Cybersecurity Challenges and Defense Strategies in Connected and Autonomous Vehicles

Veera Venkata Krishnarjun Rao Adabala

Michigan, USA
adabalaveera2@gmail.com

Abstract:
As Connected and Autonomous Vehicles (CAVs) become more prevalent, they bring with them a host of cybersecurity challenges from their reliance on complex electronics, embedded systems, and integrated communication networks. The increased interconnectivity between critical vehicle systems such as braking, steering, infotainment, and telematics introduces multiple entry points for potential cyber threats. This paper investigates these vulnerabilities, with a focus on Electronic Control Units (ECUs) and in-vehicle networks including Controller Area Network (CAN), FlexRay, and Automotive Ethernet. Traditional in-vehicle communication protocols were not originally developed with security as a priority, leaving them exposed to risks such as spoofing, message injection, denial-of-service attacks, and unauthorized control. As vehicles adopt Ethernet-based architectures to meet growing data demands, new risks emerge due to the broader system complexity and deeper integration with external networks like cloud platforms and vehicle-to-everything (V2X) interfaces. The paper analyzes plausible attack scenarios, such as remote access through infotainment systems, direct physical exploitation via diagnostic ports, tampering with over-the-air (OTA) updates, and threats to artificial intelligence systems used in autonomous functions. The study further evaluates existing and emerging defense mechanisms, such as cryptographic protocols, secure ECU communication, intrusion detection and prevention systems (IDPS), secure boot loaders, and hardware security components. Emphasis is placed on real-time detection techniques, including AI-enhanced anomaly detection models that recognize deviations from standard vehicle behavior patterns. Additionally, the paper explores cutting-edge developments like blockchain-based firmware distribution, next-generation cryptographic solutions resistant to quantum threats, and virtual simulation tools used for cybersecurity validation. Regulatory and industry frameworks such as ISO/SAE 21434 and UNECE WP.29 are also discussed to provide insight into evolving compliance expectations. By presenting an overview of the threats and mitigation strategies, this paper provides more resilient automotive ecosystems as the industry continues its transformation toward fully connected, software-defined vehicles.

Keywords: Cybersecurity, Autonomous Vehicles, ECUs, CAN Bus, Automotive Ethernet, Intrusion Detection, Connected Vehicles, Over the Air (OTA), Vehicle to everything (V2X), Flexray, WiFi vehicle-to-grid(V2G), Public Key Infrastructure (PKI), Hardware Security Modules (HSM), Gateway Security, Cryptography, Trusted Platform Modules (TPMs), Message Authentication Code (MAC).

I. INTRODUCTION

The advancement of connected and autonomous vehicles (CAVs) is driving an important transformation in the automotive industry. These vehicles integrate a wide array of technologies including software-driven control systems, embedded electronics, and wireless communication to enable automation, real-time data exchange, and advanced user experiences. However, the increasing dependence on connectivity and digital control introduces significant cybersecurity concerns. As vehicles become more intelligent and interconnected, the potential for unauthorized access, data manipulation, and system disruption increases, making cybersecurity a great challenge for the automotive sector.

Earlier vehicle designs relied on relatively isolated subsystems, where electronic components operated with minimal external interaction. Communication between all these components was facilitated using in-vehicle protocols such as the Local Interconnect Network (LIN), Controller Area Network (CAN), and FlexRay. These protocols were developed with an emphasis on reliability, timing, and simplicity, under the assumption that internal networks would remain secure due to the vehicle's physical isolation. For example, CAN protocol, though robust and cost-effective, lacks features such as message authentication and data encryption leaving it susceptible to unauthorized message injection and spoofing if an attacker gains physical or remote access.

The introduction of CAVs has dramatically expanded the complexity of automotive architectural structures. Modern vehicles interact with cloud platforms, mobile applications, external infrastructure, and other vehicles, creating a much broader digital footprint. Capabilities such as vehicle-to-everything (V2X) communication, over-the-air (OTA) updates, remote diagnostics, and cloud-based navigation require frequent external data exchange. Subsequently, autonomous driving features mostly rely on continuous processing of information from cameras, LiDAR, radar, and various sensor systems, all of them communicate through high-speed internal networks. These enhancements, while essential for automation and convenience, significantly increase exposure to cyber threats and vulnerability.

