InSight Bulletin: A Multidisciplinary Interlink International Research Journal
Peer Reviewed International, Open Access Journal.
ISSN : 3065-7857 / Website: https://ibrj.us / Volume-3, Issue-2 / February - 2026

Original Article

Cyber-attacks on Automated Vehicles

Chetana Patil[1], Dipali Shinde[2]
[1,2] Assistant Professor, Department of Computer Science, Baburaoji Gholap College, Sangvi

Manuscript ID:
IBMIIRJ -2026-030214

Submitted: 07 Jan. 2026

Revised: 11 Jan. 2026

Accepted: 05 Feb. 2026

Published: 28 Feb. 2026

ISSN: 3065-7857

Volume-3

Issue-2

Pp. 67-71

February 2026

Correspondence Address:
Chetana Patil
Assistant Professor, Department of Computer Science, Baburaoji Gholap College, Sangvi

OPEN ACCESS

Quick Response Code:

Web. https://ibrj.us

DOI: 10.5281/zenodo.21335433

DOI Link:
https://doi.org/10.5281/zenodo.21335433

Abstract

Vehicle automation has been a major research focus within Intelligent Transportation Systems (ITS) since the 1980s. For many years, automated driving was considered impractical because of limitations in sensing, computation, and system reliability. However, recent advancements in self-driving technologies and strong commitments from automobile manufacturers indicate that automated vehicles are approaching real-world deployment. Simultaneously, transportation systems have increasingly adopted connected vehicle technologies, referred to as connected vehicles in the United States and cooperative Intelligent Transportation Systems (C-ITS) in Europe. These technologies rely on vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communications to exchange critical information for traffic management and safety applications. Despite pursuing similar objectives, automated vehicle technologies and cooperative ITS have largely evolved as separate fields of research. Their integration is essential for improving the decision-making, efficiency, and overall safety of automated vehicles. However, increased connectivity significantly expands the attack surface, exposing vehicles to various cybersecurity threats. Automated and cooperative vehicles depend heavily on software, sensors, and communication networks, making them vulnerable to cyberattacks that may compromise safety-critical functions. This study investigates security threats specific to automated vehicle systems and analyzes the vulnerabilities affecting both autonomous and cooperative automated vehicles. The findings highlight the need for higher levels of redundancy and robust security mechanisms to ensure safe and reliable operations. This study aims to raise awareness of the challenges of cyber security and promote the early inclusion of security considerations in the design of future automated vehicle systems.

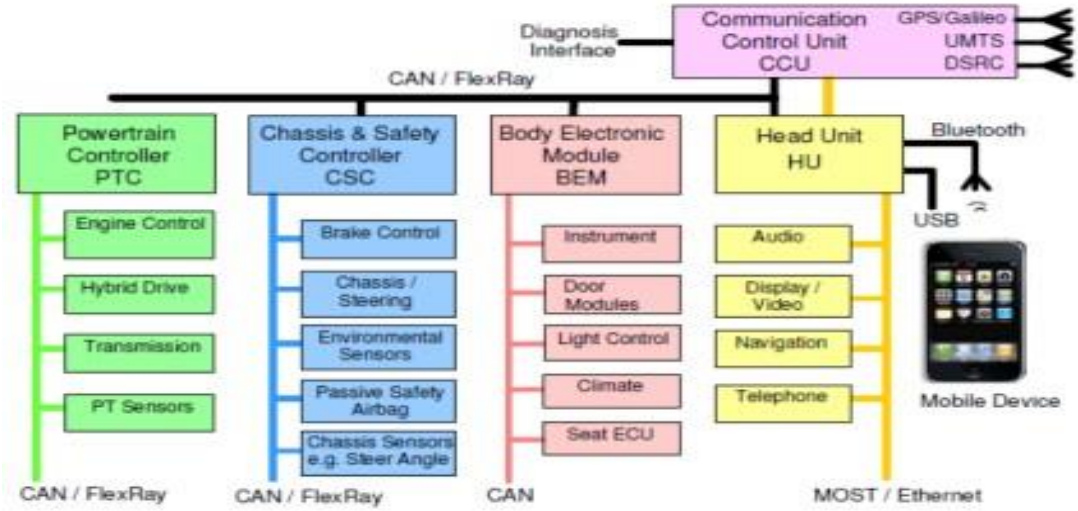
Index Terms: *Automated vehicles, intelligent transportation systems (ITS), connected vehicles, cooperative ITS, vehicle-to-vehicle communication (V2V), vehicle-to-infrastructure communication (V2I), cyber security, transportation safety.*

