TECHNICAL UNIVERSITY OF CLUJ-NAPOCA

ACTA TECHNICA NAPOCENSIS

Series: Applied Mathematics, Mechanics, and Engineering
Vol. 69, Issue Special III, July, 2026

RESEARCH AND TECHNIQUES FOR ENHANCING INTRA AND EXTRA VEHICLE COMMUNICATION

Vasile-Cătălin MIHACEA, Remus BRAD

Abstract: *The automotive industry is rapidly transforming due to increasing connectivity and the transition to electric and autonomous vehicles. This shift entails exponential growth in on-board computing, software complexity, and data generation, rendering vehicles into complex, networked systems with heightened cybersecurity vulnerabilities. This paper analyzes key attack vectors and classifies cybersecurity incidents. Network consolidation and increased intra- and extra-vehicular communication are essential. The number of connected cars rose from 330 million in 2018 to 775 million in 2023 (a 134% increase), with projections suggesting 50 billion connected devices by 2030. Regulatory measures now mandate intelligent speed assistance, fatigue detection, emergency event recording, and advanced driver assistance systems. Vehicle-to-everything (V2X) technology offers transformative potential for traffic efficiency and road safety.*

Keywords: *Automotive Cybersecurity, Connected Cars, V2X, Intra-Vehicle Communication, Telematics, ECU, UNECE WP.29.*

1. INTRODUCTION

The rapid evolution of the automotive industry, particularly the shift from internal combustion to electric propulsion, is driving significant structural changes. Modern vehicles increasingly rely on electronic control units (ECUs), each managing specific functions and interconnected within complex system architectures. This leads to the need for more modules, processors, and extensive wiring to support both intra- and extra-vehicular communication.

Network consolidation becomes essential as vehicle connectivity expands. The number of global connected cars rose from approximately 330 million in 2018 to 775 million in 2023 [1], a 134% increase. Projections for all IoT-connected devices estimate growth from around 15.14 billion in 2023 to approximately 50 billion by 2030 [2], reflecting broader growth across the automotive sector.

New regulatory measures require systems for intelligent speed adaptation, obstacle detection when reversing, driver fatigue monitoring, emergency event recording, lane keeping, automatic braking, tire pressure monitoring, and blind spot recognition to prevent collisions with vulnerable road users.

In 2024, the risk environment reached a new intensity via large scale ransomware attacks that disrupted operations across manufactures, suppliers and mobility providers, while remote intrusion into connected vehicles and infrastructure became more frequent and sophisticated. The 2025 Global Automotive and Smart Mobility Cybersecurity Report [3] mentions 1,877 publicly documented incidents since 2010, including 209 new cases in 2024 alone. Most attacks are conducted by black hat actors, they are executed remotely, and they increasingly exploit web API connectivity between vehicles, cloud services and mobile applications.

At the same time, the current regulation driven compliance, even if this is necessary it has proved to be insufficient. The introduction of frameworks like UNECE WP.29, R155 [4] / R156 [5] and ISO/SAE 21434 [6] have driven substantial investments in Cyber Security Management Systems and software update governance, still they also foster false sense of

security once formal compliance is achieved. This paper will cover all the above-mentioned aspects.

2. CURRENT STATUS IN THE INDUSTRY

The automotive and smart mobility landscape is undergoing a profound transformation driven by increasing connectivity, the transition to electric powertrains, and the rise of autonomous functionalities. This evolution introduces complex architectures, with modern vehicles comprising numerous electronic control units (ECUs), each running millions of lines of code and interacting with both internal systems and external IoT devices. These interconnected modules significantly expand the vehicle's attack surface.

According to a Strategy Report from Upstream Security Ltd [3][7], the number of processors per vehicle has grown from about 10 in 2000 to 45 in 2020, with estimates reaching 60 by 2030. In addition, the number of incidents with a high massive impact continued to increase between 2023 and 2024, accounting for over 60% of all incidents. From this approximately 92% of attacks have been done remotely and 65% of attacks have been performed by black hack actors. This growth necessitates the adoption of domain-based network architectures [8], with distinct domain controllers for ADAS, connectivity, infotainment, body and comfort, and powertrain systems, all interconnected through additional wiring harnesses.

Table 1

Automotive evolution [3] [7] [9]

	2000	2010	2020	2030
Processors per Car	~10	~30	~45	~60
Domains / Zonal Controllers			emerging	~4
Lines of Software Code	4k	10m	100-200M	500-1.000M
Length of Copper Wiring	20 m	0.5 km	1-2 km	reduced ~50%
Length of Wiring Harness	10 kg	30 kg	75 kg	reduced ~50%
Data Generated per Day	MB's	2 - 3 GB	50 GB	10 - 12 TB
Data Transferred per Day	Minimal	50 MB	1 - 2 GB	40 - 50 GB

The volume of data generated by vehicles has increased significantly. While vehicles in the early 2000s produced only a few megabytes per day, by 2020 this rose to approximately 50 GB daily. Projections for 2030 estimate data generation between 10-12 TB per day per vehicle [7]. As data generation alone offers limited value without transmission, it is expected that 40-50 GB of this data will be transferred daily by 2030.

By 2023, cybersecurity concerns have escalated, as attacks have grown in frequency, scale, and impact, many executed remotely and targeting multiple OEMs.

