International Journal of Computer Science and Engineering Research and Development (IJCSERD)
ISSN Print: 2248-9363, ISSN Online: 2248-9371
Volume 13 Issue 2, July-December (2023), pp. 77-102
DOI: https://doi.org/10.5281/zenodo.14892661

CYBERSECURITY IN AUTOMOTIVE NETWORKS: MITIGATING THREATS IN CAN, LIN AND AUTOMOTIVE ETHERNET SYSTEMS

Siranjeevi Srinivasa Raghavan,
Independent Researcher, USA.

Abstract

The increasing complexity and interconnectivity of modern vehicles have introduced significant cybersecurity challenges in in-vehicle communication networks, particularly in Controller Area Network (CAN), Local Interconnect Network (LIN), and Automotive Ethernet. While these protocols facilitate seamless data exchange between Electronic Control Units (ECUs), they were originally designed without robust security features, making them vulnerable to message spoofing, denial-of-service (DoS) attacks, and unauthorized access. Existing mitigation strategies, including message authentication, hardware security modules (HSMs), and intrusion detection systems (IDSs), have provided partial solutions but still face latency, computational overhead, and backward compatibility challenges.

This study explores alternative security approaches for enhancing CAN bus security, including lightweight cryptographic algorithms, real-time software-based monitoring, and AI-driven anomaly detection. Additionally, emerging technologies such as blockchain-based authentication and machine learning-based intrusion detection offer promising avenues for securing in-vehicle networks against evolving cyber threats. The research also highlights the need for standardized security regulations to ensure industry-wide adoption of robust cybersecurity frameworks. By integrating cryptographic security measures, AI-powered detection mechanisms, and regulatory compliance, automakers can significantly enhance the resilience of vehicle

communication networks, ensuring safe and secure mobility in the era of connected and autonomous vehicles.

Key words: Automotive Cybersecurity, Controller Area Network (CAN) Security, Lightweight Encryption, Intrusion Detection System (IDS), Artificial Intelligence in Automotive Security, Blockchain for ECU Authentication, Automotive Ethernet Security, In-Vehicle Communication Protocols, Secure Vehicle Networks, Standardization in Automotive Cybersecurity.

Cite this Article: Siranjeevi Srinivasa Raghavan. (2023). Cybersecurity in automotive networks: Mitigating threats in CAN, LIN and automotive Ethernet systems. International Journal of Computer Science and Engineering Research and Development (IJCSERD), 13(2), 77-102. DOI: https://doi.org/10.5281/zenodo.14892661

1. Introduction

The rapid advancement of automotive technology has led to increasingly complex in-vehicle communication networks that facilitate seamless interactions between electronic control units (ECUs). These networks rely on various communication protocols such as Controller Area Network (CAN), Local Interconnect Network (LIN), and Automotive Ethernet to enable real-time data exchange for essential functions, including powertrain control, infotainment systems, and advanced driver assistance systems (ADAS). While these protocols provide efficiency and interoperability, they were initially designed with minimal security considerations, making them vulnerable to cyber threats. As vehicles become more connected and integrated with external networks, securing in-vehicle communication has become a critical concern for automakers and cybersecurity researchers.

1.1 Overview of In-Vehicle Communication Protocols

In-vehicle communication protocols form the backbone of modern automotive systems, allowing various ECUs and sensors to communicate efficiently. The Controller Area Network (CAN) is one of the most widely used protocols due to its reliability and real-time performance, making it ideal for safety-critical applications such as braking and engine management. However, CAN lacks built-in authentication and encryption mechanisms, making it susceptible to spoofing and denial-of-service (DoS) attacks. The Local Interconnect Network (LIN) is a lower-cost alternative primarily used for non-critical applications such as window regulators and climate control. While LIN offers simplicity and cost-effectiveness, it also inherits security

limitations similar to CAN. Automotive Ethernet, on the other hand, provides higher bandwidth and scalability, supporting advanced applications such as over-the-air (OTA) updates and autonomous driving systems. Despite its advantages, Ethernet-based communication introduces new security challenges, including the need for robust encryption and intrusion detection mechanisms.

1.2 Importance of Secure Communication in Modern Vehicles

With the increasing integration of connected and autonomous vehicle technologies, the security of in-vehicle communication has become a fundamental requirement for ensuring passenger safety and preventing cyber-attacks. Modern vehicles are now equipped with internet connectivity, remote diagnostics, and telematics services, exposing them to potential cyber threats from external sources. Unauthorized access to an in-vehicle network can compromise critical vehicle functions, leading to safety hazards such as unintended acceleration or braking failures. Additionally, cybersecurity breaches in connected vehicles pose risks related to data privacy, as attackers can intercept and manipulate sensitive information such as GPS locations and user credentials. Given these risks, automotive manufacturers and cybersecurity researchers are focusing on developing robust security measures to protect in-vehicle networks from emerging threats.

1.3 Research Objectives and Scope

The primary objective of this research is to analyze the security vulnerabilities associated with in-vehicle communication protocols, specifically CAN, LIN, and Automotive Ethernet. This study aims to provide an in-depth understanding of existing threats and attack vectors targeting these protocols, highlighting their implications for vehicle safety and data integrity. Additionally, the research explores various mitigation strategies, including message authentication techniques, hardware security modules (HSMs), and intrusion detection systems (IDSs). A particular focus is given to the challenges posed by legacy systems, which lack modern security mechanisms yet continue to be widely deployed in vehicles. Furthermore, this research proposes an alternative security approach for CAN-based networks, addressing the limitations of current security measures while maintaining system efficiency and real-time performance. By evaluating these solutions, this study contributes to the ongoing efforts in securing in-vehicle communication and ensuring the resilience of automotive networks against cyber threats.

2. Literature Review

As modern vehicles become increasingly connected and reliant on electronic communication, in-vehicle communication protocols have evolved to support diverse functionalities, ranging from powertrain management to infotainment and autonomous driving systems. However, these protocols were initially designed for reliability and efficiency rather than cybersecurity, leading to critical security vulnerabilities that are now being actively researched. This section provides an overview of the evolution of in-vehicle communication protocols, examines existing research on the security challenges in CAN, LIN, and Automotive Ethernet, and highlights the security risks posed by legacy systems that lack modern protection mechanisms.

