WEP Warwick Evans Publishing

International Journal of Computer Science and Information Technology

ISSN: 3005-9682 (Print), ISSN: 3005-7140 (Online) | Volume 4, Number 1, Year 2024
DOI: https://doi.org/10.62051/ijcsit.v4n1.36
Journal homepage: https://wepub.org/index.php/IJCSIT/index

Research on Network Security and Privacy Protection Technology of Autonomous Vehicle

Di Wang *

Jurong country garden school, Nanjing, China
*Corresponding Author: 2112785127@qq.com

ABSTRACT

With the rapid development of information technology and the increasing maturity of intelligent transportation systems, autonomous vehicles, as an important carrier of future travel, are gradually moving from concept to commercial application. However, the highly connected and intelligent nature of autonomous vehicles also makes them face unprecedented cybersecurity and privacy protection challenges. This paper deeply discusses the security threats and privacy disclosure risks of autonomous vehicles in network architecture, data transmission, data processing and other links, and systematically reviews the current technical means and research progress to address these challenges. This paper Outlines the data collection and transmission mechanism of autonomous vehicles, including the collection and processing of sensor data as well as the communication process between vehicles and the cloud, other vehicles and transportation infrastructure, and analyzes in detail the network security threats faced by autonomous vehicles, including remote control attacks, malware attacks, communication hijacking, etc. These threats can lead to serious consequences such as vehicle failure, data breach, or system crash. At the same time, the paper also points out the challenges faced by autonomous vehicles in terms of privacy protection, such as the risk of leakage of sensitive data such as personal location information and driving habits, as well as the risk of data abuse and sharing. In order to address the above challenges, this paper focuses on the technical research progress of cybersecurity and privacy protection of autonomous vehicles. In the aspect of network security, this paper discusses the key technical means such as data encryption, access control, intrusion detection and response system, and emphasizes the importance of security hardware and software in improving the overall security of the system. In terms of privacy protection, this paper proposes strategies such as anonymization and desensitization technology, privacy protection protocols and standards to protect users' privacy from invasion.

KEYWORDS

Self-driving cars; Network security; Privacy protection; Data encryption; Intrusion detection; Policies and regulations

1. INTRODUCTION

With the rapid progress of science and technology, autonomous vehicles, as an important part of intelligent transportation system, are gradually moving from the laboratory to the market and becoming an important trend of future travel. Autonomous vehicles integrate advanced sensor technology, artificial intelligence algorithms, big data processing and cloud computing and other cutting-edge technologies to realize the vehicle's autonomous perception, decision-making and control of the environment, which greatly improves the safety and efficiency of road traffic. However, with the continuous development of autonomous driving technology and the expansion of the scope

of application, the problems of network security and privacy protection faced by it have become increasingly prominent, which has become a key factor restricting the healthy development of the autonomous vehicle industry.

As early as the New York World's Fair held in the United States from April to October 1939, General Motors has proposed autonomous driving technology as a means to solve future urban traffic congestion and accidents [1]. The characteristics of future autonomous vehicles are collectively referred to as "CASE", that is, intelligent vehicles containing connected, autonomous, shared and service, electric and other characteristics [2]. According to the prediction of the world famous consulting firm McKinsey, after the maturity of autonomous driving technology, individual users will no longer have to own cars, and autonomous vehicles deployed by travel service providers will replace private cars and become the mainstream of travel [3]. People can quickly plan routes and travel via the Internet just by using their smartphones. From the perspective that autonomous vehicles need real-time networking, autonomous vehicles can also be regarded as Internet of Things cars [4]. However, in recent years, cyber attacks on IoT devices have become more and more intense, and autonomous vehicles that are subjected to cyber attacks not only have the risk of vehicle privacy data disclosure, but also be remotely controlled by hackers, becoming the "chicken" of DDos attacks (that is, remote computers controlled by hackers). The more terrible consequence is that it is hijacked by cyber terrorists and becomes a tool for terrorists to launch car attacks. The remote hijacking of Jeep in 2015 [5] further proves that such concerns about the cybersecurity of autonomous vehicles are not unfounded.

Wang Defu pointed out in "On the Legal Attribute and Governance Approach of Artificial Intelligence Algorithm" that the legal governance of artificial intelligence should focus on the basic attribute of technology [6]. Zhang Yunyan believes in the Contradiction and Unity of Artificial Intelligence and Data Security that in order to balance the contradiction between artificial intelligence and data security, it is necessary to improve the laws on network security [7]. Zhang Yujie pointed out in the Administrative Law Regulation of Driverless Cars that the emergence of self-driving cars not only weakens people's risk handling ability, but also poses a serious threat to people's life safety and traffic order [8]. Wu Wufei, Li Renfa, Zeng Gang and others also warned that cyber attacks against autonomous vehicles will not only cause economic losses and personal information leakage, but even endanger personal safety and national public safety in serious cases [9]. Li Shuo believes that for the legislation of autonomous vehicles, a "progressive" legislative idea should be adopted, focusing on the legal status of autonomous vehicles, legal liability and insurance, privacy protection and network security issues [10].