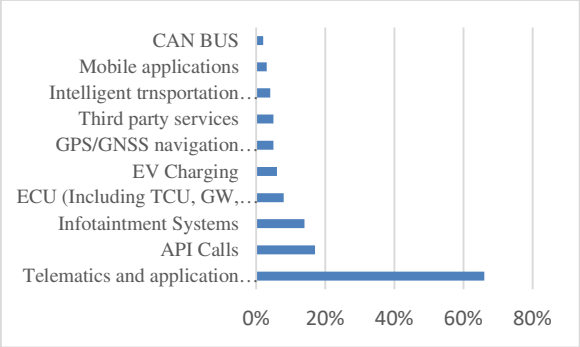


Fig. 1. Incidents by attack vectors (Authors based on [3] [7] [10])

In 2024, 43% of deep dark web cyber activities affected thousands to millions of mobility assets, as illustrated in Fig. 1. This impact is associated with increased connectivity between vehicles and OEMs, particularly through API-based integrations. While such connectivity enables capabilities such as remote software updates, it also introduces additional attack surfaces that may be exploited by malicious actors. In addition, EV charging infrastructure has emerged as a critical source of vulnerability. Moreover, AI increasingly plays a dual role: enabling automated cyberattacks and enhancing defensive capabilities through advanced threat detection.

Modern vehicles employ various connectivity technologies: satellite (e.g., GPS, emerging mega-constellations), eSIMs for cloud services, mobile protocols (Bluetooth, Wi-Fi), and broadcast systems like RDS-TMC. The industry is transitioning towards Vehicle-to-Everything (V2X) communication, through standards such as IEEE 802.11p and C-V2X, which aim to improve safety and traffic efficiency by allowing vehicles to share information with each other and their environment.

Connectivity offers significant benefits (remote diagnostics, OTA updates, infotainment

services, and improved road safety) but also introduces cybersecurity challenges. Technologies like UWB, NFC, and cellular networks enhance vehicle functionality, but simultaneously create potential attack vectors, making vehicles central nodes in digital ecosystems.

This paper analyses industry trends, connected vehicle architecture, and cyberattack patterns between 2020-2025, drawing on key reports from leading cybersecurity firms. It categorizes attacks (e.g., remote, physical, supply chain) and aligns them with emerging regulatory frameworks like UNECE WP.29. The study finds that key vehicle systems (particularly those offering the highest user value) are also the most frequent attack targets.

Future work focuses on practical countermeasures, including keyless entry system penetration testing, infotainment system manipulation, and defining secure communication boundaries. As cybersecurity becomes integral to vehicle quality, regulatory compliance and proactive threat mitigation are no longer optional, they are essential for the safety and reliability of future mobility.

2.1 Connected Cars Architecture

Connected cars represent a key segment of the Internet of Things (IoT). These vehicles are equipped to exchange data, receive software updates, and communicate with other vehicles or IoT devices through internet or Wi-Fi connections. This connectivity enhances the driving experience by offering improved infotainment and facilitating safety features. By 2030, it's projected that 700 million cars will be connected, and 90 million will be autonomous.

Contrary to the perception of novelty, connectivity has been gradually integrated into automobiles for years. Even basic cars today incorporate a range of connected technologies. The following section explores some of these technologies.

While individual manufacturers implement their car networks differently, common components and functionalities are observed. These include gateways, CAN buses, USB, Wi-Fi, and Electronic Control Units (ECUs) that interact in similar ways.

To analyze these interactions, we developed a generic car network architecture. This theoretical model visualizes the typical network topology and key components found in connected vehicles.

Key components and interactions:

- Telematics Unit: Houses the eSIM for cellular connectivity, enabling data transmission, cloud communication, and internet access.
- RDS/Satellite Unit: Receives broadcast data, including traffic alerts. Future integration with satellite connectivity will enhance data transmission capabilities.
- Bluetooth & Wi-Fi: Enable smartphone integration for various functions, including music streaming and internet access through Wi-Fi hotspots.
- OBD-II: Provides vehicle diagnostics information and communicates with the head unit.
- ECUs: Control various vehicle functions through CAN bus communication.
- Gateway ECU: Manages communication between different buses (CAN, LIN, MOST, FlexRay), ensuring message integrity and security.
- Main Board ECU: The central processor for the head unit, handling functions like navigation, display, and network management.
- Ethernet Gateway: Facilitates data exchange between RF modules and the head unit.

Approximately 89.3% of identified vulnerabilities are linked to vehicle connectivity. Key categories include [3] [7] [10]:

- **Message/Data Manipulation:** Includes alteration or spoofing of messages (e.g. 802.11p V2X or GNSS), such as Sybil attacks that simulate multiple vehicles during inter-vehicle calibration.
- **Unauthorized Code/Data Access:** Exploiting communication channels to inject, modify, rewrite, delete, or extract code or data from vehicle systems.
- **Unsafe or Unsourced Messaging:** Allowing unauthorized messages that support session hijacking or replay attacks (e.g. man-in-the-middle, version manipulation of ECUs or firmware).

- **Data Leakage:** Public exposure of information via interception, radiation interference, or unauthorized access to data files and directories.
- **Denial-of-Service (DoS) Attacks:** Disrupting vehicle function by overloading communication channels with large data packets or isolating vehicles via black hole attacks.
- **Privilege Escalation:** Unauthorized users requesting administrative-level access to vehicle systems.
- **Malware in Media Systems:** Viruses introduced through infotainment platforms, potentially impacting systems like GNSS.
- **Malicious Messaging:** Harmful content transmitted within or between vehicles, including CAN messages, vehicle-to-vehicle (V2V) data, diagnostic exploits, and proprietary component-level communications.