2.1 Evolution of In-Vehicle Communication Protocols

The development of in-vehicle communication protocols began with simple point-to-point wiring, which quickly became impractical as vehicles incorporated more electronic control units (ECUs). To address this, the Controller Area Network (CAN) was introduced in the 1980s, providing an efficient bus-based architecture that allowed multiple ECUs to communicate over a shared medium. This was later supplemented by the Local Interconnect Network (LIN) for low-cost, non-time-critical functions such as climate control and seat adjustments. With the growing need for high-speed data transmission and vehicle-to-cloud communication, Automotive Ethernet emerged as a modern alternative, enabling high-bandwidth applications such as advanced driver-assistance systems (ADAS) and over-the-air (OTA) software updates. While these protocols have significantly enhanced vehicle performance, they were not originally designed with security in mind, making them vulnerable to cyber threats and unauthorized access.

2.2 Existing Research on CAN, LIN, and Automotive Ethernet Security

Numerous studies have explored the security vulnerabilities in CAN, LIN, and Automotive Ethernet, highlighting various attack vectors and potential countermeasures. Research on CAN security has primarily focused on message authentication, encryption techniques, and intrusion detection systems (IDSs) to mitigate attacks such as message spoofing and denial-of-service (DoS) attacks. Studies on LIN security have revealed its susceptibility to eavesdropping and message injection attacks, as LIN lacks any built-in encryption or authentication mechanisms. In contrast, Automotive Ethernet incorporates modern security features such as MACsec encryption and firewalls, but researchers have identified new threats such as man-in-the-middle (MITM) attacks, IP spoofing, and remote code execution

vulnerabilities. Recent advancements have proposed lightweight encryption algorithms and AI-based anomaly detection systems to improve the overall security posture of these communication protocols.

2.3 Identified Vulnerabilities and Security Challenges in Legacy Systems

Despite advancements in vehicle security, legacy communication protocols such as CAN and LIN remain widely used in modern vehicles, creating significant security challenges. These protocols lack authentication, encryption, and access control mechanisms, making them susceptible to remote and physical cyber-attacks. One of the biggest concerns is the lack of backward compatibility with modern security enhancements, as implementing cryptographic protections or software-based monitoring requires hardware upgrades that are not feasible for older ECUs. Additionally, many vehicles still rely on CAN for safety-critical functions, meaning that a successful cyber-attack on the CAN bus could directly impact vehicle control, potentially leading to life-threatening consequences. Research continues to focus on developing security solutions that can be retrofitted into legacy systems, such as CAN intrusion detection systems, software-defined security gateways, and blockchain-based authentication mechanisms.

This literature review underscores the urgent need for robust cybersecurity solutions in modern vehicles, particularly as automakers transition to connected and autonomous mobility. The following sections will further examine the specific security challenges, existing mitigation strategies, and alternative approaches to securing in-vehicle communication networks.

3. Overview of In-Vehicle Communication Protocols

The modern automotive industry relies on several in-vehicle communication protocols to facilitate seamless data exchange between various electronic control units (ECUs) and sensors. These protocols, including the Controller Area Network (CAN), Local Interconnect Network (LIN), and Automotive Ethernet, serve different purposes based on the performance, latency, and security requirements of specific vehicle subsystems. Each protocol has unique characteristics that make it suitable for different applications, ranging from safety-critical functions to infotainment and comfort systems. Understanding these protocols is crucial for assessing their security vulnerabilities and designing effective mitigation strategies.

3.1 Controller Area Network (CAN) – Features and Applications

The Controller Area Network (CAN) is one of the most widely used communication protocols in automotive systems, providing a robust and efficient means of data exchange between ECUs without requiring a central host. Originally developed by Bosch in the 1980s, CAN has become a standard for real-time, safety-critical applications such as engine control, braking systems, and transmission management. Its key advantages include high reliability, deterministic message delivery, and fault tolerance. CAN operates on a multi-master architecture, allowing multiple nodes to transmit messages based on a priority-based arbitration scheme.

Despite its widespread adoption, CAN was designed with minimal security considerations. It lacks built-in encryption and authentication mechanisms, making it vulnerable to cyber threats such as message spoofing, denial-of-service (DoS) attacks, and bus-off attacks. Once an attacker gains physical or remote access to the CAN bus, they can manipulate messages to interfere with vehicle operations. As a result, modern vehicles require additional security layers, such as message authentication codes (MACs) and intrusion detection systems (IDSs), to protect CAN-based communications.

3.2 Local Interconnect Network (LIN) – Features and Applications

The Local Interconnect Network (LIN) is a cost-effective and simpler alternative to CAN, primarily used for non-time-critical applications such as climate control, window regulators, and seat adjustment systems. LIN is a single-master, multiple-slave protocol that operates on a lower bandwidth (typically 19.2 kbps) compared to CAN. Its primary advantage is low implementation cost, making it suitable for applications that do not require high-speed communication or complex data handling.

However, LIN also inherits significant security limitations. Due to its lack of encryption and authentication, LIN networks are highly susceptible to message injection and eavesdropping attacks. Additionally, since LIN messages follow a predefined schedule rather than an event-driven approach, attackers can predict and manipulate communication patterns with relative ease. While security is less of a concern for LIN applications compared to safety-critical CAN networks, the increasing use of electronic control in comfort and infotainment systems has raised the need for additional security measures.

3.3 Automotive Ethernet – Features and Applications

With the rise of connected and autonomous vehicles, Automotive Ethernet has emerged as a high-speed communication protocol capable of supporting data-intensive applications such as Advanced Driver Assistance Systems (ADAS), over-the-air (OTA) updates, and in-vehicle infotainment. Unlike CAN and LIN, which use serial communication, Automotive Ethernet operates on a switched network topology, offering higher bandwidth (typically 100 Mbps to 1 Gbps), low latency, and enhanced scalability.

One of the significant advantages of Automotive Ethernet is its built-in security mechanisms, including MACsec (Media Access Control security), firewalls, and authentication protocols. These security features make it more resilient against cyber threats compared to CAN and LIN. However, as Ethernet-based communication expands in modern vehicles, new attack vectors such as man-in-the-middle (MITM) attacks, IP spoofing, and data interception have become potential concerns. Additionally, implementing Ethernet in safety-critical applications requires stringent real-time constraints, which remain a challenge for automotive manufacturers.

