IOSUD – Politehnica University of Timișoara
Doctoral School for Engineering Studies

Physical Layer Security based on Timing and Voltage Features 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
by

Author: Eng. Lucian-Tudor Popa
PhD Supervisor: Prof.Univ.Dr.Ing. Bogdan-Ioan Groza

September 2023

Nowadays, Controller Area Networks (CAN) are still one of the frequently employed communication interfaces between nodes inside vehicles. Before the CAN networks were used in the vehicles, communication inside vehicles was done using point-to-point connections through separate wires. Opposed to this method, Controller Area Networks interconnect multiple nodes with the use of only two wires. This helps with regards to reducing the number of wires as well as the complexity of the networks in vehicles. Its reliability in harsh environments is another benefit of using CAN inside vehicles. This is due to the differential wires that are used as physical layer for communication between sensors, actuators, and more complex systems. There are updates of the initial CAN proposal such as CAN-FD (proposed in 2012) and CAN-XL (proposed in 2018) that will define future in-vehicle networks using the same two-wire pairs but with higher data rates and improved immunity to environmental factors.

The information exchange over the CAN networks are both safety and non-safety related signals transmitted by sensors, actuators and Electronic Control Units (ECUs). Even though safety information is exchanged between nodes over CAN, there are open gaps related to the authenticity of the data since the CAN standard does not impose any security requirements. The evolution of passenger vehicles from mechanical components to complex systems that run many software modules in parallel caused the in-vehicle communication networks to be used as a malicious interface to compromise legitimate system or even vehicle level functionalities. There are several research works as well as automotive standards that propose the use of security mechanisms for in-vehicle networks, including CAN security, which are discussed in the thesis as initial proposals before physical layer security of CAN was considered as an option. The main motivation topic for the thesis is ensuring the Controller Area Network security. The author's motivation as well as the research objectives and major contributions of the author for the research outcome are presented in Chapter I of the thesis.

In the past decade, several research papers [1], [2] have shown that Controller Area Networks that are used as communication medium in passenger vehicles have multiple vulnerabilities. The authors of [1] have emphasized that CAN frames are missing source identification or authentication field by performing packet sniffing, targeted probing, and fuzzing attacks on several Electronic Control Units (ECUs). In the second work [2] the authors emphasize an attack path provided by Tire-Pressure Monitoring Sensors (TPMS) and the Telematics ECU, exploiting the latter with the purpose to inject CAN packets on the internal vehicle networks where multiple ECUs are connected.

Due to an increasing number of threats related to in-vehicle communication, the AUTOSAR community has published a release of the specification in 2014 that requires the Secure On-Board communication (SecOC) [3] functionality to be used by safety critical systems that exchange safety related data, as also discussed in [4] by the authors. The SecOC functionality is used as a measure to protect genuine communication between nodes against injection of adversarial packets and replay attacks. There are other proposals that have been published in research works with the goal of securing CAN communication by performing message authentication [5], [6], [7] or identifier reallocation [8], [9], [10].

