Theory and Practice of Science and Technology
2025, VOL. 6, NO. 8, 202-207
DOI: 10.47297/taposatWSP2633-456937.20250608

Overview of Network Security and Risk Assessment for Intelligent Connected Vehicles

Yunfeng Wan

Manchester Metropolitan Joint Institute, Hubei University, Wuhan, Hubei, 430000, China

ABSTRACT
This paper investigates the cybersecurity risks in vehicle networking systems, comparing signature-based, anomaly-based, and deep learning-based intrusion detection technologies. It evaluates their applicability, accuracy, real-time performance, and resource consumption, and explores existing limitations. A tailored cybersecurity risk assessment system for intelligent connected vehicles is also summarized, with future threats anticipated. This study provides a systematic review, technology comparison, and assessment framework for the field.

KEYWORDS
Intelligent connected vehicles; Network security; Risk assessment; Intrusion detection; Connected vehicles

1 Introduction

With the advancement of the "new four modernizations" of electrification, intelligence, networking, and sharing in automobiles, connected cars have evolved from simple transportation tools to a fusion of "mobile intelligent terminals, distributed energy nodes, and data processing centers". However, the tight connection between vehicles and external networks (such as V2X, OTA, and cloud services) as well as internal heterogeneous networks (such as CAN/CAN-FD, in vehicle Ethernet, TSN) also poses a wider range of network security threats. At present, although some progress has been made in the fields of vehicle network security protection and intrusion detection, there are still many challenges to be solved.

On the one hand, existing research mostly focuses on the analysis of single technologies or specific scenarios, lacking a systematic review and comprehensive evaluation of network security threats to intelligent connected vehicles. For example, Zeng Fan [1] studied the intrusion detection system of the Internet of Vehicles, and Chen Junsheng [2] further analyzed the network security situation of intelligent connected vehicles by introducing the network architecture, the application of the Internet of Vehicles, and the analysis of network security issues. Li Yufeng et al [3]. introduced the electronic and network structures of intelligent vehicles, elaborated on the network security requirements of intelligent vehicles, pointed out several network attacks on intelligent connected vehicle systems, and investigated available defense measures against these attacks. Yu Mingming et al [4]. analyzed the network security threats faced by intelligent connected vehicles from four dimensions: vehicle networking cloud service platform, vehicle networking communication, in vehicle terminals, and external connection terminals, and proposed corresponding security protection strategies. In addition, Peng Haide [5] studied CAN network intrusion detection technology and proposed a detection scheme based on ID entropy and support vector machine data correlation (SVM-DR), and designed a vehicle mounted CAN network intrusion detection device. On the other hand, most existing network security risk assessment systems are based on traditional network environments, which are difficult to adapt to the complex network architecture and dynamic operating environment of intelligent connected vehicles, resulting in insufficient accuracy and reliability of assessment results.

The remaining content of this article is as follows. In Chapter 2, the network security threats faced by in vehicle networks were first classified into four categories, and their sources were explained in detail. In Chapter 3, this article introduces and classifies intelligent connected vehicle networks. Chapter 4 summarizes network attack methods and intrusion detection techniques, with a focus on specific attack methods and detection methods. At the end of this article, the future security development and several challenges faced by intelligent connected vehicles are discussed.

2 Classification and sources of security threats

This section categorizes the network security threats faced by connected vehicles. According to the different attack vectors used by attackers when launching network attacks on intelligent connected vehicles, these network security threats can be summarized into four main aspects, covering the "cloud management end" of the entire connected vehicle ecosystem, including security threats to the connected vehicle cloud service platform, connected vehicle communication, in vehicle terminals, and external connection terminals, as shown in Figure 1.