3.4 Comparison of CAN, LIN, and Automotive Ethernet

Each in-vehicle communication protocol offers distinct advantages and trade-offs based on its application requirements. CAN is highly reliable and widely used for safety-critical functions but lacks built-in security. LIN is cost-effective for non-critical applications but is vulnerable to predictable message manipulation. Automotive Ethernet, on the other hand, provides high-speed communication with enhanced security features but introduces complexity in real-time safety applications.

The following table summarizes the key differences between these three protocols:

Table: Comparative Analysis of In-Vehicle Communication Protocols

Feature	CAN	LIN	Automotive Ethernet
Topology	Multi-master	Single-master, multi-slave	Switched network
Bandwidth	1 Mbps	19.2 kbps	100 Mbps – 1 Gbps
Latency	Low (deterministic)	Higher (scheduled)	Very low

Security	No built-in encryption	No built-in security	Includes authentication & encryption mechanisms
Use Case	Safety-critical systems (engine, braking, transmission)	Non-critical applications (climate control, power windows)	High-speed data applications (ADAS, infotainment, OTA updates)
Vulnerabilities	Spoofing, DoS attacks	Message injection, predictable patterns	MITM attacks, IP spoofing, data interception
Cost	Moderate	Low	High

This comparative analysis highlights the necessity of integrating customized security solutions for each protocol based on its vulnerabilities and application scenarios. While CAN and LIN require additional security layers such as encryption, authentication, and intrusion detection, Automotive Ethernet's security mechanisms must be enhanced to counteract new cyber threats in connected vehicle environments.

4. Security Challenges in In-Vehicle Communication Protocols

As in-vehicle networks become more complex and interconnected, security vulnerabilities pose significant risks to vehicle safety and data integrity. Traditional automotive communication protocols such as Controller Area Network (CAN), Local Interconnect Network (LIN), and Automotive Ethernet were not originally designed with cybersecurity in mind, making them susceptible to various cyber threats. Attackers can exploit these weaknesses to manipulate vehicle behavior, eavesdrop on data transmission, or launch denial-of-service (DoS) attacks. Furthermore, the continued reliance on legacy systems in modern vehicles exacerbates these security risks, as older protocols often lack adequate protection mechanisms. This section explores the security challenges associated with these communication protocols, highlighting common vulnerabilities, specific cyber threats, and real-world case studies.

4.1 Common Vulnerabilities in CAN, LIN, and Ethernet

Each in-vehicle communication protocol has distinct vulnerabilities that can be exploited by attackers.

4.1.1 CAN Bus Vulnerabilities

- **Lack of Authentication**: CAN messages do not have built-in authentication, allowing attackers to inject malicious messages.
- **Message Spoofing**: Attackers can send unauthorized CAN messages to manipulate vehicle functions (e.g., disabling brakes).
- **Denial-of-Service (DoS) Attacks**: Malicious flooding of the CAN bus can prevent critical messages from reaching ECUs.
- **Bus-Off Attacks**: An attacker can cause an ECU to disconnect from the network by forcing it into an error state.

4.1.2 LIN Bus Vulnerabilities

- **No Encryption or Authentication**: LIN lacks security features, making it vulnerable to message injection.
- **Predictable Communication Patterns**: Attackers can easily manipulate scheduled messages to alter vehicle behavior.
- **Eavesdropping Risks**: Since LIN operates in a master-slave topology, an attacker gaining access to the master node can control multiple slave devices.

4.1.3 Automotive Ethernet Vulnerabilities

- **Man-in-the-Middle (MITM) Attacks**: Attackers can intercept and alter Ethernet data packets.
- **IP Spoofing**: Unauthorized devices can masquerade as legitimate ECUs to gain network access.
- **Data Exfiltration**: If not properly encrypted, sensitive vehicle data (e.g., GPS location) can be stolen.
- **Denial-of-Service (DoS) Attacks**: Flooding the Ethernet network with excessive data can disrupt critical vehicle functions.

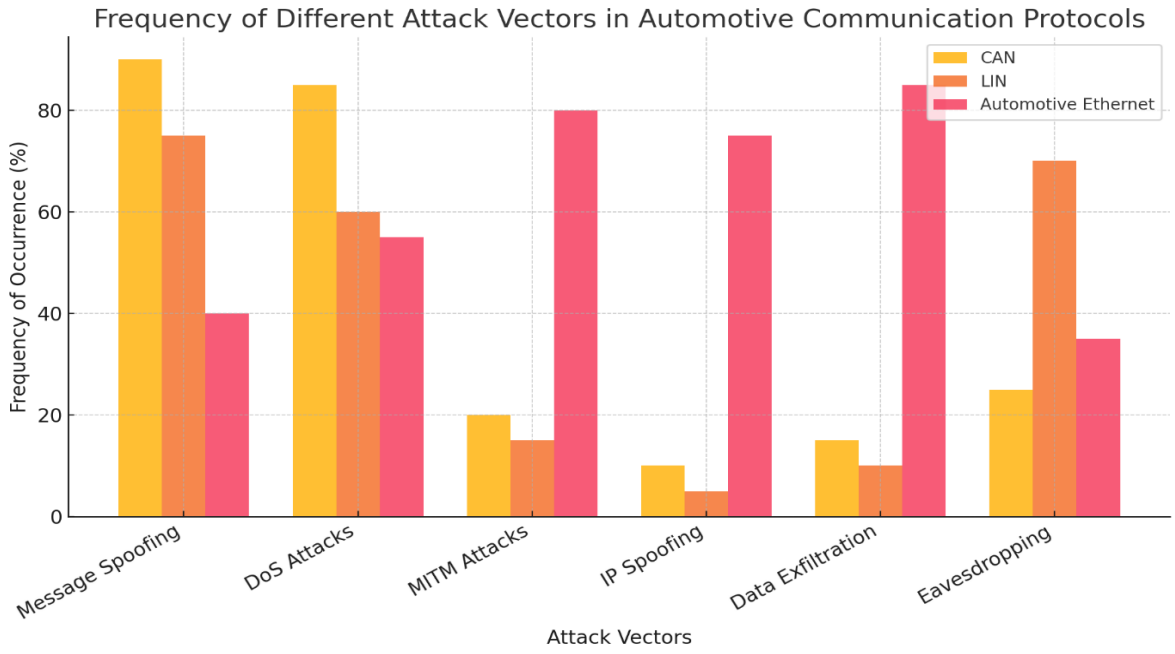


Figure: Frequency of Different Attack Vectors on Automotive Communication Protocols

The chart above illustrates the frequency of different cyber threats across CAN, LIN, and Automotive Ethernet communication protocols. CAN networks are highly vulnerable to message spoofing and DoS attacks, while LIN networks show increased susceptibility to eavesdropping and message spoofing due to their predictable communication patterns. Automotive Ethernet, despite having stronger built-in security features, is more prone to MITM attacks, IP spoofing, and data exfiltration, primarily because of its internet-based connectivity.

