IOSUD - Politehnica University of Timișoara
Doctoral School for Engineering Studies

Secure Key Exchange and Time Synchronization for Controller Area Networks

PhD Thesis – Summary

for obtaining the Scientific Title of PhD in Engineering at
Politehnica University of Timișoara
in the field of Computer and Information Technology

Author: Eng. Adrian-Eugen MUȘUROI
PhD Supervisor: Prof. Univ. Dr. Ing. Bogdan-Ioan GROZA

May 2025

The Controller Area Network (CAN) has become a foundational protocol in modern software-defined vehicles, primarily due to its low cost, robustness, and suitability for real-time systems. Alongside other protocols such as FlexRay and automotive Ethernet, CAN enables the interconnection of Electronic Control Units (ECUs)—embedded devices that manage automotive functions—forming complex, distributed in-vehicle networks. Through these networks, ECUs exchange data and coordinate operations precisely to execute a wide range of functions, relying on sensor input, user commands, and sophisticated algorithms. As such, the security of CAN communication is inherently linked to vehicle safety, since any malicious interference can result in unpredictable or uncontrollable behavior that jeopardizes both passengers and other road users. Yet, despite its critical role, CAN was originally designed without built-in security measures, and its vulnerabilities have been thoroughly demonstrated for over a decade [1], underscoring the urgent need to secure CAN communication. Although various proposals and standards have emerged to address this issue, this thesis focuses on two unresolved foundational challenges: (1) the design and deployment of group key exchange protocols, and (2) the security of time synchronization mechanisms—both of which are essential for secure, reliable communication among CAN-connected ECUs.

Authenticating CAN traffic is a fundamental security requirement, as the absence of countermeasures leaves the system vulnerable to replay and spoofing attacks that could be exploited to gain unauthorized control of the vehicle. Numerous academic contributions [2-5], along with AUTOSAR's Secure On-Board Communication (SecOC) standard [6], advocate for the use of group Message Authentication Codes (MACs) for traffic authentication, and this approach is supported by two critical factors. First, MACs are significantly faster to compute than digital signatures, which is vital in real-time automotive environments where ECUs face strict limitations in computational capacity and latency requirements. Second, MACs impose a much smaller data footprint, making them more suitable for authenticating CAN frames, which typically support

payloads of no more than 64 bytes in most current systems[1]. Additionally, since CAN employs a broadcast communication model and messages are often intended for multiple recipients, incorporating individual MACs for each receiver introduces significant overhead. Group MACs address this by enabling a single MAC to authenticate a message for all intended recipients, thus optimizing efficiency.

To enable authentication through group MACs, symmetric keys must be shared among the involved ECUs, allowing all recipients to validate the same MAC. Traditionally, these keys are injected during vehicle manufacturing or service, but this static approach presents multiple drawbacks. Since the key material originates from external sources, the risk of weak or compromised keys—due to human error or manufacturing flaws—must be mitigated through robust infrastructure, which increases overall system cost by necessitating advanced security controls. Furthermore, updating or replacing keys after the vehicle has been deployed—such as in cases involving ECU replacements—may be unfeasible outside authorized service centers. In many cases, keys remain unchanged for extended periods, leaving the vehicle unable to recover autonomously from key extraction attacks, such as the one recently documented in [7]. Key exchange protocols address these challenges by enabling ECUs to establish shared secret keys independently and periodically, without relying on pre-installed data. Despite their potential, group key exchange protocols are not yet addressed by current standards, and although several studies have evaluated their computational and communication overhead in automotive environments, the findings suggest that commonly used solutions from other domains (e.g., enterprise or internet-based networks) are often too resource-intensive for automotive use cases. As a result, many related works still rely on key distribution methods rather than true exchanges—an approach that inherits the limitations of requiring pre-shared secrets. Consequently, the development of efficient group key exchange protocols remains an open and critical research area.