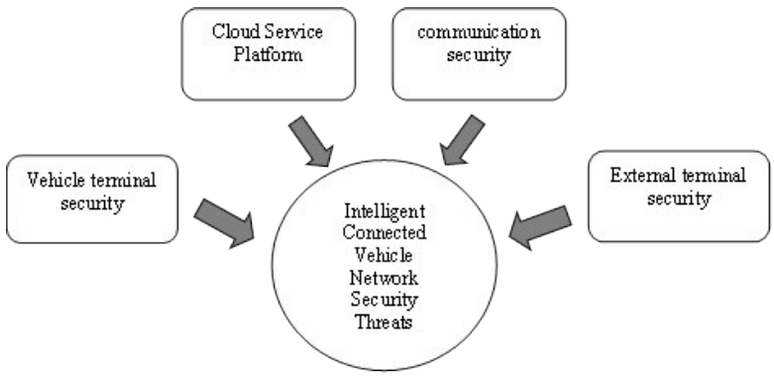

Figure 1 Network Security Threats of Intelligent Connected Vehicles

2.1 TSP security threat

As a key part of the intelligent connected vehicle ecosystem, the Connected Vehicle Service Platform (TSP) provides important functions such as vehicle monitoring, remote control, navigation services, emergency rescue, data analysis, and software updates, but also faces various network security threats. These threats mainly focus on areas such as network application security, middleware security, server security, and database security, specifically manifested as SQL injection attacks, cross site scripting attacks, unauthorized access, weak identity authentication, data breaches, malicious Trojan horse implantation, and system vulnerabilities. These issues may not only jeopardize the normal operation of vehicles, but also lead to the leakage of user privacy and instability of the entire vehicle networking system. Therefore, ensuring the security of TSP is crucial.

2.2 Security threats to vehicle networking communication

Vehicle networking communication is divided into car communication and out of car communication. In car communication is achieved through CAN bus, Ethernet, etc. to facilitate the flow of data between various control systems, facing threats such as forgery, tampering of instructions, denial of service, and replay attacks. Vehicle external communication is divided into short-range communication (such as WiFi, Bluetooth, etc.) RFID, used for information transmission between vehicles and mobile vehicle control apps, as well as remote communication (through 4G/5G communication with cloud service platforms to achieve functions such as autonomous driving), mainly face risks in identity authentication, communication transmission, and communication protocols. These communication security threats, combined with the previously mentioned issues of vehicle networking communication interference and data tampering, may endanger driving safety and traffic order.

2.3 Security threats to vehicle terminals

The security threats of car terminals mainly come from software vulnerabilities, malware infections, user privacy breaches, and hardware security issues. Software vulnerabilities may be exploited by attackers to implant malicious software, thereby controlling critical vehicle functions such as braking or steering systems. User privacy data, including location information and driving habits, may be leaked due to insufficient terminal security protection. In addition, the hardware of the in vehicle terminal may also face the risk of tampering or damage, which not only damages the normal operation of the vehicle but may also endanger the safety of the driver and passengers.

2.4 External connection terminal security threats

The security threats of external connection terminals mainly stem from the risks that may be introduced when they are connected to vehicles. These terminals, such as smartphones, tablets, or portable diagnostic devices, may carry malicious software if their security protection is insufficient. Once connected to the vehicle, they can infect the onboard system, thereby controlling critical vehicle functions or stealing user data. In addition, if the communication link during the connection process is not encrypted, it is also prone to eavesdropping or tampering, resulting in information leakage or incorrect instruction transmission.

3 Intelligent connected vehicle onboard network

3.1 Introduction to automotive onboard network

The intelligent connected vehicle network is a key infrastructure for communication between various electronic control units (ECUs), sensors, and actuators inside the vehicle. It achieves high-speed and reliable data transmission through communication protocols such as CAN bus, LIN bus, FlexRay, and Ethernet, supporting functions such as autonomous driving, intelligent cockpit, and vehicle monitoring.

3.2 Classification of automotive onboard networks

The electronic control system of intelligent connected vehicles has different requirements for real-time communication, and the onboard network is divided into high-speed, medium speed, and low-speed networks based on communication speed. According to SAE standards, in vehicle networks are divided into five categories: Class A low-speed networks, Class B medium speed networks, Class C high-speed networks, Class D multimedia networks, and Class E secure application networks. The specific classification is shown in Table 1. The five common on-board networks in ICV communication system include Controller Area Network (CAN), Local Interconnect Network (LIN), FlexRay, MOST and on-board Ethernet [6].