4.2 Cyber Threats Targeting In-Vehicle Networks

With increasing **connectivity in modern vehicles**, cybersecurity threats are becoming more sophisticated. Below are some of the most prevalent cyber threats targeting in-vehicle communication systems:

1. Message Injection and Spoofing Attacks

Attackers inject fake messages into the CAN or LIN bus to manipulate vehicle behaviour, such as disabling brakes or turning off headlights. Since CAN does not have authentication, ECUs accept and process these malicious messages.

2. Denial-of-Service (DoS) Attacks

By flooding the network with excessive messages, attackers can overwhelm ECUs, causing them to miss critical signals or enter a fail-safe mode. CAN networks are particularly susceptible due to their arbitration-based communication.

3. Man-in-the-Middle (MITM) Attacks

In Automotive Ethernet, MITM attackers intercept communication between ECUs, altering or stealing data before it reaches the intended recipient. This is a major risk for over-the-air (OTA) updates and telematics systems.

4. Remote Exploits via Internet-Connected Interfaces

Modern vehicles integrate Wi-Fi, Bluetooth, and cellular connections, which attackers can exploit to gain unauthorized access. Some attacks use vulnerabilities in infotainment systems to compromise the vehicle's internal communication network.

5. Malware Injection via OTA Updates

OTA software updates introduce a security risk if not properly authenticated. Attackers can deliver **malicious firmware updates**, compromising vehicle functions or enabling long-term backdoor access.

6. Eavesdropping and Data Exfiltration

Sensitive information, such as GPS location, driver behavior, and vehicle diagnostics, can be intercepted by attackers if transmitted without proper encryption.

4.3 Impact of Legacy Systems on Automotive Security

Legacy communication protocols, particularly CAN and LIN, were developed decades ago when cybersecurity was not a primary concern. However, many modern vehicles still rely on these legacy systems, creating significant security risks.

4.3.1 Challenges of Legacy Protocols

- **Lack of Encryption**: CAN and LIN messages are transmitted in plaintext, allowing attackers to intercept and modify them.
- **No Built-In Authentication**: Any device connected to the bus can send messages, making unauthorized message injection a major threat.
- **Backward Compatibility Issues**: Security enhancements such as encryption are difficult to implement without breaking compatibility with older ECUs.

- **Inability to Detect Intrusions**: Traditional CAN and LIN networks do not have intrusion detection mechanisms, allowing attackers to operate undetected.

4.3.2 Security Implications of Using Legacy Systems in Modern Vehicles

- **Increased Attack Surface**: Modern vehicles integrate internet-connected features while still using legacy CAN and LIN networks, creating an entry point for attackers.
- **Compromised Safety-Critical Systems**: Cyber-attacks on CAN-based braking and steering systems could lead to life-threatening situations.
- **Limited Security Upgradability**: Unlike software-defined systems, CAN and LIN networks cannot be easily updated with new security protocols, making vehicles persistently vulnerable.

To mitigate these risks, **intrusion detection systems (IDSs)** and **gateway-based security mechanisms** are being introduced to monitor and filter suspicious activities on legacy networks.

4.4 Case Studies of Security Breaches in Automotive Networks

Several real-world attacks on vehicle communication systems highlight the severity of cybersecurity threats in the automotive industry. Below are some notable cases:

4.4.1 Case Study 1: 2015 Jeep Cherokee Hack

- Researchers Charlie Miller and Chris Valasek demonstrated a remote attack on a Jeep Cherokee via its infotainment system, taking full control of the vehicle's CAN bus.
- They were able to disable brakes, control the steering, and manipulate acceleration remotely.
- This attack forced Fiat Chrysler to recall 1.4 million vehicles and sparked industry-wide efforts to improve vehicle cybersecurity.

4.4.2 Case Study 2: Tesla Model S Key Fob Exploit (2018)

- Security researchers discovered a vulnerability in Tesla's key fob encryption, allowing them to clone the key and unlock the vehicle remotely.
- The attack exploited weak cryptographic implementations in the fob's signal transmission.
- Tesla responded by introducing stronger encryption algorithms and two-factor authentication.

4.4.3 Case Study 3: BMW's ConnectedDrive Vulnerability (2015)

- A security flaw in BMW's ConnectedDrive system allowed hackers to remotely unlock car doors using fake cellular network signals.
- BMW patched the vulnerability by updating the system to use HTTPS encryption for all communications.

4.4.4 Case Study 4: Nissan Leaf App Vulnerability (2016)

- The Nissan Leaf mobile app was found to lack proper authentication, allowing attackers to remotely control air conditioning and access driving data.
- Although this did not pose immediate safety risks, it exposed a wider issue of insecure mobile-vehicle communications.

These case studies highlight the urgent need for stronger security frameworks in modern automotive networks, especially as vehicles continue to integrate wireless and internet-based communication technologies.

This section provided an in-depth analysis of security vulnerabilities, cyber threats, legacy system risks, and real-world attacks on in-vehicle networks. As the automotive industry moves toward fully connected and autonomous vehicles, addressing these security challenges will be critical in ensuring driver safety and data protection.

5. Existing Mitigation Strategies for In-Vehicle Communication Security

With the increasing risk of cyber threats targeting in-vehicle communication networks, the automotive industry has been implementing various security measures to protect vehicles from malicious attacks. These mitigation strategies aim to enhance the security of Controller Area Network (CAN), Local Interconnect Network (LIN), and Automotive Ethernet by incorporating message authentication, hardware-based security, and intrusion detection systems (IDSs). However, despite these advancements, current security mechanisms still face limitations in effectively preventing sophisticated attacks. This section explores existing mitigation strategies, their effectiveness, and challenges in implementation.

5.1 Message Authentication Techniques

Since CAN and LIN lack built-in authentication mechanisms, attackers can inject spoofed messages to manipulate vehicle behaviour. To counteract this, message authentication techniques are introduced to verify the integrity and authenticity of messages before processing.