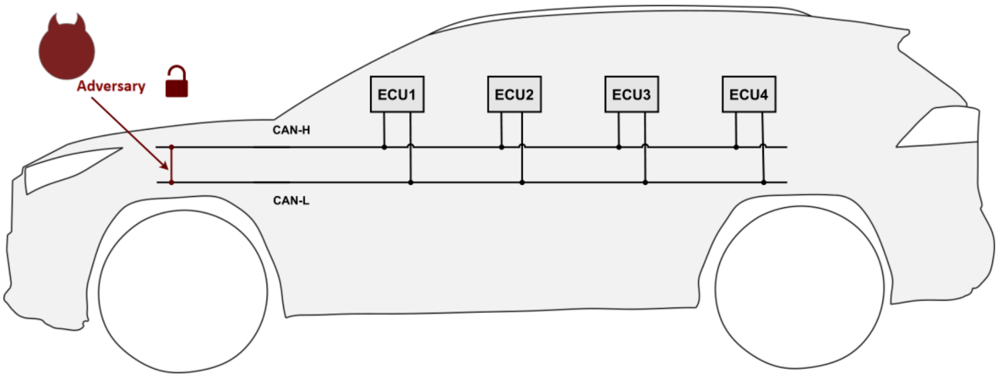

Fig. 1. Generic attack of an adversary on the CAN bus

It is worth mentioning that CAN bus attacks have negative implications. For example, more recently, several vehicles were stolen using CAN injection attacks [11]. This was possible due to an attack path that is available on the CAN network close to the headlights and near the front bumper of the vehicle. The thief was able to unlock the doors and start the engine using a malicious device that transmits the expected CAN frame sequence. Figure 1 suggests an adversary that taps the CAN line in an actual vehicle and performs an attack in order to unlock the doors. This has later been reported as a known vulnerability and was added to the CVE (common vulnerabilities and exposures) as CVE-2023-29389. Other recent weaknesses related to Controller Area Networks from real-world vehicles that were also reported as vulnerabilities are CVE-2017-14937 and CVE-2018-9322. The first vulnerability is caused by predictable security access to the CAN bus that affects airbag units. The second one is reported for the infotainment component of BMW vehicles that can be maliciously used to inject frames on the internal CAN networks. The research papers as well as the industry standards pave the road for ensuring CAN security and also opens a door for the research groups to find additional ways of protecting legitimate communication between nodes inside passenger vehicles.

Research objectives. There are several research objectives in this thesis related to ensuring the security of the Controller Area Networks as evaluation of elliptic curve cryptography for CAN, implementation of time-covert key exchange protocols and time-covert authentication, fingerprinting CAN transmitters using timing and voltage features as well as the design and evaluation of a Controller Area Network digital twin experimental setup. The research objectives of the thesis can be summarized as follows:

1) Literature review on related works for physical security for Controller Area Networks as well as for automotive system digital twins;
2) Evaluation of software libraries with support for elliptic curve cryptography in the context of key-exchange on automotive microcontrollers;

3) Implementation and evaluation of four time-covert key exchange protocols for Controller Area Networks that are fully compatible with existing networks and fully compliant with the standard;
4) Implementation of four frame scheduling optimization algorithms and evaluation of the performance of a time-covert authentication channel in the context of optimized frame transmission;
5) Data collection from four passenger vehicles of frame transmission times for clock skew computation and voltage samples for voltage feature determination in the context of Electronic Control Unit (ECU) fingerprinting;
6) Evaluation of ECU separation from nine passenger vehicles using the determined clock skews and voltage features as well as the environmental impact for these fingerprints;
7) Design and evaluation of an experimental setup that integrates a digital twin for vehicle level functionalities implemented on a Controller Area Network from real-world vehicle cables;
8) Voltage characteristic evaluation of the Controller Area Network from the experimental setup that uses real vehicle cables in comparison with Controller Area Networks from other experimental setups or real-world vehicles in the context of physical fingerprinting.

Major contributions. This thesis describes several software and hardware methods to implement security for the Controller Area Networks (CAN) used in automotive. The topics that are addressed in the thesis are the elliptic curve evaluation of cryptographic libraries for automotive microcontrollers, key exchange protocols for Controller Area Networks, frame scheduling optimization and time-covert authentication, fingerprinting of ECUs using voltage and timing data from the CAN physical layer and a digital twin design and its evaluation for automotive devices and physical fingerprinting. Considering the objectives defined, the major contributions that this thesis brings are:

1) Timing evaluation of elliptic curve operations by integration of cryptographic libraries on an automotive embedded device [12];
2) Implementation and evaluation of the key-exchange protocols that use CAN frames on automotive grade microcontrollers [13];
3) Implementation and evaluation of the frame scheduling optimization algorithms and time-covert channel authentication protocol on automotive grade microcontrollers [14];
4) Data collection of voltage and clock skew data from the CAN bus from 4 passenger vehicles [15];
5) Analysis of voltage and clock skew fingerprints for 9 passenger vehicles [15];
6) Design and implementation of a Digital Twin for a real-world vehicle CAN network using a wiring harness from a car [16];
7) Evaluation of voltage characteristics of wires used in the various experimental setups and wires from a real-world vehicle [17].

These contributions are part of peer-reviewed publications in conference proceedings and journals. The performance of elliptic curve cryptographic primitives on an automotive microcontroller was evaluated in [12]**.** Three software libraries were integrated into the source code project for the microcontroller and evaluated with respect to the duration of cryptographic primitives, e.g., key-generation, signature, verification. Two of these software libraries are implemented in C as the programming language while the third one has both C and C++ implementations. These software libraries are portable to different development environments. Nevertheless, the time required for the execution of the elliptic curve methods can be considered a shortcoming. To circumvent this, four protocols for exchanging cryptographic keys on the CAN bus based on timing characteristics are designed, implemented, and evaluated on an automotive-grade microcontroller in [13]**.** Two of the protocols rely only on the CAN protocol particularities, i.e., data/remote frames and arbitration, while the other two also depend on the internal hardware timers of the microcontroller. An extension that can be applied to these protocols is presented as an option to increase the security level from the low-entropy exchange key as basis for generating a high-entropy session key. The group version of the proposed protocols and their extension is also briefly described.