Unlike traditional systems that functioned largely in isolation, today's vehicles must defend against a wider array of attack vectors. Remote attackers can exploit vulnerabilities in infotainment units, telematics modules, and Bluetooth or Wi-Fi interfaces to access critical vehicle systems. Once an internal network is compromised, the absence of built-in security mechanisms in legacy protocols makes it possible to interfere with core functions such as braking, acceleration, or steering. Additionally, improper implementation of OTA updates can lead to firmware tampering, while sensor-based attacks may cause autonomous systems to behave unpredictably.

This paper provides an in-depth analysis of in-vehicle communication networks and the cybersecurity challenges introduced by the transition to connected and autonomous vehicles. It also provides analysis on current security practices and explores various new approaches to safeguarding vehicle systems against evolving cyber threats in multiple ways. Through this exploration, the paper also aims to support the development of resilient and secure automotive platforms capable of withstanding the demands of immediate future-generation mobility.

II. AUTOMOTIVE ECUS AND COMMUNICATION ARCHITECTURE

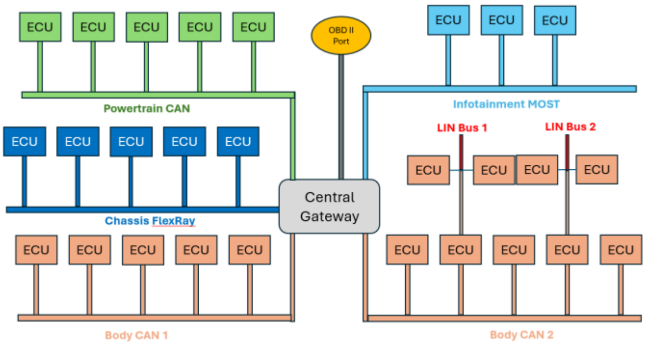

Fig. 1. *Common automotive communication ECU architecture*

Today's vehicles operate as complex electronic systems, often containing between 70 and 150 ECUs. Each ECU is responsible for a specific function ranging from safety-critical systems like braking and steering to comfort and infotainment features. These ECUs must coordinate in real-time, which is made possible through in-vehicle communication protocols. However, the evolution of these protocols, originally designed for isolated vehicle systems, presents growing cybersecurity challenges in the age of connected and autonomous vehicles.

The **Controller Area Network (CAN)** remains the backbone of in-vehicle communication due to its robustness and real-time performance. However, it lacks built-in security measures such as encryption or authentication. Once access is gained physically or remotely an attacker can inject malicious messages or spoof legitimate ones, potentially compromising critical vehicle functions.

The **Local Interconnect Network (LIN)** is used for simpler, low-speed functions like window controls or interior lighting. While cost-effective and efficient for basic tasks, LIN also lacks security features and is not suitable for sensitive systems. Nonetheless, insufficient isolation may allow an attacker to pivot from LIN-connected modules to more critical domains.

FlexRay, designed for safety-critical applications, provides deterministic communication with higher bandwidth and fault tolerance. It supports time-triggered communications(messaging), making it ideal for synchronized systems like steer-by-wire. Still, FlexRay does not include inherent cryptographic protections and requires external security layers in connected architectures.

To meet modern bandwidth needs especially for data-heavy applications such as ADAS, LiDAR, and high-definition infotainment automakers are adopting Automotive Ethernet. Unlike legacy protocols, Ethernet supports scalable topologies and IP-based communication. However, it also introduces traditional IT vulnerabilities, including exposure to packet sniffing, spoofing, and denial-of-service attacks if not properly secured.

Integrating these protocols within a single vehicle creates additional complexity. Gateways linking low-security and high-security domains can become targets for lateral attacks if not properly segmented. Features like over-the-air (OTA) updates and remote diagnostics demand end-to-end integrity and secure communication across all protocol layers.

To summarize, while the communication architecture of modern vehicles is essential to their performance and functionality, its legacy design and increasing exposure to external networks introduce serious cybersecurity risks. Addressing these requires layered defense strategies, including network isolation, message validation, secure boot mechanisms, and real-time intrusion detection tailored for automotive environments.

