International Journal of Multidisciplinary Innovative Research
ISSN: 2583-0228 Volume 6, Number 1 (Jan' 2026) pp. 38-45
© CIIR, Noida, INDIA (www.ciir.in)
https://www.ijmir.org
Article Received: 10 Nov' 2025
Final Revision: 26 Nov' 2025
Accepted for Publication: 12 Dec' 2025

Review Article

OPEN ACCESS

Study of Digital Transformation of the Automotive Industry and the Security of Communication Protocols

Gordana Ostojic and Stevan Stankovski

Faculty of Technical Sciences, University of Novi Sad, Serbia.

Email: goca@uns.ac.rs

ABSTRACT: ***The automotive industry's rapid digital transformation has led to modern vehicles being fitted with advanced communication networks, intelligent control systems and Internet of Things (IoT) technologies. While these developments enable seamless connectivity, autonomous functionalities and enhanced user experience, they also introduce new cybersecurity challenges. This paper analyses the evolution of in-vehicle communication protocols, such as CAN, LIN, FlexRay and Automotive Ethernet, emphasizing their role in facilitating data exchange between electronic control units (ECUs). Particular focus is placed on identifying potential security vulnerabilities arising from limitations in protocol design and inadequate authentication or encryption mechanisms. Furthermore, the study explores contemporary approaches to securing automotive communication, including message authentication, intrusion detection systems, and cryptographic solutions. The aim is to emphasize the importance of incorporating cybersecurity principles into the architecture of connected and autonomous vehicles, ensuring reliability, safety and data integrity in the digital mobility era.***

KEYWORDS: ***Network Security, Communication Protocol, Cloud Computing, LIN, IoT, ECU, Automotive Industry.***

INTRODUCTION

Industry, especially automotive, is undergoing a deep digital transformation, driven by advances in automation, connectivity and data-driven technologies (Bohnsack et al., 2021; Verhoef et al., 2021). Modern vehicles are no longer isolated mechanical systems, but rather complex cyber-physical platforms that are equipped with hundreds of sensors, actuators and electronic control units (ECUs), and which continuously exchange data. Supported by technologies such as the Internet of Things (IoT), cloud computing, artificial intelligence (AI) and vehicle-to-everything (V2X) communication, this shift towards intelligent mobility has redefined how vehicles are designed, operated and maintained.

At the heart of this transformation are a variety of communication protocols that facilitate the reliable and efficient transfer of data between vehicle subsystems. Protocols such as Controller Area Network (CAN), Local Interconnect Network (LIN), FlexRay and Automotive Ethernet are fundamental to in-vehicle communication architectures. These protocols ensure the

Copyright2026@CIIR

coordination of safety-critical components such as braking, steering and powertrain systems, as well as comfort and infotainment functions. However, as these protocols were originally developed for closed systems with limited external connectivity, they often lack built-in authentication, encryption and intrusion detection mechanisms. The increasing integration of vehicles with external networks, mobile devices and cloud platforms makes them vulnerable to potential cybersecurity threats. Unauthorized access, data manipulation and remote attacks on vehicle communication networks can compromise passenger safety, privacy and the reliability of the overall system. Therefore, securing automotive communication protocols has become a critical challenge for manufacturers, researchers and regulators.

This paper aims to analyze the impact of digital transformation on in-vehicle communication systems, explore the vulnerabilities of existing protocols and present modern approaches to enhancing their security. Combining insights from automotive engineering and cybersecurity, the study emphasizes the necessity of adopting a security-by-design approach when developing connected and autonomous vehicles.

COMMUNICATION PROTOCOLS IN AUTOMOTIVE SYSTEMS

Reliable communication between the numerous ECUs in a vehicle is essential for its operation. Communication protocols define the rules that govern data transfer, synchronisation and verification across the vehicle network. Each protocol has been developed for a specific purpose, balancing factors such as data rate, system complexity, cost and safety. The most frequently used protocols in the automotive industry are CAN, LIN, FlexRay and Automotive Ethernet.

