Security Risk Analysis of Intelligent Vehicle Outdoor Remote Driving System Based on 5G Network

Chen Chen[a], Yan Xu[b*], Zhaona Lu[c], Shaojie Pang[d], Yueyue Ma[e]

College of Automotive Engineering, Nantong Institute of Technology, Nantong, China

[a]CCNOVCC@163.com, [b*]937783136@qq.com
[c]595199881@qq.com, [d]pangshajie@outlook.com
[e]2903809524@qq.com

Abstract. With the promotion of 5G technology, the outdoor remote driving system of intelligent vehicle has been developed rapidly. However, this emerging field also brings many security risks and challenges. This study analyzes in detail the security risks of intelligent vehicle outdoor remote driving system based on 5G network in network communication, system control and data processing. It is found that although 5G technology provides higher data transmission rate, lower delay and larger connection capacity for intelligent transportation, it also makes the system more vulnerable to threats such as hacking, data leakage and illegal control. To this end, we put forward a series of security countermeasures and suggestions, including strengthening 5G network security protection, improving system control security and improving data security. In addition, we also discuss future research directions and challenges, such as how to effectively deal with DDoS attacks, end-to-end encryption technology and privacy protection strategies. In short, in order to ensure the safe and stable operation of the intelligent vehicle outdoor remote driving system, it is necessary to comprehensively use a variety of technologies and strategies to deal with various potential risks.

Keywords:5G network technology; intelligent vehicle outdoor remote driving system; security risk analysis.

1 Introduction

1.1 Research Background

With the continuous development of mobile communication technology, especially the popularization and application of the fifth generation mobile communication (5G) network, its characteristics such as ultra-high speed, ultra-low delay and large-scale connection are bringing major changes to the field of intelligent transportation [1]. Especially in the outdoor remote driving system of intelligent vehicles, the application of 5G technology realizes real-time, accurate and efficient remote control of autonomous vehicles, and greatly broadens the boundaries of unmanned application scenari-

Y. Feng et al. (eds.), *Proceedings of the 4th International Conference on Internet, Education and Information Technology (IEIT 2024)*, Atlantis Highlights in Social Sciences, Education and Humanities 26,
https://doi.org/10.2991/978-94-6463-574-4_70

os, such as emergency rescue, dangerous environment operation and special transportation tasks. However, with the improvement of networking and intelligence, new security threats and challenges have followed. Since the remote driving system involves multiple links such as vehicle information processing, network communication transmission, and cloud data interaction, security vulnerabilities in any link may lead to serious safety accidents, including but not limited to malicious control of vehicles, data leakage or tampering, and system function failure.

In recent years, there have been frequent cases of cyber security attacks on intelligent connected vehicles, and the global attention to automobile network security has been increasing. According to the Upstream research organization 's " 2024 Global Automotive Network Security Report, " [2] more than 95 % of attacks against cars are carried out by remote means, which highlights the safety protection of intelligent vehicle outdoor remote driving system based on 5G network is urgent. The statistical graph of remote attacks in 2023, shown in Figure 1, can clearly reflect the grim situation of such attacks.

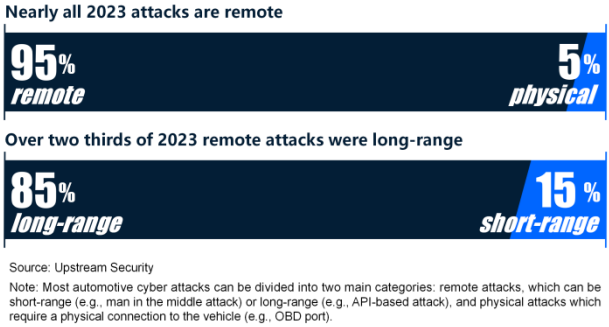

Fig. 1. Remote attack statistics in 2023

Network attacks against cars will not only cause privacy leakage and economic losses, but also endanger life safety in severe cases, and even rise to national public safety issues. Therefore, the security of intelligent connected vehicles has become a hot topic of current research [3]. Due to the slow speed of network communication in the past, when the traditional algorithm is used to control the automatic driving of the car, the algorithm has a long processing time and poor application effect, which makes the car unable to avoid risks in time and accurately, and the safety is low [4]. However, the current advanced information and communication technology not only brings a higher level of driving efficiency and driving experience to the car, but also exposes the vehicle to the negative risks brought by the Internet [5].