III. CYBERSECURITY THREAT LANDSCAPE

CAVs are exposed to a wide range of cybersecurity threats because of their integration of wireless communication and digital systems. Technologies such as Bluetooth, Wi-Fi, cellular networks, and V2X interfaces enhance functionality but also create entry points for remote attacks. Vulnerabilities in infotainment systems or telematics units can be exploited to get unauthorized access to vehicle networks, allowing malicious actors to potentially take full control or disrupt vehicle operations without physical contact.

In addition to remote threats, physical access remains a concern, particularly through the OBD-II diagnostic port. Although this interface is critical for maintenance, it can provide a direct pathway to internal networks like the Controller Area Network (CAN) if not properly secured. Through this port, attackers can inject unauthorized messages, overwrite ECU firmware, or alter vehicle behavior.

Firmware integrity is another key concern in modern vehicles. Over-the-air (OTA) update mechanisms, while convenient, can also become attack vectors if they lack proper encryption and authentication. Malicious updates or compromised update channels can allow unauthorized code execution or persistent backdoors within vehicle systems.

Real time scenarios and incidents have underscored the severity of these risks. In a widely publicized 2015 case, researchers remotely manipulated a Jeep’s steering and braking through its infotainment system. Also, security experts demonstrated vulnerabilities in a Tesla’s internal communication network in 2016. These cases highlight how connected systems can be compromised if cybersecurity is not embedded throughout the vehicle's architecture.

To systematically assess and address these threats, frameworks such as STRIDE (Spoofing, Repudiation, Information Disclosure, Tampering, Elevation of Privilege and Denial of Service,) are employed. STRIDE enables security analysts to evaluate risks across multiple dimensions, helping to design more resilient systems by identifying all the potential vulnerabilities early in the development cycle.

As vehicles continue evolving toward higher levels of autonomy and connectivity, the attack surface expands, demanding proactive layered security strategies that integrate intrusion detection along with threat modeling, and secure software practices.

IV. SECURITY CHALLENGES

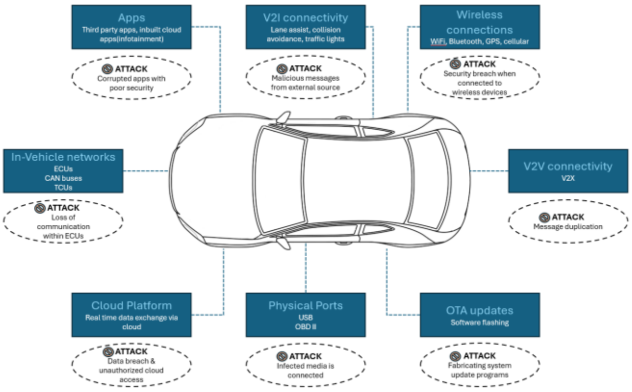
Apps
Third party apps, inbuilt cloud apps(infotainment)
ATTACK
Corrupted apps with poor security
V2I connectivity
Lane assist, collision avoidance, traffic lights
ATTACK
Malicious messages from external source
Wireless connections
WiFi, Bluetooth, GPS, cellular
ATTACK
Security breach when connected to wireless devices
In-Vehicle networks
ECUs
CAN buses
TCUs
ATTACK
Loss of communication within ECUs
V2V connectivity
V2X
ATTACK
Message duplication
Cloud Platform
Real time data exchange via cloud
ATTACK
Data breach & unauthorized cloud access
Physical Ports
USB
OBD II
ATTACK
Infected media is connected
OTA updates
Software flashing
ATTACK
Fabricating system update programs

Fig. 2. *Possible cyber attack scenarios*

Cybersecurity in automotive systems involves overcoming a set of complex, domain specific obstacles. One of the biggest challenges arises from the limitations of computational resources availability within ECUs. These embedded systems are typically designed for very specific functions and incrementally optimized for efficiency and cost, which restricts their ability to handle intensive cryptographic operations. Implementing strong encryption or real-time authentication algorithms can strain these systems or interfere with their intended performance.