2. DATA COLLECTION AND TRANSMISSION FOR AUTONOMOUS VEHICLES

2.1. Data Collection Mechanism

Data collection for self-driving cars is a complex and multi-dimensional process that relies on multiple sensors and devices working together. These sensors include, but are not limited to, LiDAR, radar, cameras, ultrasonic sensors, inertial navigation systems, and global positioning systems. Each sensor has its own unique advantages and scope of application, which together constitute the "sensory system" of autonomous vehicles.

LiDAR builds a three-dimensional point cloud map of the surrounding environment by firing a laser beam and measuring its reflection time, providing vehicles with high-precision distance and depth information. Radar is not affected by lighting conditions, can detect the speed and distance of objects ahead, and is particularly sensitive to dynamic obstacles. The camera captures visual information about the surrounding environment and, combined with image recognition technology, is able to identify road signs, pedestrians, vehicles, etc. Ultrasonic sensors are mainly used for close detection,

such as parking assistance, to provide a detailed profile of the vehicle's surroundings. The inertial navigation system combines sensors such as accelerometers and gyroscopes to provide precise position, speed and attitude information of the vehicle. The Global positioning System provides the geographic location information of the vehicle around the world and is the basis for the navigation and positioning of autonomous vehicles. This data is pre-processed and fused by on-board computing units to form a comprehensive perception of the surrounding environment. At the same time, the vehicle will also collect its own status information, such as speed, fuel, temperature, etc., as well as the user's operating instructions and preferences.

2.2. Data Transmission Mechanism

Data transmission in autonomous vehicles involves multiple layers, including communication between systems inside the vehicle, communication between the vehicle and cloud servers, and communication between the vehicle and other vehicles or transportation infrastructure.

Vehicle internal communication: Through the vehicle network (such as CAN bus, FlexRay, etc.) to achieve the data exchange between the sensors, actuators and controllers inside the vehicle. These networks are often high-speed, reliable and real-time, ensuring that the various systems inside the vehicle work together.

Vehicle and cloud communication: Autonomous vehicles need to upload some or all of their data to cloud servers for processing and analysis. The cloud server has powerful computing and storage capabilities, can process massive data in real time, and provide services such as remote upgrade, fault diagnosis and path planning for vehicles. The communication between the vehicle and the cloud usually uses wireless communication technologies, such as 4G/5G, Wi-Fi, etc.

V2X communication: Vehicle-to-Everything communication technology is an important means for autonomous vehicles to interact with the external environment. It includes a variety of communication modes such as vehicle-to-vehicle, vehicle-to-pedestrian, vehicle-to-infrastructure. Through V2X communication, autonomous vehicles can obtain real-time dynamic information about the surrounding environment, such as the driving status of other vehicles, the status of traffic lights, and road construction information, thereby improving the safety and efficiency of driving.

2.3. Data Security and Privacy Challenges

There are many security and privacy challenges in the collection and transmission of data from autonomous vehicles. First, because the data needs to pass through multiple nodes and networks during transmission, it is vulnerable to threats such as hacking and eavesdropping. Secondly, the disclosure of sensitive data may lead to the violation or abuse of user privacy. For example, data such as personal location information and driving habits may be used to track a user's whereabouts or for commercial marketing. In addition, the security of vehicle internal communication is also crucial, once maliciously tampered with or controlled, will directly lead to vehicle function failure or even lead to traffic accidents.

Therefore, in the process of data collection and transmission of autonomous vehicles, a series of technical means and management measures must be taken to ensure the security and privacy of data. This includes the development of data encryption, access control, intrusion detection and prevention systems, and the formulation of privacy protection protocols and standards.

3. CYBERSECURITY THREATS TO SELF-DRIVING CARSIMPACTS OF THE BELT AND ROAD INITIATIVE ON BIODIVERSITY

3.1. Remote Control Attack

Remote control attacks are one of the most serious cybersecurity threats to autonomous vehicles. Attackers can remotely access the vehicle control system through network vulnerabilities or weaknesses to achieve complete control of the vehicle. This type of attack may lead to dangerous behaviors such as vehicle loss of control, emergency stop, acceleration or steering, seriously threatening road traffic safety.

3.2. Malware Attacks

Malware is another common cybersecurity threat. Attackers can implant malicious software (such as viruses, worms, Trojans, etc.) into vehicles through vulnerabilities in on-board systems or improper operations by users. These malware could compromise vehicle systems, steal sensitive data, or serve as a platform for further attacks.