1. Message Authentication Codes (MACs)

- Description: Uses cryptographic hashes (HMAC, CMAC) to attach an authentication code to messages.
- Advantage: Prevents unauthorized message injection by ensuring only valid ECUs can send messages.
- Limitation: Adds computational overhead, leading to increased latency in real-time applications.

2. Challenge-Response Authentication

- Description: Before executing a command, the receiving ECU sends a cryptographic challenge to the sender. The sender must return a valid response using a secret key.
- Advantage: Prevents replay attacks and unauthorized message injection.
- Limitation: Requires time synchronization and additional computational resources.

3. CAN Message Authentication with Lightweight Encryption

- Description: Implements encryption techniques optimized for low-latency automotive systems, such as TESLA and CAN-FD Secure.
- Advantage: Provides a balance between security and performance.
- Limitation: Some lightweight encryption methods are vulnerable to side-channel attacks.

Despite these authentication mechanisms, CAN and LIN networks still struggle with real-time constraints, making it difficult to implement strong cryptographic protections.

5.2 Hardware Security Modules (HSM) and Their Role

To enhance vehicle cybersecurity, Hardware Security Modules (HSMs) are integrated into modern ECUs. HSMs are dedicated cryptographic processors that securely store and manage encryption keys.

5.2.1 Key Functions of HSMs in Automotive Security

- **Encryption and Decryption**: Ensures that messages transmitted over in-vehicle networks are protected from unauthorized access.
- **Key Management**: Stores encryption keys securely to prevent key extraction attacks.
- **Secure Boot and Firmware Updates**: Protects vehicle software from being tampered with during OTA updates.

5.2.2 Advantages of Using HSMs

- Stronger security: Resistant to software-based attacks since cryptographic operations are performed in hardware.
- Tamper-resistance: Protects against key extraction through physical access.
- Low Latency: Can handle encryption tasks efficiently without significantly impacting real-time communication.

5.2.3 Limitations of HSMs

High Cost: Increases the cost of ECUs, making them less viable for low-end vehicles. **Backward Compatibility**: Many existing CAN and LIN systems do not support HSM-based security, requiring major hardware upgrades.

While HSMs are effective for protecting cryptographic operations, their deployment in legacy systems remains a challenge due to cost and compatibility issues.

5.3 Intrusion Detection Systems (IDS) in Automotive Networks

Intrusion Detection Systems (IDSs) are designed to monitor in-vehicle networks for anomalous activities and alert the system when a potential attack is detected. IDSs are especially useful for detecting message spoofing, DoS attacks, and unauthorized access.

5.3.1 Types of Automotive IDSs

1. Signature-Based IDS

- **Function**: Compares incoming messages against a database of known attack patterns.
- **Advantage**: Highly effective against previously known attacks.
- **Limitation**: Cannot detect new or zero-day attacks.

2. Anomaly-Based IDS

- **Function**: Uses machine learning to analyze traffic patterns and detect deviations from normal behaviour.

- **Advantage**: Can detect unknown and emerging attacks.
- Limitation: High false positive rate, requiring continuous training and fine-tuning.

3. Hybrid IDS (Signature + Anomaly-Based)

- **Function**: Combines both methods for better accuracy.
- **Advantage**: Balances detection effectiveness and false alarm reduction.
- **Limitation**: Requires higher computational power.

5.3.2 Challenges in Implementing IDS in Vehicles

- **Real-time Constraints**: IDSs must operate with low latency to avoid delays in critical vehicle functions.
- **Limited Processing Power**: ECUs have restricted computational capabilities, making it difficult to run advanced IDS algorithms.
- **False Positives**: IDSs may incorrectly flag legitimate messages as threats, leading to system malfunctions.

Despite these challenges, IDSs are becoming an essential security layer for monitoring and detecting cyber threats in modern vehicles.

5.4 Limitations of Current Security Measures

While existing security mechanisms improve in-vehicle network protection, they still face significant limitations. Below is a summary of key drawbacks:

Security Measure	Main Benefit	Key Limitation
Message Authentication Codes (MACs)	Prevents unauthorized message injection	Increases network latency
Challenge-Response Authentication	Prevents replay attacks	Requires time synchronization
HSM (Hardware Security Module)	Provides strong encryption & key protection	High cost & compatibility issues
Signature-Based IDS	Detects known attacks with high accuracy	Cannot detect new attack types
Anomaly-Based IDS	Identifies new attack patterns	High false positive rate

Since automotive security is an evolving field, researchers are exploring alternative solutions such as lightweight encryption, AI-based anomaly detection, and blockchain for secure communication.

