Journal of Engineering Research and Reports

Volume 26, Issue 11, Page 1-6, 2024; Article no.JERR.124408
ISSN: 2582-2926

Intelligent Connected Vehicle Information Security Risks and Countermeasures

Yang Shuhai [a*]

[a] *School of Mechanical Engineering, North China University of Water Resources and Electric Power, 450045, China.*

Author's contribution

The sole author designed, analysed, interpreted and prepared the manuscript.

Article Information

DOI: https://doi.org/10.9734/jerr/2024/v26i111310

Open Peer Review History:
This journal follows the Advanced Open Peer Review policy. Identity of the Reviewers, Editor(s) and additional Reviewers, peer review comments, different versions of the manuscript, comments of the editors, etc are available here: https://www.sdiarticle5.com/review-history/124408

Short Communication

Received: 12/08/2024
Accepted: 14/10/2024
Published: 22/10/2024

ABSTRACT

The development of intelligent connected vehicles has promoted the upgrading of the transportation system, but it also brings challenges in information security. This paper analyzes the current information security vulnerabilities of intelligent connected vehicles, including attack methods, security vulnerabilities, and protective measures. Firstly, through the analysis of the existing attack methods and their principles, the potential security vulnerabilities and threats are summarized. Then, based on security and cryptography technology, relevant measures for information security protection are proposed to achieve all-round protection of intelligent connected vehicle information. Finally, The paper puts forward the measures to solve the information security problem of intelligent connected vehicle from three aspects: Encryption and Authentication, Firewall and Intrusion Detection System, and Over-the-air (OTA).

**Corresponding author: Email: ysh20000706@163.com;*

Cite as: *Shuhai, Yang. 2024. "Intelligent Connected Vehicle Information Security Risks and Countermeasures". Journal of Engineering Research and Reports 26 (11):1-6. https://doi.org/10.9734/jerr/2024/v26i111310.*

Keywords: Intelligent connected vehicle; information security; data encryption.

1. INTRODUCTION

As an emerging industry, intelligent connected vehicle is developing rapidly and has become a hot topic in the current automobile industry.

Intelligent connected vehicle refers to the all-round interconnection between vehicles, vehicles and roads, vehicles and people and the background on the basis of traditional vehicles, through vehicle networking technology, intelligent control technology, automatic driving technology, etc., to improve the safety, comfort, fuel economy and intelligent level of vehicles (Gong et al. 2024, Wang et al. 2024, Wu et al. 2017).

It is predicted that by 2025, the global sales of intelligent connected vehicles will reach 42 million units, and the Chinese market will occupy more than 40 % of the global market share of intelligent connected vehicles (Park et al. 2018). However, in the development of intelligent connected vehicles, there are still some problems.

The problem of information security is an important risk point faced by intelligent connected vehicles. With the rapid development of intelligent connected vehicles, it has attracted more and more attention. In fact, the security threats faced by intelligent connected vehicles are no longer limited to points and surfaces. Problems in any link can lead to attacks and even physical damage to the car (Wang 2020, Song 2024). Therefore, it is particularly important to ensure the information security of intelligent connected vehicles.

In the development process of intelligent connected vehicles, we need to fully consider the issues of information security, strengthen technical research and development, improve laws and regulations, and strengthen management measures, so as to comprehensively improve the information security level of intelligent connected vehicles and ensure the healthy and stable development of the intelligent connected vehicle industry.

2. THE NECESSITY OF ENSURING INFORMATION SECURITY FOR INTELLIGENT CONNECTED VEHICLES

The intelligent connected vehicle is a new generation of cars, equipped with advanced technology and functions, making it safer, more efficient and more environmentally friendly than traditional cars. Although traditional cars still dominate the road today, it is clear that intelligent connected cars are the future of transportation and will play a key role in shaping our way of travel in the next few years (Song 2023).

