Vikas Kumar Sihag, 2026, 14:6
ISSN (Online): 2348-4098
ISSN (Print): 2395-4752

International Journal of Science, Engineering and Technology
An Open Access Journal

Cybersecurity of Connected and Autonomous Vehicles: A Review of Attacks, Open Challenges And Research Directions

Vikas Kumar Sihag,
Sardar Patel University Of Police, Security And Criminal Justice, Jodhpur
Vikas.Sihag@Policeuniversity.Ac.In

Abstract- Connected and autonomous vehicles (CAVs) are widely recognised as a key element of future intelligent transportation systems. Their reliance on sensors and in-vehicle networks exposes them to a broad range of cyberattacks. Wireless connectivity widens that exposure further. This paper reviews the security of CAVs. It first outlines the key terminology and the SAE levels of driving automation. The sensing technologies behind autonomous driving are then described. A taxonomy of attacks follows, divided into in-vehicle network attacks and vehicle-to-everything (V2X) network attacks. Open challenges are discussed, ranging from dynamic risk assessment to spectrum sharing. The review indicates that technical countermeasures alone cannot secure CAVs. Non-technical factors such as consumer trust and governance also determine whether these vehicles reach wide adoption.

Keywords: autonomous vehicles; connected vehicles; cybersecurity; in-vehicle networks; V2X; intrusion detection

I. INTRODUCTION

Road vehicles were once the preserve of mechanical engineering. Advances in embedded systems and the Internet of Things (IoT) have since turned them into networked machines that sense their surroundings and exchange data with other entities. Autonomous vehicles (AVs) represent the most advanced form of this shift [1]. An AV monitors its environment and follows traffic rules. It plans routes and reacts to sudden events with little or no human input [1].

Several factors drive AV development. Road safety is the first. Irresponsible human conduct such as drunk or distracted driving causes life-threatening incidents, and governments have already deployed CCTV cameras and road sensors to enforce traffic law. Connected and autonomous vehicles are being studied as a complementary way to reduce such incidents. Population growth is the second factor.

It increases the number of vehicles and strains roads and fuel stations. Machines that drive also relieve people of a tiring task and allow time to be used more efficiently. The progress rests on IoT, embedded systems, sensors, ad hoc networks, wireless communication and artificial intelligence [1].Connectivity has a price. Every additional sensor or communication module widens the attack surface of the vehicle [2]. An attacker can then enter the vehicle from outside [2,3]. Automakers and governments are investing in vehicle security. Cooperation between industry and government is considered necessary to address the problem [2].

A published taxonomy of automotive security attacks classifies 162 attacks and 413 multi-stage attacks at varying levels of detail [2]. It lets security engineers and testers describe attacks in a uniform way and supports threat analysis and risk assessment (TARA). Other surveys examine vehicular cyberattacks from different angles [3–5].

This paper aims to consolidate the attack taxonomy and the open challenges of CAV security in a single review. Section II introduces the terminology and the levels of automation. It also describes the sensing technologies. Section III classifies the attacks. Section IV discusses open challenges and Section V outlines future research directions. Section VI concludes the paper.

© 2026 Vikas Kumar Sihag, This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/4.0/), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly credited.

II. BACKGROUND

1. Common Terminology

The dynamic driving task (DDT) comprises the real-time functions needed to drive a vehicle in on-road traffic. It excludes trip planning and destination selection [6]. The DDT covers (a) longitudinal control; (b) lateral control; (c) environment monitoring; and (d) manoeuvre planning. An automated driving system (ADS) is the hardware and software that performs the entire DDT on a sustained basis, even when limited to a specific operational design domain (ODD) [6]. The term normally refers to levels 3 to 5. The ODD is the set of conditions under which a driving automation feature is designed to operate. These conditions depend on factors such as time of day, location, road type, weather and the presence of traffic.

Object and event detection and response (OEDR) is a subtask of the DDT. It covers the detection and classification of objects, together with the appropriate reaction to events that threaten safety. Active safety systems monitor the surroundings inside and outside the vehicle to detect real and potential threats. They intervene automatically by warning the driver or by acting on subsystems such as the throttle and the brakes [1].