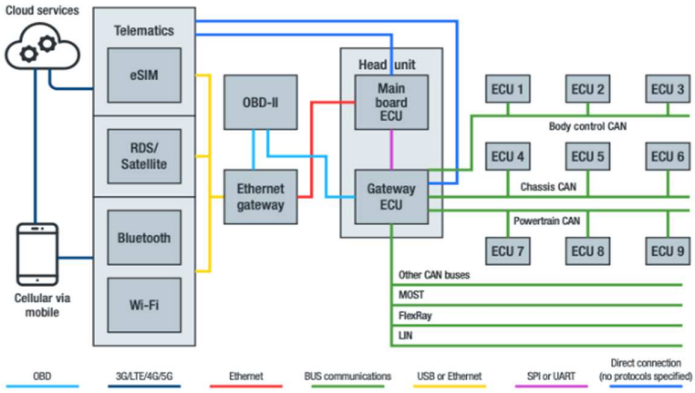


Fig. 2. A theoretical visualization of a generic network architecture for a modern car [11]

Between 2020-2025 there were some notable attacks which translated into 87.7% from all incidents reported [3] [7] [10]. The following potential vulnerabilities related to vehicle data and code have been identified: extraction, modification and deletion of data and code from vehicles; data entry and malicious code; introduction of new software that allows rewriting the existing one; disruption of systems or operations; manipulation of parameters in vehicles.

Between 2020-2025 around 50.8% of the vulnerabilities and threats reported were related to software solutions of devices not being appropriately protected [3]. For example, during this period six potential vulnerabilities have been reported:

- use of cryptographic technology that may be either compromised or not applied correctly,
- vehicle components that can be compromised and allow critical systems to attack,
- applications or devices developed without applying security policies automatically allowing vulnerabilities,
- incorrect architectures of systems or applications that in turn introduce vulnerabilities,
- data transfer not allowed,
- physically attacking systems, thus enabling an attack.

Several of these attacks were identified on Bluetooth communication modules of different physical components (CVE-2021-28139). This allowed various attacks that affected the correct functioning of components and critical systems. These problems were identified with about 1400 different products from different industries.

The need for vehicles to become more interconnected automatically exposed different vulnerabilities, which represent 47.1% of the threats reported. For example, in the European documentation, three possible vulnerabilities related to external communication and connectivity of vehicles have been identified:

- incorrect handling of telematics and remote operation using wireless short-distance communication systems,
- allowing external software to be installed, such as on vehicle media systems, thus enabling attacks on these systems,

- equipment connected to external communication interfaces such as USB ports, integrated OBD used as a means of attacking vehicles.

For example, in January 2021, an Asian manufacturer's media system was penetrated, and vulnerabilities were found allowing access at the operating system level using USB equipment. Another example was identified in September 2021, when a team specialized in luxury car theft was able to use hardware to connect via the OBD port to the vehicle, allowing them to rewrite new keys that allowed them access to all the vehicle's functionalities.

These vulnerabilities account for approximately 24.1% of attacks. Key issues include the use of connection servers to target vehicles or extracting data. Notable methods involve:

- abuse of privileges, typically via internal resources of the equipment manufacturer,
- unauthorized server access, enabled through intentional backdoors, poor system maintenance leading to software flaws, or attacks such as SQL injection.

Interrupting server services that automatically affect the vehicle. This type of attack effectively means the lack of communication between the vehicle and the server. Automatically, the vehicle cannot be operational due to the services it depends on by connecting to the server.

Compromised or lost data from servers. These types of attack can be carried out by the following methods:

Abuse of privileges: usually, internal resources.

Loss of information through the cloud: usually, sensitive data can be lost through attacks or incidents when splints are held in the cloud servers of various external operators.

Unauthorized access to the server: most of the time they can be achieved by leaving open doors or software that is not maintained with changes based on the latest vulnerabilities, SQL attacks or others.

Physical unauthorized access using USB drives or other media connection methods.

Unintentional data exposure mistakes, most often administration errors.

One of the vulnerable areas, representing 4.3% of the total attacks, is related to vehicle update procedures [3] [7] [10]. Incorrect use of these procedures can lead to potential attacks on vehicles. Several such attacks have been identified:

- compromising procedures for online transmission of updates to vehicles, including software or update programs,
- compromising local or physical maintenance procedures by transmitting compromised firmware or programs,
- manipulating applications before the maintenance process, thus having firmware or programs compromised,
- compromise of cryptographic keys allowing the installation of invalid versions.

The most well-known potential hazards, representing 3.2% of the vulnerabilities, may be caused by the following human mistakes:

- an administrator, operator or any other authorized user can be tricked into loading malicious software that allows an attack to be activated,
- cybersecurity procedures are not followed.

For example, in June 2023, the North American division of a European automaker allowed personal data for 1,000 customers or potential customers to be made available due to such an attack. The attack was possible because the data was improperly saved to a cloud server, without applying security policies, by a partner who had access to that database. Even if it was the partner who saved the data in an unprotected location and who did not comply with security policies, in the end it was the manufacturer who was exposed. Another case is that of a large Asian manufacturer that was suddenly faced with the source code for their mobile application exposed in January 2021. Thus, hackers were able to gain access to source code from the misconfigured GIT server and therefore to internal libraries, with access to the logistics portal; this way parts with automotive diagnostic solutions were exposed to the public.

2024: Expanding Attack Surface and Strategic Targeting

January 2024: exposed 585 GB database at a US EVSE provider, a cyberattack on a global Tier-2 supplier with 1.2 TB of data breached,

and research showing ELD vulnerabilities that allow truck control and malware spread, illustrating early-year focus on large data breaches and fleet-scale risks [12] [13] [14].

February: A redirect vulnerability on German OEM subdomains, ransomware on a major semiconductor manufacturer, a PII exposure at a South Korean OEM, a Lithuanian EV charging cyberattack that shut down chargers and leaked 20,000 customer records, and a UK suspension of non-compliant EV chargers, showing strong activity in both enterprise IT and EV infrastructure [15] [16] [17].