Accurate time synchronization plays a central role in supporting key exchange, other security protocols, and the broader coordination between ECUs. When ECUs on a shared CAN bus are tightly synchronized to a common time base, they can employ timestamps to validate message freshness (as in AUTOSAR SecOC) and to accurately align sensor data for high-precision applications such as Sensor Fusion. Moreover, real-time synchronization enables effective coordination between ECUs residing on different buses and facilitates interaction with external entities, such as other vehicles or roadside infrastructure. In addition to these operational benefits, secure time synchronization supports essential security tasks, including verifying digital certificate validity, generating reliable telemetry logs, and enabling forensic analysis. All these applications depend on the integrity of the synchronization process itself. While current literature lacks comprehensive proposals for securing time synchronization among CAN-connected ECUs, the AUTOSAR Time Synchronization over CAN (CanTSyn) standard [8] does incorporate some security mechanisms. Nevertheless, this protocol is not immediately deployable, as its security framework relies on additional components that must be designed and implemented by external

[1] Since 2024, a new version of the CAN standard—ISO 11898-1:2024—has introduced CAN XL, supporting payloads of up to 2048 bytes and data rates of up to 20 Mbit/s. However, the adoption of CAN XL remains limited, as it requires significant updates to both hardware and software across the automotive supply chain.

stakeholders, such as the Original Equipment Manufacturer (OEM). Furthermore, the standard focuses only on bus-level synchronization, neglecting higher-level threats that may arise at the system integration layer. These limitations underscore the importance of further research in this area.

In the light of the previously mentioned challenges and limitations of CAN security, the objectives followed in this work are:

1. Deploy efficient key exchanges over CAN-FD using embedded automotive-grade devices for evaluation;

2. Explore alternative mechanisms for managing ECU asymmetric keys required for authentication in key exchange protocols;

3. Design scalable group extension schemes to facilitate group key establishment for CAN traffic authentication, a requirement frequently emphasized in both academic literature and industry standards;

4. Evaluate and enhance the security of CAN-FD time synchronization protocols, ensuring that added protections and overhead do not compromise system load or the precision required by applications such as sensor fusion;

5. Investigate practical implementation strategies for time synchronization protocols, such as timestamp acquisition via Direct Memory Access (DMA) without CPU interruption;

6. Propose a security-oriented synchronization architecture that addresses vulnerabilities stemming from compromised or impersonated time moderators.

The thesis is structured as follows. Chapter 1 presents the introduction and motivation, while Chapter 2 provides the theoretical background relevant to the concepts explored throughout the thesis. The main contributions are divided into two parts. The first part, covered in Chapters 3 and 4, focuses on key exchange mechanisms over CAN. Chapter 3 explores fast pairwise key exchanges using Four$\mathbb{Q}$ as the underlying elliptic curve, whereas Chapter 4 introduces group extension schemes that enable an arbitrary number of ECUs to establish a common group key. The second part, discussed in Chapters 5 and 6, addresses secure time synchronization for CAN-connected ECUs. Chapter 5 examines the security of bus-level time synchronization, while Chapter 6 shifts the perspective to system-level synchronization, addressing higher-level attacks in typical automotive network topologies. Finally, Chapter 7 presents the conclusions of the thesis. In summary, the main contributions of this thesis, aligned with the objectives outlined above, are:

1. Porting and performance evaluation of the Four$\mathbb{Q}$ elliptic curve on automotive-grade microcontrollers. Experimental results on Aurix devices show that Diffie-Hellman and digital signature operations based on the Four$\mathbb{Q}$ elliptic curve are 4–6 times faster than equivalent operations using the NIST P-256 curve [9];

2. Implementation and comparative analysis of two authenticated key exchange protocols: the Station-to-Station (STS) protocol [10] using classical ECC and Cao's Identity-Based Key

Exchange (IBKE) protocol [11]. The protocols are assessed in the context of automotive deployment, focusing on key management implications [9];

3. Design and evaluation of three group key extension schemes based on elliptic curve Diffie-Hellman. The most efficient variant, integrated with FourQ, enables secure group key establishment for 32 ECUs in under 0.6 seconds on Aurix entry-level microcontrollers [9];

4. Development and evaluation of security enhancements to the AUTOSAR CanTSyn protocol [8], addressing spoofing, delay, replay, and forecasting attack vectors [12];

5. Implementation of clock rate correction algorithms to complement offset correction in AUTOSAR time synchronization, achieving consistent sub-microsecond accuracy on Aurix hardware in a realistic testing environment [12];

6. Development of a novel timestamp acquisition method using DMA, eliminating reliance on CPU interrupts and thereby improving resilience and system schedulability [12];

7. Design and deployment of a blockchain-based mechanism for secure incident reporting from intrusion detection systems, using smart contracts on the Ethereum platform [13];

8. Creation of a secure time synchronization framework with redundant time sources, enabling verification and detection of compromised or impersonated moderators in topologies with potential single points of failure [14].