2. Levels Of Autonomy

SAE International defines six levels of driving automation [6]. At level 0 the driver performs the entire DDT, although active safety functions may assist. At level 1 the system controls either longitudinal or lateral motion. Adaptive cruise control is a typical example. The driver must remain in the vehicle and be ready to take over at any moment. Level 2 extends this support to both longitudinal and lateral control, but the system still cannot perform the full OEDR. The driver therefore remains responsible for monitoring the road and acts as the fallback.

Level 3 is the first level at which the ADS performs the entire DDT within its ODD. However, the driver remains the fallback and must respond when the ODD limits are about to be exceeded or when a system failure degrades performance. At level 4 no human intervention is required inside a restricted ODD with suitable road structures and maps. The ADS also performs the fallback and minimises risk when needed, although an occupant may still take control. Level 5 removes the ODD restriction. The ADS drives under all conditions and handles the fallback, and a human takes control only on request.

3. Sensors Used In Autonomous Vehicles

Autonomous vehicles combine several sensors to build a complete picture of their surroundings [7]. Visible-light cameras provide a 360-degree view and perform well in object detection and recognition. The AI-based perception algorithms consume their data. Cameras produce large volumes of data and are imprecise in low light. Infrared cameras are therefore added to improve night performance.

Radar computes distance, velocity and angle from reflected radio waves. It works well over long ranges and in most weather conditions but can misidentify objects [7]. LiDAR measures distance from the time that emitted laser pulses take to return to a photodetector. The returns form a point cloud that renders the surroundings in three dimensions. The sensor is accurate and robust but expensive. Ultrasonic sensors are inexpensive and have a short range. They suit low-speed manoeuvres such as parking.

Global navigation satellite systems (GNSS), of which GPS is one, determine receiver position by measuring distances to several satellites. GNSS supplies timing and location data for navigation and is free to the public. Its signals are weak and vulnerable to interference and manipulation. Fig. 1 depicts the typical placement of these sensors on a vehicle.

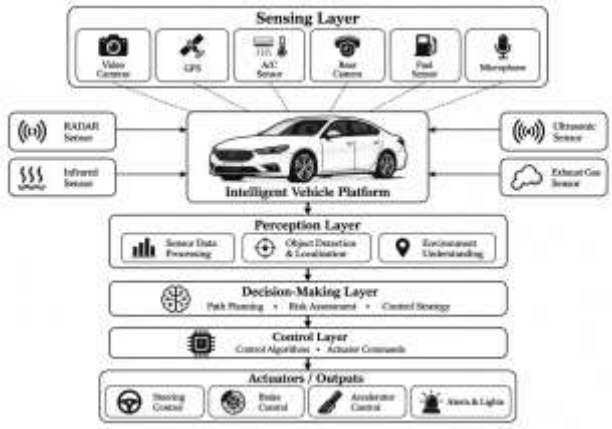


Fig. 1: Types of sensors in a vehicle.

III. CYBERATTACKS ON CONNECTED AND AUTONOMOUS VEHICLES

Attacks on CAVs can be grouped into in-vehicle network attacks and V2X network attacks [2]. Table I summarises the main categories together with their impact and method. The subsections below describe each attack in turn.

TABLE I. Summary of attacks on CAVs, adapted from [2].

Category	Attack	Impact	Method
In-vehicle	Remote sensor	Injected signals accepted as legitimate	Various attack vectors
In-vehicle	GPS spoofing	Arbitrary manipulation of position and time	Stronger fake GPS broadcast
In-vehicle	Location trailing	Exposure of driver behaviour and profile	Linking pseudonymous position samples
In-vehicle	Close proximity	Compromise of short-range communication	Bluetooth or keyless-entry exploits
In-vehicle	CAN and J1939 bus	Eavesdropping and frame injection	Abuse of arbitration; missing authentication
In-vehicle	ECU flashing	Corrupted information; degraded hardware	Reverse engineering; code modification; fuzzing; phishing
In-vehicle	Integrated business services	Client-level and system-level access	Phishing; malicious code
V2X	DoS	Delayed or blocked responses	Jamming; useless messages
V2X	Impersonation	Fake or modified messages	Spoofed identities
V2X	Replay	Misled traffic and authorities	Retransmission of valid packets
V2X	Routing	Disturbed routing; dropped packets	Compromised or cooperating nodes
V2X	Data falsification	Misled receivers	False information and alerts
V2X	Eavesdropping	Leaked identity and keys	Overhearing the wireless medium
V2X	Password and key	Cracked credentials	Repeated trial of values
Other	Infrastructure	Cut communication	Message-transfer vulnerabilities
Other	Slight	Hazardous conditions	Small random data deviations
Other	Machine learning systems	Modified training data and algorithm	Poisoning; evasion; model stealing; model inference

1. In-Vehicle Network Attacks

In-vehicle network attacks target the sensors and electronic units inside the car. Seven types are described below.