3.3. Communication Hijacking

Autonomous vehicles rely on communication with the cloud, other vehicles, and transportation infrastructure to share information and work together. However, these communication links can also be targeted by attackers. Attackers can interfere with the normal operation of vehicles by hijacking communication links and tampering or falsifying the transmitted data.

3.4. Supply Chain Attack

The supply chain for autonomous vehicles involves multiple links and multiple suppliers, any one of which could be a breakthrough for attackers. By infiltrating a link in the supply chain, an attacker can implant malicious code or components into a vehicle to achieve remote control or data theft.

3.5. Physical Interface Attack

While autonomous vehicles increasingly rely on wireless communication technology, physical interfaces remain an important channel for vehicles to interact with the outside world. Attackers can inject malicious code into vehicles or tamper with vehicle data through physical interfaces (such as OBD interfaces, USB interfaces, etc.).

3.6. Sensor Spoofing

Self-driving cars rely on sensors to sense their surroundings. Attackers can mislead the vehicle's perception system by deceiving the sensor (such as interfering with sensor signals by optical or electronic means, falsifying sensor data, etc.), leading the vehicle to make wrong decisions and actions.

4. PRIVACY CHALLENGES IN SELF-DRIVING CARS

4.1. Collection and Storage of Privacy Data

In the process of driving, self-driving cars collect a large amount of data through various sensors and devices, including vehicle status, road conditions, driving habits and personal information of passengers. These data are of great value for optimizing the autonomous driving algorithm and

improving the driving experience, but they also bring the risk of privacy disclosure. Much of the data collected by self-driving cars involves the user's personal privacy, such as location information, driving trajectory, driving habits, and so on. Once this data is leaked, it can be used to track user movements, analyze user behavior, and even carry out illegal activities. At the same time, self-driving cars need to transfer the collected data to the cloud or local servers for storage and processing. During storage, data may be exposed to the risk of unauthorized access, tampering, or disclosure.

4.2. Data Sharing and Utilization

The development of autonomous vehicles is inseparable from the sharing and utilization of data. Car manufacturers, service providers and government agencies need to share data to optimize autonomous driving algorithms and improve road safety. However, data sharing also brings privacy protection challenges. Ownership of the data generated by self-driving cars is still up for debate. Should the data belong to the vehicle owner, the manufacturer or the service provider? This is directly related to the right to use data, the right to profit and the responsibility to protect privacy. At the same time, in the process of data sharing, there is a risk of data abuse. For example, without user consent, the platform uses user data for commercial marketing, advertising push and other purposes, violating user privacy.

4.3. Technical Challenges and Legal Standards

There are also many technical challenges to privacy protection in self-driving cars. How to achieve real-time data transmission, efficient processing and effective application of privacy protection technology under the premise of ensuring data security is an urgent problem to be solved at present. At the same time, laws and regulations on privacy protection of autonomous vehicles are not perfect at present, and there is a lack of unified standards and norms. This requires relevant departments to increase research and development investment in data encryption, identity authentication, privacy protection technology and other aspects to promote technological innovation and application. Accelerate the formulation and improvement of laws and regulations on the privacy protection of autonomous vehicles, and clarify issues such as data ownership, use rights, and privacy protection responsibilities. Strengthen international cooperation and exchanges to promote the unification and mutual recognition of privacy protection standards for autonomous vehicles. Automobile manufacturers and service providers are encouraged to strengthen industry self-discipline and establish and improve privacy protection mechanisms and management systems. Strengthen the public's awareness and understanding of the privacy protection of autonomous vehicles, and improve users' self-protection awareness and ability.

5. RESEARCH ON NETWORK SECURITY AND PRIVACY PROTECTION TECHNOLOGY

5.1. Research on Network Security Technology

The research of network security technology mainly consists of encryption technology, authentication technology and security protocol. Encryption technology is an important means to protect the security of data transmission. In autonomous vehicles, encryption technology is widely used to encrypt communications between vehicles and the cloud, between vehicles, and to encrypt sensitive information such as vehicle identification numbers. Authentication technology is the key technology to ensure the authenticity of the identity of the communication parties. In autonomous vehicles, authentication technology is applied to authenticate communications between the vehicle and the cloud, vehicle to vehicle, and vehicle to roadside infrastructure. Security protocols ensure the security of data during transmission through a series of predefined rules and processes. Common security protocols used in autonomous vehicles include SSL/TLS, IPSec, and IEEE 1609.2.