Also, many vehicles still rely mainly on legacy communication protocols such as LIN and CAN, which were developed in the era when security was not a priority. These protocols mainly lack very essential built-in mechanisms for data confidentiality or message authentication, making them vulnerable to spoofing and tampering. Modernizing these protocols across the entire vehicle architecture is a complex task, especially when considering compatibility with older systems still in operation.

Real-time performance is another critical constraint. Automotive systems responsible for essential safety features—such as braking, steering, and stability control—must react within milliseconds. Adding cybersecurity measures can introduce processing delays in every stage, so solutions must be designed to meet strict timing requirements without compromising security or system behavior.

Furthermore, the lack of unified security standards across original equipment manufacturers (OEMs) and suppliers adds to the difficulty. Automotive development is widely distributed across various parties involved at every stage, and each party may implement different security strategies, Guidelines, tools, Frameworks or priorities. So, the lack of consistency increases the likelihood of integration issues and security gaps. Although international standards such as ISO/SAE 21434 are beginning to guide cybersecurity efforts in the automotive domain, industry-wide adoption and implementation still vary widely.

All these mentioned factors make automotive cybersecurity uniquely demanding, requiring solutions that are both lightweight and robust, while also adaptable to a fragmented ecosystem of technologies and legacy systems and speed.

V. CURRENT SECURITY MECHANISMS IN AUTOMOTIVE EMBEDDED SYSTEMS

As the automotive industry advances towards connectivity and automation, securing vehicle electronics particularly ECU modules has become a primary focus. The increasing attack surface due to integration with wireless interfaces necessitates robust, multi-layered defense strategies.

A. Message Authentication Codes(MACs)

To ensure that messages exchanged between ECUs remain untampered and originate from legitimate sources, cryptographic authentication techniques such as Message Authentication Codes (MACs) are employed. These codes are typically generated using a secret key in combination with a hash function and are attached to the transmitted data.

- **Key Distribution**: A significant challenge is establishing a secure and scalable key distribution mechanism across all ECUs, especially in complex vehicular networks involving multiple suppliers.
- **Processing Constraints**: Embedded platforms with limited computational resources may face performance bottlenecks when computing MACs in real time.

The inclusion of hardware-based security components such as Hardware Security Modules (HSMs) allows for more efficient cryptographic operations and secure key storage, helping to overcome these constraints.

B. Intrusion Detection System (IDS)

Intrusion Detection Systems (IDS) acts as another defense layer by continuously analyzing in-vehicle network traffic to identify deviations from normal behavior. These systems are broadly divided into:

- **Signature Based IDS**: Detect known attack patterns using predefined signatures. Signature-based systems may not detect novel attacks.
- **Anomaly Based IDS**: Learn normal traffic behavior and identify deviations that may indicate new or unknown threats. Anomaly-based methods can produce high false positive rates.

Efforts are underway to develop lightweight, embedded-friendly IDS models, and to utilize federated learning approaches that allow IDS to evolve based on distributed data without compromising privacy.

C. Secure Boot and Firmware Integrity Verification

To prevent unauthorized or malicious software from executing on startup, modern ECUs employ secure boot mechanisms. This process verifies the digital signature of the firmware before execution begins. The ECU contains a root of trust, which is a securely stored cryptographic key. During startup, the bootloader checks the digital signature of the firmware image. If the validation fails, the ECU enters a safe state or recovery mode.

Secure boot relies on the integrity of cryptographic keys, which must be updated or revoked securely in the field. Legacy ECUs without secure storage or cryptographic accelerators may not support modern secure boot implementations.

Secure boot is increasingly supported by dedicated hardware components such as Trusted Platform Modules (TPMs), which enable tamper-resistant key storage and verification operations.

D. Network Segmentation and Gateway Security

To prevent external threats from propagating across internal vehicle systems, the in-vehicle network is segmented using secure gateways and firewalls. These gateways control data flow between domains such as infotainment and powertrain.

Gateways can inspect message content, enforce rules, and isolate critical systems from non-critical ones. Firewalls may be implemented in software, firmware, or as part of a dedicated gateway ECU. Some of the challenges are Fixed firewall rules may become inadequate as vehicle features evolve with over-the-air updates. Some filtering mechanisms could introduce delays that are unacceptable for safety-critical applications.