March: Representative incidents include an extended cyber-espionage campaign against a major German OEM group, and research exposing serious CAN-bus injection weaknesses in e-scooters, marking a shift toward IP theft and micromobility safety threat [18] [19].

April: Discovery of a German OEM cloud misconfiguration exposing sensitive data, a large-scale ransomware attack on a South Korean OEM with 3 TB of data exfiltrated, and a Chinese OEM telematics issue affecting GPS, emphasizing OEM-centric data and service risks [20] [21].

May: Incidents include a cyberattack halting production at a global agricultural machinery manufacturer, a data breach at a European vehicle tracking and fleet management provider, and an Irish smart-mobility taxi database leak exposing over 300,000 passenger records, highlighting operational disruption and large PII exposures [22].

June: A major US dealership-management software provider suffered ransomware that shut down 15,000 dealerships for nearly three weeks, and security researchers exposed serious vulnerabilities in a Korean OEM dealer API that enabled vehicle control via license plates, underlining how single incidents can scale to thousands of assets [23] [24].

July: Vulnerabilities in EV charging stations enabling unauthorized access, a DoS-related weakness in traffic controllers in Norway, and cyber-attacks on traffic systems and smart-mobility infrastructure, stressing critical-infrastructure exposure in mid-year [25] [26].

August: Ransomware attack on a South Korean automotive supplier compromising 2.3 TB of data, and discovery of a hardware backdoor in widely used MIFARE technology for transit, reflecting deep supply-chain and transport-system risk [27] [28].

September: Research revealed critical vulnerabilities in autonomous driving systems via ICMP-based attacks, and a critical Dutch traffic pre-emption system flaw that forced replacement of thousands of traffic lights, underscoring safety-critical ADAS/AV and ITS weaknesses [29] [30] [31].

October: A ransomware group claimed theft of internal records and PII from a German OEM group, and security flaws in VCSEC immobilizer ECUs at a US EV OEM were documented, showing continued focus on OEMs and high-value EV targets [32] [33] [34].

November: A UK telematics provider was hit by cyberattack causing business disruption and suspected data theft for many international fleets, and a multi-CPO data breach led to over 116,000 consumers' PII and OCPP data being leaked on a hacking forum [35] [36] [37].

December: Multiple infotainment vulnerabilities were published for German, Chinese and Japanese OEM systems, together with attacks on a global auto-parts supplier in Canada, reinforcing that the year closed with continued pressure on in-vehicle systems and suppliers [38] [39] [40].

2.2 Vectors and Attack Types

Since 2020, the automotive sector has experienced a marked escalation in cyberattacks, particularly those carried out by Black-Hat actors with malicious or financial intent, rising to 52.2% that year and further to 63% in 2022. White-Hat activities declined to 37%. These attacks are increasingly remote, by 2022, nearly 97% of them, split into short-range (70%, e.g., man-in-the-middle) and long-range (30%, e.g., app-based or physical OBD port access).

Real-world incidents underline these risks. A researcher exploited keyless entry using only a phone and a $20 Bluetooth device. Another compromised 25 U.S. vehicles via vulnerabilities in an open-source data solution, gaining control over critical functions such as door locks, engine start, and security systems. Attacks now often target not just infotainment or sensor systems, but central communication frameworks, echoing threats seen in energy and

healthcare infrastructures. A cyberattack on Denmark's largest rail operator disrupted national operations for hours, underscoring the broader societal impact.

The exponential growth of data transmission further magnifies the attack surface. By 2025, connected vehicles are expected to transmit 25 GB/hour, with autonomous vehicles reaching up to 500 GB/hour. This necessitates securing the intra- and extra-vehicular communication layers, commonly structured using the OSI model. For instance, CAN Bus communication involves the Data Link layer (LLC and MAC) and the Physical layer (PLS, PMA, MDI), each vulnerable to exploitation if not properly secured.

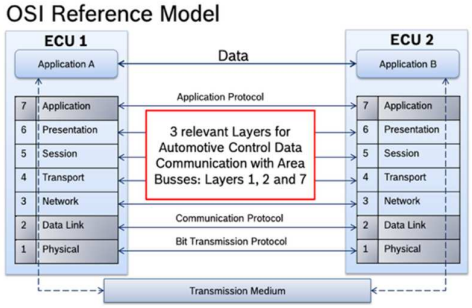


Fig. 3. OSI Reference Model [43]

Bluetooth Low Energy (BLE) is heavily used for internal equipment communication. In 2022, researchers demonstrated control over vehicle functions via BLE manipulation. Similarly, media systems (connected via Bluetooth and the internet) are vulnerable to unauthorized app installations that enable remote monitoring or manipulation when Wi-Fi is present.

Remote access applications, which offer users functionalities such as vehicle tracking, heating control, and diagnostics, are also targeted. Weak password practices or insecure mobile apps can lead to identity theft, GPS-based stalking, or full account compromise. Android Automotive's

System Service Architecture attempts to mitigate these risks through:

- **application-layer validation** and permission enforcement,
- **well-defined APIs** that reject arbitrary data transmissions,
- **secure update services** with full-disk encryption and verified boot,
- **vehicle HAL** restrictions that validate message types and enforce SELinux protections.