1) Remote sensor attacks. Sensors such as lidar and cameras are linked through the in-vehicle network. Some of them can also be reached by external entities through existing wireless access technologies [2]. A weak peripheral sensor is therefore an easier entry point than the vehicle as a whole. Once the attacker controls the device, remote sensor attacks become possible. The sensor cannot distinguish legitimate input from injected input and treats forged signals as genuine.

2) GPS spoofing attacks. CAVs rely heavily on GPS for location and time. In a spoofing attack, the adversary broadcasts a fake GPS signal that is stronger than the genuine one [2]. Receivers then ignore the true signal. The attack operates at the physical layer. A vehicle inside the affected area accepts any false position or time chosen by the adversary and veers off its intended course.

3) Location trailing attacks. By tracking vehicle location, an adversary can uncover driving behaviour and activities and can even build a driver profile [2]. Messages are normally sent anonymously and identities are changed regularly. However, a single pseudonym does not suffice against tracing, because pseudonymous position samples can be combined into location profiles and linked to specific vehicles. Profiles that share a start and an end point on workday mornings, for instance, can reveal home and work addresses.

4) Close proximity vulnerabilities. Short-range communication protocols expose weaknesses that may arise by accident. Bluetooth and tire pressure monitoring systems (TPMS) are common examples, as are key fobs and keyless entry. The Bluetooth control code has been shown to contain a memory exploit that allows code execution from any paired device [2]. A compromised paired device can then attack the engine control units without the driver noticing. Secure Bluetooth protocols built on cryptographic algorithms exist. Most commercial products do not adopt them because the protocols are inefficient. They also fail to prevent memory exploitation, although they do block the open-source tools used to analyse packets in the public domain. TPMS messages use standard modulation schemes and simple protocols without cryptography, so the communication can be reverse engineered. Spoofing and battery-drain attacks can make the system malfunction. An inexpensive antenna receives the messages up to 10 m from the vehicle, and a simple low-noise amplifier extends this to 40 m [2]. A nearby adversary can therefore overhear or spoof the broadcasts. Each message also carries a fixed 32-bit sensor identifier, which is unique enough to allow low-cost vehicle tracking. Two entry methods exist: key fob entry and keyless entry. Against a key fob, an adversary can jam the locking signal with inexpensive devices such as garage door openers, so that the car stays unlocked. Hidden in bushes and left on for long periods, such devices block fob signals across parking lots and public spaces. A keyless system cannot be jammed in this way, but its constant signal can be recorded and replayed to open the car. A small low-cost device hidden near a locked car can record one keyless entry code for later use. It jams the reception of the rolling code from the owner's fob and records the owner's two unlocking attempts. Some alarms and immobilisers rely on weak secret keys, which a laptop can break within minutes.

5) CAN and SAE J1939 bus vulnerabilities. The controller area network (CAN) bus lacks authentication and encryption [8]. Any unauthorised node can therefore join the network and read every message. Because the messages are unencrypted, an adversary who sniffs the bus can collect personal data such as the driver's phone details and location. The adversary can also insert unauthorised frames.

Denial of service (DoS) attacks are possible as well. CAN arbitration gives the node with the highest priority the right to transmit first. A rogue node that is always online with the highest priority prevents every other node from communicating. DoS attacks can also exploit the error containment mechanism. If the adversary causes errors during communication, the error counter of the victim node rises until the node is eliminated from the bus. The SAE J1939 bus derives from CAN and inherits these weaknesses. An adversary can flood it with frames whose identifier field holds the lowest possible value. In addition, either party can break a connection-mode transfer to a specific destination, so an abort message addressed to both sender and recipient terminates the connection.