1.2 Research Purpose

In the 5G network driven intelligent transportation system, the security challenge of intelligent vehicle outdoor remote driving system is becoming increasingly prominent, especially involving key areas such as network communication security, data

transmission security and system control stability. Through this research, we are committed to providing comprehensive and in-depth theoretical guidance for the safe development of outdoor remote driving systems for intelligent vehicles.

2 Relevant Theoretical and Technical Basis

2.1 5G Network Technology Features and Advantages

As the fifth generation mobile communication technology, the core advantages of 5G network include higher data transmission rate, lower delay and the ability to connect more devices. Specifically, 5G network can theoretically provide a peak data rate of up to 20Gbps and an end-to-end delay of less than 1ms, which is crucial for real-time vehicle outdoor remote driving systems. The comparison between 4G and 5G technologies, as shown in Table 1, clearly compares the differences in key performance indicators between the two generations of technologies. In addition, the spectrum efficiency of 5G technology has been greatly improved, making it possible to deploy denser networks, thus ensuring stable connectivity within coverage. According to relevant data, compared with 4G network, 5G network can achieve more than 10 times of transmission rate improvement and less than 100 times of delay reduction. This means that in the intelligent vehicle outdoor remote driving system, the vehicle can receive sensor data faster and make real-time decisions and control, thereby improving the accuracy and safety of driving. In addition, the 5G network has lower power consumption characteristics, which can achieve long-term continuous connection of intelligent vehicles and provide long-term network support for vehicles.In summary, the advantages of high-speed transmission, low latency, stable connection and low power consumption of 5G network provide a good foundation for the safety and reliability of intelligent vehicle outdoor remote driving system.

Table 1. Comparison of 4G and 5G Technologies

Project	*4G*	*5G*
Latency	60 to 98 ms	Less than 1 ms
Potential Download Speed	1 Gbps	20 Gbps
Base Stations	Cell towers	Small cells
OFDM Encoding	20 MHz channels	100 to 800 MHz channels
Goal For Cell Density	200 to 400 users per cell	100 times greater than 4G

2.2 Overview of Intelligent Vehicle Outdoor Remote Driving System

The intelligent vehicle outdoor remote driving system combines advanced automatic driving technology, on-board sensors, communication technology and cloud computing platform, aiming to achieve safe driving of vehicles without direct control [6]. Real-time data collected by on-board devices and sensors can be quickly transmitted

to remote drivers or autonomous driving systems to achieve accurate control and real-time decision-making of vehicles. The entire process of the remote driving system architecture shown in Figure 2 relies heavily on a powerful and reliable communication network, namely the 5G network, to ensure the speed and stability of data transmission. In the intelligent vehicle outdoor remote driving system, the vehicle can sense the surrounding environment in an all-round way by carrying various sensors, such as cameras, radars, and lidars, and obtain real-time data such as road condition information, obstacle location, and pedestrian behavior. After being processed and analyzed, these data can be transmitted to a remote driver or an autonomous driving system for vehicle control and decision-making. Through the instructions of the remote driver or the automatic driving system, the vehicle can achieve accurate steering, braking and acceleration, so as to achieve safe driving. The application of intelligent vehicle outdoor remote driving system can not only improve the driver 's driving experience and driving efficiency, but also reduce the risk of traffic accidents, improve the efficiency of road traffic and reduce energy consumption.