Considering the timings for Controller Area Network communication and the size limitation of the data field of its frames, an option to implement security protocols is by using timing information relative to the frame transmission and reception. A time-covert authentication channel was already described in [18] and included in the author's Master Thesis. Unfortunately, the performance of the time-covert channel is reduced by un-optimized traffic due to frame arbitration in case frames are transmitted with a low inter-frame time. An improvement that can be considered for the time-covert channel is through optimizing the frame scheduling on Controller Area Networks as later done by the author in [14]. There are four frame scheduling optimization algorithms that are presented in this work, with details related to optimal values for the minimum and maximum inter-frame times. One of the frame scheduling algorithms is analyzed in the context of adversarial models with both optimized and un-optimized traffic and with single or multiple nodes implementing the protocol. The time-covert channel data rate, security level and the impact of the frame scheduling algorithms on the worst-case arrival times are shown.

Even though time-covert channels are a good method for authenticating frames transmitted on the CAN bus, they still carry small amounts of entropy, and their security level is low. Authenticating the frame transmitters is also possible through physical fingerprints that are studied by the authors in [15]. The work presents specific limitations with regards to using physical fingerprints alone, i.e., clock skews or only 1-2 voltage characteristics, and the effects of environmental changes to the initial physical fingerprints. The major contribution of the study is the number of collected and evaluated fingerprints since it is done on 9 passenger vehicles from which 51 ECUs are identified using a dataset of physical samples from ~400 different frame identifiers. The values determined for the clock skews and voltage features are also presented in a supplemental material in the work as well as in this thesis.

Since vehicle-level functionalities are usually tested on an experimental setup, it is recommended that the setup is as close as possible to the real implementation in the car. In this regard, the work from [16] proposes a Digital Twin for automotive Electronic Control Units (ECUs) that communicate on CAN. The contribution of this work is the design of an experimental setup that contains automotive-grade embedded boards connected on a CAN bus that is part of three wiring harnesses that were removed from a real-world vehicle. The evaluation of the Digital Twin models is done as a statistical analysis by comparing its vehicle speed and engine speed outputs with those from a real-world car when providing the same input for both, i.e., brake input. Possible applications for the CarTwin [16] are suggested in the context of cyber-security and functional safety studies. Furthermore, as the results from [17] show, the experimental setup designed for CarTwin [16] can be used for voltage fingerprinting studies. That is, because, compared to other experimental setups from previous works [19]**,** [20] and to real-world conditions [15]**,** the voltage characteristics of the CAN bus from the CarTwin [16] setup are very close to those from the cars.

As a summary of the major contributions, the thesis author has contributed to 16 research papers:

1) **L. Popa**, B. Groza, and P.-S. Murvay, "Performance Evaluation of Elliptic Curve Libraries on Automotive-Grade Microcontrollers", in Proceedings of the 14th International Conference on Availability, Reliability and Security, 2019, pp. 1–7,
2) B. Groza, **L. Popa**, and P.-S. Murvay, "TRICKS—Time TRIggered Covert Key Sharing for Controller Area Networks", IEEE Access, vol. 7, pp. 104 294–104 307, 2019,
3) B. Groza, **L. Popa**, and P.-S. Murvay, "CANTO-Covert AutheNtication with Timing channels over Optimized traffic flows for CAN", IEEE Transactions on Information Forensics and Security, vol. 16, pp. 601–616, 2020,
4) **L. Popa**, B. Groza, C. Jichici, and P.-S. Murvay, "ECUPrint—Physical Fingerprinting Electronic Control Units on CAN Buses Inside Cars and SAE J1939 Compliant Vehicles", IEEE Transactions on Information Forensics and Security, vol. 17, pp. 1185–1200, 2022,
5) **L. Popa**, A. Berdich, and B. Groza, "CarTwin—Development of a Digital Twin for a Real-World In-Vehicle CAN Network", Applied Sciences, vol. 13, no. 1, p. 445, 2022,
6) **L. Popa**, C. Jichici, T. Andreica, P.-S. Murvay, and B. Groza, "Impact of Wiring Characteristics on Voltage-based Fingerprinting in Controller Area Networks", May 2023, accepted for publication at IEEE 17th International Symposium on Applied Computational Intelligence and Informatics (SACI 2023),
7) B. Groza, **L. Popa**, and P.-S. Murvay, "INCANTA-INtrusion detection in Controller Area Networks with Time-covert Authentication" in Security and Safety Interplay of Intelligent Software Systems: ESORICS 2018 International Workshops, ISSA 2018 and CSITS 2018, Barcelona, Spain, September 6–7, 2018, Revised Selected Papers. Springer, pp. 94–110, 2019,
8) P.-S. Murvay, **L. Popa**, and B. Groza, "Accommodating Time-Triggered Authentication to FlexRay Demands", in Proceedings of the Third Central European Cybersecurity Conference, 2019, pp. 1–6.,
9) B. Groza, **L. Popa**, and P.-S. Murvay, "CarINA-Car sharing with IdeNtity based Access control re-enforced by TPM", in Computer Safety, Reliability, and Security:SAFECOMP 2019 Workshops, ASSURE, DECSoS, SASSUR, STRIVE and WAISE, Turku, Finland, September 10, 2019, Proceedings 38. Springer, pp. 210– 222,
10) B. Groza, H. Gurban, **L. Popa**, A. Berdich, and S. Murvay, "Car-to-Smartphone Interactions: Experimental Setup, Risk Analysis and Security Technologies", in 5th International Workshop on Critical Automotive Applications: Robustness \& Safety, 2019,
11) B. Groza, **L. Popa**, and P.-S. Murvay, "Highly Efficient Authentication for CAN by Identifier Reallocation With Ordered CMACs", IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 6129–6140, 2020,
12) 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,
13) Groza, **L.Popa**, P.-S. Murvay, Y. Elovici, and A. Shabtai, "CANARY-a reactive defense mechanism for Controller Area Networks based on Active RelaYs.", in USENIX Security Symposium, pp. 4259–4276, 2021,
14) P.-S. Murvay, **L. Popa**, and B. Groza, "Securing the Controller Area Network with covert voltage channels", International Journal of Information Security, vol. 20, no. 6, pp. 817–831, 2021,

15) B. Groza, P.-S. Murvay, **L. Popa**, and C. Jichici, "CAN-SQUARE-Decimeter Level Localization of Electronic Control Units on CAN Buses", in Computer Security – ESORICS 2021: 26th European Symposium on Research in Computer Security, Darmstadt, Germany, October 4–8, 2021, Proceedings, Part I 26. Springer, pp. 668–690,
16) B. Groza, **L. Popa**, T. Andreica, P.-S. Murvay, A. Shabtai, and Y. Elovici, "PanoptiCANs - Adversary-Resilient Architectures for Controller Area Networks", in Computer Security–ESORICS 2022: 27th European Symposium on Research in Computer Security, Copenhagen, Denmark, September 26–30, 2022, Proceedings, Part III. Springer, pp. 658–679.

The thesis examines various security applications and their evaluation for Controller Area Networks. The security applications utilize the physical layer for cryptographic key-exchange, sender and frame authentication and transmitter fingerprinting. These applications are either compared with existing proposals by emphasizing the performance improvements or analyzed in the context of existing related works from the literature.

Chapter 2 presents the background of Controller Area Network communication with details for the CAN physical layer, bit encoding, types of frames that are used as well as some information related to stuffing bits. The transmission lines that are used by sensors and actuators from vehicles to exchange signals as well as the voltage levels that correspond to the bits that are transmitted as well as the maximum baud rate are presented at the beginning of the chapter. An example of bits transmitted on the CAN lines is shown in Figure 2 for bits that are sent with a baud rate of 500Kbps (bit time of 2µs) which is commonly used in vehicles. The structure of standard and extended CAN frames related to the bit order and corresponding states for the frame header, frame payload, checksum and acknowledgement bit fields are discussed. In what follows from the same chapter, the error frames and error states for Controller Area Networks are presented with regards to the failures that are reported during CAN communication, e.g., bit errors, checksum errors or stuffing bit errors. The requirements related to stuffing bits as well as other aspects regarding CAN communication are discussed at the end of the second thesis chapter.