Chapter 3 addresses the main limitation of automotive key exchange protocols: the computational overhead that can cause ECUs to become temporarily unresponsive, hampering secure communication. To mitigate this, the chapter adopts FourQ, a modern elliptic curve previously demonstrated to outperform traditional choices like NIST P-256 in high-performance computing contexts. This thesis extends that evaluation to embedded automotive platforms, including Infineon's Aurix architecture, which is common in production vehicles. Experiments show that FourQ delivers up to a sixfold speedup for digital signature and ECDH operations compared to NIST P-256. Comparative benchmarks with similarly sized elliptic curves from the literature—obtained using the same hardware platforms as in [15]—further confirm FourQ's performance edge, as illustrated in Figures 1 and 2. Using FourQ as a foundation, two authenticated key exchange protocols are implemented. The first, the Station-to-Station (STS) protocol, uses conventional digital certificates, delegating all asymmetric key operations to the ECUs. This approach secures key material locally but assumes access to high-entropy sources. The second protocol employs identity-based cryptography, where authentication is derived from identity strings rather than certificates. Here, a trusted authority manages key generation and distribution, reducing ECU-side requirements but necessitating secure infrastructure. Experimental results show both protocols achieve similar performance, allowing deployment decisions to be guided by available infrastructure. Notably, both surpass known alternatives in literature.

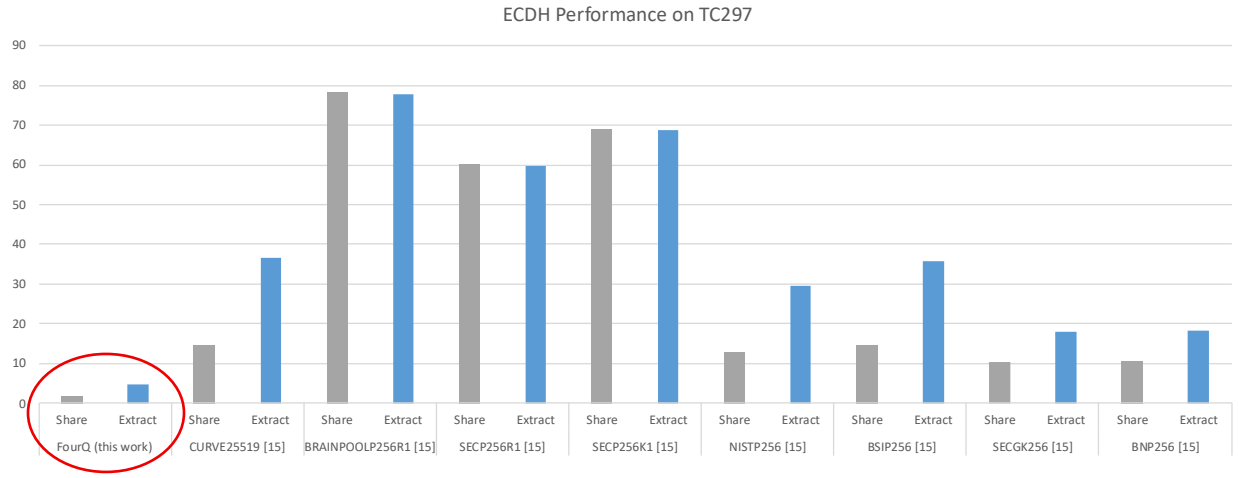

Figure 1: Performance comparison between ECDH operations based on Four$\mathbb{Q}$ and other elliptic curves of similar size evaluated in [15], on Infineon's TC297 platform. The red circle highlights the speed advantage of Four$\mathbb{Q}$ over other elliptic curves