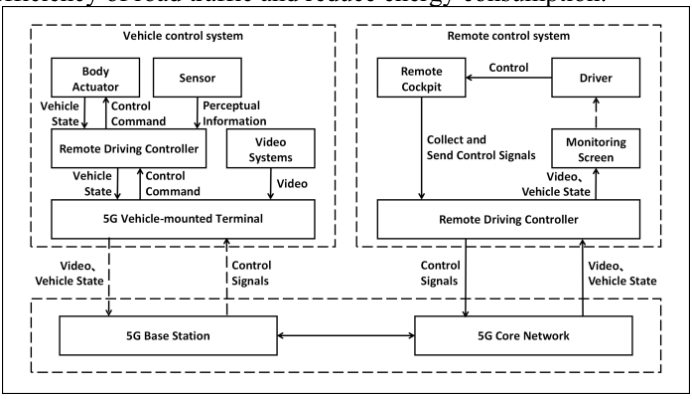

Fig. 2. Remote driving system architecture

2.3 Theory and Method of Security Risk Assessment

Safety risk assessment is the process of identifying, analyzing and evaluating potential risks to ensure the safety of intelligent driving systems. The process usually includes three steps: risk identification, risk analysis and risk evaluation [7]. The purpose of risk identification is to identify possible security threats in the system and discover potential sources of risk through comprehensive inspection and analysis of the system. In the intelligent vehicle outdoor remote driving system, risk identification can include but is not limited to the following aspects: First, the network communication security risks of the system, such as hacker attacks, data leaks, etc.; Secondly, the system control security risks, such as software vulnerabilities, physical attacks, etc. Finally, the system's data processing security risks, such as data tampering, information leakage and so on. Risk analysis is the further analysis and assessment of the identified risks. Assess the severity and priority of each risk by considering its likelihood of occurrence, its consequences, and the security measures in place.

In the assessment process, tools and methods such as fault tree analysis (FTA) and Event tree analysis (ETA) are used to quantitatively describe the generation mechanism and propagation path of risks in order to better identify and evaluate potential risks [8]. Finally, in the risk assessment stage, each risk is assigned a specific priority, and corresponding mitigation and safety measures are proposed. For example, for network communication security risks, 5G network security protection measures can be strengthened, and encryption and authentication technologies can be used to ensure the security of communications. For system control security risks, software security protection can be strengthened, vulnerabilities can be detected and repaired, and access rights can be restricted. For data processing security risks, measures such as data encryption and integrity check can be adopted to prevent data tampering and information leakage. Through such risk assessment and prevention and control strategies, the safety risks of the intelligent vehicle outdoor remote driving system can be minimized and the operation safety and stability of the system can be ensured.

3 Security Risk Identification of Intelligent Vehicle Outdoor Remote Driving System based on 5G Network

3.1 Network Communication Security Risks

With the wide application of 5G technology, the security problem of intelligent vehicle outdoor remote driving system is becoming increasingly prominent. As an innovative technology, 5G network provides high-speed, large-capacity and low-latency communication services for intelligent vehicles, however, it also brings unknown security risks [9]. According to TDIA, the number of 5G users worldwide reached 1.01 billion in 2022, while the number is expected to reach 1.6 billion by 2025. Compared with traditional vehicle communication networks, the openness and software-defined network characteristics of 5G networks make the network interfaces and protocols of intelligent vehicle systems easier targets for attackers. According to the data analysis, in 2022, the global network attack on the remote driving system of intelligent vehicles increased by 21.4% year-on-year, of which man-in-the-middle attacks and deception attacks are the most common means of attack.

3.2 System Control Security Risks

The key to the safety of intelligent vehicle outdoor remote driving system is to realize remote accurate control, and the main risks to be dealt with in this process include software vulnerabilities, hardware failures and illegal control command injection. To reduce the risk of software vulnerabilities, development teams need to conduct rigorous code reviews and testing to keep software up to date. For the risk of physical failure of system components, vehicle manufacturers must select high-quality components and go through a rigorous quality control and testing process, while conducting regular system inspections and maintenance. In view of the major security risks of illegal control instruction injection, the control system design should focus on securi-

ty, use encryption technology to protect the security of instruction transmission, and build a sound access control mechanism, including identity authentication function to prevent unauthorized access and instruction execution [10]. In short, through the above rigorous technical measures and management strategies, the risks of intelligent vehicle outdoor remote driving system in software vulnerabilities, hardware failures and command security can be effectively mitigated, so as to improve the safety and stability of the entire system.

3.3 Data Processing Security Risks

The intelligent vehicle outdoor remote driving system is crucial to the real-time safe processing and analysis of all kinds of key data (such as environmental perception, vehicle status and driver operation data), but there are three major security risks in this process: data tampering, loss and privacy disclosure. In order to deal with the risk of data tampering, the system should adopt encryption technology and data integrity check mechanism to ensure that the data is not tampered with maliciously. To address the risk of data loss, a reliable data backup and recovery mechanism should be deployed to ensure the complete acquisition of critical data even if hardware faults occur. In the face of the risk of privacy disclosure, the system should adopt strict encryption algorithms and access control mechanisms to effectively protect the user personal information contained in it from illegal theft and use. Therefore, the intelligent vehicle system must integrate the above security protection measures to ensure the integrity, availability and confidentiality of the entire data processing process to support the safe and stable operation of the system and provide a safe and reliable remote driving experience.