CAN Protocol

The CAN protocol has become the backbone of in-vehicle communication. Designed to enable real-time data exchange between multiple ECUs without the need for a central computer, it has become the backbone of in-vehicle communication. CAN uses a multi-master bus architecture, whereby each node can transmit when the bus is free, and message priority is determined by its identifier (Barbosa et al., 2003). The classic version of CAN supports data rates of up to one megabit per second, whereas the modern CAN FD (Flexible Data Rate) extends this to around eight megabits per second. CAN's main strengths lie in its reliability and robustness against electromagnetic interference, as well as its effective arbitration system, which ensures the timely transmission of high-priority messages. CAN is also cost-efficient and widely standardised, facilitating integration among different manufacturers. However, as it was developed for closed vehicle systems, CAN lacks modern security mechanisms such as encryption and authentication. This leaves it vulnerable to message spoofing and replay attacks, particularly in connected vehicles communicating with external networks. Additionally, its limited data rate and increased bus load in complex systems reduce its scalability for data-intensive applications.

LIN Protocol

The LIN protocol was introduced as a simpler, more economical alternative to CAN for non-critical systems. Operating at data rates of up to 20 kilobits per second, LIN is based on a single-master, multiple-slave topology. It is primarily used for functions such as controlling windows, adjusting mirrors, positioning seats, and adjusting interior lighting. Communication is fully deterministic, meaning message timing is predictable and defined by the master node's schedule. The main advantages of LIN are its low cost, minimal hardware requirements and

Copyright2026@CIIR

straightforward implementation. However, it offers limited bandwidth and scalability, and its single-master architecture limits flexibility. Furthermore, as it provides no inherent security features, LIN is unsuitable for safety-critical or real-time systems (LIN Protocol and Physical Layer Requirements, 2022). In practice, LIN subsystems are often connected to higher-level CAN networks via gateway units.

FlexRay Protocol

FlexRay was developed in response to the growing need for high-speed, fault-tolerant communication in systems that require precise timing, such as brake-by-wire, steer-by-wire and other active safety technologies. Supporting data rates of up to 10 megabits per second, it offers a dual-channel architecture that provides redundancy in the event of a line failure. Combining time-triggered and event-triggered communication, FlexRay enables both deterministic control and flexible data exchange. Its key advantages are high speed, synchronisation precision and fault tolerance, making it ideal for safety-critical applications. However, implementing FlexRay is expensive and technically complex due to its synchronisation requirements and configuration procedures (X. Li et al., 2024). Although it is reliable, it has not achieved widespread use, largely due to its cost and the growing preference for Automotive Ethernet, which offers higher scalability and bandwidth at lower prices. FlexRay also lacks integrated security mechanisms, instead relying on external protection layers.

Automotive Ethernet

Automotive Ethernet is the automotive sector's most advanced and forward-looking communication technology. Depending on the standard used (100BASE-T1 or 1000BASE-T1), it provides data rates ranging from 100 megabits to 10 gigabits per second. Unlike bus-based architectures, Automotive Ethernet uses a point-to-point or switched topology, allowing simultaneous communication between multiple devices without congestion. It supports a variety of IT protocols, including TCP/IP and UDP, enabling seamless integration with external networks and cloud-based systems. The main advantages of Automotive Ethernet are its extremely high bandwidth, scalability, and compatibility with modern data-intensive applications such as advanced driver-assistance systems (ADAS), infotainment, and autonomous driving (Matheus and Kaindl, 2023). However, the use of Ethernet technology introduces new challenges, including increased electromagnetic emissions, higher software complexity, and the need for precise synchronisation. Because it relies on IP-based communication, it is also more exposed to cyberattacks, such as denial-of-service or man-in-the-middle attacks. Nonetheless, ongoing development of standards and security frameworks, such as IEEE (Institute of Electrical and Electronics Engineers) and AUTOSAR (AUTomotive Open System ARchitecture), aims to address these vulnerabilities.

Comparative Overview of Protocols

A comparison of these protocols reveals that each serves a distinct purpose within the vehicle's network hierarchy. CAN and LIN remain dominant in conventional control systems thanks to their simplicity, robustness and low cost. While offering superior determinism and reliability, FlexRay is mainly used in specific high-safety applications. Meanwhile, Automotive Ethernet is becoming the backbone of next-generation vehicles, supporting the vast data flows and advanced connectivity features required for intelligent mobility. This evolution in communication protocols reflects the broader digital transformation of the automotive industry, in which mechanical systems are increasingly being replaced by connected, software-defined

Copyright2026@CIIR

architectures. While this transition enables unprecedented functionality, it also introduces new vectors for cybersecurity risks, demanding innovative protective mechanisms and a proactive security-by-design approach.

In order to compare these technologies, several important criteria have been considered, such as: maximum data rate, topology, main use case, security level, key advantages and main limitations. These criteria are represented in Table 1.