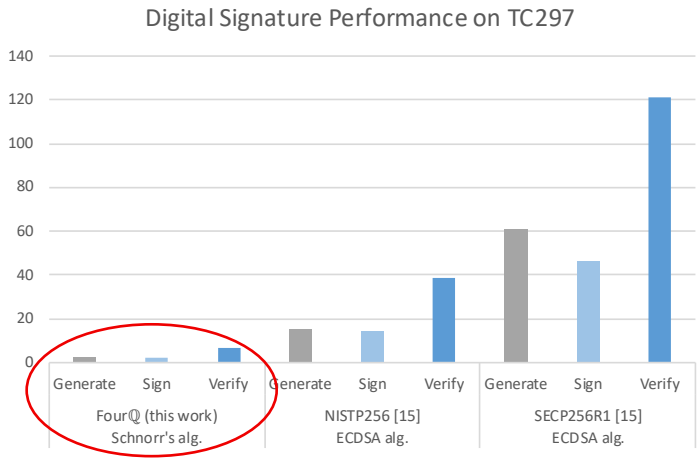

Figure 2: Performance comparison between Schnorr's digital signature based on Four$\mathbb{Q}$ and ECDSA based on other elliptic curves of similar size evaluated in [15], on Infineon's TC297 platform. The red circle highlights the speed advantage of Four$\mathbb{Q}$ over other elliptic curves

Chapter 4 builds on this foundation by introducing three group extension schemes for orchestrated key exchanges. These schemes enable multiple ECUs to collectively agree on a shared secret, facilitating secure future communication. A dedicated Security Orchestrator ECU (SoECU) oversees the process, preventing unauthorized group initiations that could disrupt vehicle responsiveness. The primary scheme, illustrated in Figure 3, uses CAN's broadcast capability and introduces logical ECUs—abstract entities composed of physical ECU subsets. The group key exchange is structured as a binary tree, enabling parallel operations at each level. Additionally, it establishes individual secrets between each ECU and the SoECU for enhanced monitoring. The second scheme maintains the binary tree structure while reducing SoECU involvement to prioritize performance. The third uses a more conventional key distribution method but still preserves secret channels with the SoECU. All three schemes are benchmarked using Four$\mathbb{Q}$-based timing data from Chapter 3. Results show the fastest method can securely link 32 ECUs in under 0.6 seconds

on entry-level microcontrollers, surpassing typical CAN requirements. The most secure option achieves group agreement among 15 ECUs in approximately 0.5 seconds, which may be suitable for real-world use cases. Integration with AUTOSAR software stacks is also explored to support practical deployment.