4 Safety Risk Case Analysis and Coping Strategies

4.1 Related Case Analysis

In recent years, the frequent occurrence of intelligent vehicle safety accidents not only reveals the potential hidden dangers of intelligent vehicles in terms of network information security, system control security and data processing security, but also poses severe security challenges to intelligent vehicle manufacturing enterprises. Taking Tesla as a typical example, in February 2022, its keyless access system was hacked several times, which clearly violated the basic principles of network communication security. Hackers have successfully achieved vehicle unlocking, engine start-up and even disable vehicle safety systems by using software vulnerabilities, showing the limitations of Tesla in software update maintenance and system anti-attack design. It is urgent to build a more rigorous authentication mechanism and an efficient security patch management system.

On the other hand, Toyota 's T-Connect service information leakage incident reveals its security protection defects in the data processing stage. Due to the misuse of source code, a large number of users ' personal information has been accessed by unauthorized third parties for a long time, and the detailed information of nearly

296,000 customers has been leaked. This reflects that Toyota has significant omissions in the use of data encryption technology, access control and data backup and recovery strategy, especially in the comprehensive implementation of end-to-end encryption measures and the formulation of effective data backup and recovery programs, which still need to be further improved.

The above examples have sounded the alarm bell for us. In the whole process of product design and operation, intelligent automobile enterprises must integrate safety risk management strategies into the overall planning. The specific measures can include : strengthening the security of communication protocols, such as adopting the latest encryption standards and safety communication protocols ; optimize the software update process and security vulnerability management system, and regularly carry out strict security audit and strengthening of the system ; implement a rigorous rights control and authentication mechanism to ensure that only authorized users can access and control the vehicle ; in the data processing stage, end-to-end encryption technology is adopted, and a perfect database backup and recovery mechanism is established to minimize the risk caused by data leakage or loss. In addition, companies also need to improve their emergency response capabilities. Once a security vulnerability is detected, they must quickly take repair measures and notify the affected users in a timely manner, thereby comprehensively improving the overall safety performance of smart cars.

4.2 System Safety Design and Optimization Suggestions

In order to further improve the safety of the intelligent vehicle outdoor remote driving system based on 5G network, this study emphasizes that a series of comprehensive safety design and optimization measures must be taken to ensure that the system can maintain its stability and safety in the face of evolving security threats.

In terms of network security, physical layer security is crucial. The combination of Advanced Encryption Standard (AES) and Quantum Key Distribution (QKD) can provide a high-level encryption protection for signal transmission [11]. For the specific implementation of AES and QKD, we can configure the AES algorithm to use 256-bit key length to provide higher security. At the same time, combined with QKD technology, the key can be safely and reliably transmitted to the receiver through the quantum channel. In this way, even if the attacker tries to intercept the key, he cannot obtain any information about the key, thus ensuring the security of the key. AES provides symmetric encryption to ensure the confidentiality of data transmission, while QKD uses the characteristics of quantum states to generate and distribute keys to enhance the security of keys. In addition, end-to-end encrypted communications ensure that data is not intercepted or tampered with during transmission between a smart vehicle and a remote control center by using the Secure Real-Time Transport Protocol (SRTP) or Transport Layer Security Protocol (TLS / SSL). These encryption measures together constitute a strong defense line, which effectively resists security risks such as signal forgery and man-in-the-middle attacks.

