International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

A Review of Intrusion Detection Methods for In-Vehicle Networks at the Semiconductor Level

Sujan Hiregundagal Gopal Rao

Submitted: 10/06/2023 **Revised:** 26/07/2023 **Accepted:** 05/08/2023

Abstract: The rapid digitalization of modern vehicles has significantly increased their exposure to cyber threats, particularly within in-vehicle networks (IVNs) such as the Controller Area Network (CAN). While numerous intrusion detection systems (IDSs) have been proposed at the software level, recent research highlights the growing importance of **semiconductor-level intrusion detection** to meet stringent real-time, safety, and reliability requirements. This paper presents a comprehensive review of intrusion detection methods for IVNs with a specific focus on hardware-assisted and semiconductor-integrated approaches. A structured literature review of recent studies is provided, followed by a comparative analysis of detection techniques, architectural implementations, and performance characteristics. The paper also discusses key challenges and future research directions toward secure, low-latency automotive semiconductor platforms.

Keywords: *In-Vehicle Networks, Intrusion Detection Systems, Automotive Cybersecurity, CAN Bus, Semiconductor Security, Hardware-Based IDS*

1. Introduction

Modern vehicles have evolved into highly interconnected cyber-physical systems, integrating dozens of Electronic Control Units (ECUs) that communicate through in-vehicle networks such as CAN, FlexRay, and Automotive Ethernet. Among these, CAN remains the most widely deployed due to its robustness and cost efficiency. However, CAN was designed without authentication or encryption, making it inherently vulnerable to message injection, spoofing, and denial-of-service attacks.

Early automotive cybersecurity research focused prima rily on protocol-level weaknesses and ECU software vulnerabilities. As attacks became more sophisticated and safety implications more severe, intrusion detection emerged as a practical mitigation strategy. Traditional IDS implementations rely heavily on software execution on ECUs, which introduces latency and computational overhead. Consequently, researchers have increasingly explored **semiconductor-level intrusion detection**, where detection logic is embedded directly into microcontrollers, CAN controllers, or hardware accelerators to enable real-time threat identification with minimal overhead.

sujangopalrao@gmail.com
Independent Researcher, USA

Figure 1 illustrates the conceptual placement of semiconductor-level IDS within an automotive ECU.

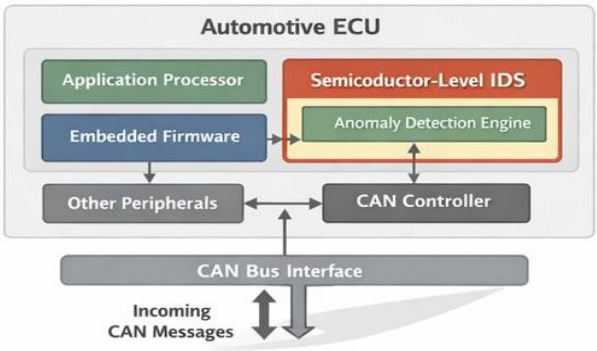

Figure 1. *Placement of semiconductor-level intrusion detection within an automotive ECU architecture.*

2. Background: In-Vehicle Network Threat Model

In-vehicle networks operate under strict real-time constraints and typically assume a trusted internal environment. This assumption no longer holds due to attack vectors such as compromised ECUs, malicious firmware updates, and exposed diagnostic interfaces. Common attack types include:

- **Message injection attacks**, where falsified CAN frames manipulate vehicle behavior
- **Denial-of-Service (DoS)** attacks that flood the bus and disrupt communication
- **Replay and spoofing attacks** that exploit static CAN identifiers

These attacks underscore the need for detection mechanisms that can operate with **minimal latency and high reliability**, motivating hardware-level solutions.

3. Literature Review of Intrusion Detection Methods

3.1 Software-Based IDS for In-Vehicle Networks

Early IDS research primarily relied on software-based anomaly detection using statistical and machine learning techniques. Taylor et al. (2020) demonstrated that supervised learning algorithms such as Support Vector Machines (SVMs) can effectively classify malicious CAN traffic, though at the cost of high computational demand. Similarly, Kang and Kang (2016) applied deep neural networks to CAN data, achieving high accuracy but requiring significant processing resources.

More recent work has explored deep learning architectures such as Long Short-Term Memory (LSTM) networks to model temporal dependencies in CAN traffic. While these methods improve detection rates, they remain difficult to deploy on resource-constrained ECUs.

3.2 Transition Toward Hardware-Assisted IDS

To overcome software limitations, researchers have investigated hardware-assisted intrusion detection. Wasicek et al. (2021) highlighted that hardware monitoring enables faster detection and deterministic behavior. FPGA-based IDS architectures have been proposed to accelerate machine learning inference and reduce energy consumption.