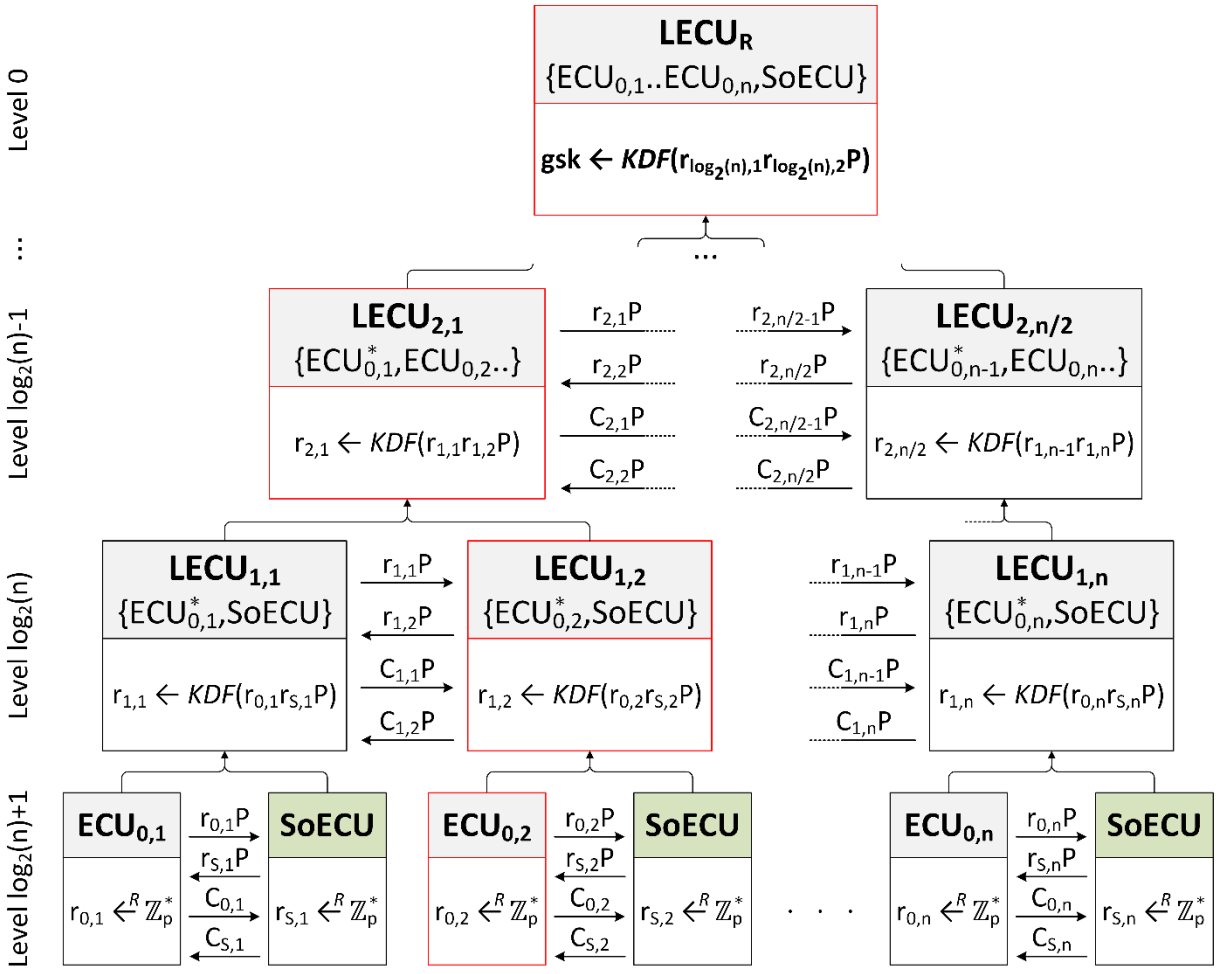

Figure 3: Group key exchange with SoECU participating in the formation of each logical ECU. The logical ECUs highlighted with red show the key exchanges that must be re-executed in case of a corrupted ECU, in this case $ECU_{0,2}$

Chapter 5 introduces the second core contribution of this thesis: secure time synchronization. It begins by analyzing the AUTOSAR CAN Time Synchronization protocol [8] against a practical adversary model, revealing vulnerabilities to spoofing, replay, delay, and forecasting attacks. To counter these, a hardened version of the protocol is proposed. Key enhancements include a challenge-response mechanism for freshness, multi-MAC authentication to prevent spoofing by local ECUs, and clock rate correction for improved long-term precision. These additions address advanced threats like double replay and forecasting attacks while maintaining compatibility with the AUTOSAR standard. Although additional messages could strain the CAN bus, evaluations using real-world traces from a commercial vehicle show the extra

load is minimal, even with 16 time subordinates. Experiments further reveal that the unmodified protocol, which is limited to correcting only clock offsets, can accumulate errors of up to 8 µs at 1-second intervals, which may be unacceptable for time-sensitive applications. The enhanced version incorporates four clock rate correction algorithms, each tested for convergence speed and robustness under realistic disturbances. The results of a simulation showing the theoretical performance of the four algorithms are illustrated in Figure 4. During testing, all maintain synchronization errors below 1 µs, representing a major improvement. Practical concerns such as floating-point precision and clock adjustment methods are also addressed. To avoid dependence on CPU interrupts for timestamping, a novel DMA-based approach is introduced and experimentally validated, successfully offloading this task from the CPU.