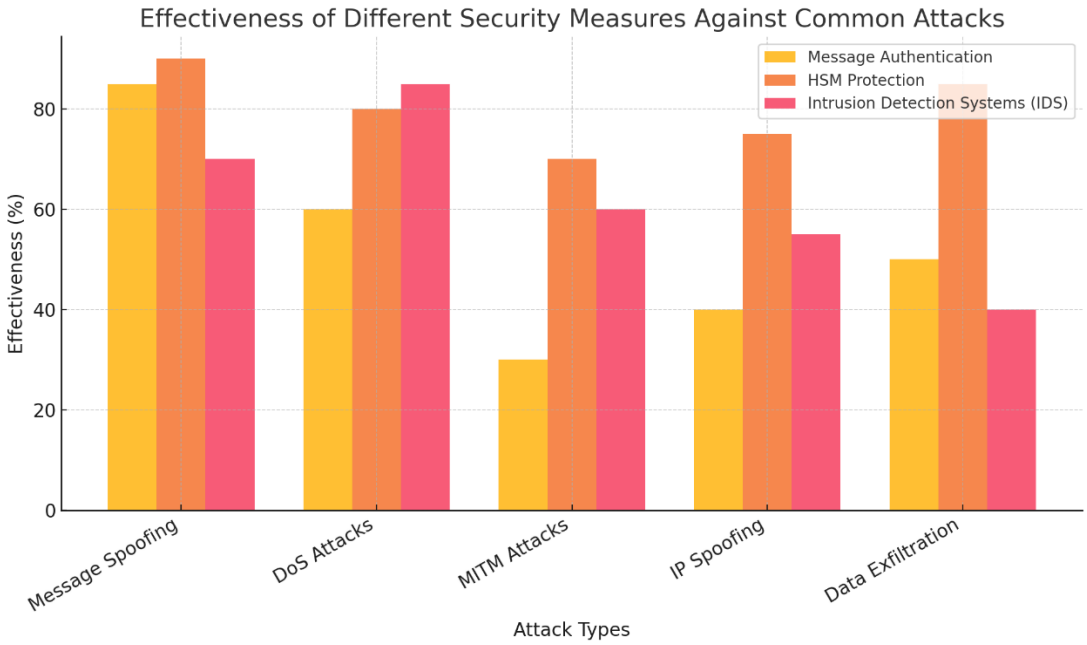


Figure: Effectiveness of Different Security Measures Against Common Attacks

The chart above illustrates the effectiveness of different security measures in mitigating common cyber threats in automotive networks. Message authentication is highly effective against message spoofing but struggles against network-level attacks such as MITM and IP spoofing. Hardware Security Modules (HSMs) provide the strongest overall protection across all attack types but are costly and challenging to integrate into legacy systems. Intrusion Detection Systems (IDSs) excel at detecting DoS and anomaly-based attacks but are less effective against direct message manipulation attacks.

5.5 Conclusion

This section has explored existing mitigation strategies for securing in-vehicle networks, including message authentication, hardware security modules, and intrusion detection systems. While these techniques significantly improve vehicle security, they still face challenges such as real-time performance constraints, high implementation costs, and detection accuracy issues.

To address these limitations, future research is focusing on AI-driven anomaly detection, lightweight encryption methods, and blockchain-based authentication for securing vehicle communications. As automotive cybersecurity threats evolve, a multi-layered security approach integrating hardware-based protection, real-time monitoring, and cryptographic enhancements will be essential to safeguarding modern vehicles.

6.1 Limitations of Existing CAN Bus Security Mechanisms

The CAN protocol was originally designed for real-time performance, prioritizing speed and reliability over security. While recent security enhancements, such as message authentication codes (MACs), Hardware Security Modules (HSMs), and IDS solutions, have improved protection, they also present the following limitations:

1. Computational Overhead and Latency Issues

- Traditional encryption methods increase processing time, which can delay real-time critical messages in systems such as braking and steering.
- Security solutions such as challenge-response authentication introduce additional delays, making them impractical for high-speed automotive networks.

2. Limited Backward Compatibility with Legacy CAN Systems

- Many older vehicles and ECUs do not support advanced cryptographic implementations, making firmware upgrades difficult.
- Retrofitting security features into existing CAN architectures requires expensive hardware modifications.

3. Ineffectiveness Against Physical and Side-Channel Attacks

- If an attacker gains physical access to the CAN bus, they can bypass software security measures and directly manipulate messages.
- Certain encryption schemes are vulnerable to timing attacks and differential power analysis (DPA), which extract cryptographic keys by analyzing power consumption patterns.

Given these challenges, alternative security approaches that balance efficiency, cost-effectiveness, and compatibility with existing automotive architectures are needed.

6.2 Cryptographic Enhancements and Lightweight Encryption for CAN

To address the computational and latency constraints of CAN networks, researchers are developing lightweight encryption algorithms tailored for real-time embedded systems.

1. Lightweight Cryptographic Algorithms

- **AES-CCM (Advanced Encryption Standard with Counter Mode and CBC-MAC)**: Provides message authentication and encryption with low computational overhead.
- **TEA (Tiny Encryption Algorithm)**: A lightweight alternative to AES that requires minimal processing power, making it suitable for CAN networks.
- **SPECK and SIMON (NSA-developed lightweight ciphers)**: Optimized for low-power and resource-constrained environments.

2. CAN-FD Secure (CAN with Flexible Data-Rate and Security Enhancements)

- Enhances CAN-FD (Flexible Data-Rate) by integrating built-in authentication and encryption at the protocol level.
- **Reduces latency** compared to traditional encryption schemes by optimizing security computations for real-time performance.
- Still in **development and adoption phases**, requiring industry-wide standardization.

3. Challenges of Cryptographic Approaches

- **Key Management Complexity**: Secure distribution of encryption keys remains a challenge.
- **Hardware Upgrade Requirements**: Legacy ECUs may lack the necessary computing power to support cryptographic operations.

While lightweight cryptographic solutions enhance security, they must be combined with additional security measures to fully protect CAN networks.

6.3 Software-Based Security Solutions and Real-Time Monitoring

In addition to cryptographic methods, software-based security solutions provide an additional layer of protection by detecting and mitigating cyber threats in real-time.

1. Secure Gateway Modules

- Act as an intermediary between CAN networks and external interfaces, filtering out malicious messages.
- Authenticate ECUs before allowing them to communicate over the CAN bus.

2. CAN Bus Firewalls

- Monitor incoming and outgoing traffic to detect anomalies.
- Prevent unauthorized ECUs from injecting or modifying messages on the network.

3. Real-Time Traffic Monitoring Systems

- Continuously analyze message timing, frequency, and payload structure to detect suspicious behaviour.
- Can be integrated with Intrusion Detection Systems (IDSs) for improved attack prevention.

4. Advantages of Software-Based Approaches

- **No additional hardware required**: Can be implemented via firmwareupdates.
- **Dynamic threat detection**: Unlike static cryptographic solutions, real-time monitoring can detect new and evolving attacks.

5. Limitations

- **High false positives**: Identifying cyber threats without disrupting normal traffic is challenging.
- **Not effective against physical attacks**: Cannot prevent an attacker from physically tapping into the CAN bus.

Software-based security solutions improve detection capabilities but should be combined with other techniques to enhance overall protection.

6.4 Exploring AI-Driven Anomaly Detection in CAN Networks

Artificial Intelligence (AI) and Machine Learning (ML) are emerging as powerful tools for identifying and mitigating cyber threats in automotive networks. AI-driven security solutions leverage anomaly detection models to identify deviations from normal communication patterns.

1. AI-Based Intrusion Detection Systems (AI-IDS)

- Use machine learning algorithms to detect abnormal CAN bus traffic.
- Can differentiate between legitimate and malicious messages based on historical data.
- Improve over time through continuous learning and adaptive response mechanisms.

2. Deep Learning for Threat Analysis

- **Recurrent Neural Networks (RNNs)** and Long Short-Term Memory (LSTM) models analyze CAN message sequences to detect patterns associated with cyber-attacks.
- Capable of identifying previously unknown attack vectors through unsupervised learning techniques.

