Frontiers in Computing and Intelligent Systems
ISSN: 2832-6024 | Vol. 15, No. 1, 2026

Network Intrusion Detection for Intelligent Driving

Yinqin Tong *

Computer Science and Technology, Xidian University, Xi'an, Shaanxi, 710126, China
*** Corresponding author Email:** tongyinqin14@gmail.com

Abstract: The rapid advancement of intelligent driving technology has increased communication between vehicles, external networks, cloud platforms, and other vehicles, significantly elevating cybersecurity risks. Since intelligent driving systems rely heavily on in-vehicle networks and wireless communications, they are vulnerable to various network attacks. Traditional security measures often fail to meet the stringent real-time and accuracy requirements of such systems, making it urgent to develop efficient and intelligent intrusion detection systems to ensure safe and stable operation. This paper begins by analyzing the network architecture and security requirements of intelligent driving systems, and reviews mainstream network intrusion detection technologies—including feature matching, anomaly detection, and methods based on machine learning and deep learning. By comparing the strengths and weaknesses of different approaches, it highlights the challenges related to real-time performance and accuracy that conventional detection techniques face in intelligent driving environments. The study also discusses future trends in intelligent driving cybersecurity, emphasizing the importance of integrating AI technology with cybersecurity to enhance intrusion detection capabilities. Finally, the paper proposes research directions such as multi-level defense systems and cross-domain collaborative defense, offering both theoretical and practical support for securing intelligent driving systems.

Keywords: Intelligent Driving; Network Intrusion Detection; Machine Learning; Deep Learning.

1. Introduction

1.1. Research Background

The field of intelligent driving has seen rapid advancements, particularly in the development of automated driving systems. According to forecasts, the global intelligent driving market is set to grow from US $42 billion in 2023 to US $150 billion by 2030. This growth is propelled by increasing levels of automation in driving systems, from assisted driving (L2) to highly automated driving (L4). As these technologies evolve, the security risks associated with network vulnerabilities in intelligent driving systems also grow. Table 1 presents the market share prediction for different levels of autonomous driving, showing the shift towards higher levels of automation as technology progresses.

Table 1. Prediction of different autonomous driving levels and market share

Autonomous driving level	function description	Market share in 2023	Market share in 2030
L0	No automation	40%	10%
L1	Driving assistance	30%	15%
L2	Part autonomous driving	20%	25%
L3	Conditional autonomous driving	7%	30%
L4	Highly autonomous driving	3%	20%

1.2. Research Objectives and Research Questions

The goal of this study is to develop a real-time, efficient intrusion detection model to protect intelligent driving systems from cyber threats. The key question is: "How can we build an efficient, real-time network intrusion detection model for intelligent driving systems?" Figure 1 presents the logical framework diagram for improving network intrusion detection capability of intelligent driving system.

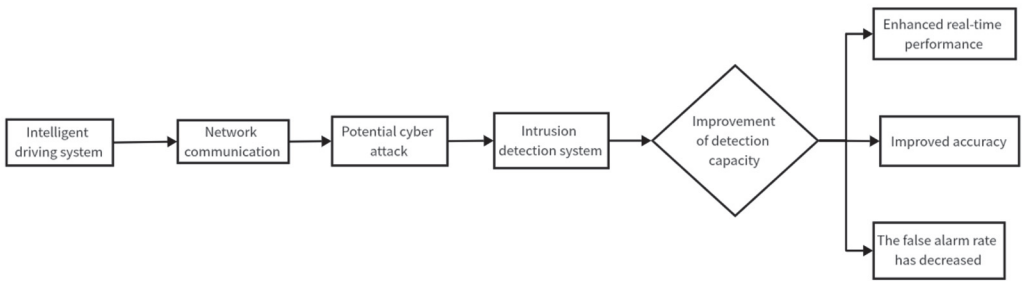

Figure 1. Logical framework diagram for improving network intrusion detection capability of intelligent driving system

The following table 2 presents the performance indicators of various detection models within the intelligent driving environment:

Table 2. Performance comparison of intelligent driving network intrusion detection models

Model type	Detection accuracy rate (%)	False alarm rate (%)	Response Time (ms)	Resource consumption (%)
Rule matching model	85.2	12.5	150	30
Traditional machine learning	90.8	8.3	120	45
Deep learning model	94.5	5.7	200	70
Integrate multi-source data models	96.3	4.1	130	50

