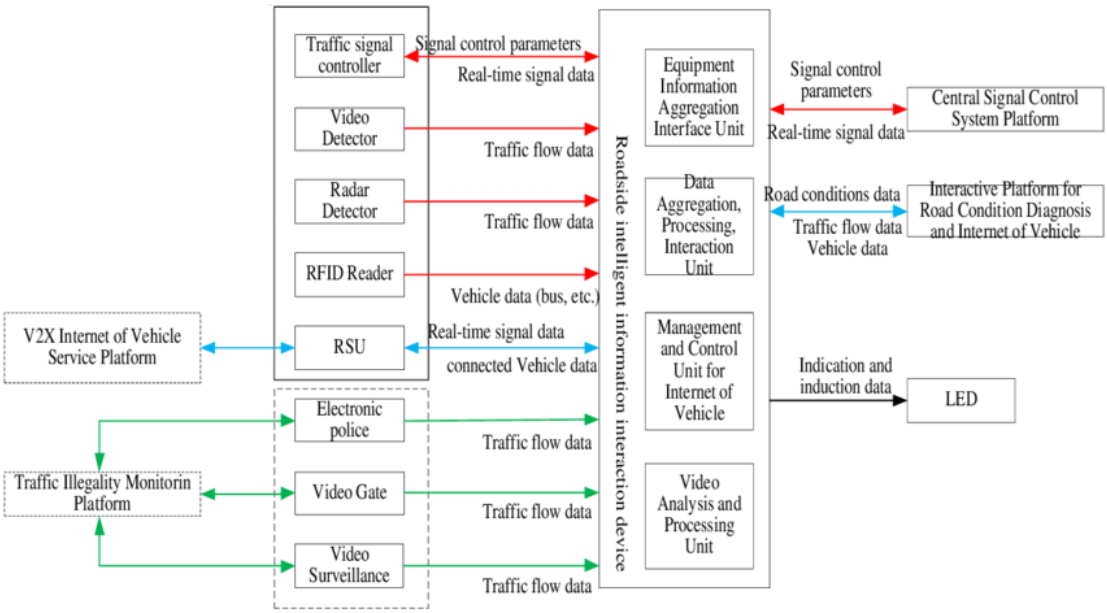

Figure 2: Vehicle Information Interaction System

3.2 Security Threats of Communication Protocols

Communication protocols include external communication protocols and internal communication protocols. External communication protocols include public remote communication protocols (such as HTTP, FTP, etc.), private remote communication protocols, Bluetooth communication protocols, and Wi-Fi communication protocols. Internal communication protocols mainly refer to CAN bus protocol and Ethernet protocol. Whether it is an external communication protocol or an internal communication protocol, it faces the security threat of being attacked.

3.3 Operating System Security Threats

The operating systems of connected cars are mainly embedded Linux, QNX, and Android operating systems. However, the codes used in these operating systems are very complex and will inevitably lead to security vulnerabilities [5]. Therefore, the operating systems have security vulnerabilities, which will lead to connected cars. The system faces the risk of being maliciously invaded and controlled. In addition to the threat of its own vulnerabilities, the operating system also faces threats such as system privilege escalation and operating system upgrade file tampering. Some automotive operating systems retain administrator rights, and attackers can obtain administrator rights through commands to view or modify files in the system.

3.4 Application Software Security Threats

According to the survey, the application software that comes with the vehicle information interaction system and the connected car remote control apps on the market generally lack software protection mechanisms and security protection mechanisms. Most vehicles do not restrict the installation of unknown application software, and even retain the hidden entrance of the browser, which allows hackers to download malicious software through the browser, thereby launching an attack on the in-vehicle information interaction system.

3.5 Data Security Threats

Connected car data security also faces various threats. Connected car data includes personal sensitive data of car owners, location information and Wi-Fi passwords. Most of the connected car data is stored by distributed technology. However, some manufacturers do not encrypt the data when storing the data, so it is easy for attackers to steal, access and illegally use the data through system vulnerabilities.