Table 1: Shows different criteria for communication protocols

Protocol	Max Data Rate	Topology	Main Use Case	Security Level	Key Advantages	Main Limitations
CAN / CAN FD	1–8 Mbps	Bus	Powertrain, body control	Low	Robust, reliable, cost-effective	Limited bandwidth, no native security
LIN	20 kbps	Master-slave	Local subsystems	Very low	Cheap, simple, deterministic	Slow, not secure, limited flexibility
FlexRay	10 Mbps	Dual-channel	Safety-critical systems	Medium	Deterministic, fault-tolerant	Expensive, complex, declining use
Automotive Ethernet	100 Mbps–10 Gbps	Star/switch	ADAS, infotainment, V2X	High (with extensions)	High bandwidth, scalable, future-ready	Complex, costly shielding, security challenges

CYBERSECURITY CHALLENGES IN AUTOMOTIVE COMMUNICATION SYSTEMS

The rapid digitalization of vehicles and integration of advanced communication networks has significantly enhanced functionality, comfort and connectivity. However, these advancements have also introduced serious cybersecurity risks that can compromise vehicle safety, user privacy and system reliability. Modern vehicles contain dozens of interconnected ECUs that communicate via protocols such as CAN, LIN, FlexRay and Automotive Ethernet. As many of these protocols were designed decades ago when vehicles were isolated from external networks, they often lack authentication, encryption and intrusion detection mechanisms. Consequently, contemporary vehicles' attack surface has expanded dramatically, creating new opportunities for malicious interference.

Depending on the attacker's objective and access level, cyberattacks on automotive systems can take several forms. One common method is message spoofing, whereby an attacker injects false data into the communication bus, causing certain ECUs to perform unauthorized actions. In a CAN network, for example, spoofed messages could trigger unintended acceleration, disable safety systems or manipulate dashboard indicators. Another prevalent form of attack is a denial-of-service (DoS) attack, whereby the communication channel is flooded with high-priority or malformed messages to prevent legitimate data from being transmitted. Replay

Copyright2026@CIIR

attacks involve recording and retransmitting valid messages to perform certain actions without authorization. Man-in-the-middle (MITM) attacks intercept and modify data between communicating nodes, particularly in Ethernet-based systems.

In the context of the CAN protocol, cybersecurity challenges primarily stem from the lack of sender authentication. As all nodes on the CAN bus share the same physical medium and messages are broadcast without encryption, any compromised node can send seemingly legitimate data. This makes CAN networks vulnerable to spoofing and eavesdropping (Ileri et.al, 2025). Efforts to improve CAN security include introducing Message Authentication Codes (MACs) and using hardware-based Trusted Platform Modules (TPMs) to verify messages. However, such mechanisms often encounter limitations due to the processing and timing constraints that are inherent in real-time automotive systems.

Though simpler and less critical, the LIN protocol is not immune to exploitation. Its single-master architecture means that if the master node is compromised, control of all slave devices can be easily obtained. Furthermore, the lack of any form of message integrity verification in LIN communication makes it susceptible to manipulation through diagnostic interfaces or physical access points. Security in LIN networks is usually achieved indirectly by isolating them from external connections and controlling access via the gateway linking the LIN and CAN domains (LIN Protocol and Physical Layer Requirements, 2022).

By contrast, FlexRay's dual-channel architecture and time-triggered operation give it a more robust communication structure, making it less vulnerable to random interference and DoS attacks. However, FlexRay was developed without integrated encryption or authentication features. This means that attackers who gain access to the bus can manipulate data frames or disrupt synchronization, which can have severe consequences for safety-critical functions such as braking or steering. To mitigate these risks, research efforts have focused on integrating cryptographic protection and intrusion detection systems that monitor network timing behaviour and message consistency (Püllen et al., 2020; J. Li et al., 2025).

The Automotive Ethernet protocol introduces new possibilities, as well as new threats. While its reliance on IP-based communication makes it compatible with external networks, it also exposes vehicles to well-known IT vulnerabilities. Potential attacks include packet sniffing, address spoofing and remote exploitation via compromised in-vehicle infotainment systems or wireless interfaces. Unlike traditional automotive protocols, Ethernet supports a range of standardized security measures, such as MAC Security for encryption and authentication, as well as firewalls and intrusion detection systems (IDS), which analyze traffic anomalies. Furthermore, the adoption of the AUTOSAR Adaptive Platform has integrated modern cybersecurity practices into automotive architectures, including secure boot, certificate-based authentication and over-the-air (OTA) update protection. However, the complexity of Ethernet networks necessitates continuous monitoring and a systematic approach to cybersecurity management throughout the vehicle's lifecycle.