Building an efficient and real-time network intrusion detection model requires not only technical innovation, but also the actual application scenario of intelligent driving system to ensure that the detection system can ensure safety without affecting the normal operation of vehicles. The following Figure 2 presents workflow diagram of intelligent driving network intrusion detection system:

1.3. Research Significance

As a new cross-cutting field, intelligent driving network security integrates multi-disciplinary knowledge such as autonomous driving technology, communication network and information security, which is of great significance to promote the development of its theoretical system. The complexity and real-time character of intelligent driving system pose new challenges to traditional network security theory, prompting researchers to improve intrusion detection model and defense mechanism continuously. By constructing a theoretical framework of network security adapted to intelligent driving environment, various attack scenarios and their effects can be systematically analyzed, and the guidance and application value of the theory can be improved. Theoretical innovation provides scientific basis for standard formulation and policy support of intelligent driving network safety technology, and promotes healthy development of industry. The following Table 3 shows the key elements and their roles in the development of cybersecurity theory for intelligent driving:

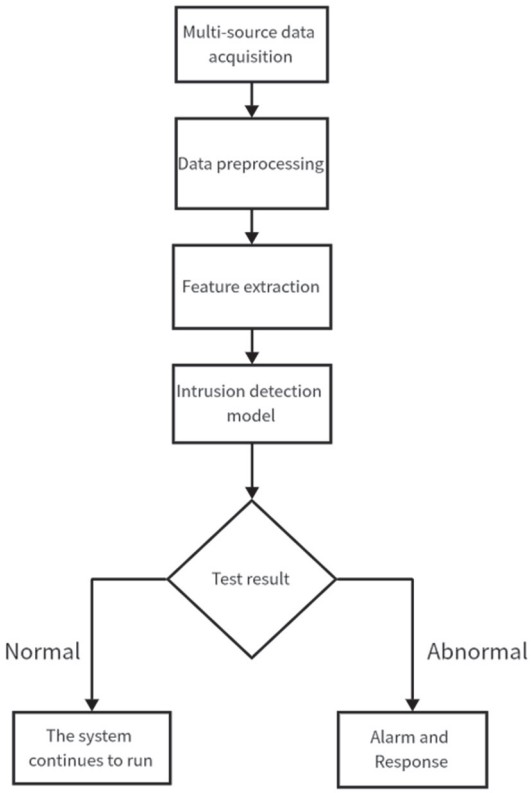

Figure 2. Workflow diagram of intelligent driving network intrusion detection system

Table 3. Key elements and functions of intelligent driving network safety theory development

Element	Function description	Key technologies
Real-time	Support rapid response and decision-making	Real-time monitoring algorithm
Multi-source data fusion	Comprehensive analysis of multidimensional information	Data fusion model
Anomaly detection	Identifying unknown attacks	Machine learning algorithms
Collaborative Defense	Multi-node collaboration achieves defense	Distributed Defense Mechanism

The intelligent driving safety theoretical system, with the intelligent driving network security theory at its core, extends into four key research directions: real-time performance (corresponding to real-time monitoring algorithms), multi-source data fusion (corresponding to data fusion models), anomaly detection (corresponding to machine learning algorithms), and collaborative defense (corresponding to distributed defense mechanisms).

The perfection of this theoretical system not only promotes the academic research of intelligent driving network security, but also provides a solid foundation for the safety design of practical systems.

2. Literature Review

2.1. Foreign Research Status

2.1.1. Research Progress on Smart Driving Network Security

Nie et al. proposed a data-driven method based on deep convolutional neural network (CNN) for network intrusion detection of intelligent networked vehicles, which effectively improved the accuracy and real-time performance of detection and made up for the shortcomings of traditional methods in complex environments[1]. Fang et al. designed an enhanced cyclic consistency generative adversarial network

model based on generative adversarial network (GAN), which enhanced the recognition ability of unknown attacks and improved the safety protection level of intelligent driving system [2]. Donghua Normal University teamproposed a lightweight intelligent intrusion detection system, which takes into account detection efficiency and resource consumption, is suitable for embedded platforms, and realizes efficient real-time detection [3]. These studies promote the development of intelligent driving network security technology from different perspectives, highlighting the important role of deep learning and lightweight design in intrusion detection.