6) ECU software flashing attacks. Electronic control units (ECUs) are embedded systems that govern functions such as climate control, servo steering, gear shift, ignition and electric window lifts. They can be reprogrammed, which allows bugs to be fixed and features to be added without replacing the hardware. ECU software flashing denotes the development, delivery and installation of this software. Attackers exploit unpatched vulnerabilities through reverse engineering, code modification, fuzzing or phishing [2]. Successful attacks can disclose or corrupt information and degrade hardware performance. Safe operation

therefore depends on protecting the integrity of the flashing process [9].

7) Integrated business services attacks. The back-end network of the manufacturer can be linked to the embedded systems of a vehicle. Drivers then gain access to manufacturer services such as entertainment and remote software updates. These services are themselves targets [2]. Through phishing or malicious code, an adversary can obtain client-level access to the business platform. That access can be used to launch a further attack for system-level access. If the adversary can run arbitrary software on the in-vehicle platform, the embedded system falls under their control and other vehicle systems may become reachable. User data tied to third-party applications, such as online banking, is also at risk.

2. Vehicle-To-Everything Network Attacks

Vehicle-to-everything networks allow a connected vehicle to exchange data with other vehicles and with infrastructure [10]. Attackers exploit this exchange to find network access points. A car can also open channels to devices such as smartphones through short-range links such as WiFi and Bluetooth or through cellular protocols such as the Global System for Mobile Communications (GSM). Once connected, vehicles are exposed to the attacks described below.

1) DoS attacks. In a DoS attack, the adversary uses interference signals to block the communication channel completely or injects pointless messages that cause problems for network nodes. Legitimate users then cannot use network services and correct messages do not reach their destinations [2]. The attack delays responses. In a CAV environment even a slight delay can compromise driving safety, because an accident can be prevented or caused within a split second. Response-time demands are strict, so DoS attacks are potentially fatal for CAVs.

3. Impersonation Attacks

Every vehicle holds a distinctive identity used to identify the car and its messages. Impersonation attacks adopt a false or foreign identity. They take two forms. Node impersonation spoofs one identity at a time, whereas Sybil attacks spoof many identities simultaneously. A Sybil adversary can additionally drop important messages. It can also transmit fictitious messages or disseminate altered copies of received ones.

3) Replay attacks. In a replay attack, the adversary records valid packets and retransmits them later [2]. The attack frequently occurs at the transport or network layer. It typically targets authorisation and key agreement protocols so that the adversary can imitate a genuine vehicle or roadside unit (RSU). The consequences include misled traffic and confused authorities, as well as damage to transportation safety.

4. Routing Attacks

Routing attacks exploit weaknesses in routing protocols to disrupt normal routing or to drop forwarded packets. A black hole attack can be launched by one compromised node or by a few cooperating nodes. In a gray hole attack, the adversary drops packets selectively and may switch between correct behaviour and black hole behaviour. The intermittent correct behaviour makes gray hole attacks hard to detect. A wormhole attack involves at least two cooperating nodes that form a private high-speed tunnel. Packets captured at one location are tunnelled to another.

5) Data falsification attacks. Truthfulness is a basic requirement of vehicular communication for road safety. In data falsification attacks, the adversary supplies or broadcasts false information and safety alerts [2]. The false message may be created by tampering, suppression, fabrication or alteration. Recipients then react wrongly, which can lead to fatalities. A false alert can clear the road ahead. A fake accident message can cause a traffic jam. In transportation cyber-physical systems, such attacks can also degrade route guidance and lengthen trip times.

5. Eavesdropping Attacks

Eavesdropping attacks overhear the wireless medium. They are also known as stealth attacks. The adversary secretly tracks the victim's whereabouts and network traffic and can then obtain personal data of the CAV. The victim is unaware of the attack and the network is not directly affected, which makes detection difficult.

7) Password and key attacks. Password and key attacks are difficult to execute, since they usually need specialised software and hardware. Financial motives can nevertheless drive them. The adversary tests values

repeatedly until the password or key is cracked [2]. The attacks fall into three categories: (a) dictionary attacks; (b) rainbow table attacks; and (c) brute force attacks. A dictionary attack works through a list of words. A rainbow table attack uses a list of precomputed hashes generated from the chosen hash function and all candidate passwords. A brute force attack goes through every combination of letters and numbers and so also finds non-dictionary passwords.