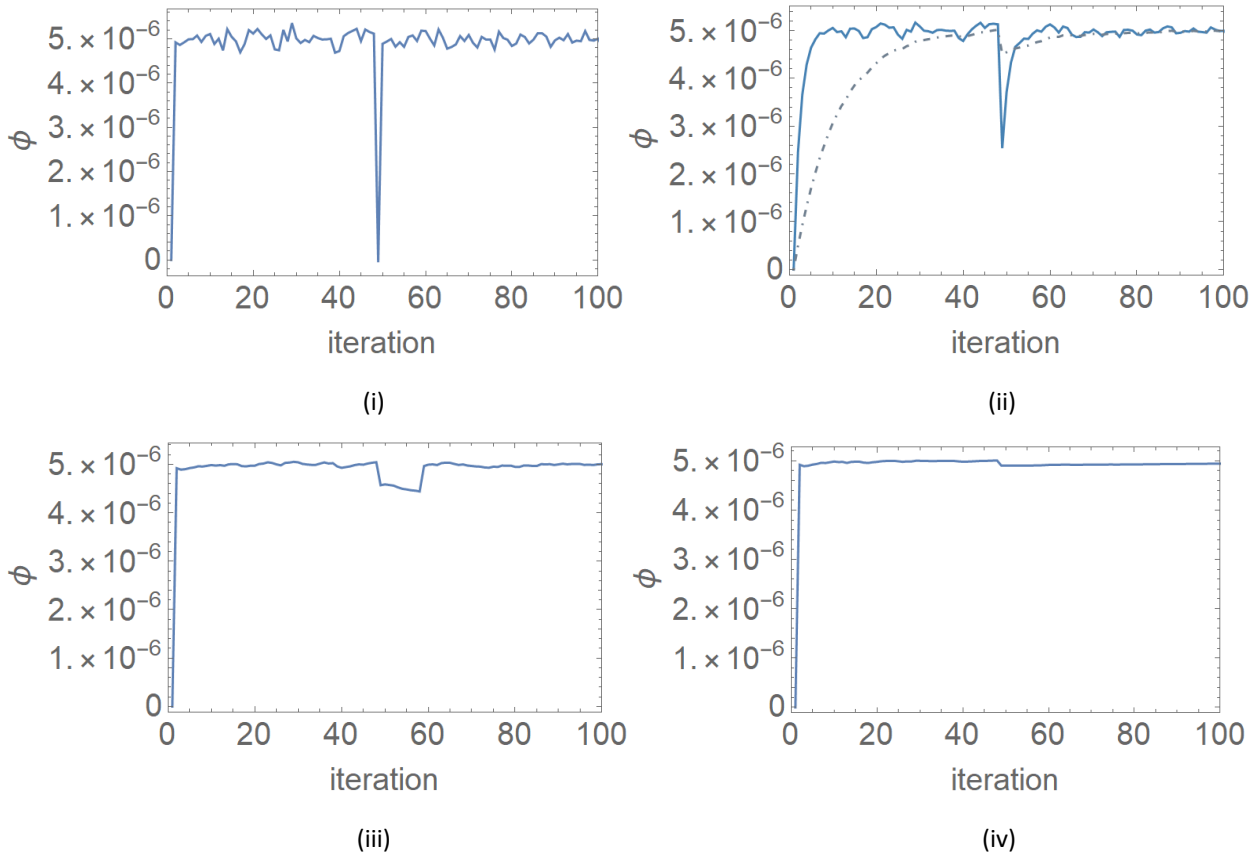

Figure 4: Simulated performance of the (i) immediate, (ii) weighted learning, (iii) windowed averaging and (iv) continuous averaging clock rate adjustment algorithms, with random noise and a glitch inserted at the 50th iteration

Chapter 6 elevates time synchronization to a system-wide concern, targeting threats from compromised or spoofed time sources, which are often single points of failure in vehicle networks. Two simulated attack scenarios illustrate the risks of poor synchronization: one involving delayed steering commands that may evade detection, and another showing how a corrupted clock can mislead an intelligent intersection system, potentially causing collisions. Unlike traditional fault-tolerant architectures that focus on reliability, the proposed design adopts a security-oriented view. It considers varying levels of trust in time sources, differences in ECU accuracy requirements, and dynamic synchronization behaviors. Figure 5 shows the relation between overhead, security and

accuracy, factors which are used to create a rating system for time moderators. Recognizing that a single time moderator on the CAN bus may not suffice, the architecture enables synchronization with external or cross-bus moderators via bus-agnostic protocols like Network Time Protocol (NTP). To address the one-to-one communication overhead of NTP, a collective bus-wide synchronization strategy is analyzed, reducing overhead while maintaining robustness.