In the field of system control security, the multi-factor identity authentication framework provides a strong security defense for the control signal by integrating

public key infrastructure (PKI), biometric technology and one-time password (OTP). The multi-factor authentication scheme shown in Figure 3 shows the structure and process of this integrated security assurance system in detail. Specifically, with the PKI-based digital certificate mechanism, the user 's public key information can be applied to the data encryption and decryption process, thus achieving a highly reliable authentication [12]. At the same time, the integration of biometric technologies, such as fingerprint recognition or facial recognition, further enhances the level of authentication, ensuring that only users with tight biometric matching can initiate or receive control commands. In addition, the use of one-time password (OTP) as a dynamic password means that different passwords need to be entered each time you log in, which greatly improves the security of the system. The instantaneity and unpredictability of OTP make it difficult for attackers to steal and use effective OTP, thus effectively resisting password guessing and replay attacks.In order to fully maintain the integrity of the control signal, on the basis of multi-factor authentication, cyclic redundancy check (CRC) [13] and message authentication code (MAC) [14] are widely used to detect and prevent any form of signal tampering in real time, so as to ensure the authenticity and consistency of each control command transmitted to the system. In short, the multi-factor identity authentication framework and the effective application of CRC and MAC technologies together build a strong system control security barrier.

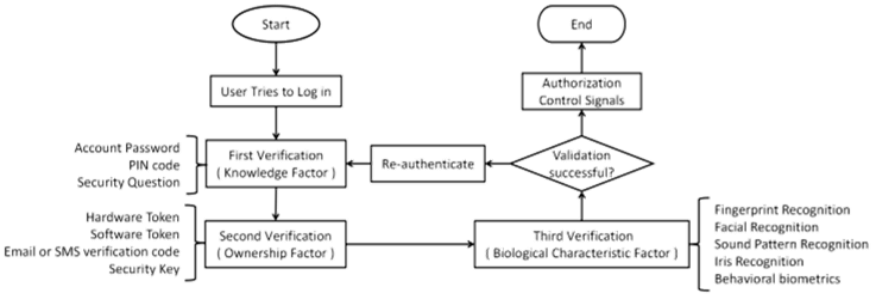

Fig. 3. Multi-factor identity authentication scheme

In terms of ensuring data security, we have adopted multi-level protection measures. First, by using advanced encryption algorithms such as AES and SM4, we guarantee the security of data storage and transmission, and verify the integrity of data through SHA-256 or higher-level hash functions to ensure that the data is not unauthorized modification. In order to protect personal privacy while conducting effective statistical analysis, we adopt differential privacy technology. This technology masks personal identity information by adding random noise in the data processing process, realizes data de-identification processing, and allows statistical analysis of the overall data set without exposing any personal details. In addition, we have established a role-based access control (RBAC) mechanism to strictly limit the access rights of different users to sensitive data [15]. At the same time, we record all data access behaviors through the audit log system, which provides a basis for tracking and

analyzing potential security incidents, thus further strengthening our data security line.

In summary, by integrating the above safety principles and technical details into the system design, and continuously monitoring and optimizing these measures in the actual operation process, the overall safety level of the intelligent vehicle outdoor remote driving system based on 5G network can be significantly improved. This requires system designers and operation and maintenance personnel not only to pay close attention to emerging security threats and technology development trends, but also to regularly evaluate and update security policies to cope with the increasingly complex network security environment. Only in this way can we ensure that the intelligent vehicle outdoor remote driving system can maintain safe and stable operation in a more challenging environment in the future.

5 Conclusion

5.1 Research Summary

This study conducted a comprehensive security risk analysis for the outdoor remote driving system of intelligent vehicles under the background of 5G network. Through a comprehensive review of relevant theories and emerging technologies, the potential security threats and challenges faced by remote driving tasks in the current and future communication network environment are identified [16]. Based on the systematic risk assessment framework, this study identifies and quantitatively analyzes the key security risks in all aspects of network communication, system control and data processing, and then builds the corresponding security rating model and risk matrix. Through in-depth data analysis and experimental verification, this study proposes a series of targeted prevention and control strategies and recommendations to enhance the security performance of the system and the ability to resist potential risks [17].

5.2 Research Prospects

Although the current work has achieved certain results, with the continuous development of 5G and post-5G technology and the continuous innovation of outdoor remote driving technology of intelligent vehicles, future research will focus on improving the security and reliability of 5G network [18]. To this end, the key issues include how to effectively deal with DDoS attacks, end-to-end encryption technology, privacy protection policies, etc., while facing technical challenges such as designing efficient network traffic monitoring mechanisms and developing new encryption algorithms. In addition, optimizing the control algorithm of the intelligent vehicle outdoor remote driving system is also one of the focuses of future research, which needs to balance real-time and stability, develop control strategies in complex environments, and ensure that system faults can be quickly diagnosed and recovered, which requires the development of higher-precision sensors and actuators, and improve the anti-interference ability of the system. Another research direction is to improve the risk assessment model, which involves how to update threat intelligence in real time,