4 DESIGN OF INFORMATION SECURITY PROTECTION SYSTEM FOR INTELLIGENT NETWORKED VEHICLES

4.1 Architecture Design

This paper proposes a method of vehicle information security threat identification, which improves the accuracy and coverage of threat identification by constructing attack surfaces at each level, so as to more accurately and comprehensively identify information security threats to intelligent networked vehicles. Figure 3 shows the flow of the computer-based method for the identification of layered security threats to intelligent networked vehicles (the picture is quoted from Implementation of a Sensor Big Data Processing System for Autonomous Vehicles in the C-ITS Environment).
Through this method, information leakage, information tampering, denial of service, spoofing, replay attacks, and denial operations can be identified for each layer of the ICV architecture.

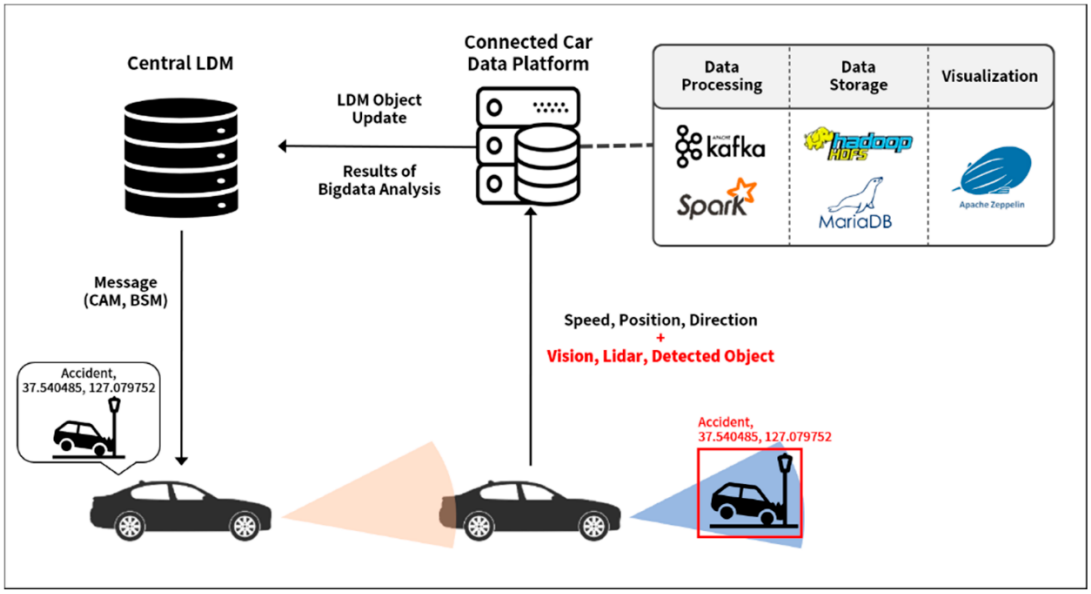

Figure 3: ICV safety identification method

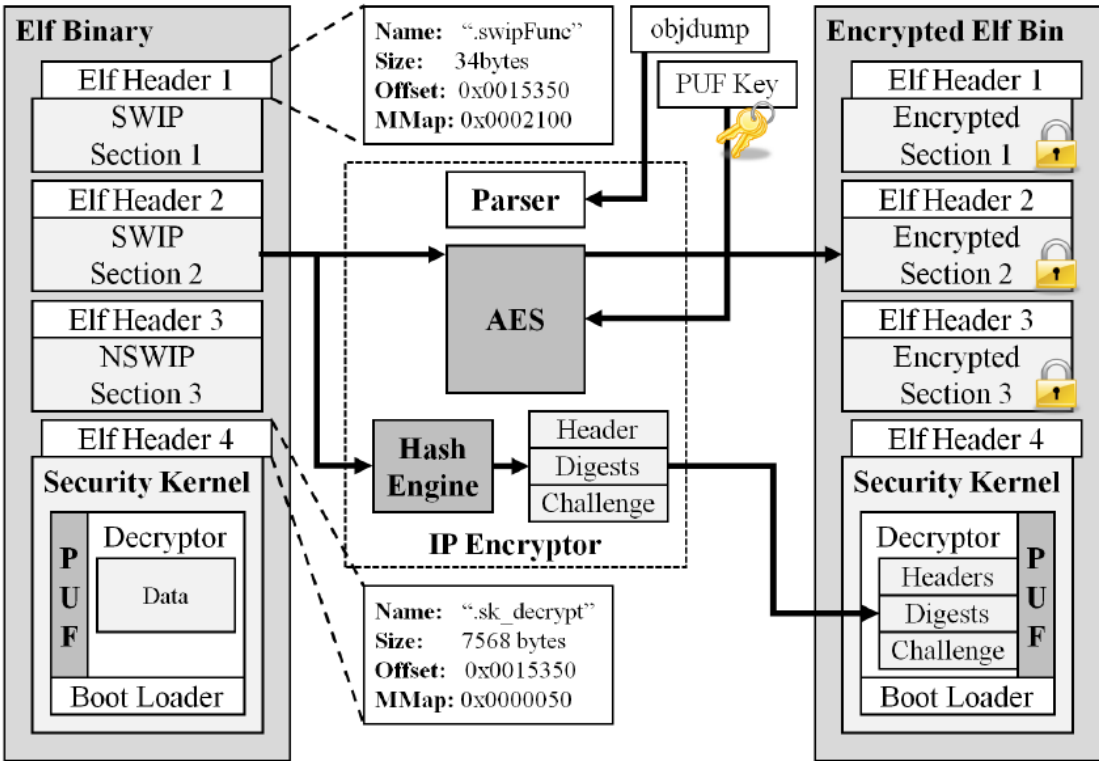

Figure 4: ELF binary protection function diagram

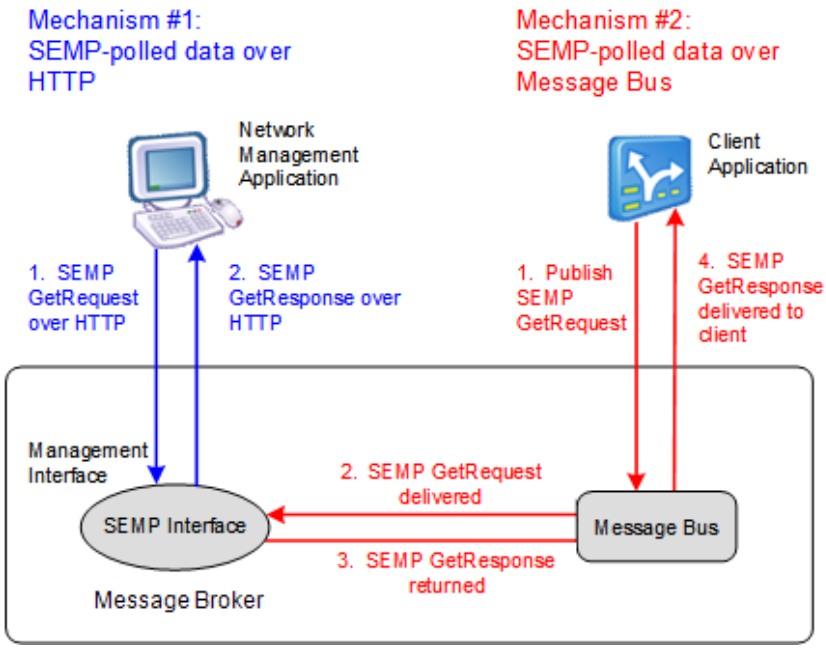

Figure 5: Bus message processing mechanism

4.2 Functional Design

4.2.1 Security monitoring function of information security protection system. Port scanning detection, local privilege escalation detection, system library tampering detection, traffic monitoring, process injection detection, process debugging detection, cache file tampering, malicious program scanning and detection of users logging in to the system [6]. Port scanning detection is to perform self-inspection on the ports running in the information security protection system, and close some port services with potential security risks; at the same time, according to the configuration policy of the server, the IP of external access can be restricted to ensure the security of the information security protection system. The local privilege escalation detection is to rationally classify and organize the privileges of the programs running in the information security protection system, so as to discover the hidden security programs with unreasonable privileges. The system library tampering detection is aimed at key system libraries such as I/O library and ssl library in the system, and performs matching, hook detection and tampering detection between the binary hash value of other dynamic running and the binary hash value of the file form after memory expansion. Process debugging and injection detection are to detect the status bit of the program running in the system to find the suspected stop status bit; at the same time, to compare the snapshot of the program map space to find the injected program. The cache file tampering is to identify the user ID of each file in the program's cache installation directory. If an abnormal user ID file is found, the tampered cache file is identified. Malware scanning is based on the comparison and detection of the server-side security knowledge base.