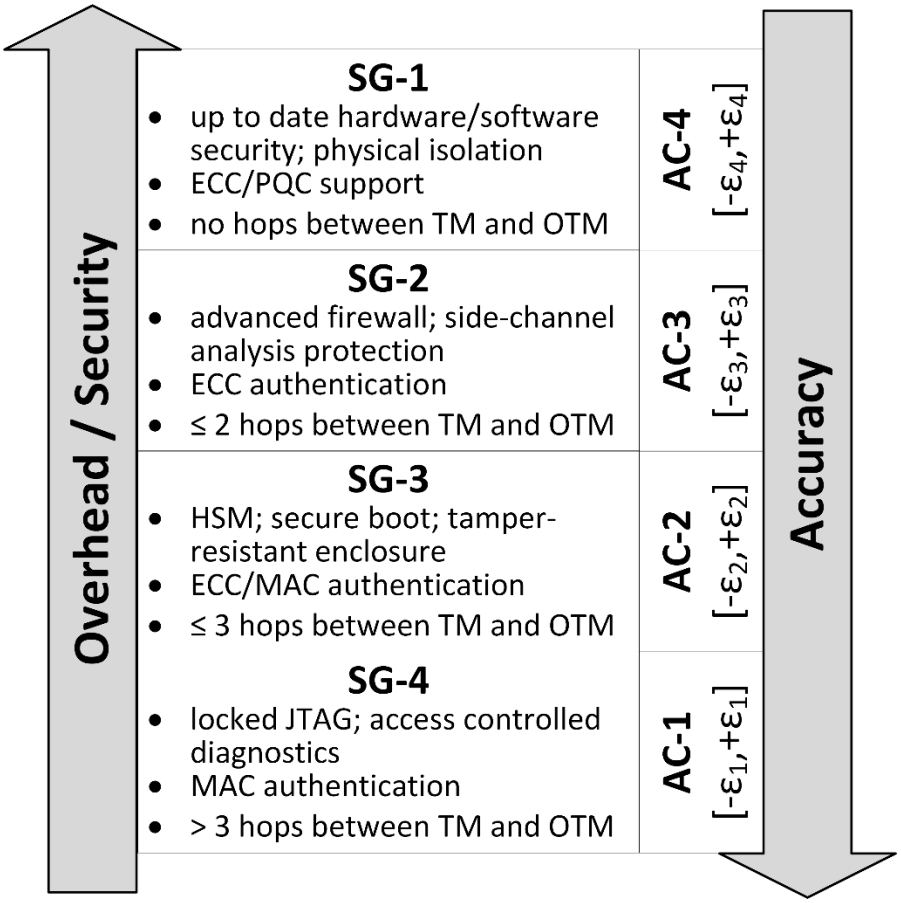

Figure 5: Rating system for a secure time synchronization framework based on overhead, security grades (SGs) and accuracy classes (ACs)

These contributions have undergone peer review and have been published in academic journals. The list of publications to which the author has contributed during his doctoral studies is presented below:

1. **A. Musuroi**, B. Groza, L. Popa, and P.-S. Murvay, "*Fast and Efficient Group Key Exchange in Controller Area Networks (CAN)*", IEEE Transactions on Vehicular Technology, vol. 70, no. 9, pp. 9385–9399, 2021,
2. C. Jichici, A. Berdich, **A. Musuroi**, and B. Groza, "*Control System Level Intrusion Detection on J1939 Heavy-Duty Vehicle Buses*", IEEE Transactions on Industrial Informatics, vol. 20, no. 2, pp. 2029-2041, 2024,

3. T. Andreica, **A. Musuroi**, A. Anistoroaei, C. Jichici, and B. Groza, "*Blockchain integration for in-vehicle CAN bus intrusion detection systems with ISO/SAE 21434 compliant reporting*", Scientific Reports, vol. 14, p. 8169, 2024,
4. **A. Musuroi** and B. Groza, "*Secure Time Synchronization with Submicrosecond Accuracy in Controller Area Networks*", IEEE Transactions on Industrial Informatics, pp. 1-11, 2025.