3. Advantages of AI-Driven Anomaly Detection

- **Reduces reliance on predefined attack signatures** (unlike traditional IDSs).
- **Scalable across different vehicle models and architectures**.

4. Challenges in AI-Driven Security

- **Computational overhead**: Deep learning models require significant processing power.
- **Training data limitations**: AI models need large datasets of both normal and malicious CAN messages to improve accuracy.

AI-driven solutions enhance real-time security monitoring but require optimized models that can operate efficiently within automotive ECUs.

6.5 Feasibility Analysis and Future Research Directions

Feasibility of Alternative Security Approaches

Security Approach	Effectiveness	Implementation Cost	Compatibility with Legacy CAN	Real-Time Performance
Lightweight Encryption (AES, TEA, SPECK)	High	Moderate	Low	Medium
CAN-FD Secure	Very High	High	Low	High
Software-Based Monitoring (Firewalls, IDS)	Moderate	Low	High	High
AI-Driven Anomaly Detection	Very High	High	Medium	Medium

6.6 Conclusion

To address the limitations of traditional CAN security mechanisms, alternative approaches such as lightweight cryptography, software-based monitoring, and AI-driven anomaly detection are being explored. Each method has unique strengths and challenges, and a multi-layered security strategy is necessary to provide comprehensive protection against cyber

threats. Future research should focus on integrating these technologies in a cost-effective and scalable manner, ensuring secure and resilient automotive networks.

7. Future Challenges and Research Directions

As the automotive industry progresses towards fully connected and autonomous vehicles, securing in-vehicle communication networks will become more complex due to the integration of wireless technologies, over-the-air (OTA) updates, and vehicle-to-everything (V2X) communication. The transition from traditional protocols such as CAN and LIN to high-speed alternatives like Automotive Ethernet and Time-Sensitive Networking (TSN) introduces new security challenges that require advanced protection mechanisms. To address these concerns, future research must focus on developing robust cybersecurity frameworks, integrating artificial intelligence (AI) and blockchain-based security models, and establishing global security standards. This section explores the challenges and research directions that will shape the future of automotive cybersecurity.

7.1 Securing Future Automotive Networks with Evolving Protocols

Next-generation vehicles will rely on high-bandwidth, real-time communication networks such as Automotive Ethernet, TSN, and wireless V2X technologies to support autonomous driving and cloud-based services. While these advanced protocols provide higher data rates and lower latency, they also introduce new security risks, including remote cyber-attacks, unauthorized data access, and network-based exploits. Future security mechanisms must include end-to-end encryption, secure key management systems, and adaptive intrusion detection systems (IDS) capable of detecting anomalous activities in real-time. Additionally, as edge computing and software-defined networking (SDN) become more prevalent in automotive systems, ensuring secure data transmission between ECUs, cloud services, and external devices will be a major challenge.

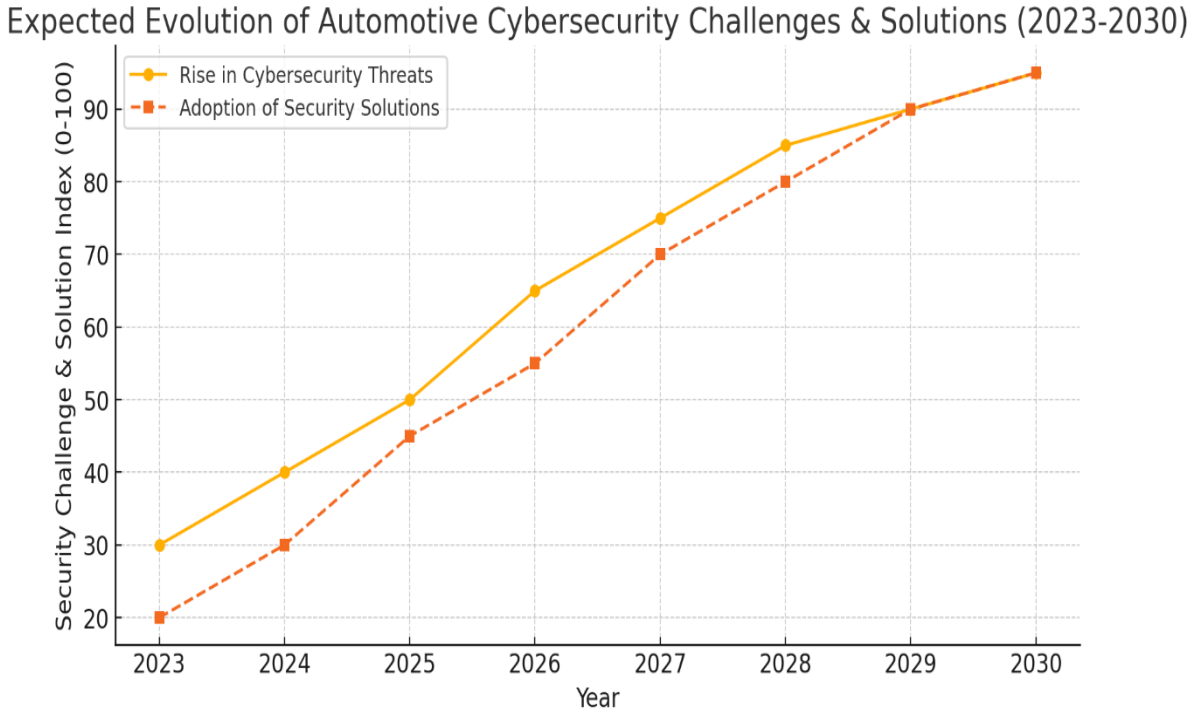
7.2 Potential Integration of Blockchain and AI for Automotive Security

Blockchain technology has the potential to revolutionize automotive security by providing decentralized and tamper-proof authentication for in-vehicle networks. Blockchain-based security frameworks can enable secure ECU communication, cryptographic key management, and immutable data storage, preventing unauthorized access and message tampering. Similarly, AI-driven anomaly detection can significantly enhance real-time security

monitoring by leveraging machine learning algorithms to identify and respond to cyber threats dynamically. By combining AI-based security models with blockchain authentication, researchers can develop self-learning, trust-based cybersecurity ecosystems that can autonomously detect, prevent, and mitigate cyber-attacks in connected vehicles. However, implementing these technologies in resource-constrained ECUs requires lightweight AI models and efficient blockchain architectures to minimize computational overhead and network latency.