5.2. Research on Privacy Protection Technology

The research of network security and privacy protection technology of autonomous vehicle and intelligent connected vehicle involves many aspects. In order to protect user privacy, self-driving cars need to anonymize and desensitize the collected data; Access control technology restricts access to data and prevents unauthorized persons from accessing sensitive data; Privacy protection algorithm introduces protection mechanism in the process of data processing and analysis to prevent privacy disclosure; Blockchain technology, with its decentralized and immutable characteristics, has shown great potential in the field of privacy protection. Through the comprehensive application of these technologies and means, a comprehensive and multi-level protection system can be built to effectively protect user privacy and data security. At the same time, it is also necessary to strengthen legal and regulatory compliance, regular safety assessment and audit, and user education and awareness to jointly promote the healthy development of the autonomous vehicle industry.

6. CONCLUSION

As an important trend of future transportation, the development and popularization of autonomous vehicles are inevitably accompanied by the challenges of network security and privacy protection. Every step in the data collection, storage, sharing and processing process can become a source of privacy breaches and security risks. In order to cope with these challenges, the industry and academia have conducted in-depth research on encryption technology, authentication technology, security protocols, data anonymization and desensitization, access control, privacy protection algorithms, and blockchain technology, and have achieved a series of important results. These technologies provide a strong support for the cybersecurity and privacy protection of autonomous vehicles. A single protection approach is difficult to fully address the complex security threats faced by autonomous vehicles. Therefore, it is particularly important to build a multi-level protection system including encryption, authentication, access control, privacy protection algorithms and blockchain technology. This comprehensive protection system can protect the network security and privacy of autonomous vehicles in an all-round and multi-angle manner. In addition to technical means, the formulation of laws, regulations and standards is also an important part of ensuring the network security and privacy of autonomous vehicles. Perfect laws and regulations and unified standards can provide legal protection and code of conduct for the development of autonomous vehicles.

With the continuous progress of technology, new network security and privacy protection technologies will continue to emerge and deeply integrate with existing technologies. For example, emerging technologies such as artificial intelligence and quantum computing are expected to bring revolutionary changes to the cybersecurity and privacy protection of autonomous vehicles. With the popularization of autonomous vehicles and the expansion of application scenarios, relevant laws, regulations and standards will continue to improve and refine. This will provide more clear and specific guidance for cybersecurity and privacy protection of autonomous vehicles. In the future, users will pay more attention to the cybersecurity and privacy protection of autonomous vehicles. Therefore, strengthening user education and enhancing user awareness will become an important part of promoting the healthy development of autonomous vehicles. At the same time, user participation will also become an important force for network security and privacy protection. Cybersecurity and privacy protection for autonomous vehicles are global issues that require concerted efforts from governments, businesses and academia. Strengthening international cooperation and exchange, sharing security threat information and prevention experience will become an important trend of future development.

REFERENCES

[1] SONAL PANSE, Futurama–Unveiling the City of the Future at the 1939 New York World's Fair, at https://www.ststworld.com/1939-new-york-worlds-fair/, NOV.21, 2018.

[2] Mercedes-Benz, What is the Mercedes-Benz CASE Initiative? at https://www.silverstarny.com/blog/what-is-the-mercedes-benz-case-initiative/, Jun.26, 2018.

[3] McKinsey Center for the Future of Mobility: "China May Become the World's Largest Autonomous Driving Market", source: https://www.mckinsey.com.cn/%e9%ba%a6%e8%82%af%e9%94%a1%e6%9c%aa%e6%9d%a5%e5%87%ba%e8%a1%8c%e7%a0%94%e7%a9%b6%e4%b8%ad%e5%bf%83%ef%bc%9a%e4%b8%ad%e5%9b%bd%e6%88%96%e5%b0%86%e6%88%90%e4%b8%ba%e5%85%a8%e7%90%83%e6%9c%80%e5%a4%a7/

[4] Keisuke Nonaka, Ryo Watanabe, Kohei Tsukamoto, Real-time transmission of free view image using 5g network, Journal of Image Information Media Society, Vol 74, 2020, p.180-186.

[5] Andy Greenberg, The Jeep Hackers Are Back to Prove Car Hacking Can Get Much Worse, at https://www.wired.com/2016/08/jeep-hackers-return-high-speed-steering-acceleration-hacks/, AUG.1, 2016.

[6] Wang Defu, "On the Legal Attribute and Governance Approach of Artificial Intelligence Algorithm", Journal of Wuhan University (Philosophy and Social Sciences Edition), No.5, 2021.

[7] Zhang Yunyan, "The Contradiction and Unity of Artificial Intelligence and Data Security", Shanghai Law Research, volume 7, volume 55, 2021.

[8] Zhang Yujie, "On the Administrative Law Regulation of Driverless Cars", Administrative Law Research, 2018 (1).

[9] Wu Wufei et al. "Review on the Network Security of Intelligent Connected Vehicles", Journal of Communications, No. 6, 2020.

[10] Li Shuo, "Research on the Legislation of Autonomous Vehicles", Administrative Law Studies, 2019 (2).