4.2.2 Information security protection system performance monitoring function. Including CPU occupancy, memory occupancy, resource occupancy and other related information, it provides auxiliary data for information security protection of server platforms.

4.2.3 Information Security Protection Network Monitoring Function. Traffic attack monitoring provides a reliable data source for the server analysis platform to evaluate information security protection network anomalies. The connectivity attack is to identify the SOCKET connection type of the network interface of the information security protection system, and block the SYN flood attack to ensure the security of the information security protection system.

4.2.4 In-vehicle application protection. For the core programs in information security protection, ELF binary protection and application security reinforcement are provided to prevent the core programs in information security protection from leaking private data after being reversed [7]. The ELF binary protection function is shown in Figure 4 (the picture is quoted from Securing Software Intellectual Property on Commodity and Legacy Embedded Systems).

4.3 Gateway Design

In the standard automobile network, the gateway uses CAN, LIN, Flex Ray, etc. to realize the data exchange of each ECU. Based on the mechanism of CAN data broadcasting itself and the defect of no data verification, it is vulnerable to DoS attacks. In order to have a protective effect on the vehicle, the safest vehicle network model is adopted. In order to protect the vehicle bus from being disturbed by external network attacks, a security control node is chosen to be added to the bus application. Based on the ODB (On-vehicle automatic diagnosis system) and the Internet car bus application

system of the information security protection interface, it uses the mechanism in the security control to intercept the external information system, so as to directly control the car bus [8]. This part mainly filters DoS through an independent gateway. Attacks; legitimate requests that need to be controlled can be added to the trusted type model. The hardware isolation technology is used in the gateway to hide the gateway information and not expose the network communication. Different microcontrollers are used between the wireless communication and the gateway, and they are isolated at the same time, and the physical isolation between the bus network and the wireless network must be guaranteed, and then Perform unit judgment and forwarding, judge the source of the diagnosis request in the interrupt program, and then start to make a specific forwarding response to avoid bus information leakage and forwarding errors, and effectively protect the confidentiality and safety of user vehicle data information. Its processing mechanism is shown in Figure 5 (the picture refers to Using SEMP to Manage and Monitor Event Brokers).

5 CONCLUSION

In this paper, the intelligent vehicle networking data protection solution based on artificial intelligence technology connects base stations into distributed artificial intelligence technology to properly deal with the problems of high delay, poor scalability, and single point of failure in the centralized trust management system, and ensures that the unity and coordination of user data storage provides a new idea for data security protection for the Internet of Vehicles.

REFERENCES

[1] Hao Jingjing, Han Guangxing. Research on information security threat identification and protection methods for intelligent networked vehicles. Modern Electronic Technology, vol. 44, pp. 65-71,Twenty-three 2021.
[2] Li Fangli, Wu Xiaojian. Simulation of Information Security Encryption Method for Communication Terminals of Intelligent Connected Vehicles. Computer Simulation, vol.37, pp. 54-59,May 2020.
[3] Zhao Shijia, Xu Ke, Song Juan, *et al.* Implementation Strategies for the Development of Operating Systems for Intelligent Connected Vehicles in my country. Science and Technology Management Research, vol. 40, pp. 59-61, September 2020.
[4] Li Yufeng, Lu Xiaoyuan, Cao Chenhong, *et al.* Network security analysis of intelligent networked vehicles. Telecommunications Science, vol. 36, pp. 108-114,April 2020.
[5] Chen Yisong, Xing Yunxiang, Xiong Xiaoqin, *et al.* Research on the Technology and Economic Evaluation System of Intelligent Connected Vehicles Based on Patent Analysis. Automotive Engineering, vol.43, pp. 79-82,September 2021.
[6] Li Keqiang, Chang Xueyang, Li Jiawen, *et al.* Cloud control system for intelligent networked vehicles and its realization. Automotive Engineering, vol.42, pp. 111-115,December 2020.
[7] Chen Wei, Du Luyao, Kong Haiyang, *et al.* Collaborative map matching algorithm for intelligent networked vehicle positioning. Traffic Information and Security, vol.39, pp. 10-15, June 2021.
[8] Wu Wufei, Li Renfa, Zeng Gang, *et al.* A review of network security research on intelligent networked vehicles. Journal of Communications, vol.41, pp. 14-19,June 2020.