Introduction

Intelligent Transportation Systems (ITS) have been an active area of research since the mid-1980s, with vehicle automation representing one of its most ambitious and transformative goals. For decades, automated driving has been largely considered a long-term or futuristic vision, constrained by limitations in sensing, computing, and system reliability. However, in recent years, rapid advances in sensing technologies, artificial intelligence, and embedded systems have significantly accelerated this progress. The emergence of commercially tested self-driving vehicles and public announcements by major automobile manufacturers have shifted vehicle automation from a theoretical concept to real-world deployment. In parallel with automation, the intelligent transportation system (ITS) community has increasingly focused on vehicle connectivity. Concepts such as connected vehicles in the United States and cooperative IT'S in Europe emphasize the exchange of information through vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I/I2V) communication. These systems aim to enhance traffic efficiency, safety, and situational awareness by allowing vehicles and infrastructure to share real-time data with each other. Although both automated driving and cooperative ITS have advanced independently, their integration remains limited despite their strong interdependence. The convergence of automation and connectivity is expected to play a critical role in the future of transportation. Cooperative communication can provide automated vehicles with information beyond the capabilities of onboard sensors, such as hidden hazards, traffic conditions, and the intentions of nearby vehicles.

How to cite this article:
Patil, C. & Shinde, D. (2026). Cyber-attacks on Automated Vehicles. InSight Bulletin: A Multidisciplinary Interlink International Research Journal, 3(2), 67–71.
https://doi.org/10.5281/zenodo.21335433

However, this increased reliance on communication also expands the attack surface of automated vehicle systems, introducing new cybersecurity risks that can directly impact safety. As automated and cooperative vehicle technologies approach large-scale deployment, understanding and addressing their cybersecurity vulnerabilities is essential. This study focuses on identifying and analyzing cyber threats specific to autonomous and cooperative automated vehicles, highlighting the unique challenges they present. By examining potential attack scenarios and system weaknesses, this study aims to raise awareness of cybersecurity concerns and emphasize the need for robust, redundant, and resilient system designs in future vehicle automation architectures.



Objectives

1. To identify the cyber security risks in automated vehicles.
2. To study security issues in vehicle-to-vehicle and vehicle-to-infrastructure communications.
3. To highlight the importance of a safe and reliable system design for automated vehicles.

Contribution of This Work

This study contributes to the growing body of research on vehicle automation and ITS security by systematically analysing the cyber threats affecting both autonomous and cooperative automated vehicles. It highlights the attack vectors unique to cooperative systems and emphasizes the need for robust security-by-design principles. By addressing these issues at an early stage of technology development, this study aims to inform researchers, system designers, and policymakers, ultimately supporting the safe and secure deployment of future automated transportation systems.

1. Definitions And Assumptions

A. Definitions

Automated Vehicle (AV): A vehicle capable of performing driving functions, such as steering, braking, and acceleration, through automated control systems with limited or no human intervention.

Autonomous Automated Vehicle: An automated vehicle that relies primarily on onboard sensors and internal processing without continuous dependence on external communication.

Cooperative Automated Vehicle (CAV): An automated vehicle that utilizes vehicle-to-vehicle (V2V) and/or vehicle-to-infrastructure (V2I/I2V) communication to enhance situational awareness and driving performance.

Intelligent Transportation Systems (ITS): Systems that integrate communication, sensing, and control technologies to improve transportation safety, efficiency, and mobility.

Cybersecurity: The protection of vehicle systems, networks, and data from unauthorized access, manipulation, or disruption.

Cyber-attack: A malicious action intended to compromise the confidentiality, integrity, or availability of vehicle systems or communications.

B. Assumptions

1. Vehicles operate at a high level of automation, where control decisions are primarily made by onboard systems.
2. Cooperative automated vehicles have access to wireless V2V and V2I communication channels.
3. Automated vehicle systems operate under strict real-time and safety-critical constraints.
4. Adversaries are assumed to have access to wireless communication interfaces but not direct physical access to vehicle hardware.
5. Cyber incidents are assumed to have the potential to affect vehicle safety and system performance.