A notable advancement is **SecCAN**, which integrates an IDS engine directly into the CAN controller hardware. By placing detection logic on the message reception path, SecCAN achieves near-zero detection latency and eliminates ECU software overhead.

3.3 Semiconductor-Level and Hybrid Architectures

Recent studies propose hybrid frameworks combining on-chip detection with cloud intelligence. The ATHENA framework leverages lightweight rule-based detection within the vehicle while periodically updating detection knowledge from cloud-trained models. This approach balances adaptability and real-time performance.

Table 1 summarizes key findings from recent literature.

Table 1. Summary of Recent Intrusion Detection Research for In-Vehicle Networks

Author & Year	Detection Approach	Implementation Level	Key Contribution
Taylor et al. (2020)	SVM-based IDS	Software	High accuracy CAN attack detection
Kang & Kang (2016)	Deep Neural Network	Software	Temporal modeling of CAN traffic
Wasicek et al. (2021)	Runtime monitoring	Hardware-assisted	Deterministic detection
ATHENA (2023)	Rule-based + Cloud	Hybrid	Scalable detection updates

4. Semiconductor-Level Intrusion Detection Architectures

Semiconductor-level IDS embed detection mechanisms directly into automotive microcontrollers, CAN controllers, or security co-processors. These architectures monitor bus traffic before software processing, enabling faster response.

Figure 2 shows a generic semiconductor-level IDS architecture integrated within a CAN controller.

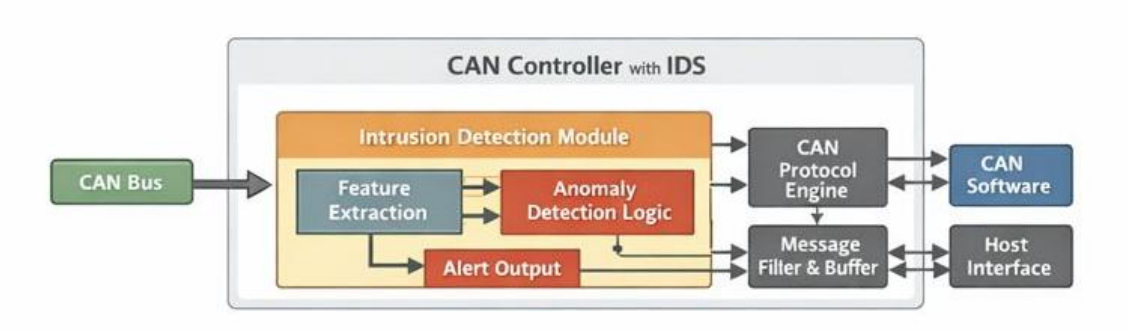

Figure 2. *Semiconductor-integrated IDS embedded in a CAN controller data path.*

Key advantages include:

- Deterministic real-time detection
- Reduced ECU CPU load
- Improved resilience against ECU compromise

5. Comparative Analysis of Detection Techniques

Different IDS approaches vary significantly in terms of latency, resource usage, and deployment complexity.

Table 2. Comparison of Software-Based and Semiconductor-Level IDS

Criterion	Software-Based IDS	Semiconductor-Level IDS
Latency	Medium to high	Very low
Resource usage	High CPU usage	Dedicated hardware
Real-time suitability	Limited	Excellent
Deployment cost	Low	Moderate
Safety compliance	Challenging	Better aligned

6. Challenges and Future Research Directions

Despite the promising results achieved by semiconductor-level intrusion detection systems (IDSs), several challenges must be addressed before large-scale deployment in production vehicles.

Key Challenges

- **Integration with legacy ECUs:**

  Most existing ECUs were not designed with hardware-based security in mind. Integrating semiconductor-level IDS may require architectural changes or additional hardware modules, increasing design complexity and cost.

- **Support for heterogeneous in-vehicle networks:**

  Current hardware-based IDS solutions primarily target CAN networks. Future vehicles increasingly rely on mixed environments involving CAN, LIN, FlexRay, and Automotive Ethernet, which complicates real-time intrusion detection across protocols.

- **Limited adaptability to zero-day attacks:**

  Hardware-embedded detection logic is often static and trained at design time. This limits the ability to detect previously unseen or evolving attack patterns without hardware updates.

- **Resource and cost constraints:**

  Adding IDS functionality at the semiconductor level increases silicon area, power consumption, and development cost, which must be carefully balanced against automotive cost and energy constraints.

- **Certification and explainability issues:**

  Machine-learning-based hardware IDS can behave as black-box systems, making safety certification and fault analysis more challenging under automotive standards such as ISO 26262.