Adaptive firewalls capable of real-time rule updates, and gateways that use machine learning to monitor traffic patterns, are being researched to improve both scalability and responsiveness.

E. Secure Over the Air (OTA) Software Update

OTA updates are required for maintaining vehicle software without physical intervention. Ensuring the authenticity and integrity of updates is critical, particularly since compromised updates could affect safety.

Security Requirements:

- Confidentiality: Update packages must be encrypted to prevent interception or tampering.
- Authentication: Updates are signed using asymmetric cryptography to confirm their origin.
- Integrity Checking: Digital signatures are verified by each ECU before installation.
- Rollback Protection: Mechanisms are implemented to prevent outdated or vulnerable firmware from being reinstalled.

Challenges:

- Connectivity Constraints: Vehicles may lose network access during updates, leading to partial installations or failures.
- Distributed Verification: Every ECU must independently verify updates without central dependency, increasing complexity.

Use of lightweight cryptographic techniques and blockchain-based tracking of firmware history is gaining attention to ensure update traceability and resilience against tampering.

VI. EMERGING TRENDS AND RESEARCH IN AUTOMOTIVE CYBERSECURITY

As modern vehicles evolve into complex, interconnected systems, traditional cybersecurity measures are no longer sufficient on their own. To counter the growing cyber threats, innovative technologies that provide intelligent, resilient, and scalable defense mechanisms are needed. Some of the most promising emerging trends and areas of active research in the field are mentioned below.

A. Intelligent Threat Detection Using AI and Machine Learning

Machine learning and AI are playing a transformative role in the detection of cyber threats in vehicular networks. Unlike conventional methods that rely on predefined patterns or static rules, AI-based systems can learn from historical and real-time data to recognize anomalies that might indicate intrusions or malfunctions.

Advantages:

- Anomaly Detection: Models trained on typical vehicle behavior can flag unusual activity, such as unauthorized ECU commands or unusual sensor values.
- Dynamic Adaptation: AI algorithms can update their decision models based on new threat patterns, improving resilience to evolving attacks.
- Context Awareness: AI can factor in driving conditions, user behavior, and environmental inputs to make more accurate security decisions.

Research Opportunities:

- Development of compact, efficient models suitable for embedded automotive systems.
- Federated learning techniques that allow model improvement across multiple vehicles while preserving data privacy.
- AI explainability and certification frameworks to support deployment in safety-critical applications.

B. Adoption of Hardware Security Modules (HSMs)

Hardware Security Modules provide a physical layer of protection for sensitive cryptographic operations. They are specifically designed to resist tampering and can securely perform functions such as key management, digital signing, and secure boot verification.

Advantages:

- Offloads computationally intensive security tasks from the main ECU processors.
- Prevents unauthorized access to encryption keys by isolating them within tamper-resistant hardware.
- Validates the integrity and authenticity of the software before it executes.

Research Opportunities:

- Integration of low-power HSMs into cost-sensitive automotive platforms.
- Extension of HSM capabilities to support post-quantum cryptographic algorithms.
- Development of standardized APIs to support cross-platform compatibility.

C. Distributed Security with Blockchain Technology

Blockchain introduces a decentralized approach to data integrity and verification. In automotive environments, this concept is being explored to improve transparency, trust, and traceability across various operations.

Advantages:

- Software Update Logging: Securely recording update events ensures traceability and auditability across the vehicle lifecycle.
- Component Authenticity Tracking: Using blockchain to validate parts in the supply chain decreases the risk of counterfeit components.
- Secured Data Sharing: Blockchain can enhance trust in vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication by providing immutable records.

Research Opportunities:

- Designing lightweight blockchain protocols suitable for embedded environments with limited resources.
- Balancing decentralization with real-time performance needs.
- Exploring hybrid architectures that combine blockchain with centralized verification for critical scenarios.

D. Secure Vehicle to Everything (V2X) Communication

V2X communication enables real-time data exchange between vehicles, roadside units, pedestrians, and other infrastructure. Ensuring the security of this data is critical, as compromised messages could lead to accidents or traffic disruptions.