Table 1 [3] Vehicle network classification

Network category	Network category	Communication speed	Cost
A-class low speed network	TTP/A、LIN	Less 10Kbps	Low
B-class medium speed network	Low speed CAN、VAN	10Kbps – 125Kbps	Low
C-class high speed network	High speed CAN、CAN-FD、TTP/C、FlexRay	125Kbps – 1Mbps	Medium
D-class multimedia network	MOST、Bluetooth、ZigBee	250Kbps – 100Mbps	High
E-class secure application network	Bytelight	10Mbps	High

CAN (Controller Area Network) is a serial data communication protocol with a bus topology structure, first proposed by Bosch in 1983 and becoming an international standard. From a security perspective, the low latency and high reliability of CAN networks enable them to quickly respond to vehicle control commands [7], but their openness and broadcast characteristics also increase the attack surface, making them vulnerable to data injections, tampering, and replay attacks. Therefore, although CAN networks play an important role in vehicle communication, their security measures also need to be continuously strengthened to cope with increasingly complex network security threats.

LIN (Local Interconnect Network) is a low-cost serial communication protocol, which is mainly used for low-speed communication inside the vehicle. The advantages of LIN network are low cost and simple structure, but its low fault tolerance makes it vulnerable to attacks. Due to the fact that LIN networks are typically used as auxiliary networks for CAN networks, their security measures also need to be coordinated with CAN networks to reduce potential attack surfaces and data tampering risks.

FlexRay is a high-speed, fault-tolerant in vehicle network technology developed by the FlexRay Alliance. The dual channel design of FlexRay significantly improves system reliability and reduces the risk of system failure caused by single point failures. Its high transmission speed reduces communication latency and ensures timely transmission of critical control instructions. However, FlexRay's openness and broadcast features also increase the potential attack surface, which may be vulnerable to data injection, tampering, and replay attacks. In addition, its high cost limits its large-scale application and is typically used in conjunction with CAN networks to balance cost and security.

MOST (Media Oriented System Transport) is a network designed specifically for automotive multimedia systems, using a ring topology with a theoretical maximum bandwidth of 150 Mbps [8]. The MOST network uses plastic optical fibers as the physical layer, which can effectively isolate electromagnetic interference and ensure the clarity and stability of information transmission. From a security perspective, the use of plastic optical fibers enhances the security of the physical layer and reduces the risk of data tampering caused by external interference. The ring topology structure enhances the fault tolerance of the network, allowing data to be transmitted through other paths even if some links are damaged. However, the high cost and complex gateway development of MOST networks limit their widespread application, mainly in high-end automobiles. Although its closure reduces the attack surface to a certain extent, once the access point is breached, it may still face security threats such as data leakage.

Vehicle Ethernet is an emerging vehicle networking technology with a bandwidth of up to 100 Mbps [8], which is expected to increase to 1 Gbps in the future, approximately 100 times faster than traditional CAN networks. Vehicle Ethernet has the characteristics of high bandwidth and low latency, which can meet the increasing demand for high bandwidth in modern cars, such as laser radar, safety radar, ECU flash interface, etc. However, due to its much higher cost than CAN networks, in car Ethernet is unlikely to completely replace CAN networks, but rather serve as an auxiliary network to enhance automotive communication capabilities.

4 Attack methods and intrusion detection techniques

With the rapid development of information technology, automobiles have shifted from closed local area control networks to intelligent networking modes. As a key underlying control network for intelligent connected vehicles, the CAN network includes many ECUs and sensors, responsible for sending control commands, monitoring status information, and external communication. Nowadays, there are over a hundred ECUs inside high-end cars, which are connected to the external environment through various wired and wireless interfaces such as USB, OBD, Bluetooth, WIFI, 4G/5G communication, etc. Although this provides convenience and diversified functions for drivers and passengers, it

also brings safety hazards. This chapter will focus on CAN network attack methods, analysis of information security issues, and security protection technologies.