2. Attacker Model

In this study, we considered a realistic attacker model that targets the electronic architecture of automated vehicles. The attacker may operate remotely, locally, or with physical access to the vehicle and is assumed to have the capability to exploit software vulnerabilities in externally exposed components, such as the head unit and communication control unit. Through wireless interfaces, including cellular, Bluetooth, Wi-Fi, and V2X, a remote adversary may gain initial access and subsequently

pivot to internal in-vehicle networks, such as CAN, FlexRay, or Ethernet. Owing to the limited authentication and trust assumptions inherent in legacy in-vehicle communication protocols, an attacker can inject, modify, or replay messages, potentially affecting both non-safety-critical and safety-critical ECUs. The model assumes no access to manufacturer cryptographic secrets and excludes nation-state-level capabilities, focusing on practical and scalable attacks relevant to modern connected and automated vehicles.

1. **Attacker Goals**

The attacker aims to compromise the confidentiality, integrity, or availability of automated vehicle systems to achieve the following:

- Manipulate vehicle behaviour (steering, braking, acceleration)
- Disrupt vehicle operation (Denial of Service)
- Eavesdrop on or extract sensitive data (location, user data)
- Gain persistent control over in-vehicle networks
- Propagate attacks to other vehicles or infrastructure

2. **Attacker Capabilities**

We assume that the attacker has one or more of the following capabilities:

- Network access to in-vehicle communication channels (CAN, FlexRay, Ethernet, MOST)
- Ability to inject, modify, or replay messages on unsecured buses
- Capability to exploit software vulnerabilities in ECUs
- Knowledge of vehicle protocols, message formats, and ECU behavior
- Ability to compromise external interfaces (e.g., mobile device, wireless links)
- Moderate computational resources (no need for physical supercomputers)

3. **Attacker Type**

1. **Remote Attacker**

A remote attacker exploits the wireless interfaces without physical access to the vehicle.
Entry points include:

- Cellular (UMTS/LTE/5G) via the Communication Control Unit (CCU)
- Bluetooth or Wi-Fi via the Head Unit (HU)
- GPS or V2X (DSRC/C-V2X) interfaces
- Mobile device pairing and companion applications
  Potential impact:
- Remote code execution on infotainment systems
- Pivoting from HU/CCU to CAN or Ethernet networks
- Large-scale fleet attacks

2. **Local (Proximity) Attacker**

A local attacker requires close proximity but does not necessarily require physical access to the device.
Examples:

- Bluetooth spoofing
- Malicious Wi-Fi access points
- V2X message injection
  Potential impact:
- Unauthorized access to infotainment or telematics ECUs
- Data exfiltration
- Limited control over non-safety ECUs

3. **Physical Attacker**

A physical attacker has direct access to the vehicle.
Entry points include:

- OBD-II port
- Debug interfaces (UART, JTAG)
- Direct ECU replacement or reflashing
  Potential impact:
- Full CAN bus control
- ECU firmware modification
- Long-term persistence

4. **Mapping Attacker Model to Vehicle Architecture**

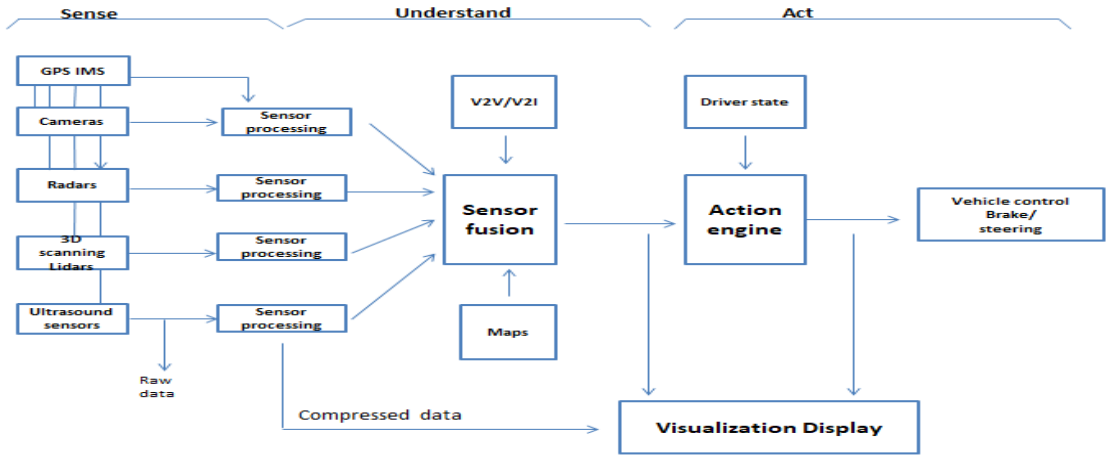
The system architecture shown in Figure is used.