In general, automotive cybersecurity cannot be viewed as a static or isolated discipline. A holistic approach is required that integrates hardware protection, software security and continuous risk assessment. The concept of security by design has become fundamental to the development of new vehicle architectures. This approach emphasizes that security mechanisms must be incorporated into communication protocols from the earliest design stages rather than being added as post-production features. Furthermore, cooperation between car manufacturers,

Copyright2026@CIIR

component suppliers and regulatory bodies is essential in order to establish unified standards and testing procedures that ensure the resilience of connected vehicles.

The increasing number of connected and autonomous vehicles underscores the pressing requirement for sophisticated cybersecurity frameworks that can safeguard in-vehicle communication networks against internal and external threats. Future development is likely to focus on combining lightweight cryptographic algorithms, real-time intrusion detection and secure communication architectures based on hardware trust anchors. Only by ensuring the integrity and confidentiality of communication protocols can the automotive industry realize the full potential of digital transformation and maintain the highest levels of safety and user trust.

DISCUSSION

As vehicles evolve into highly connected digital platforms, cybersecurity has become an integral part of automotive system design. The increasing complexity of in-vehicle networks and their connection to external systems requires new strategies that surpass traditional security measures. The aim is to create a multi-layered defence model combining cryptographic protection, intrusion detection, secure communication architecture and regulatory compliance. This section explores existing and emerging security solutions designed to protect automotive communication systems, as well as future trends that will shape the next generation of secure vehicle networks.

One of the most fundamental approaches to securing in-vehicle communication is to implement cryptographic mechanisms. Encryption and authentication ensure that only authorized engine control units can send and receive valid messages, thereby preventing unauthorized manipulation and data theft. Symmetric cryptography, which uses shared secret keys, is well-suited to real-time applications such as CAN or FlexRay, where low latency is critical. Conversely, asymmetric cryptography offers greater security through public and private key pairs, but incurs higher computational costs. To balance these factors, hybrid methods that combine symmetric and asymmetric algorithms are becoming increasingly popular. However, as traditional automotive microcontrollers have limited processing power, there is growing interest in lightweight cryptography, which offers sufficient protection at minimal computational cost.

Another crucial defence layer involves Intrusion Detection and Prevention Systems (IDS/IPS). These systems continuously monitor network traffic to detect abnormal behaviour that may indicate a cyberattack is in progress. In automotive environments, IDS/IPS can be implemented in various ways, including signature-based detection, which relies on known attack patterns, and anomaly-based detection, which identifies deviations from normal communication behaviour. For example, timing-based intrusion detection recognizes unauthorized messages on a CAN bus by analyzing deviations in message intervals. Integrating machine learning algorithms into IDS enables adaptive learning and the detection of new, previously unknown attack vectors. When combined with prevention mechanisms such as automatic node isolation, IDS/IPS systems play a vital role in safeguarding network integrity.

The AUTOSAR framework provides a standardized approach to software development and system integration across the automotive industry. Its Adaptive Platform introduces comprehensive cybersecurity functionalities, including secure boot processes, certificate-based authentication, key management and secure communication channels. Secure boot ensures that only trusted software can be executed during system startup, thereby preventing unauthorized

Copyright2026@CIIR

modifications or malware infections. The Key Management Infrastructure (KMI) securely distributes and stores cryptographic keys, and secure communication modules ensure the integrity and confidentiality of data exchanged between ECUs. Together, these mechanisms establish a trusted environment for vehicle operation and software updates (https://www.autosar.org/).

Efforts in the areas of regulation and standardization also play a critical role in defining cybersecurity practices for the automotive sector. The international standard ISO/SAE 21434 – Road Vehicles: Cybersecurity Engineering', provides a structured framework for managing cybersecurity risks throughout a vehicle's lifecycle — from the initial concept and design stages through to production, operation and maintenance. It requires manufacturers to perform continuous risk assessments, implement protective measures and ensure the traceability of all cybersecurity-related activities. Concurrently, the UNECE WP.29 (UNECE World Forum for Harmonization of Vehicle Regulations) regulation defines that all new vehicle models must demonstrate compliance with cybersecurity management systems before approval for sale (https://unece.org/). Together, these frameworks promote accountability and consistency across the global automotive ecosystem.