4.1 Typical attack methods and risk assessment

Attackers often exploit vulnerabilities in data resource servers, cloud servers, communication links, identity authentication, CAN buses, and other links in connected vehicles to launch attacks. In response to the limitations of intelligent in vehicle networks and their external interfaces, hackers mainly use DoS, sniffing, replay, discard, impersonation and other attacks. As shown in Table 2, each attack causes corresponding abnormal in vehicle network communication based on its attack characteristics.

Table 2 Network security attack methods and risk assessment

Attack mode	Threat level	Degree of protection	Attack Results
DoS attack	High	Low	Communication failure, network crash
Sniffing attack	Medium	High	Privacy message leakage
Replay attack	High	Medium	Load rate increases, affecting communication function
Discard attack	High	High	Some important functions of the car have failed
Sybil attack	High	Medium	Network load rate and ID entropy increase

4.1.1 Dos attack

Denial of Service (DoS) attack is a common network attack method in which attackers exhaust the resources of the target system (such as network bandwidth, processing power, and memory) by sending many false requests or interfering signals, causing legitimate users to be unable to access services normally and resulting in system paralysis. Somani G et al [9] provides a detailed introduction to the threats of Dos attacks to cloud security, and proposes corresponding preventive measures. For example, deploying firewalls and intrusion detection systems that can monitor network traffic in real-time, identify and block abnormal traffic; Implement traffic filtering technology by setting access control lists (ACLs) or using deep packet inspection (DPI) devices to restrict traffic from specific IP addresses or ports; The comprehensive application of these measures can significantly enhance the system's ability to resist DoS attacks and ensure the stable operation of network services.

4.1.2 Sniffing attack

Sniffing attacks are carried out by attackers by inserting listening devices or using software tools in network links. In intelligent connected vehicles, attackers often target communication links such as CAN bus, Bluetooth, WiFi, etc. to capture driving data, user information, and control commands of the vehicle. Sniffing attack is the most common and effective method used in CAN bus attacks. To prevent sniffing attacks in intelligent connected vehicles, firstly, end-to-end encryption of vehicle communication data is carried out, and mutual authentication protocols such as TLS are used to ensure the security of data transmission [10]. Secondly, utilizing intrusion detection systems (IDS) to monitor network traffic in real-time and identify abnormal activities [10]. In addition, intrusion detection techniques based on signal features, such as using clock signals or voltage features to detect abnormal CAN frames, can also effectively prevent ECU spoofing attacks.

4.1.3 Replay attack

Replay attack is a simple attack method, in which the attacker invades the network, captures the messages in the network, replays them directly to the network without modification, and interferes with the communication of the car network. In the field of intelligent connected vehicles, attackers can capture legitimate command data packets such as unlocking car doors and starting the engine, and resend them at the right time to illegally control the vehicle. This type of attack can bypass the vehicle security authentication mechanism, endanger the safe operation of vehicles, and lead to user information leakage and property damage.

4.1.4 Discard attack

In discard attacks, attackers manipulate network nodes to discard specific packets or messages, preventing them from reaching their targets. In intelligent connected vehicles, attackers often target V2X communication links, discarding critical information such as emergency braking signals, traffic congestion information, or software update packages, disrupting normal vehicle communication, and affecting driving safety and traffic efficiency. If the attacker is on the only critical communication path between two groups of users and there are no other alternative paths, then a black hole attack will cause these two groups of users to be unable to communicate and isolated from each other [11].

4.1.5 Sybil attack

Sybil attack is a malicious behavior in which attackers create false identities or nodes to disrupt distributed systems

and networks. Attackers use fake nodes to send incorrect information, disrupt the vehicle decision-making system, reduce system performance, and cause security issues. To prevent such attacks, it is necessary to use identity authentication and encryption technology to verify node identity, and combine reputation mechanisms and anomaly detection algorithms to identify and isolate abnormal nodes, ensuring the security and reliability of the communication system.