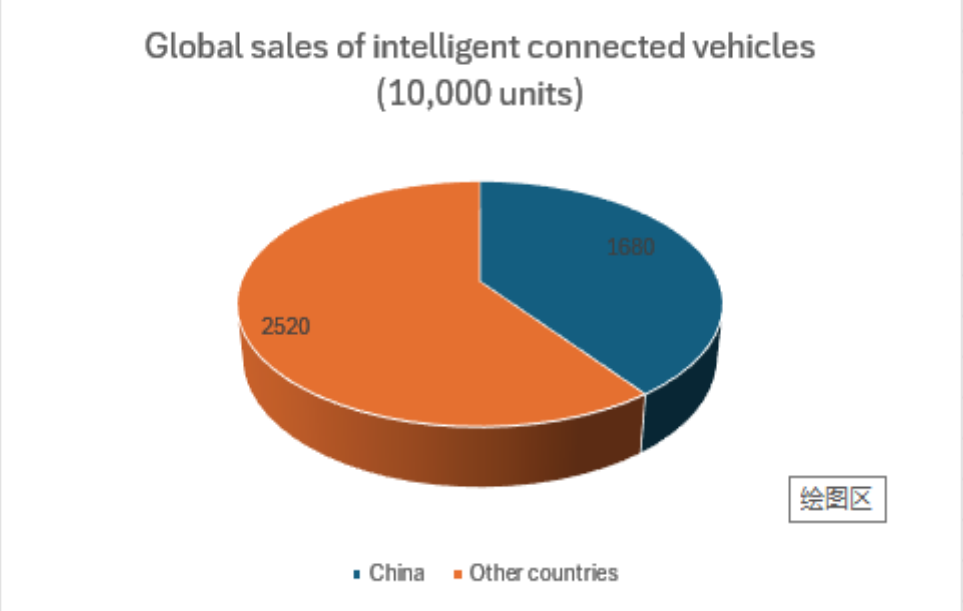

Fig. 1. The Global sales of intelligent connected cars

Intelligent connected vehicles are equipped with a series of sensors and cameras that can collect a large amount of data about the vehicle 's surrounding environment, as well as information about driver behavior and preferences (Pan et al. 2023).

These data are then transmitted to other vehicles, infrastructure, and clouds where they are processed and analyzed to improve vehicle performance and safety. However, these data are also highly sensitive and valuable, and may be used for malicious purposes if they fall into the wrong hands. For example, hackers can use this data to access the vehicle system and control it, or to steal personal information from drivers and passengers. This is why information security is critical to intelligent connected vehicles, and why it is important to implement strong security measures to protect these data (Donglin 2025, Angélica Pigola et al. 2024).

3. ANALYSIS OF THE CAUSES OF INFORMATION SECURITY PROBLEMS IN INTELLIGENT CONNECTED VEHICLE

At present, the information security problems existing in the intelligent connected automobile industry are as follows:

(1) Vulnerability of intelligent connected vehicles.
(2) Intelligent connected vehicle communication security issues.
(3) Intelligent connected vehicle supply chain security issues.

4. MEASURES TO SOLVE THE INFORMATION SECURITY OF INTELLIGENT CONNECTED VEHICLE

The Intelligent Connected Vehicle (ICV) is equipped with advanced technology that enables it to communicate with other vehicles, infrastructure and the cloud. However, this connection also makes them vulnerable to cyberattacks, which may have serious consequences for the safety and privacy of passengers. In order to cope with these risks, intelligent connected car manufacturers are implementing a series of measures to ensure the information security of these cars.

For common cyber attacks, intelligent connected car manufacturers generally take the following three measures: Encryption and Authentication, Firewall and Intrusion Detection System, and Over-the-air (OTA). In order to protect the safety of users' cars and prevent the disclosure of personal privacy, as shown in Fig. 2.

4.1 Encryption and Authentication

With the development of intelligent connected vehicles, security issues have become increasingly important. Encryption and authentication are the key to ensuring the safety of intelligent connected vehicles.

Therefore, a combination of symmetric encryption algorithm and asymmetric encryption algorithm can be used to apply the symmetric encryption algorithm to the data transmission process, and the asymmetric encryption algorithm is used to protect the security of the key.

Secondly, certificate-based authentication is adopted. This approach requires the use of digital certificates and protocols such as SSL / TLS to achieve, using a digital signature mechanism to ensure the identity of both parties to the communication authentication and data integrity.

Of course, a distributed identity system can also be used. This system can be implemented by blockchain technology, which can achieve anonymity and traceability while ensuring security. By storing identity information on the blockchain, the risk of single point of failure and information leakage can be avoided, thereby ensuring the safety of intelligent connected vehicles (Brown et al. 2024, Wu et al. 2020).

4.2 Firewall and Intrusion Detection System

Firewalls and intrusion detection systems are key to ensuring security. In the construction of firewalls and intrusion detection systems, the need to take the following aspects of technical means:

(1) **Security domain division:** The intelligent connected vehicle is divided into different security domains, and security control and access restrictions are imposed on different domains to reduce the attack surface and risk.
(2) **Vulnerability repair and update:** Vulnerability scanning and security evaluation of each system of the intelligent

connected vehicle are carried out regularly, and the vulnerabilities are repaired and updated in time. Pay attention to the security patches and updates issued by the manufacturer, upgrade the vehicle software system in time, reduce the loopholes in the system, and enhance the defense ability (Ortiz et al. 2023).