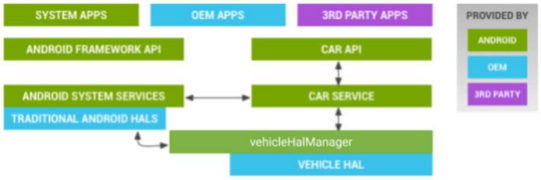


Fig. 4. System Service Architecture [40]

Despite these safeguards, vulnerabilities remain. In 2021, the **Log4Shell exploit** exposed backend servers that store vehicle diagnostics, location data, and user information. Similarly, Android Automotive apps are subject to hijacking, phishing, and **repackaging attacks**, where malicious code is embedded into modified applications. Mobile Device Management (MDM) and anti-malware tools remain essential for mitigation [40] [41] [42].

The **Telematic Control Unit (TCU)** is another critical vulnerability point. It enables vehicle-to-server communication via VPN and SIM modules. Attackers have exploited TCUs by removing and repurposing SIM cards, impersonating legitimate devices to gain unauthorized access to manufacturer networks.

Keyless entry systems are frequently exploited using:

- **signal amplification**, extending key fob range,
- **message replay**, copying and reusing unlock/start signals,
- **OBD-based key reprogramming**, connecting to the vehicle's diagnostic port,
- **signal tampering**, intercepting and altering key communication.

There have also been cases of **OEM key theft**, use of modified audio speakers for signal injection, and widespread vehicle theft (745,000 cases reported in North America alone in 2022).

Emerging attack vectors include **Wi-Fi-enabled drones** that exploit wireless communication modules to access critical vehicle ECUs, responsible for controlling the engine, steering, brakes, windows, and locks. In one case, attackers remotely disabled a vehicle's steering and engine control through delayed CAN responses, without altering the physical hardware.

The **OBD port**, originally designed for diagnostics, has become a significant vulnerability. Attackers have successfully manipulated it to rewrite critical software modules, such as the **Battery Management System**, altering charging behavior to improve battery longevity or disrupt functionality.

2.3 Cybersecurity Impact in the Automotive Field

Cyber security is becoming one of the most important aspects for anyone working in the field of vehicle production, especially due to the impact that any attack can have not only from a financial perspective, but especially from the perspective of citizen safety.

Thus, cyber-attacks can have a financial impact on several strategic areas. It is estimated a market of $197 trillion by 2030 in all communication in and between vehicles. An Accenture article mentions that the automotive industry will lose about $505 trillion due to attacks between 2019 and 2025.

In fact, this type of attack changes from year to year. If car theft was 3rd in 2022, in 2023 the impact on manufacturers or car charging systems was even greater.

All these attacks are putting additional pressure on the Automotive Industry to define, implement, and audit more best practices, standards and policies.

Connectivity is a fundamental enabler of future vehicle technologies, particularly autonomous driving and advanced driver-assistance systems (ADAS), which rely heavily on continuous data exchange. However, increased connectivity introduces significant cybersecurity risks, prompting manufacturers to enhance protective measures to safeguard user data and vehicle functionality.

Key Connected Car Technologies include:

- **Telematics:** Enables real-time tracking, driving behavior analysis, and emergency services such as crash notifications.
- **Infotainment Systems:** Integrate GPS navigation, Bluetooth, audio streaming, Wi-Fi hotspots, and smartphone mirroring (e.g., Apple CarPlay, Android Auto).
- **ADAS:** Enhances safety with features like adaptive cruise control, lane departure warnings, emergency braking, and blind spot monitoring.
- **Remote Access:** Allows users to start/stop engines, lock/unlock doors, and check diagnostics via smartphone apps or key fobs.
- **Over-the-Air (OTA) Updates:** Deliver performance improvements, security patches, and new features without physical servicing.

This interconnected ecosystem creates a vast and complex attack surface. While most communication is wireless, vehicles depend on networked Intelligent Transport Systems (ITS) infrastructure, further increasing exposure to cyber threats.

Identified Attack Vectors include:

- **V2X Manipulation:** Spoofing or passively intercepting vehicle-to-everything communications.
- **ITS Infrastructure Targeting:** Injecting false commands, executing MitM attacks, or sniffing traffic between vehicles and back-end systems.
- **Remote Exploitation:** Includes firmware manipulation, jamming, CAN bus hijacking, RF-based head unit access, and remote control of systems.
- **In-Vehicle Exploitation:** Leveraging malicious apps, sensor jamming, image manipulation, and software misconfigurations to compromise systems.
- **Network Exploitation:** Utilizing tools like Shodan, phishing, DDoS, and weak authentication to breach vehicle or ITS networks.
- **Supply Chain Attacks:** Involving malvertising, SQL injection, XSS, DNS spoofing, session hijacking, and manipulation of update mechanisms.

Although some attack methods overlap, their execution and impact vary. The growing reliance on connectivity and data exchange necessitates robust cybersecurity strategies to ensure the safe deployment of future vehicle technologies.

3. FUTURE OF THE INDUSTRY, DISCUSSION AND IMPLICATIONS

According to McKinsey [45], there are approximately 1.3 billion vehicles globally, with

the vast majority privately owned. In the U.S., for instance, there are 868 vehicles per 1,000 people. Despite projections of future shifts toward shared mobility, private cars remain the dominant mode of urban transport, followed by public transportation. As public transit expands new challenges emerge, including the need for wireless charging and automated vehicle charging systems.

