Security and Safety, Vol. 5, E2026014 (2026)
https://doi.org/10.1051/sands/2026014
sands.edpsciences.org

Security and Safety in Intelligent Connected Vehicle

Editorial

Open Access

Preface: Security and safety in intelligent connected vehicle

Xinsheng Ji[1,2,*], Yan Li[3], Shichun Yang[4], and Yufeng Li[2,5,**]

[1] *National Digital Switching System Engineering & Technological R&D Center, Zhengzhou 450002, China*
[2] *Purple Mountain Laboratories, Nanjing 211111, China*
[3] *Qualcomm Wireless Communication Technologies (China) Limited, Beijing 100013, China*
[4] *School of Transportation Science and Engineering, Beihang University, Beijing 100191, China*
[5] *School of Computer Engineering and Science, Shanghai University, Shanghai 200444, China*

Received: 29 April 2026 / Revised: 29 April 2026 / Accepted: 30 April 2026 / Published online: 30 April 2026

Citation Ji X, Li Y, Yang S, et al. Preface: Security and safety in intelligent connected vehicle. Security and Safety 2026; **5**: E2026014. https://doi.org/10.1051/sands/2026014

Intelligent connected vehicles (ICVs) represent a significant milestone in the evolution of transportation, facilitating the seamless integration of traditional automotive systems with the expansive connectivity of the Internet. By unifying vehicles, roadside infrastructure, mobile devices, and cloud platforms, ICVs establish an interconnected ecosystem that supports advanced capabilities such as remote scheduling, autonomous driving, and over-the-air (OTA) updates. This heterogeneous, mobile, and wide-area distributed IoT environment–spanning the domains of vehicle, road, human, and cloud–substantially improves traffic efficiency and user experience, heralding a transformative trend in the future of mobility.

Nevertheless, the integration of ICVs into this open and dynamic framework introduces unprecedented security and safety challenges. Unlike traditional closed-loop automotive systems, ICVs expand the attack surface through diverse interfaces–including wireless communications (such as V2X, cellular, and Bluetooth), physical access points, and cloud servers–making them susceptible to a wide array of cyber threats. Potential risks include data breaches, unauthorized access, signal spoofing, and remote hijacking, all of which threaten both user privacy and the physical safety of passengers and infrastructure. Moreover, the intricate interplay between heterogeneous hardware, software architectures, and rapidly changing network environments complicates the development of robust, unified defense mechanisms.

In response to these urgent challenges, this special topic is dedicated to advancing research and practice in the security and safety of intelligent connected vehicles. Following rigorous peer review and revision, six papers have been selected, each contributing valuable insights across a spectrum of critical research directions. The topics addressed encompass dynamic game modeling for security optimization, physical-layer vulnerabilities in EV charging protocols, novel fault detection methods for ADAS, integrated safety and security monitoring solutions for connected automated vehicles, trust mechanisms for C-V2X communications, and the risks associated with LLM-based traffic motion prediction under cyberattacks. Collectively, these works provide a comprehensive reference for researchers and practitioners, fostering innovation and collaboration in the ongoing development of secure and safe intelligent connected vehicle systems.

In the paper "Dynamic Game Modeling and DNAS^2 Framework for Dual-S Security in Internet of Vehicles [1]", the authors propose the DNAS^2 framework. This work introduces a dual-layer game model

* Corresponding author (email: jxs@ndsc.com.cn)
** Corresponding author (email: liyufeng_shu@shu.edu.cn)

to resolve the conflict between functional safety and cybersecurity. By formalizing cooperative and non-cooperative games, it provides a mathematical foundation for achieving Pareto optimality in ICV security design, offering a unified analytical tool for endogenous security optimization.

In the paper "Physical-Layer Exploits on EV Chargers: Authentication and Systemic Protocol Weaknesses [2]", the authors uncover critical vulnerabilities in major EV charging protocols. The authors demonstrate practical physical signal spoofing attacks via a hardware implant (PORTulator). This work highlights the risks of denial-of-service and hardware damage, exposing the lack of robust authentication in current charging infrastructure and urging systemic protocol enhancements.