2.1.2. Development and Application of Network Intrusion Detection Technology

The application of network intrusion detection technology in intelligent driving system attracts much attention. Ridwan et al. proposed a hybrid intrusion detection system based on machine learning, which combined with intelligent routing algorithm in multipath label switching (MPLS) network, effectively improved detection accuracy and response speed, demonstrating the advantages of machine learning in complex network environment[4]. Kiran and Nandhakumar use chaotic mapping to construct intrusion detection model suitable for mobile cell network, improve the recognition ability of network coding attack by enhancing the unpredictability of data, and embody the innovative application of nonlinear dynamics method[5]. Nagalalli and Ravi proposed an intelligent intrusion detection system based on MegaBAT optimization algorithm, focusing on wireless sensor network security[6]. By optimizing feature selection and classifier parameters, the robustness and real-time performance of the system are significantly improved. These studies show that combining advanced optimization algorithms with machine learning techniques can effectively address complex and diverse network intrusion threats in intelligent driving environments.

2.1.3. Intrusion Detection Methods Based on Machine Learning and Deep Learning

Network intrusion detection methods utilizing machine learning and deep learning have garnered significant attention in the domain of intelligent driving network security. Hollósi et al. employed capsule networks to identify driver head positions in dynamic driving environments, thereby demonstrating the advantages of deep learning in processing complex dynamic data and offering innovative approaches for detecting abnormal behavior[7]. Lamiae et al. conducted a comparative analysis of the intrusion detection performance of support vector machines and artificial neural networks within software-defined networks[8]. Their findings indicated that deep learning models outperformed traditional methods in terms of accuracy and real-time performance, making them well-suited for the rapid response requirements of intelligent driving environments. Nuno et al. introduced an intelligent attack detection and classification method that integrates multiple machine learning algorithms, which significantly enhanced detection sensitivity and robustness, highlighting the potential of multi-model fusion in complex networks[9]. Intrusion detection based on machine learning and deep learning significantly enhances the security protection capabilities of intelligent driving systems by deeply mining network traffic and behavioral characteristics, aiming to achieve the goals of $\max Accuracy, \min Delay$

2.2. Domestic Research Status

2.2.1. Policies and Standards Related to Intelligent Driving Network Safety

Intelligent driving cybersecurity has emerged as a critical area of research and policy development both domestically and internationally. Guan Yuxin et al. noted that the rapid advancement of intelligent networked vehicles has rendered vehicle CAN network security vulnerable [10]. They identified network intrusion detection systems as essential protective measures that can effectively identify and mitigate various attacks, thereby ensuring the security of vehicle communications. Huang Dihighlighted that intelligent connected vehicles interface with cloud platforms via V2X communication, which increases the number of potential attack surfaces [11]. The traditional CAN bus lacks adequate security mechanisms, necessitating the development of detection models based on information entropy and deep learning to enhance accuracy and real-time performance. Relevant governmental agencies have established standards to delineate the technical requirements for intelligent driving network security and to foster the development of a robust industry safety framework.

2.2.2. Research Status of Network Intrusion Detection Technology in China

Domestic researchers have achieved significant advancements in the domain of intrusion detection within intelligent driving networks. Chen Li introduced a detection method that utilizes the Gramm angle field and a simplified VGG network[12]. This approach transforms CAN bus data into images, enabling the efficient identification of denial-of-service and fuzzy attacks, achieving an accuracy rate exceeding 99%. Song Hechun employed ECU voltage signal characteristics in conjunction with GBDT, PCA, and OCSVM to effectively detect camouflage and injection attacks, thereby enhancing detection robustness [13]. While domestic research has made notable strides in feature fusion and the application of intelligent algorithms, improvements in real-time processing and cross-brand applicability remain necessary.