This evolution aligns with industry projections, such as those from NXP [44], which state that the modern vehicle is becoming more electric, connected, and autonomous. This transformation demands a shift from hardware-centric designs to software-driven ecosystems, centralizing the **Vehicle-to-Everything (V2X)** communication paradigm. V2X encompasses various communication types:

- **V2I (Vehicle-to-Infrastructure):** Communicates with road infrastructure for alerts on accidents, construction, or parking.
- **V2V (Vehicle-to-Vehicle):** Shares data to avoid congestion or collisions.
- **V2N (Vehicle-to-Network):** Interfaces with traffic lights, lane markings, and road systems.
- **V2C (Vehicle-to-Cloud):** Enables real-time cloud-based services and analytics.
- **V2P (Vehicle-to-Pedestrian):** Communicates with pedestrian devices and infrastructure to enhance safety.
- **V2D (Vehicle-to-Device):** Connects with in-vehicle electronic devices.
- **V2G (Vehicle-to-Grid):** Interacts with the power grid to manage energy flow.

These functions rely on emerging wireless technologies like **DSRC (Dedicated Short-Range Communications)** and **C-V2X (Cellular-Vehicle-to-Everything)**, the latter already supported by major producers such as Qualcomm through 4G LTE and 5G standards.

According to NXP [44], the shift to a connected ecosystem introduces new use cases:

- **Predictive Maintenance:** Prevents failures by forecasting component wear, optimizing maintenance schedules, and reducing downtime.
- **Advanced Vehicle Diagnostics:** Enables real-time diagnostics, FOTA (Firmware Over-The-Air) updates, and autonomous functionality [46].
- **Usage-Based Insurance and Fleet Management:** Allows tailored insurance plans and efficient fleet operations.
- **Vehicle Safety and Security:** Supports real-time monitoring, emergency services, and OTA security patches.
- **Feature Analytics and Public Safety:** Enhances insight into vehicle usage and contributes to intelligent transport systems.

The reliability of future smart vehicle networks depends on **IoT-based Prognostics and Health Management** (PHM) systems [45]. To prevent in-service failures that could degrade network performance, vehicles must be removed from operation when health deteriorates [47]. A comprehensive framework combining driving dynamics, system performance, and crash data is needed to assess vehicle integrity [48]. Wireless car-to-car and car-to-infrastructure (C2X) communication further enhances road safety.

However, in-vehicle networks, typically based on the **Controller Area Network (CAN)**, present significant security vulnerabilities. Although valued for reliability and real-time performance, the CAN bus lacks built-in security, having been designed with the assumption that all ECUs are trusted. High-speed CAN (500 kbps) is used for critical ECUs, while low-speed CAN serves non-time-sensitive systems. External interfaces such as OBD-II, Bluetooth, Wi-Fi, and GPS allow entry points for attackers.

Koscher et al. [49] demonstrated that full vehicle control could be achieved through these interfaces. In 2015, researchers [50] remotely hijacked a Jeep Cherokee by exploiting ECU vulnerabilities.

As vehicles integrate AI and Recommender Systems (RS), new ethical concerns arise. Users acknowledge the usefulness of such features but express unease over their intrusive nature and potential for misuse of personal data [51]. Features like emotion or mood detection are seen as both helpful and privacy invasive. The primary concern revolves around data privacy and the improper use of personal information, especially when collected without clear user consent or lacking compliance with security standards.

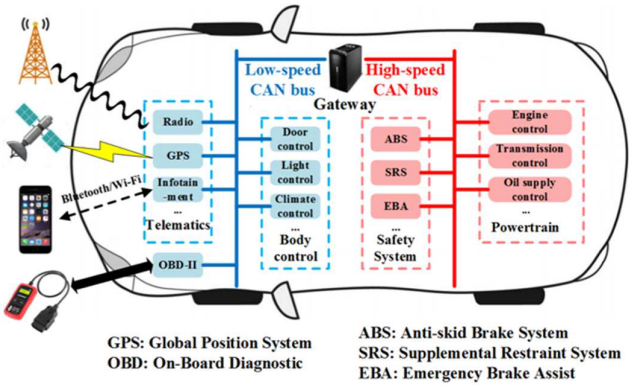


Fig. 5. In-vehicle networks based on the CAN bus [46]

Addressing these risks requires multi-stakeholder collaboration. Partnerships between automotive companies and cybersecurity firms are essential to proactively manage vehicle cyber risks, secure vehicles by design, detect and respond to threats, ensure safe and secure software updates and perform regular penetration testing and system audits [52].

4. CONCLUSIONS

The automotive industry is undergoing a profound and rapid transformation, driven by connectivity and the shift toward electric and autonomous vehicles. This evolution is characterized by a massive increase in on-board computing power, software lines of code, and data generation, making modern cars complex, networked systems.

However, this heightened connectivity has introduced significant cybersecurity risks. The analysis of cyber security incidents from 2020 to 2025 reveals that:

- Communication Channels and Vehicle Data/Code are the most frequent targets, highlighting critical vulnerabilities in the core functions that enable both intra and extra-vehicle connectivity.
- Remote and large-scale attacks are the primary threat method, often targeting multiple Original Equipment Manufacturers (OEMs) simultaneously.
- New threat landscapes, such as attacks on EV charging infrastructure and the dual role of AI in both offense and defense, are emerging and demand proactive security measures.

The research directions outlined in this paper, specifically keyless system penetration testing, manipulation of an Infotainment System, and the analysis of intra- and extravehicular communication limitations are critical steps to directly address the highest-frequency and highest-impact vulnerabilities identified in the industry status quo.

In conclusion, cybersecurity is no longer an optional feature but a mandatory and non-negotiable extension of quality in the automotive sector. Moving forward, the industry must prioritize compliance with regulations like UNECE WP.29, secure vehicles by design, and establish strong partnerships with cybersecurity firms to manage risk, detect incidents, and ensure the safety and privacy of drivers in the connected car era. The automotive industry is undergoing a profound and rapid transformation, driven by connectivity and the shift toward electric and autonomous vehicles. This evolution is characterized by a massive increase in on-board computing power, software lines of code, and data generation, making modern cars complex, networked systems.