4.2 Vehicle network intrusion detection technology

Vehicle mounted network intrusion detection identifies behaviors that deviate from normal modes by analyzing network traffic and communication patterns. The normal mode is established through long-term observation and statistical analysis of network communication of the car in a safe driving state. Once abnormal behavior is detected, the system will issue an alert and take corresponding protective measures. At present, this detection technology is usually based on abnormal feature libraries, statistical learning, or machine learning methods. This section summarizes and categorizes them from three directions. This section summarizes and categorizes them from three perspectives. The following table shows the advantages, disadvantages, and applicability of these three methods.

Table 3 Comparison of in vehicle network intrusion detection methods

Methods	Detection rate	real-time	Applicable scenarios	Advantage	Disadvantage
Construct an abnormal feature library	Medium	Medium	Scenarios with multiple known attack modes	Quickly identify and determine the type of anomaly	The feature library needs regular maintenance
statistical analysis	Medium	High	Scenarios with frequent periodic messages	The threshold can be adjusted according to user habits	Suitable for simple abnormal behavior
machine learning	High	Medium	Complex attack detection	Good detection performance for complex attacks	Need a large amount of labeled data for training

4.2.1 Construct an abnormal feature library

Intrusion detection based on abnormal feature library, which describes intrusion behavior through features and stores abnormal features and pattern rules in the feature library. When detecting, match user behavior with the feature library, and a successful match indicates an exception. The feature library needs to be regularly maintained, with updated data and the addition of anomalous new features. This method can quickly identify and determine the type of anomaly, but it relies on professional knowledge to establish a feature library. If the feature library is missing, it will seriously affect the accuracy of detection. In addition, the cross-sensor data cross correlation and authentication method proposed by Daksh et al [12]. can quickly locate damaged locations, but its application scope is relatively narrow.

4.2.2 Information theory and statistical methods

The in car network intrusion detection technology based on statistical learning learns its patterns by analyzing the state of normal communication networks (such as cycle, traffic, time, etc.) and compares the obtained network packets with these patterns to determine whether there are abnormalities. This method does not rely on prior knowledge of attack behavior, can detect unknown attacks, and can adjust thresholds based on user driving habits to optimize the detection system. However, it is mainly suitable for simple abnormal behaviors such as flooding, replay, and discard attacks, and has limited detection capabilities for complex tampering attacks. In addition, using statistical methods to study the bus frame data flow, extracting frame message flow features to establish an anomaly detection model, can monitor the in-car network in real time. The research of Han et al. [13] and Marchetti et al. [14] shows that such models have good detection performance for periodic messages, but poor detection performance for event triggered messages.

4.2.3 Machine learning

Machine learning is a technique that utilizes algorithms to parse data, learn from it, and make decisions based on the learning results. It automatically identifies normal and abnormal behavior patterns by analyzing large amounts of network traffic data, without the need for manual setting of specific rules. Its advantage lies in its ability to process complex data, automatically discover patterns and relationships hidden in the data, and effectively detect various types of attacks, including complex tampering attacks. However, machine learning also has some drawbacks. Firstly, training the model requires a large amount of annotated data, and the process of collecting and annotating this data may be time-consuming and costly. Secondly, the training and operation of machine learning models typically require high computational resources, which may limit their application in resource constrained in vehicle environments. Finally, the decision-making process of machine learning models often lacks interpretability, making it difficult to intuitively understand why the model produces specific detection results, which poses certain challenges for security analysis and auditing.

5 The development trend of network security for intelligent connected vehicles

The development trend of intelligent connected vehicle safety presents multidimensional integration and deepening. From a technical perspective, cutting-edge technologies such as information theory and machine learning will deeply integrate with traditional network security technologies, providing stronger support for intrusion detection and risk assessment. For example, detection methods based on information entropy can effectively identify abnormal changes in network traffic, while machine learning algorithms can build models by learning large amounts of data to automatically identify complex attack patterns, thereby improving the accuracy and reliability of detection. This technological integration will enable intelligent connected vehicles to more accurately respond to increasingly complex network security threats.