Emerging technologies are expected to enhance automotive cybersecurity further. Hardware Security Modules (HSMs) and TPMs are being integrated into more and more vehicle ECUs to provide secure storage for cryptographic keys and execute security-critical operations in isolated environments. Secure gateways are also being developed to control and filter the exchange of data between internal networks, such as CAN or LIN, and external interfaces, such as Bluetooth, Wi-Fi and cellular connections. Furthermore, blockchain technology is attracting attention due to its potential to enable decentralized trust management and secure OTA software updates, eliminating the need for centralized servers.

CONCLUSION

Looking to the future, the field of automotive cybersecurity will increasingly be shaped by artificial intelligence, cloud-based threat intelligence and cooperative security architectures. AI-driven systems will be able to detect and respond to attacks in real time by correlating data from multiple vehicles and infrastructure sources. Cloud-based platforms will facilitate continuous security updates and global monitoring of threat patterns. The development of V2X communication, which connects vehicles, infrastructure, and pedestrians, will require a new generation of secure communication protocols that can handle large-scale data exchange while meeting strict latency and safety requirements. Ultimately, the future of automotive cybersecurity hinges on successfully integrating advanced technical measures, industry standards and ongoing collaboration between manufacturers, researchers and policymakers. By embedding security into every layer of vehicle communication architecture, from hardware to the cloud, manufacturers can build resilient systems capable of withstanding the growing complexity of digital threats. This enables the automotive industry to embrace digital transformation fully while maintaining the highest levels of safety, reliability and user confidence.

ACKNOWLEDGMENT

The research for this paper was funded by the project “Unapređenje kvaliteta nastave na studijskim programima Departmana kroz implementaciju rezultata naučno-istraživačkog rada u oblasti Industrijskog inženjerstva i menadžmenta” (“Improving the quality of teaching in the

Copyright2026@CIIR

Department's study programs through the implementation of the results of scientific research work in the field of Industrial Engineering and Management").

REFERENCES

[1] R. Bohnsack, H. Kurtz and A. Hanelt, "Re-examining path dependence in the digital age: The evolution of connected car business models", Research Policy, vol. 50, no. 9, 2021.

[2] P.C. Verhoef, T. Broekhuizen, Y. Bart, A. Bhattacharya, J. Qi Dong, N. Fabian, M. Haenlein, "Digital transformation: A multidisciplinary reflection and research agenda", Journal of Business Research, vol. 122, 2021, pp 889-901.

[3] M., Barbosa, M., Farsi, C. Allen, and A.S., Carvalho, "Formal validation of the CANopen communication protocol", IFAC Proceedings Volumes, vol. 36, no.13, 2003, pp. 225-230.

[4] LIN Protocol and Physical Layer Requirements, Texas Instruments Incorporated, 2022.

[5] X. Li, K. Cheng, Z. Wang, L. Zhu and G. Wei, "Distributed interval observer-based robust control for multirate systems under the FlexRay protocol", Journal of the Franklin Institute, vol. 361, no. 8, 2024, 106708.

[6] K. Matheus and M. Kaindl, "Automotive High Speed Communication Technologies: SerDes and Ethernet for Sensor and Display Applications", Carl Hanser Verlag, Munich, 2023.

[7] K. Ileri, A. Rakib and S. Djahel, "MetaCAN: An optimized adaptive hybrid metaheuristic-based intrusion detection system for CAN bus security", Vehicular Communications, vol 55, 2025, 100956.

[8] D. Püllen, N.A. Anagnostopoulos, T. Arul and S. Katzenbeisser, "Securing FlexRay-based in-vehicle networks", Microprocessors and Microsystems, vol. 77, 2020, 103144.

[9] J. Li, J. Hu, J. Du, M. Zhu and R. Zhang, "Nonlinear distributed filtering for time-varying saturated stochastic systems with cyber-attack via FlexRay regulation mechanism", Journal of the Franklin Institute, vol. 362, no. 11, 2025, 107762.

[10] L.F. Marques da Luz, P. Freitas de Araujo-Filho, D.R. Campelo, "Multi-stage deep learning-based intrusion detection system for automotive Ethernet networks", Ad Hoc Networks, vol. 162, 2024, 103548.

This is an open access article distributed under the terms of the Creative Commons NC-SA 4.0 License Attribution—unrestricted use, sharing, adaptation, distribution and reproduction in any medium or format, for any purpose non-commercially. This allows others to remix, tweak, and build upon the work non-commercially, as long as the author is credited and the new creations are licensed under the identical terms. For any query contact: research@ciir.in

Copyright2026@CIIR