(3) **Intrusion detection and prevention:** Build intrusion detection and prevention system, constantly monitor network data traffic and system log information, timely discover and prevent malicious operations and intrusions.

(4) **Security incident response:** Establish a sound security incident response mechanism to deal with and respond to network security incidents in a timely manner (Yang et al. 2021).

4.3 Over-the-air (OTA) updates

While solving the safety technical problems of intelligent connected vehicles, OTA update is also one of the important means of daily maintenance and update of intelligent connected vehicles. In order to better realize the OTA update, the technical implementation is carried out in the following aspects:

(1) **Encrypted transmission:** When performing OTA updates, data should be transmitted in an encrypted manner to ensure its security. At the same time, it is necessary to use the certificate authentication mechanism to authenticate the OTA update server to prevent man-in-the-middle attacks.

(2) **Secure storage:** OTA update files should be stored securely to avoid malicious attacks and unauthorized access. The OTA update file can be digitally signed or verified using a hash algorithm to ensure the integrity and correctness of the OTA update file. At the same time, it is necessary to store the OTA update file on a secure server and ensure its reliability through security testing and evaluation.

(3) **Verification and rollback:** After the OTA update is completed, verification and rollback operations should be performed to ensure that the OTA update does not cause serious impact. If a function is detected to be faulty or abnormal, it should be rolled back to the previous version as soon as possible and deal with the problem in time (Shimada 2021, Ye et al. 2020).

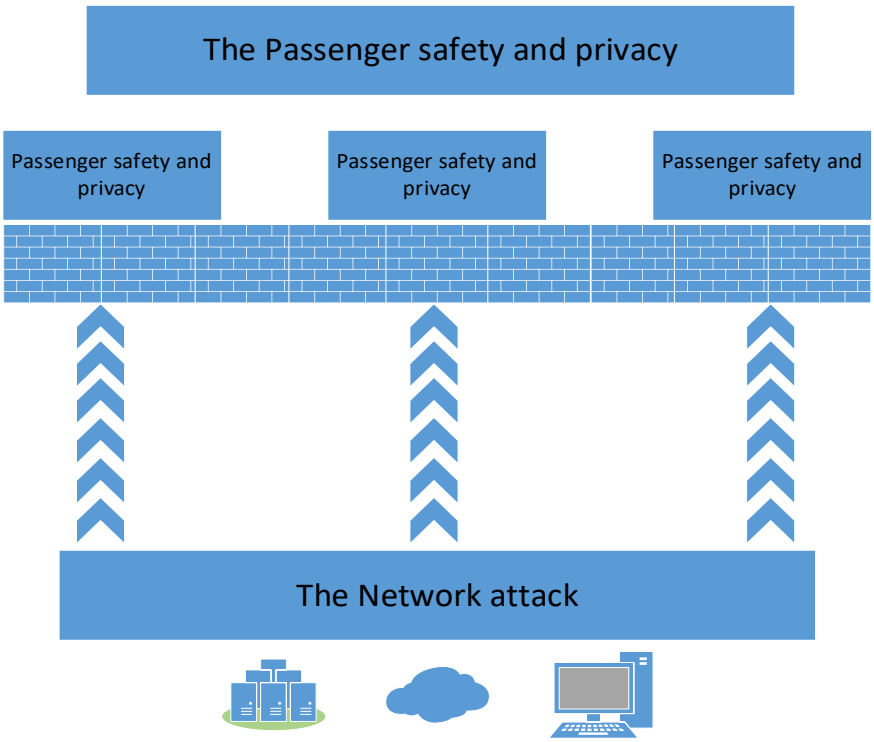

Fig. 2. Measures to resist cyber attacks on intelligent connected vehicles

4.4 Realistic Technical Protection Situation

In addition to the above three measures to protect information security, various intelligent network car manufacturers are also developing more advanced security protection systems, but these are also based on the above three measures to develop and improve.

Encryption and Authentication, Firewall and Intrusion Detection System, and Over-the-air (OTA), These three measures have their own advantages and disadvantages. At present, the mainstream solutions use the three measures to work together. The vehicle has been encrypted and certified before leaving the factory, and a firewall system has been added to protect against network attacks in offline state. Finally, Over-the-air (OTA) is used for regular daily maintenance updates. Thus better protect the user's information security and driving safety.

5. CONCLUSION

The information security of intelligent connected vehicles is a complex and continuous challenge. This paper focuses on the information security problem of intelligent connected vehicle, analyzes the causes of the information security problem of intelligent connected vehicle, and from Encryption and Authentication, Firewall and Intrusion Detection System, Over-the-air (OTA) updates this. Three aspects put forward measures to solve the problem of intelligent connected vehicle information security.