In the paper "From Fault Tolerance to Fault Detection: A DHR-Based Contrastive Testing Method and Its Validation on ADAS [3]", the authors present a novel contrastive testing method for ADAS. Inspired by dynamic heterogeneous redundancy (DHR), this approach utilizes heterogeneous executors to detect faults via output inconsistency. Experiments show it reduces testing time by 63.9% and enables precise defect localization without requiring a priori expected results.

In the paper "Dynamic Heterogeneous Redundancy-Based Endogenous Security and Safety for Connected Automated Vehicles [4]", the authors design an integrated safety and security monitoring module based on DHR. The prototype achieves a 95.9% defense success rate against 122 vulnerability cases. By employing dynamic reconfiguration, the system maintains 100% performance during attacks, validating the effectiveness of endogenous security in CAVs.

In the paper "Research on Trust Mechanism of C-V2X [5]", the authors propose a lifecycle-oriented trustworthiness evaluation framework. Addressing the dynamic and distributed nature of C-V2X, this work establishes a systematic solution encompassing trust management and decision-making. It provides a robust method for ensuring information reliability among heterogeneous traffic participants in high-mobility environments.

In the paper "Problems and Challenges in LLM-Based Intelligent Traffic Motion Prediction under Cyberattacks [6]", the authors analyze the risks of integrating large language models (LLMs) in autonomous driving. The authors argue that LLMs' susceptibility to hallucinations and input perturbations conflicts with control theory's demand for determinism. This commentary highlights how cyberattacks can exploit these traits, threatening the closed-loop stability of next-gen ITS.

In the paper "Research on Functional Safety Design for Passenger Vehicles Based on STPA at the Vehicle Level [7]", the authors propose a vehicle-level safety analysis methodology. By integrating STPA with HARA, this work addresses the gap in cross-system risk identification, enabling a shift from single-system analysis to system-theoretic vehicle-level safety analysis. It provides theoretical support and practical pathways for functional safety design in intelligent vehicles.

We are confident that the wide range of perspectives and technical advancements featured in this special topic will provide an important resource for both researchers and practitioners, inspiring continued progress and innovation within the field. In closing, we extend our heartfelt thanks to all contributing authors for their outstanding work, and we sincerely appreciate the commitment and thoughtful evaluations offered by our editorial board and reviewers.

References

[1] Sun S, Yu N and Liang L. Dynamic game modeling and DNAS^2 framework for Dual-S security in Internet of Vehicles. Secur Saf 2026; **5**: 2026008. https://doi.org/10.1051/sands/2026008

[2] Shi H, Song S, He Y, et al. Physical-layer exploits on EV chargers: Authentication and systemic protocol weaknesses. Secur Saf 2026; **5**: 2026012. https://doi.org/10.1051/sands/2026012

[3] Qin W, Yang F, Shen Y, et al. From fault tolerance to fault detection: A DHR-based contrastive testing method and its validation on ADAS. Secur Saf 2026; **5**: 2026006. https://doi.org/10.1051/sands/2026006

[4] Liu Q, Wang Z, Wang P, et al. Dynamic heterogeneous redundancy-based endogenous security and safety for connected automated vehicles: Preliminary test results and assessment. Secur Saf 2026; **5**: 2025009. https://doi.org/10.1051/sands/2025009

[5] Xi Y, Hu J, Zhao L, et al. Research on trust mechanism of C-V2X. Secur Saf 2026; **5**: 2026004. https://doi.org/10.1051/sands/2026004

[6] Yang J, Gao S, Rao K, et al. Problems and challenges in LLM-based intelligent traffic motion prediction under cyberattacks. Secur Saf 2026; **5**: 2026007. https://doi.org/10.1051/sands/2026007

[7] Zhong Y, Fang J, Wang X, et al. Research on functional safety design for passenger vehicles based on STPA at the vehicle level. Secur Saf 2026; **5:** 2026013. https://doi.org/10.1051/sands/2026013