2.2.3. Challenges and Countermeasures of Intrusion Detection in Intelligent Driving Environment

Network intrusion detection in intelligent driving environments encounters several challenges, including data diversity, real-time requirements, and the complexity of attacks. Yang Yuanda noted that the architecture of intelligent networked automobile on-board networks is intricate, making traditional rule-based detection inadequate for addressing evolving attacks and insufficient in real-time performance [14]. Chen Xi emphasized that resource constraints within the Internet of Things environment necessitate lightweight detection algorithms, which are also applicable to intelligent driving systems[15]. Dai Junhao proposed that lightweight detection for vehicle-mounted networks must balance accuracy and real-time responsiveness while implementing multi-layer defense strategies to enhance security [16]. He Jiahao investigated deep learning anomaly detection in the context of the CAN bus, highlighting that limited training data restricts model generalization [17]. The integration of multi-source data and the development of advanced models, such as adversarial networks, significantly enhance detection sensitivity and robustness while mitigating data scarcity. Therefore, intelligent driving intrusion detection must be lightweight, multi-level, and intelligent to ensure system security.

3. Results

The intelligent driving system is a crucial component of future transportation, with its safe and stable operation directly influencing traffic efficiency and public safety. Network intrusions can result in vehicle control failures, information tampering, and even traffic accidents, leading to significant casualties and property damage. Statistics from safety events within an intelligent driving platform indicate that system failures due to network attacks account for 35% of all failures, with 70% of these attacks occurring at the communication link layer. This data underscores the urgency and necessity of implementing robust network security measures. By developing an efficient network intrusion detection system, it is possible to monitor abnormal behaviors in real time, promptly address potential threats, and minimize both the false alarm rate and the overall incidence of false alarms, thereby ensuring the continuity and stability of vehicle operations. The table 4 below illustrates the effectiveness of various intrusion detection technologies in their application to intelligent driving systems.

Table 4. Comparison of intrusion detection technology effects in intelligent driving system

Technical Type	Detection accuracy (%)	False alarm rate(%)	Response time(ms)	Applicable scenarios
Traditional feature matching	85	10	150	Simple attack detection
Parazacco spilurus subsp. spilurus behavioral monitoring	88	8	120	New type of attack identification
Machine learning methods	92	5	100	Complex attack detection
Deep learning methods	95	3	80	Multi-source data fusion detection

Through the application of the above technologies, the intelligent driving system can realize accurate identification and rapid response to network threats, significantly improve the safety protection capability of the system, and ensure the safety and stability of vehicles in complex network environments. The following Figure 3 presents schematic diagram of data processing and response flow of intelligent driving network intrusion detection system:

Figure 3. Schematic diagram of data processing and response flow of intelligent driving network intrusion detection system Fixed operation.

4. Discussion

4.1. Key Technologies and Methods for Intrusion Detection in Intelligent Driving Networks

The core technologies for intrusion detection in intelligent driving networks include feature extraction, anomaly detection, and behavior analysis. While methods leveraging deep learning and multi-source data fusion have enhanced detection accuracy, real-time performance, and system robustness, current research still faces challenges. These include balancing detection accuracy with a low false alarm rate, effectively integrating multi-modal data, and meeting stringent real-time requirements due to computational complexity. Future improvements should focus on optimizing algorithm generalization, advancing multi-source data fusion models, and refining model structures to achieve efficient and real-time intrusion detection, thereby ensuring the network security of intelligent driving systems.

4.2. Future Expectations

4.2.1. Construction of Intelligent Intrusion Detection System Based on Fusion of Multi-source Data

In the future, the enhancement of cybersecurity for intelligent driving will highly rely on the in-depth application of multi-source data fusion and artificial intelligence (AI). The construction of an intelligent intrusion detection system based on multi-source data fusion is the core direction. By integrating multi-dimensional information such as vehicle sensors, network traffic, and behavioral characteristics, it can achieve comprehensive perception and analysis of abnormal behaviors, thereby significantly improving the ability to identify covert attacks, reducing false alarm rates, and enhancing system robustness. Combined with the edge-cloud computing architecture, a distributed and multi-level collaborative defense system can be further formed to meet real-time requirements.

4.2.2. The Prospect of Deep Integration of Artificial Intelligence and Network Security

At the same time, the deep integration of AI and

cybersecurity will be a key driving force. By using machine learning and deep learning algorithms, the system can autonomously learn complex attack patterns, achieve precise defense and timely response to unknown threats, and dynamically adjust security strategies to enhance the system's adaptability and anti-interference ability. With the advancement of algorithms and computing power, AI will promote the construction of a more intelligent, efficient, and reliable protection system, ultimately ensuring the security and stable operation of intelligent driving networks.