5. REFERENCES

[1] Juniper Research, *Consumer Connected Cars: Telematics, In-vehicle Apps & Connected Car Commerce 2018-2023*

[2] Statista/Global Data IoT growth estimates, *IoT in 2023 and beyond,* https://techinformed.com/iot-in-2023-and-beyond

[3] Upstream Security, *Global Automotive Cybersecurity Report,* 2025, https://upstream.auto/ty-2025-gacr-executive-summary/

[4] *Addendum 154 – UN Regulation No.155,* 2021, https://unece.org/sites/default/files/2021-03/R155e.pdf

[5] *Addendum 154 – UN Regulation No.156,* 2021, https://unece.org/sites/default/files/2021-03/R156e.pdf

[6] ISO SAE 21434 / 2021, *ISO SAW 21434, 2021*, https:/ /www.iso.org/standard/70918.html

[7] Upstream Security, *Global Automotive Cybersecurity Report,* 2022, https://upstream.auto/

[8] Birnie, A. et al., *Identifying the challenges and solutions for the emerging era of automotive zonal architectures*, White Paper Zonal Architectures, NXP, 2021, http://www.nxp.com/vehiclenetworking

[9] NXP, *The Evolution of Automotive Processing*, Investor Teach-In, 2021, https://investors.nxp.com/

[10] Upstream Security, *Automotive Cyber Trend Report H1'2023*, https://upstream.auto/

[11] Huq, N. et al., *Cybersecurity for Connected Cars*, Trend Micro Research, 2021, https://documents.trendmicro.com

[12] Paganini, P.*, Don't trust links with known domains: BMW affected by redirect vulnerability,* 2024,https://securityaffairs.com/156843/reports/bmw-affected-by-redirect-vulnerability.html

[13] Antoniuk, D.*, Taiwanese Semiconductor company hit by ransomware attack,* 2024, https://therecord.media/foxsemicon-ransomware-attack-taiwan

[14] Singh, J.*, Hyundai Motor India fixes bugs that expose customers personal data,* 2024, https://techcrunch.com/2024/01/11/hyundai-motor-india-data-exposed/

[15] Page, C.*, BMW security lapse exposed sensitive company information,* 2024, https://techcrunch.com/2024/02/14/bmw-security-lapse-exposed-sensitive-company-information-researcher-finds/

[16] Abrams, L.*, Hyundai Motor Europe hit by Black Basta ransomware attack,* 2024, https://www.bleepingcomputer.com/news/security

[17] Broga, K.*, Data of 20,000 Ignitis ON clients leaked in cyber incident,* 2024, https://www.delfi.lt/en/business/data-of-20-000-ignitis-on-clients-leaked-in-cyber-incident-95857777

[18] Lyons, J.*, Truck-to-Truck worm could infect – and disrupt – entire US commercial fleet,* 2024, https://www.theregister.com/2024/03/22/boffins_tucktotruck_worm/

[19] Waqas*, Leading EV Charging Firm Spills Trove of Customer Info in a Server Leak,* 2024, https://hackread.com/ev-charging-firm-spills-trove-of-customer-info/

[20] Maddison, L.*, Taxi software firm breach expose details over 300,000 passengers,* 2024, https://www.techradar.com/pro/security/

[21] *Chinesische Hacker sollen Volkswagen ausspioniert haben,* 2024, https://www.manager-magazin.de/unternehmen/autoindustrie

[22] Khaitan, A.*, Cybersecurity alert: Frotcom International Faces Alleged Data Breach,* 2024, https://thecyberexpress.com/alleged-frotcom-data-breach/

[23] NIST*, CVE-2024-35537,* 2024, https://nvd.nist.gov/vuln/detail/CVE-2024-35537

[24] Ddos*, CVE-2024-35213Critical Vulnerability Discovered in BlackBerry QNX SDP,* 2024, https://securityonline.info/cve-2024-35213-critical-vulnerability-discovered-in-blackberry-qnx-sdp/

[25] Dates, J.*, CHARX Vulnerability Discovered,* 2024, https://blog.ret2.io/2024/07/17/pwn2own-auto-2024-charx-bugs/

[26] Baran, G.*, Critical Flaws In Traffic Light Controller Let Attackers Change Signal Lights,* 2024, https://cybersecuritynews.com/traffic-light-controller-authentication-bypass-vulnerability/

[27] Petkauskas, V.*, Black Hat USA 2024:vehicle head unit can spy on you,* 2024, https://cybernews.com/security/android-head-units-drivers-data-safety/

[28] Eun-jin, K.*, Ransomware makes the third attack on Hanon Systems, Resulting in 2.3TB of Data Leakage,* 2024, https://www.businesskorea.co.kr/news/articleView.html?idxno=223166

[29] Laio., *Chip hacking poses threat to public transport security,* 2024, https://innovationorigins.com/en/chip-hacking-poses-threat-to-public-transport-security/

[30] Bonnotte, N., Mohammed, S., Stübler, T., Amodei, A., *arXiv preprint 2409.01324,* 2024, https://arxiv.org/html/2409.01324v1

[31] Kevin2600, *Braktooth Hunting in the Car Hacker's Wonderland,* 2024, https://kevin2600-cmd.github.io/2024/09/13/Braktooth-Hunting-in-the-Car-Hacker's-Wonderland.html

[32] Rivera, N., Curry, S., Rhinehart, J., Carroll, I., Lugo, K., *Hacking Kia*, 2024, https://samcurry.net/hacking-kia

[33] Cybernews., *Dutch government will replace hackable traffic lights,* 2024, https://cybernews.com/news/dutch-government-will-replace-hackable-traffic-lights/