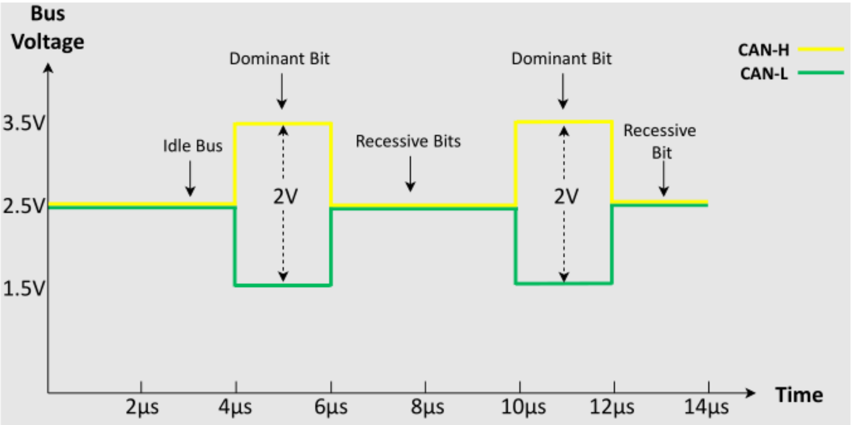

Fig. 2. Bit states and voltage levels for CAN lines on a CAN bus with the bit time of 2µs

Chapter 3 presents a time-covert key exchange mechanism for the Controller Area Networks. The chapter begins with a presentation of the computational cost with regards to timing if only software-based elliptic curve cryptography is utilized for key exchange or digital signatures on Controller Area Networks. Evaluation of software execution time for the Elliptic

Curve Diffie-Hellmann (ECDH) key exchange and Elliptic Curve Digital Signature Algorithms (ECDSA) is performed on an automotive grade microcontroller from the AURIX family produced by Infineon. The experimental results are compared between three open-source libraries which provide the implementation of the primitives for the evaluated elliptic curve security algorithms. Nevertheless, the ECDH key exchange requires multiple CAN frames to be transmitted until the key negotiation is performed. In what follows from the same chapter, a time-covert key-exchange protocol between two CAN nodes is described, after the background and related studies are discussed. The evaluation platform used for the protocol evaluation is also presented before the protocol. The key-exchange protocol has four different key exchange methods proposed. The first one is Data vs. Remote frame negotiation which is based on the arbitration procedure on the physical layer of the CAN bus between randomly transmitted as data frame or remote frames, with the same identifier, at fixed time intervals. The next key exchange method is Minimax Negotiation that is also based on the arbitration procedure but requires data frames to be transmitted with random identifiers, at fixed time slots, as shown in Figure 3. The following key exchange method is the Time-Triggered Minimax Negotiation which is based on both random identifiers and random time slots inside the same time interval. The last method is the Randomized Time-Triggered Key Exchange that is based on a specified number of frames and random time slots when these frames are transmitted. All key exchange methods are compared with respect to three characteristics. These are the probability that a frame can be used for extraction of a bit from the session key, the mean entropy, and the time it takes to execute the method. Since the shared secret resulting from the key exchange has a lower entropy than the key normally used in cryptographic protocols, an extension of the last two methods is proposed using the Simple Password Exponential Key Exchange (SPEKE) protocol. The multi-party version of the proposed methods or their extension is described at the end of this chapter.

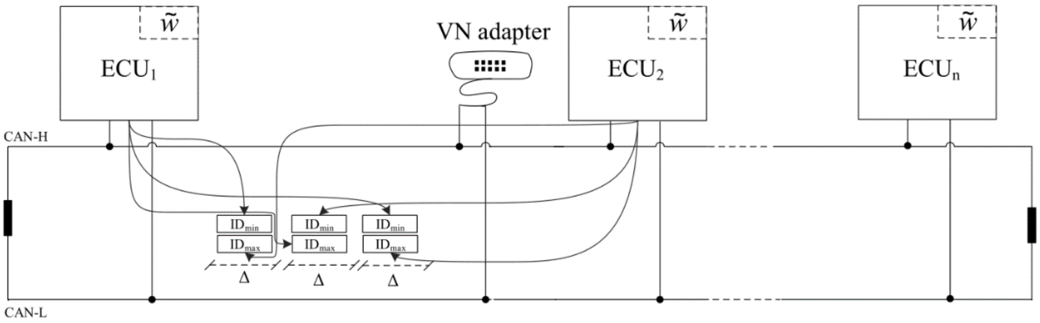

Fig. 3. Structure of the CAN bus and addressed scenario for time-triggered key exchange