In summary, this thesis advances the state of CAN security by addressing two critical yet underexplored challenges: group key exchange and secure time synchronization. The proposed solutions enhance both performance and resilience without compromising compatibility with established automotive standards, including AUTOSAR. Through extensive experimental evaluations under realistic conditions—supported by peer-reviewed validation—this work demonstrates the practical feasibility and deployment readiness of the proposed approaches.

Bibliography

[1] H. J. Jo and W. Choi, "*A survey of attacks on controller area networks and corresponding countermeasures*", IEEE Transactions on Intelligent Transportation Systems, vol. 23, no. 7, pp. 6123-6141, 2022.

[2] Q. Wang and S. Sawhney, "*Vecure: A practical security framework to protect the can bus of vehicles*", Proceedings of the International Conference on the Internet of Things (IOT), pp. 13-18, 2014.

[3] R. Kurachi, Y. Matsubara, H. Takada, N. Adachi, Y. Miyashita, and S. Horihata, "*Cacan-centralized authentication system in CAN (controller area network)*", Proceedings of the 14th International Conference on Embedded Security in Cars (ESCAR 2014), pp. 10, 2014.

[4] G. Bella, P. Biondi, G. Costantino, and I. Matteucci, " *Toucan: A protocol to secure controller area network*", Proceedings of the ACM Workshop on Automotive Cybersecurity, New York, USA, pp. 3-8, 2019.

[5] B. Groza, S. Murvay, A. V. Herrewege, and I. Verbauwhede, "*Libra-can: Lightweight broadcast authentication for controller area networks*", ACM Transactions on Embedded Computing Systems, vol. 16, no. 3, 2017.

[6] AUTOSAR, "*Specification of Secure Onboard Communication Protocol R23-11*", Standard, no. 969, November 2023, accessed: 2025-03-10, available at: https://www.autosar.org/fileadmin/standards/R23-11/CP/AUTOSAR_CP_SRS_CryptoStack.pdf.

[7] W. Melching and G. Hogan, "*My Car, My Keys: Obtaining CAN Bus SecOC Signing Keys*", Presented at Hardwear.io USA, 2024.

[8] AUTOSAR, "Specification of Time Synchronization over CAN R23-11", Standard, no. 674, November 2023, accessed: 2025-03-10, available at: https://www.autosar.org/fileadmin/standards/R23-11/CP/AUTOSAR_SWS_TimeSyncOverCAN.pdf.

[9] A. Musuroi, B. Groza, L. Popa and P.-S. Murvay, "*Fast and efficient group key exchange in controller area networks (CAN)*", IEEE Transactions on Vehicular Technologies, vol. 70, no. 9, pp. 9385-9399, 2021.

[10] W. Diffie, P. C. Van Oorschot, and M. J. Wiener, "*Authentication and authenticated key exchanges*", Designs, Codes and Cryptography, vol. 2, no. 2, pp. 107-125, 1992.

[11] X. Cao, W. Kou, and X. Du, "*A pairing-free identity-based authenticated key agreement protocol with minimal message exchanges*", Information Sciences, vol. 180, no. 15, pp. 2895-2903, 2010.

[12] A. Musuroi and B. Groza, "*Secure time synchronization with submicrosecond accuracy in controller area networks*", IEEE Transactions on Industrial Informatics, pp. 1-11, 2025.

[13] T. Andreica, A. Musuroi, A. Anistoroaei, C. Jichici, and B. Groza, "*Blockchain integration for in-vehicle can bus intrusion detection systems with ISO/SAE 21434 compliant reporting*", Scientific Reports, vol. 14, no. 1, p. 8169, 2024.

[14] A. Musuroi, A. Berdich, and B. Groza, "*A secure automotive architecture for redundant time synchronization*", Submission in progress, 2025.

[15] L. Popa, B. Groza, and P.-S. Murvay, "*Performance evaluation of elliptic curve libraries on automotive-grade microcontrollers*", Proceedings of the 14th International Conference on Availability, Reliability and Security (ARES `19), New York, USA, 2019.