Component	Attacker Entry Point	Attack Potential
Head Unit (HU)	Bluetooth, USB, Mobile device	CAN injection, data theft
CCU	Cellular, V2X, GPS	Remote compromise, pivoting
CAN/FlexRay	Internal bus	Message spoofing, DoS
Body ECUs	CAN	Unauthorized actuation
Chassis/Safety ECUs	CAN/FlexRay	Safety-critical manipulation

The identified cyber-attacks were classified based on their target components and potential impact, as shown in Table I.

Table I Attack Classification for Automated and Cooperative Vehicles

Attack Category	Target Component	Description	Potential Impact
Sensor Attacks	Cameras, LiDAR, Radar, GPS	Manipulation or disruption of sensor data	Incorrect perception, unsafe maneuvers
Communication Attacks	V2V, V2I/I2V	Injection of false messages or message blocking	Wrong driving decisions, traffic instability
Software Attacks	Control software, firmware	Exploitation of software vulnerabilities	Loss of control, system malfunction
In-Vehicle Network Attacks	ECUs, CAN bus	Unauthorized access to internal networks	Compromise of safety-critical functions
Denial-of-Service Attacks	Communication or processing units	Overloading system resources	Reduced availability, system shutdown



Methodology

This study adopts a systematic methodology to analyze cyber-attacks on the electronic architectures of automated vehicles and evaluate their potential impact on safety and security. The methodology consists of four main phases: system modeling, attack surface identification, attack execution and analysis, and impact assessment. First, the in-vehicle electronic architecture is modeled based on a domain-oriented design comprising the powertrain, chassis and safety, body electronics, and infotainment domains interconnected through CAN, FlexRay, and Ethernet networks. Key externally exposed components, including the Head Unit (HU) and Communication Control Unit (CCU), are identified as primary gateways between external interfaces and internal vehicle networks.

Second, potential attack surfaces are identified by analyzing the communication interfaces and trust relationships between electronic control units (ECUs). This includes wireless interfaces such as cellular, Bluetooth, and vehicle-to-everything (V2X), as well as physical access points such as the On-Board Diagnostics II (OBD-II) port. Based on the defined attacker model, feasible attack vectors, such as message injection, spoofing, replay, and denial-of-service, are mapped to specific vehicle domains and communication buses. Third, representative cyber-attacks are designed and executed in controlled experimental or simulated environments. These attacks focus on exploiting the lack of authentication and integrity protection in in-vehicle networks to demonstrate how a compromised infotainment or telematics ECU can influence other vehicle subsystems. The network traffic was monitored and analyzed to observe the attack propagation across the ECUs. Finally, the impact of each attack is evaluated with respect to confidentiality, integrity, and availability, with particular emphasis on safety-related consequences of the attack. The results were used to assess the system resilience and identify the security weaknesses in the current vehicle architectures. Based on these findings, mitigation strategies and design recommendations are discussed to enhance the cybersecurity of automated vehicles.

Security and Privacy Threats in Automated Vehicles: Autonomous vehicles integrate numerous sensors, ECUs, and in-vehicle networks to enable automated driving, which introduces multiple security vulnerabilities. Attacks targeting in-vehicle communication buses, infotainment systems, or telematics units can lead to unauthorized access, message manipulation, or denial of service, potentially affecting safety-critical vehicle functions. In addition, compromised software components may allow persistent control of the vehicle subsystems. From a privacy perspective, autonomous vehicles continuously generate and store sensitive information, including location data, driving behavior, and user-related data, which can be exposed through insecure onboard systems or backend services.