[34] Lekander, A., *Volkswagen says it's "monitoring the situation" following 8Base ransomware claims,* 2024, https://cyberinsider.com/volkswagen-says-its-monitoring-the-situation-following-8base-ransomware-claims/

[35] Berard, D., Imbert, T., Dehors, V., *0-click RCE on Tesla Model 3 through TPMS sensors light,* 2024,

https://www.synacktiv.com/sites/default/files/2024-10/hexacon_0_click_rce_on_tesla_model_3_through_tpms_sensors_light.pdf
[36] Fleet News., *Telematics giant Microlise suffers cyber attack,* 2024 https://www.fleetnews.co.uk/news/telematics-giant-microlise-suffers-cyber-attack
[37] Lekander, A., *Zero-day flaws in Mazda's infotainment expose cars to takeover attacks,* 2024, https://cyberinsider.com/zero-day-flaws-in-mazdas-infotainment-expose-cars-to-takeover-attacks/
[38] Cyber Daily, *Tesla data breach falsely claimed by IntelBroker; third-party EV charging firm actually breached*, 2024, https://www.cyberdaily.au/security
[39] TechCrunch, *Researchers find security flaws in Skoda cars that may let hackers remotely track them*, 2024, https://techcrunch.com/2024/12/12/researchers-find-security-flaws-in-skoda-cars-that-may-let-hackers-remotely-track-them/
[40] zgsnj123, *BYD head unit vulnerabilities* (repository), 2024, https://github.com/zgsnj123/BYD_headunit_vuls/tree/main
[40] Android Open Source Project, *Vehicle System Isolation*,https://source.android.com/docs/automotive/security/vehicle_system_isolation
[41] Sungjae, H. et. al., *All about activity injection: Threats, semantics, detection, and defense*, Journal of Software: Practice & Experience, 50(7), 2020, pp. 1061-1086, https://doi.org/10.1002/spe.2792
[42] Smys, S. et. al, Proc. 2nd Int. Conf. on Computer Networks & Comm. Tech (ICCNCT 2019), Lecture Notes on Data Engineering and Communications Technologies, Vol. 44, Springer, 2020, https://doi.org/10.1007/978-3-030-37051-0
[43] Aboubacar, D., *OSI Layers in Automotive Networks*, IEEE 802.1 Meeting, Orlando, 2013, https://ieee802.org/
[44] Andrew, Z., *The Future of Automotive Connectivity*, NXP & ABI research, White Paper, 2021, https://abiresearch.com/
[45] Heineke, K. et. Al., *The Future of Mobility*, McKinsey Quarterly, 2023
[46] Lu, Z. et al., *LEAP: Lightweight Encryption and Protocol for In-Vehicle Communications*, 2019, https://doi.org/10.48550/arXiv.1909.10380
[47] Kwon, D. et. al., *IoT Based Prognostics and Systems Health Management for Industrial Applications*, IEEE Access, 4, 2016, pp. 3659-3670,https://doi.org/10.1109/ACCESS.2016.2587754
[48] Kompass, K. et. al., *Adaptive Restraint Systems: Toward Integral Safety*, Encycl. of Automotive Engineering, Wiley, 2014, https://doi.org/10.1002/9781118354179.auto259
[49] Koscher, K. et. al., *Experimental Security Analysis of a Modern Automobile*, IEEE Symp. Security & Privacy, 2010, pp. 447-462, https://www.autosec.org/pubs/cars-oakland2010.pdf
[50] Valasek, C., Miller, C., *Remote Exploitation of an Unaltered Passenger Vehicle*, IOActive, 2015, https://www.ioactive.com/
[51] Vrščaj, D. et al., *Is Tomorrow's Car Appealing?*, AI & SOCIETY, 35, 2019, p. 7729, https://doi.org/10.1007/s00146-020-00941-z
[52] Deichmann, J. et. al, *The Race for Cybersecurity: Protecting the Connected Car*, McKinsey & Co., 2019

Cercetări și tehnici pentru îmbunătățirea comunicării în interiorul și în exteriorul vehiculului

Rezumat: Industria auto se transformă rapid datorită conectivității crescânde și tranziției către vehicule electrice și autonome. Această schimbare implică o creștere exponențială a calculului la bord, a complexității software-ului și a generării de date, transformând vehiculele în sisteme complexe, conectate în rețea, cu vulnerabilități sporite în materie de securitate cibernetică. Acest document analizează vectorii cheie de atac și clasifică incidentele de securitate cibernetică. Consolidarea rețelelor și creșterea comunicării intra și extra-vehiculare sunt esențiale. Numărul de mașini conectate a crescut de la 330 de milioane în 2018 la 775 de milioane în 2023 (o creștere de 134%), iar prognozele sugerează că vor exista 50 de miliarde de dispozitive conectate până în 2030. Măsurile de reglementare impun acum asistență inteligentă la viteză, detectarea oboselii, înregistrarea evenimentelor de urgență și sisteme avansate de asistență a șoferului. Tehnologia Vehicle-to-everything (V2X) oferă un potențial transformator pentru eficiența traficului și siguranța rutieră.

Vasile-Cătălin MIHACEA, PhD Candidate, "Lucian Blaga" University of Sibiu, Doctoral School of Engineering Sciences and Mathematics, vasilecatalin.mihacea@ulbsibiu.ro, +40 269 217 779.
Remus BRAD, Professor PhD, "Lucian Blaga" University of Sibiu, Faculty of Engineering, remus.brad@ulbsibiu.ro, +40 269 217 779, 10 Victoriei Blvd., Sibiu, Romania.