Advantages:

- Public Key Infrastructure (PKI): Ensures that all V2X messages are signed by verified entities.
- Message Encryption and Integrity Checks: Protects data in transit and ensures it has not been altered.
- Certificate Management: Regular updates and revocation of certificates help maintain trust in the communication system.

Research Opportunities:

- Implementation of IEEE 1609.2 standards for message authentication and encryption.
- Research into fast, scalable certificate revocation methods for large networks.
- Investigation of post-quantum V2X security protocols to future-proof systems against quantum computing threats.

VII.CONCLUSION

As CAVs become more integrated into transportation networks, the need for advanced cybersecurity solutions becomes even more critical. This paper has emphasized that as CAV technologies evolve, cybersecurity strategies must evolve concurrently to ensure the safety and reliability of these systems. The growing complexity of CAVs, which rely on diverse communication networks, real-time data processing, and automated decision-making, exposes them to a wider array of cyber threats that could compromise vehicle safety, passenger security, and public infrastructure.

To address these emerging risks, cybersecurity must be embedded in the design process from the outset. A security-by-design approach is essential, ensuring that all components, including onboard systems, communication interfaces, and cloud services, are developed with robust security protocols. This proactive approach will help mitigate vulnerabilities before they can be exploited.

The complexity of CAV ecosystems requires a collaborative effort across various sectors, including automotive manufacturers, cybersecurity professionals, regulatory bodies, and technology providers. Only through joint efforts can effective standards and protocols be established, ensuring that security measures remain consistent and comprehensive across the entire CAV system.

Moreover, ongoing research is crucial in this rapidly evolving domain. As cyber threats continue to grow, new methods of detecting and responding to attacks must be developed. Research in areas such as AI-driven cybersecurity, secure communication protocols, and resilient vehicle architectures will play an important role in safeguarding the future of CAVs. By fostering a research-driven, security-conscious approach, the industry can be ahead and respond to the challenges , ensuring that CAVs can operate safely in an increasingly interconnected world.

In conclusion, securing Connected and Autonomous Vehicles is not just a technical challenge but a must for the industry. Collaborative industry efforts, a security-by-design mindset, and continuous research are key to ensuring that CAVs contribute to a safe, efficient, and sustainable future for mobility. demands.

REFERENCES:

1. **Weimerskirch, A. (2016).** Cybersecurity of connected and automated vehicles. ATZ Elektronik Worldwide, 11(6), 26–31**.**
2. **Kumar, A. D., Chebrolu, K. N. R., R, V., & Soman, K. P. (2018).** A brief survey on autonomous vehicle possible attacks, exploits, and vulnerabilities. *arXiv preprint arXiv:1810.04144*.
3. **Commission on Enhancing National Cybersecurity**. (2016). *Final Report*. Retrieved from https://www.nist.gov/cybersecurity.
4. **Pham, M., & Xiong, K**. **(2020)**, *Securing Connected & Autonomous Vehicles: Challenges Posed by Adversarial Machine Learning and The Way Forward Volume 109 Elsevier publication .*
5. **Qayyum, M. Usama, J. Qadir and A. Al-Fuqaha(2020),** "Securing Connected & Autonomous Vehicles: Challenges Posed by Adversarial Machine Learning and the Way Forward," in IEEE Communications Surveys & Tutorials, vol. 22, no. 2, pp. 998-1026, Secondquarter 2020, doi: 10.1109/COMST.2020.2975048.
6. **Dibaei, M., Zheng, X., Jiang, K., Maric, S., Abbas, R., Liu, S., Zhang, Y., Deng, Y., Wen, S., Zhang, J., Xiang, Y., & Yu, S. (2019).** An Overview of Attacks and Defenses on Intelligent Connected Vehicles. arXiv:1907.07455
7. **Lim, H. S. M., & Taeihagh, A. (2018).** *Autonomous vehicles for smart and sustainable cities: An in-depth exploration of privacy and cybersecurity implications. arXiv preprint arXiv:1804.10367.*
8. **Taeihagh, A., & Lim, H. S. M. (2018)**. Governing autonomous vehicles: Emerging responses for safety, liability, privacy, cybersecurity, and industry risks. *arXiv preprint arXiv:1807.05720.*