In terms of security assessment system, in the future, more emphasis will be placed on the integrity and comprehensiveness of the system. No longer limited to the security assessment of a single component or network, but starting from multiple aspects such as vehicle internal and external networks, in vehicle terminals, cloud service platforms, etc., a comprehensive network security risk assessment system is constructed. This system will cover the entire lifecycle from design, development, testing to operation and maintenance, ensuring effective security protection for intelligent connected vehicles at all stages. At the same time, with the development of vehicle to road collaborative V2X communication technology, V2X communication safety will become an important component of evaluation, ensuring the safety of communication between vehicles and infrastructure.

Supply chain security issues will receive more attention. The complexity of intelligent connected vehicles makes every link in the supply chain a potential target for attack. Therefore, in the future, we will strengthen the security management of the supply chain to ensure the safety of components and software. Establish a collaborative defense mechanism for the supply chain, jointly respond to network security threats through information sharing and collaborative cooperation, and enhance the anti attack capability of the entire supply chain. This will help ensure the safety of intelligent connected vehicles from the source.

In addition, vehicle road collaboration and V2X communication security will become research hotspots. With the continuous development of vehicle road collaboration technology, communication between vehicles and infrastructure will become more frequent. This not only brings convenience to intelligent transportation, but also presents new safety challenges. Future research will focus on how to ensure the security of V2X communication, prevent communication data from being tampered with, forged, or leaked, and how to achieve secure authentication and authorization between vehicles and infrastructure. This will help establish a safer and more reliable intelligent transportation system.

References

[1] Chen, J. (2023). Cybersecurity Analysis of Intelligent Connected Vehicles. Mechanical and Electrical Technology, (4), 90-93.

[2] Li, Y., Lu, X., Cao, C., et al. (2020). A Preliminary Analysis of Cybersecurity in Intelligent Connected Vehicles. Automotive Engineering, (5), 1-10.

[3] Guan, Y., Ji, H., Cui, Z., et al. (2023). A Review of Intrusion Detection Methods for In-Vehicle CAN Networks. Automotive Engineering, (6), 1-10.

[4] Yu, M., Ning, Y., Shen, S., et al. (2023). Practical Exploration and Research on Automotive Cybersecurity. Information Security Research, (5), 476-481.

[5] Peng, H. (2021). Research on Intrusion Detection Methods for Automotive CAN Networks. Dalian University of Technology.

[6] Elkhail, A. A., Refat, R. U. D., Habre, R., et al. (2021). Vehicle Security: A Survey of Security Issues and Vulnerabilities, Malware Attacks and Defenses. IEEE Access, 9, 162401-162437.

[7] ISO. (2015). Road Vehicle - Interchange of Digital Information - Controller Area Network (CAN) for High-Speed Communication. ISO 11898.

[8] Dibaei, M., Zheng, X., Jiang, K., et al. (2021). Attacks and Defences on Intelligent Connected Vehicles: A Survey. Digital Communications and Networks, 6(4), 399-421.

[9] Somani, G., Gaur, M. S., Sanghi, D., et al. (2017). DDoS Attacks in Cloud Computing: Issues, Taxonomy, and Future Directions. Computer Communications, 107, 30-48.

[10] Ning, J., & Liu, J. (2019). An Experimental Study Towards Attacker Identification in Automotive Networks. In IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 1-6.

[11] Dibaei, M., Zheng, X., Jiang, K., et al. (2019). An Overview of Attacks and Defences on Intelligent Connected Vehicles. arXiv preprint arXiv: 1907.07455.

[12] Ning, J., & Liu, J. (2019). An Experimental Study Towards Attacker Identification in Automotive Networks. In IEEE Global Communications Conference (GLOBECOM), Waikoloa, HI, USA, 1-6.

[13] Tian, M. Q., Jiang, R. B., Xing, C. Q., et al. (2019). Exploiting Temperature-Varying ECU Fingerprints for Source Identification in In-Vehicle Network Intrusion Detection. In IEEE 38th International Performance Computing and Communications Conference (IPCCC), Piscataway: IEEE Press, 1-8.

[14] Zhao, Y. L., Xun, Y. J., Liu, J. J. (2022). ClockIDS: A Real-Time Vehicle Intrusion Detection System Based on Clock Skew. IEEE Internet of Things Journal, 9(17), 15593-15606.