Security and Privacy Threats in Cooperative Automated Vehicles: Cooperative automated vehicles further expand the threat landscape by enabling vehicle-to-vehicle and vehicle-to-infrastructure communication. Security threats in such environments include false data injection, replay, and impersonation attacks on V2X messages, which can distort cooperative awareness and decision making. A single malicious participant can influence multiple vehicles, thereby amplifying the attack's impact. Privacy risks are also increased because of the periodic broadcast of vehicle state information, allowing adversaries to correlate messages over time and track vehicle movements. Consequently, cooperative systems require stronger protection mechanisms to ensure secure communication and user privacy.

Conclusion

This study examines cyber security threats to automated vehicles and provides an initial idea of how serious these threats are, along with ways to reduce them. This study is an early study that identifies the main challenges in building safe automated vehicles and determines which problems should be addressed first. A key point is that both autonomous and cooperative automated vehicles face similar threats, and similar strategies can help protect them. This study does not specify which type is safer but demonstrates that security is crucial for both. Cooperative automated vehicles have additional sources of information that can help verify whether the vehicle is functioning correctly and can detect attacks. However, these additional sources can also be exploited by attackers. Therefore, vehicles should have multiple layers of information so that they can make correct decisions even if one source is compromised. Systems should also be designed to handle attacks safely without causing serious problems. The main goal of this study is to raise awareness of these cybersecurity issues and encourage further research on how to prevent them. Among all threats, GNSS spoofing (faking GPS signals) and sending fake messages are the most dangerous. For autonomous vehicles, GPS is critical for positioning on the map; therefore, faking GPS signals could cause the vehicle to move incorrectly and endanger the passengers. Using secure GPS systems, such as SAASM hardware, can help, but these solutions are expensive and restricted. For cooperative vehicles, fake messages are an additional threat. In addition to authentication to prevent outside attacks, systems also need ways to detect misbehavior from inside the network or accidental errors. Adding misbehavior detection may require software updates and changes to the existing vehicle security architecture, such as the ETSI reference model.

Future Work

Future research should focus on creating measurable risk assessment methods and validating cyber-attack scenarios using simulations and testbeds. Standardized security frameworks, intrusion detection systems, and trust management mechanisms must be developed specifically for cooperative automated vehicles. In addition, further studies on regulations and policies are required to ensure the safe and secure large-scale deployment of automated transportation systems in the future.

Acknowledgment

The authors sincerely express their gratitude to the management of Baburaoji Gholap College, Sangvi, for providing the academic environment and institutional support necessary to carry out this research work.

Financial support and sponsorship

Nil.

Conflicts of interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

1. Shivanshi Sharma et al., Security in Autonomous Vehicles: A Review of Attacks and Defenses, IJRASET (2025) — Provides an overview of attack types and defenses in AVs.
2. Attacks and defences on intelligent connected vehicles: a survey, Digital Communications and Networks (2020) — Discusses vehicle architecture vulnerabilities including invehicle network and V2X attack
3. M. M. Abrar et al., GPSIDS: An Anomalybased GPS Spoofing Attack Detection Framework for Autonomous Vehicles (2024) — Anomaly detection for GPS spoofing in AV environments
4. Impact of cyberattacks on safety and stability of connected and automated vehicles, OSTI — Simulation study of message falsification, spoofing, and DoS impacts in CAV environments.
5. Intrusion detection system for V2X communication…, Scientific Reports — Machine learning-based intrusion detection for cooperative V2X messages.
6. G. K. Kommineni, Cybersecurity in Autonomous and Connected Vehicles: A SystemsLevel Threat Analysis and Resilience Framework, J. Comp. Sci. & Tech. Studies, 2025 — comprehensive threat analysis and resilience framework for AVs and CAVs.
7. ISO/SAE 21434 – Road Vehicles — Cybersecurity Engineering, ISO & SAE International, 2021.
8. SAE J3061 – Cybersecurity Guidebook for Cyber-Physical Vehicle Systems, SAE International, 2016.
9. ETSI TS 103 485 – Intelligent Transport Systems (ITS); Security; Security Services and Threats, ETSI, 2022.