6. Other Attacks

Three further categories appear in Table I. Infrastructure attacks cut off communication in the infrastructure and relate to cloud services. Slight attacks, as termed in [2], deviate communicated data randomly from the true values while staying below the detection threshold. They can still create hazardous conditions and serious safety problems. Attacks on machine learning systems arise in several phases of the learning pipeline. Known methods include data poisoning, evasion, model stealing and model inference attacks, and they modify the training data or the training algorithm.

IV. DETECTION-BASED COUNTERMEASURES

Intrusion detection is a widely studied countermeasure. Mehedi et al. in [11] proposed a deep transfer learning based intrusion detection system for electric vehicular networks. Seo et al. in [12] introduced GIDS, an intrusion detection system for in-vehicle networks that builds on generative adversarial networks. Desta et al. in [13] analysed identifier sequences on the CAN bus with long short-term memory networks to detect intrusions. These works show that learning-based detection can be applied to the CAN bus and to wider vehicular networks. The attack classes in Table I indicate where such detectors are needed.

1. Challenges And Open Problems

This section describes the main open problems and possible research directions.

A. Dynamic risks. CAVs are mobile systems whose surroundings change constantly. Cyber-risk assessment of CAVs has been studied extensively [2]. However, few studies address the dynamic risks that CAVs face. Because risk assessment can update and present risks from several perspectives, it would be worth investigating whether it can anticipate unforeseen threats.

B. Lightweight security model. Road entities in a V2X connection differ in capability and resources. A security model should therefore use device resources efficiently. Existing models have largely ignored power consumption, because they were deployed on vehicles with long-lasting batteries. Other entities such as mobile phones have limited battery life during V2X communication. A balance between device resources and security level is needed, and a lightweight security model is required for V2X.

C. Degrees of trust. A single trusted component in a CAV is a single point of failure that can compromise the security of the whole system. Defenders can place redundant security resources in different components that cross-check one another. However, an adversary who corrupts several components may undermine the cross-check. Each component should therefore be designed with an appropriate degree of confidence. When discrepancies arise, the designed trust levels determine which components are preferred for security decisions.

D. Security of 5G cellular V2X. The security of 5G cellular V2X (C-V2X) is another important research area. The products are still under development, so related attacks may emerge as deployment grows. The 5G security mechanisms now being defined are well specified and rely mostly on encryption and authentication. Their efficacy must nevertheless be examined carefully before and after CAVs enter the field. The security protocols may eventually need revision.

E. Testing standard. Vehicle systems undergo rigorous cybersecurity verification before reaching consumers. No single testing standard exists, and manufacturers typically select their own testers. Some testing recommendations are available, but they must be updated to cover complex scenarios. Current testing also identifies only simple weaknesses, whereas an adversary may try any technique to compromise vehicle systems.

F. Data collection and storage. Law enforcement and judicial authorities can use vehicle data to investigate traffic incidents and identify responsible parties. For this

purpose, data should be gathered in a pattern that yields a complete chain of evidence. It should then be stored in a format that permits safe and independent access.

G. Zero-knowledge proofs. Zero-knowledge proofs can verify vehicle data while concealing trade contents and transaction links. Their performance is a problem, however: the prover algorithm takes too long to execute. Efficient use of zero-knowledge proofs in CAVs therefore deserves investigation.

H. Blockchain. Blockchain can prevent an attacker from altering or deleting transaction data, so it can protect vehicle data privacy in CAVs. Most blockchains cannot handle large numbers of users. No standard exists for smooth communication between different blockchains. Consensus mechanisms also demand considerable processing power, which lowers overall operating efficiency.

I. Spectrum sharing. The US Department of Transportation applied spectrum sharing in the 5.9 GHz dedicated short-range communication (DSRC) band [2]. This approach removes the need for a licence before equipment is used in that spectrum, which saves time and money. The WiFi industry proposed the detect and vacate and the detect and mitigate procedures within the European Telecommunications Standards Institute. Both suffer from delayed detection. A WiFi device can typically identify DSRC transmissions only while it is not transmitting itself. Detection performance can be improved by adding idle periods, which is needed because of the unilateral hidden terminal problem. Even so, detect and mitigate can cause up to 30% additional packet loss for DSRC transmissions once DSRC devices are detected. This loss weakens safety applications that depend on vehicle-to-vehicle communication.