DISCLAIMER (ARTIFICIAL INTELLIGENCE)

Author(s) hereby declare that NO generatve Al technologies such as Large Language Models (ChatGPT, COPlLOT, etc.) and textto-image generators have been used during the writing or editing of this manuscript.

COMPETING INTERESTS

Author has declared that no competing interests exist.

REFERENCES

Brown, D., Batra, G., Zafar, H., et al. (2024). Reducing fraud in organizations through information security policy compliance: An information security controls perspective. Computers & Security, 144, Article 103958. https://doi.org/10.1016/j.cose.2024.103958

Donglin, Z. (2025). Interactive experience of cross-cultural Japanese communication e-learning intelligent system based on computer information security. Entertainment Computing, 52. https://doi.org/10.1016/j.entcom.2024.100769

Gong, W., Yang, S., Guang, H., et al. (2024). Multi-order feature interaction-aware intrusion detection scheme for ensuring cyber security of intelligent connected vehicles. Engineering Applications of Artificial Intelligence, 135, Article 108815. https://doi.org/10.1016/j.engappai.2024.108815

Ortiz, F. M., Costa, L. H. M. K., & Sammarco, M. D. M. (2023). Road traffic safety assessment in self-driving vehicles based on time-to-collision with motion orientation. Accident Analysis and Prevention, 191, Article 107172. https://doi.org/10.1016/j.aap.2023.107172

Pan, J., Nguyen, A. T., Wang, S., et al. (2023). Fuzzy unknown input observer for estimating sensor and actuator cyber-attacks in intelligent connected vehicles. Automotive Innovation, 2, Article 6. https://doi.org/10.1007/s42154-023-00228-1

Park, J., Abdel-Aty, M., Wu, Y., et al. (2018). Enhancing in-vehicle driving assistance information under connected vehicle environment. IEEE Transactions on Intelligent Transportation Systems, 1-10. https://doi.org/10.1109/TITS.2018.2878736

Pigola, A., Meirelles, F. D. S., Costa, P. R. D., et al. (2024). Trust in information security technology: An intellectual property analysis. World Patent Information, 78, Article 102281. https://doi.org/10.1016/j.wpi.2024.102281

Shimada, D., & Morimoto, A. (2021). A study on the evaluation of smoothness and safety of traffic flow on the general road mixed with autonomous vehicles. JSTE Journal of Traffic Engineering, 7, A_86-A_93. https://doi.org/10.14954/jste.7.2_A_86

Song, T., & Zhu, W. X., & Ma, W. X. L. (2024). Distributed sliding mode control strategy for intelligent connected vehicle platoon in complex media. Applied Mathematical Modelling, 125(Pt. B), 404-424.

Song, T., Zhu, W. X., & Su, W. W. (2023). Distributed "End-Edge-Cloud" structural

car-following control system for intelligent connected vehicle using sliding mode strategy. Communications in Nonlinear Science and Numerical Simulation, 126(Nov.), 1-17.

Wang, M., & Liu, Y. (2020). Wisdom city under the perspective of intelligent factors of the brand of meta-analysis in colleges and universities to explore. Journal of Physics: Conference Series, 1533(3), Article 032079. https://doi.org/10.1088/1742-6596/1533/3/032079

Wang, Y., Lyu, N., & Wen, J. (2024). Game theory-based mandatory lane change model in intelligent connected vehicles environment. Applied Mathematical Modelling, 132, 146-165. https://doi.org/10.1016/j.apm.2024.04.047

Wu, W., Head, L., Yan, S., et al. (2017). Development and evaluation of bus lanes with intermittent and dynamic priority in connected vehicle environment. Journal of Intelligent Transportation Systems. https://doi.org/10.1080/15472450.2017.1313704

Wu, Y., Duan, J., Dai, T., et al. (2020). Managing security outsourcing in the presence of strategic hackers. Decision Analysis. https://doi.org/10.1287/deca.2019.0406

Yang, S., Du, M., & Chen, Q. (2023). Impact of connected and autonomous vehicles on traffic efficiency and safety of an on-ramp. Simulation Modelling Practice and Theory, 113, Article 102374.

Ye, W., Wang, C., Chen, F., et al. (2020). Approaching autonomous driving with cautious optimism: Analysis of road traffic injuries involving autonomous vehicles based on field test data. Injury Prevention. https://doi.org/10.1136/injuryprev-2019-043402

Peer-review history:
The peer review history for this paper can be accessed here:
https://www.sdiarticle5.com/review-history/124408