7.3 Standardization and Regulatory Challenges in Securing In-Vehicle Networks

A major challenge in automotive cybersecurity is the lack of standardized security frameworks and global regulations. Currently, automotive manufacturers and suppliers follow different security protocols, leading to inconsistencies in cybersecurity implementation across vehicle models. Efforts by organizations such as ISO, SAE, and the UNECE WP.29 cybersecurity regulation aim to establish common security guidelines for protecting in-vehicle networks, software updates, and vehicle-to-cloud communication. However, regulatory frameworks must continuously evolve to address emerging cyber threats, compliance challenges, and ethical concerns surrounding autonomous vehicle security. Additionally, ensuring seamless integration of cybersecurity standards across different vehicle manufacturers and suppliers will require industry-wide collaboration and compliance enforcement.



The graph above illustrates the expected increase in cybersecurity threats in automotive networks from 2023 to 2030, alongside the adoption of security solutions. While cyber threats are projected to grow steadily, the implementation of advanced security mechanisms, including AI-based anomaly detection, blockchain authentication, and regulatory compliance measures, is expected to counteract these risks effectively.

8. Conclusion

8.1 Summary of Key Findings

The rapid evolution of in-vehicle communication networks has introduced significant cybersecurity challenges, particularly in traditional protocols such as CAN and LIN, which lack built-in encryption and authentication mechanisms. Automotive Ethernet offers enhanced security but introduces new vulnerabilities, including MITM attacks and IP spoofing. While existing mitigation strategies such as message authentication, hardware security modules (HSMs), and intrusion detection systems (IDSs) provide partial protection, they face limitations related to latency, computational overhead, and backward compatibility with legacy systems. To address these challenges, alternative security approaches such as lightweight encryption, real-time monitoring, and AI-driven anomaly detection are being explored, paving the way for more robust automotive cybersecurity frameworks.

8.2 Practical Implications for Automotive Security

The findings of this research highlight the urgent need for a multi-layered security approach to protect modern and legacy vehicle networks. Automakers must adopt hybrid security solutions that integrate cryptographic protections, software-defined security measures, and AI-driven detection mechanisms. Additionally, regulatory compliance with standards such as ISO 21434 and UNECE WP.29 cybersecurity guidelines will be essential for ensuring industry-wide adoption of secure communication protocols. Furthermore, future vehicle architectures must prioritize real-time cybersecurity monitoring, enabling proactive threat detection and response.

8.3 Final Recommendations

1. Enhance CAN Bus Security: Implement lightweight cryptographic algorithms (AES-CCM, TEA) to minimize latency while improving message authentication.

2. Deploy AI-Driven Security Solutions: Utilize machine learning-based anomaly detection to identify and mitigate emerging cyber threats in real time.
3. Adopt Blockchain-Based Authentication: Develop blockchain-secured ECU authentication frameworks to prevent unauthorized access and message tampering.
4. Implement Secure OTA Updates: Ensure firmware updates use secure boot mechanisms and end-to-end encryption to prevent malicious code injection.
5. Standardize Cybersecurity Measures: Collaborate with automotive regulatory bodies to establish universal security protocols that can be adopted across all vehicle manufacturers.

By implementing these recommendations, the automotive industry can significantly improve vehicle cybersecurity resilience, ensuring safe and secure mobility in the era of connected and autonomous vehicles.

References

[1] Woo, S., Jo, H. J., & Lee, D. H. (2015). A practical wireless attack on the connected car and security protocol for in-vehicle CAN. *IEEE Transactions on Intelligent Transportation Systems, 16(2), 993-1006.*

[2] B., Anderson, D., Shacham, H., Savage, S., & Kohno, T. (2011). Comprehensive experimental analyses of automotive attack surfaces. *Proceedings of the USENIX Security Symposium, 20, 6-13.*

[3] Checkoway, S. (2010). Experimental security analysis of a modern automobile. *IEEE Symposium on Security and Privacy, 447-462.*

[4] Miller, C., & Valasek, C. (2015). Remote exploitation of an unaltered passenger vehicle. *Black Hat USA 2015 Conference.*

[5] Groza, B., Murvay, P. S., Pop, T., & van Herrewege, A. (2016). LiBrACAN: Lightweight broadcast authentication for CAN. *ACM Transactions on Embedded Computing Systems, 16(3), 1-21.*

[6] Van Herrewege, A., Singelee, D., &Verbauwhede, I. (2011). CANAuth – A simple, backward-compatible broadcast authentication protocol for CAN bus. *ECRYPT Workshop on Lightweight Cryptography.*

[7] Kang, M., Choi, W., & Kim, J. (2019). CAN protocol security enhancement through message authentication and anomaly detection. *IEEE Access, 7, 58632-58644.*

[8] Petit, J., &Shladover, S. E. (2015). Potential cyberattacks on automated vehicles. *IEEE Transactions on Intelligent Transportation Systems, 16(2), 546-556.*

[9] Van Bulck, J., Piessens, F., &Strackx, R. (2017). SGX-step: A practical attack framework for precise enclave execution control. *Proceedings of the USENIX Security Symposium, 2017, 495-510.*

[10] Lukáš, P., & Urbanec, J. (2016). Intrusion detection system for automotive networks: CAN bus anomaly detection. *International Conference on Software, Telecommunications and Computer Networks (SoftCOM), 2016.*

[11] Javed, A., & Rana, O. (2024). A robust multi-stage intrusion detection system for in-vehicle network security using hierarchical federated learning. Vehicular Communications, Elsevier.

[12] Barletta, V. S., Caivano, D., & Catalano, C. (2024). Quantum-based automotive threat intelligence and countermeasures. Proceedings of the 28th ACM International Conference.

[13] Maodah, K. A., & Alhomdy, S. A. (2024). A comprehensive survey on automotive hacking. 1st International Conference on Security in Digital Transformation, IEEE.

[14] Shen, L., Xiu, J., Zhang, Z., & Yang, Z. (2024). A fuzz testing method based on DDPM for intelligent connected vehicles CAN communication. SAE Technical Paper.

[15] Du, L., Zeng, L., & Gu, Z. (2024). Vehicle network intrusion detection based on K-nearest neighbor variational autoencoder using contrastive learning. IEEE 9th International Conference.

[16] Zhang, D., Liu, J., Fan, Z., & Cai, Y. (2024). Research on vehicle CAN communication cybersecurity. Fourth International Conference on Information Security, SPIE.