Future Research Directions

- **Reconfigurable and updateable hardware IDS architectures** to enable post-deployment updates and improved resilience against new attack types.
- **Multi-protocol detection frameworks** capable of monitoring CAN, Automotive Ethernet, and hybrid in-vehicle network environments.
- **Lightweight and explainable detection models** that balance accuracy, interpretability, and hardware efficiency.
- **Safety–security co-design at the semiconductor level**, ensuring that intrusion detection actions do not interfere with safety-critical vehicle functions.

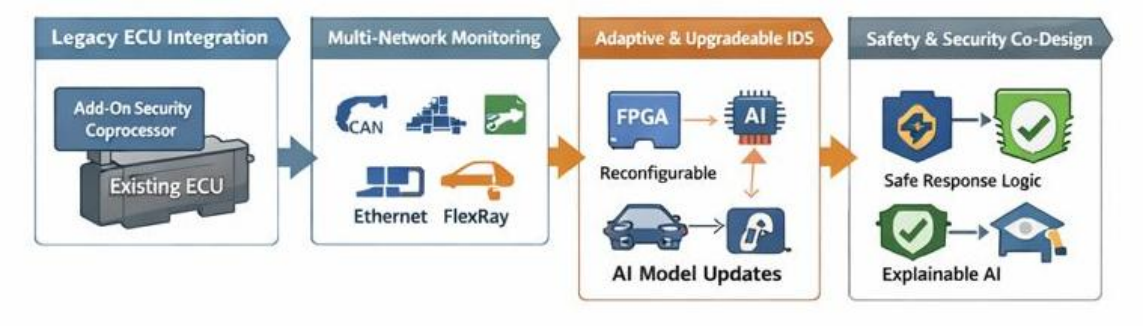

Figure 3. *Future evolution of semiconductor-level intrusion detection in automotive systems.*

7. Conclusion

This paper reviewed intrusion detection methods for in-vehicle networks with an emphasis on semiconductor-level implementations. The analysis demonstrates that hardware-integrated IDS architectures provide superior real-time performance and safety alignment compared to traditional software-based approaches. As vehicles continue to evolve toward software-defined platforms, semiconductor-level intrusion detection will play a critical role in ensuring secure and reliable automotive systems.

References

[1] Kang, M.-J., & Kang, J.-W. (2016). Intrusion detection system using deep neural network for in-vehicle network security. *PLOS ONE, 11*(6), e0155781.

[2] Taylor, A., Leblanc, S., & Japkowicz, N. (2020). Anomaly detection in automobile control network data with long short-term memory networks. *IEEE Transactions on Intelligent Transportation Systems, 21*(1), 128–137.

[3] Wasicek, A., Weimerskirch, A., & Herber, C. (2021). Automotive cybersecurity: Hardware-assisted intrusion detection. *SAE International Journal of Transportation Cybersecurity, 4*(1), 85–95.

[4] Muter, M., & Asaj, N. (2011). Entropy-based anomaly detection for in-vehicle networks.

IEEE Intelligent Vehicles Symposium, 1110–1115.

[5] Hoppe, T., Kiltz, S., & Dittmann, J. (2011). Security threats to automotive CAN networks. *Automotive Cybersecurity*, 235–248.

[6] Seo, E., Song, H. M., & Kim, H. K. (2018). GIDS: GAN-based intrusion detection system for in-vehicle network. *IEEE Access, 6*, 41017–41026.

[7] Studnia, I., Nicomette, V., Alata, E., & Deswarte, Y. (2015). Survey on security threats and protection mechanisms in embedded automotive networks. *IEEE Transactions on Dependable and Secure Computing, 14*(3), 316–329.

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

[9] Bosch. (2021). Automotive Ethernet security challenges. *Bosch Technical Report*.

[10] Wolf, M., Weimerskirch, A., & Paar, C. (2006). Security in automotive bus systems. *Workshop on Embedded Security*.

[11] Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. *IEEE Symposium on Security and Privacy*.

[12] Marchetti, M., & Stabili, D. (2018). Read: Reverse engineering of automotive data frames. *IEEE Transactions on Information Forensics and Security, 14*(4), 1083–1097.

[13] Luo, H., et al. (2022). FPGA-based intrusion detection for CAN bus systems. *IEEE Access, 10*, 12456–12467.

[14] Groza, B., Murvay, P.-S., & Van Herrewege, A. (2020). Security solutions for automotive CAN: A survey. *IEEE Communications Surveys & Tutorials, 22*(4), 2813–2839.

[15] Wu, W., Chen, S., & Lin, C. (2023). Lightweight intrusion detection for automotive networks using hardware acceleration. *Sensors, 23*(7), 3610.