5. Conclusion

5.1. Summary of Findings

The study has successfully demonstrated that intrusion detection systems based on deep learning and multi-source data fusion can significantly improve the security of intelligent driving systems. Future research should focus on optimizing these models to better handle real-time constraints and improve robustness.

5.2. Future Directions

Future work should focus on the construction of intelligent intrusion detection systems using AI and multi-source data integration. A more intelligent, adaptable, and efficient protection system will ensure the safety and stability of intelligent driving networks.

References

[1] Nie, L., Ning, Z., Wang, X., Hu, X., Cheng, J., & Li, Y. (2020). Data-driven intrusion detection for intelligent Internet of Vehicles: A deep convolutional neural network-based method. IEEE Transactions on Network Science and Engineering, 7(4), 2218–2227. https://doi.org/10.1109/TNSE.2020.2990984.

[2] Fang, M., Wang, Y., Yang, L., Yang, Y., & He, J. (2024). Reinventing Web security: An enhanced cycle-consistent generative adversarial network approach to intrusion detection. Electronics, 13(9), 1674. https://doi.org/10. 3390/electronics 13091674.

[3] Networking; New findings in networking described from East China Normal University (A lightweight and intelligent intrusion detection system for integrated electronic systems). (2020). Journal of Technology, 2020(1847).

[4] Ridwan, A. M., Radzi, M. A. N., Azmi, M. H. K., & Zaki, M. M. (2023). A new machine learning-based hybrid intrusion detection system and intelligent routing algorithm for MPLS network. International Journal of Advanced Computer Science and Applications, 14(4). https://doi.org/10.14569/ IJACSA. 2023. 0140442.

[5] Kiran, C. K., & Nandhakumar, R. (2024). Intrusion detection model using chaotic MAP for network coding enabled mobile small cells. School of Computer Science and Engineering, VIT-AP University, Amaravati, Andhra Pradesh, 522241, India, 78(3), 3151–3176.

[6] Nagalalli, G., & Ravi, G. (2023). A novel MegaBAT optimized intelligent intrusion detection system in wireless sensor networks. Intelligent Automation & Soft Computing, 35(1), 475–490. https://doi.org/10.32604/iasc.2023.026571.

[7] Hollósi, J., Ballagi, Á., Kovács, G., & Németh, B. (2024). Bus driver head position detection using capsule networks under dynamic driving conditions. Computers, 13(3), 66. https:// doi. org/10.3390/computers13030066.

[8] Lamiae, B., Siham, E., & El, K. M. (2023). Intelligent intrusion detection in software-defined networking: A comparative study of SVM and ANN models. Procedia Computer Science, 224, 26–33. https://doi.org/10.1016/j.procs.2023.08.003.

[9] Nuno, O., Isabel, P., & Eva, M. (2021). Intelligent cyber attack detection and classification for network-based intrusion detection systems. Applied Sciences, 11(4), 1674. https://doi. org/10.3390/app11041674.

[10] Guan, Y., Ji, H., Cui, Z., Li, H., & Chen, L. (2023). Overview of intrusion detection methods for intelligent networked vehicle CAN network. Automotive Engineering, 45(6), 922–935.

[11] Huang, D. (2021). Research on intrusion detection system of intelligent networked vehicle [Master's thesis, Shanghai University of Engineering Science].

[12] Chen, L. (2020). Research on intrusion detection method of vehicle-bus network based on deep learning[Master's thesis, Zhejiang University of Science and Technology].

[13] Song, H. (2020). Research on intrusion detection system for vehicle network[Master's thesis, Xidian University].

[14] Yang, Y. (2020). Research on key technologies of intrusion detection for intelligent connected vehicle network security [Doctoral dissertation, Hunan University].

[15] Chen, X. (2023). Research on network intrusion detection technology for Internet of Things. Network Security and Informatization, 2023(10), 148–150.

[16] Dai, J. (2023). Research on lightweight intrusion detection and security enhancement design for in-vehicle network [Master's thesis, Nanchang University].

[17] He, J. (2023). Research on key technology of intrusion detection for intelligent network vehicle CAN bus [Master's thesis, Guangzhou University].