conduct multi-source data fusion analysis, and dynamically adjust security policies. Building an adaptive risk assessment framework will be a technical challenge in this field. Finally, it is also critical to focus on interdisciplinary cooperation to enhance security, including the application of artificial intelligence in anomaly detection, the role of big data analytics in behavioral prediction, and the effective integration of cross-domain knowledge, and the establishment of interdisciplinary teams to jointly develop new security solutions will be the main task in this direction. All in all, future research needs to focus on improving network security capabilities, optimizing remote driving control algorithms, perfecting risk assessment models, and addressing new challenges of outdoor remote driving technology of intelligent vehicles through interdisciplinary cooperation [19].

Reference

1. M. Zheng, "Application of 5G mobile communication technology in intelligent transportation", Information and computer, vol.35, pp.35-37, 2023.
2. 2024 Global Automotive Cybersecurity Report.: Upstream, 2024. [Online]. Available: https://upstream.auto/reports/global-automotive-cybersecurity-report/
3. W. Wu, R. Li, G. Zeng, "Review of research on intelligent connected vehicle network security", JOURNAL OF COMMUNICATIONS, vol.41, pp.161-174, 2020.
4. Li, Ban, "Research on vehicle automatic driving algorithm and application safety AI in 5G network environment", Automation and Instrumentation, vol.242, pp.118-121, 2019.
5. J. Zhou, Research on network security defense technology of intelligent connected vehicles. Hunan University, 2021.
6. J. Duan, Z. Gao, X. Tu, "Design and implementation of remote driving control system based on 5G", Automation technology and application, vol.41, pp. 91-95, 2022.
7. Y. Liu, Y. Zhang, "Application of information security risk assessment in the field of intelligent connected vehicles", China Science and Technology Information, vol.20, pp.115-116+118, 2021.
8. J. Cui, B. Zhang, "VeRA: A Simplified Security Risk Analysis Method for Autonomous Vehicles," in IEEE Transactions on Vehicular Technology, vol. 69, no. 10, pp. 10494-10505, 2020.
9. D. Li, J. Xu, "Network security risk analysis of intelligent connected vehicle system", Industrial information security, vol.04, pp.73-80, 2022.
10. F. Farivar, M. Sayad Haghighi, A. Jolfaei and S. Wen, "On the Security of Networked Control Systems in Smart Vehicle and Its Adaptive Cruise Control," in IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 6, pp. 3824-3831, 2021.
11. H. Shi, T. Pu, J. Zheng, "Research on the key expansion module in quantum noise random stream ciphers", ACTA QUANTUM ELECTRONICS, vol.37, pp.196-201, 2020.
12. A. Thinn, M. Thwin, "A Hybrid Solution for Confidential Data Transfer Using PKI, Modified AES Algorithm and Image as a Secret Key," 2020 IEEE Conference on Computer Applications(ICCA), Yangon, Myanmar, pp.1-4, 2020.
13. N. Sridevi, K. Jamal, "Implementation of Cyclic Redundancy Check in Data Recovery," 2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC), Coimbatore, India, pp. 17-24, 2021.
14. Z. Xie, K. Dong, J. Zhen, "Introduction to international standards related to message authentication code (MAC)", China Quality and Standards Bulletin, vol.05, pp.10-13, 2021.

15. C Binnie, R McCune, "Kubernetes Authorizationwith RBAC," Cloud Native Security, Wiley, pp.251-263, 2021.
16. Z. Xu, "Legal Regulation of Intelligent Connected Vehicle Data Processing: Reality, Challenges and Approaches", Journal of Lanzhou University, vol.50, pp.100-111, 2022.
17. K. Zhou, "Research and design of vehicle networking security system", Chongqing Normal University, 2022.
18. C. Ge, " 5G + Internet of Vehicles Intelligent Connected Vehicles in the Future", Intelligent Connected Vehicles, vol. 04, pp.94-96, Intelligent Connected Vehicles.
19. R. Yang, P. Zhang, Q. Song, "Research and prospect of intelligent vehicle networking based on 5G technology", Telecom Science, vol.36, pp.106-114, 2020.