2. Future Scope

Research and development on vehicles and transport systems is preparing for an autonomous future. Many Internet of Vehicles (IoV) and VANET-based applications have already been proposed. The IoV has reached a stage where robust next-generation infrastructure can link sensors and whole vehicles to the Internet.

Vehicular ad hoc networks (VANETs) build on the IoV and give moving vehicles continuous access to resources such as the Internet [10]. They allow traffic and pollutant density to be monitored adaptively by grouping vehicles according to their movement and route. AVs can use this information to choose routes more flexibly. The benefits for communication and routing will become clearer once governments legalise vehicle-to-vehicle communication and vehicles adopt it.

A routing method based on collaborative learning has also been proposed for vehicular sensor networks. It aims to maximise throughput and minimise delay when vehicle density rises and routes become congested. Learning automata make fast routing decisions from experience and from nearby access points. Learning-based intrusion detection [11–13] is a further direction that merits continued study.

V. CONCLUSION

This review examined the cybersecurity of CAVs. The attack taxonomy covers in-vehicle network attacks and V2X network attacks. The open problems range from dynamic risk assessment to spectrum sharing. Adoption of AVs depends largely on non-technical factors such as consumer trust and governance. Human behaviour matters as well.

Classifying the threats supports CAV development and speeds practical deployment in intelligent transportation systems. Policymakers and engineers can draw on the lessons from past security breaches. They can also follow the safety and cybersecurity requirements for CAVs. System operators can apply cyber-risk assessment to study attacks and to prioritise mitigation. Many obstacles remain, and the community should address them without delay. We expect this review to support further work on CAV cybersecurity.

REFERENCES

1. J. Cui et al., “A review on safety failures, security attacks, and available countermeasures for autonomous vehicles,” Ad Hoc Netw., 2019.
2. X. Sun, F. R. Yu and P. Zhang, “A survey on cyber-security of connected and autonomous vehicles (CAVs),” IEEE Trans. Intell. Transp. Syst., 2022.
3. A. Singh and M. Singh, “An empirical study on automotive cyber attacks,” 2018.

4. S. K. Khan, N. Shiwakoti, P. Stasinopoulos and Y. Chen, "Cyber-attacks in the next-generation cars, mitigation techniques, anticipated readiness and future directions," 2020.
5. L. Pan, X. Zheng, H. X. Chen, T. Luan, H. Bootwala and L. Batten, "Cyber security attacks to modern vehicular systems," 2017.
6. SAE International, "Taxonomy and definitions for terms related to driving automation systems for on-road motor vehicles," SAE J3016, 2021.
7. R. Eustice, "University of Michigan's work toward autonomous cars," Univ. Michigan, Ann Arbor, MI, USA, Tech. Rep., 2015.
8. T. Hoppe, S. Kiltz and J. Dittmann, "Security threats to automotive CAN networks: Practical examples and selected short-term countermeasures," Reliab. Eng. Syst. Saf., vol. 96, pp. 11–25, 2011.
9. F. Kohnhauser, D. Pullen and S. Katzenbeisser, "Ensuring the safe and secure operation of electronic control units in road vehicles," in Proc. IEEE Secur. Privacy Workshops, May 2019, pp. 126–131.
10. M. S. Sheikh and J. Liang, "A comprehensive survey on VANET security services in traffic management system," Wireless Commun. Mobile Comput., 2019.
11. S. T. Mehedi, A. Anwar, Z. Rahman and K. Ahmed, "Deep transfer learning based intrusion detection system for electric vehicular networks," Sensors, 2021.
12. E. Seo, H. M. Song and H. K. Kim, "GIDS: GAN based intrusion detection system for in-vehicle network," in Proc. 16th Annu. Conf. Privacy, Security and Trust (PST), Belfast, Ireland, Aug. 2018, pp. 1–6.
13. A. K. Desta, S. Ohira, I. Arai and K. Fujikawa, "ID sequence analysis for intrusion detection in the CAN bus using long short term memory networks," in Proc. IEEE Int. Conf. Pervasive Comput. Commun. Workshops (PerCom Workshops), Mar. 2020, pp. 1–6.