Chapter 4 presents a time-covert authentication protocol on the Controller Area Networks that is improved through frame scheduling optimization. In the first part of the chapter, the background and related studies are discussed together with limitations from existing works that are overcome with the proposal discussed in the next sections. The worst-case arrival times for CAN frames are discussed as a theoretical background that is practically evaluated using the frame arrival times from real vehicle times. Considering the delays that one CAN frame may have from the expected transmission time to the time it is actually sent and, in the end, received by the other nodes, the frame scheduling optimization is proposed to overcome these findings.

As input for the frame scheduling optimization, there is a dataset defined that contains all the frame identifiers, their cycle times and the time offset that is added to the cycle time for each frame identifier. The evaluation platform which consists of an automotive device for CAN communication and an embedded device is described before the algorithms are discussed. There are four scheduling optimization algorithms which are described as part of this chapter. The first one is the Binary Symmetric Allocation algorithm which is simple to determine and integrate but has some timing issues in the practical implementation compared to the theoretical distribution caused by small inter-frame spaces. The second is the Randomized Search Allocation algorithm that, even though it has an increased inter-frame space compared to the first algorithm, it still has timing issues in the practical implementation. The next one is the Greedy Allocation algorithm which is described both in single layer and multi-layer variants. The Multi-Layer Greedy variant allows an inter-frame space that is two times the one from the single-layer Greedy Allocation or the Randomized Search Allocation. The experimental results for Multi-Layer Greedy implementation are those expected from the theoretical distribution. The last algorithm is the GCD-based Allocation which allows the same inter-frame space as the Multi-Layer Greedy Allocation. Thereby, its practical implementation follows the theoretical distribution with no deviations. Each algorithm is evaluated based on the minimization of a quality factor that depends on the optimization of inter-frame spacing and the minimum value of the inter-frame space. After the frame scheduling optimization algorithms are described, the time-covert authentication protocol from a previous work [18] is presented together with the adversary model that is considered for its evaluation. The evaluation of the time-covert authentication protocol is done in different scenarios. The first scenario is based on optimized traffic and a single sender. The next scenario is based on both optimized and unoptimized traffic with multiple senders. The scenario with optimized traffic and two senders is shown in Figure 4. In the case of multiple senders, there are additional actions proposed to improve the performance of the time-covert channel. These are the re-synchronization of the transmitters time and the de-skewing of their clocks. The channel data rate and security level of the time-covert authentication protocol is described at the end of the second section. The final section of this chapter presents the comparison of the time-covert channel with frame scheduling optimization with related studies.

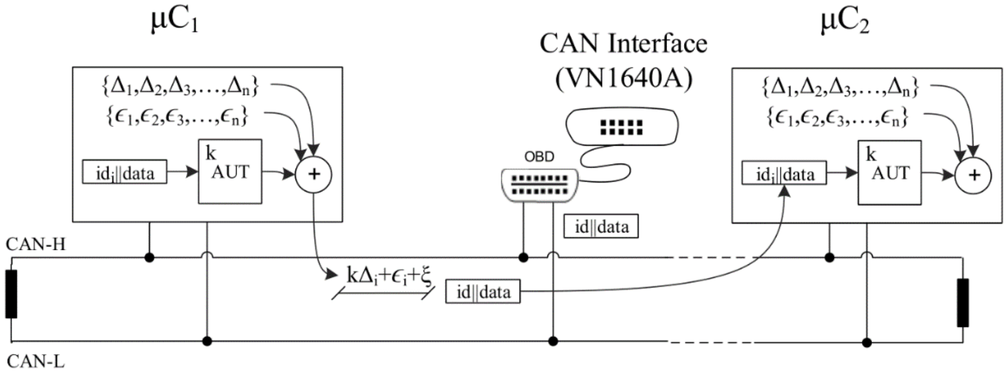
μC_1
CAN Interface (VN1640A)
μC_2
$\{\Delta_1,\Delta_2,\Delta_3,\ldots,\Delta_n\}$
$\{\epsilon_1,\epsilon_2,\epsilon_3,\ldots,\epsilon_n\}$
$id_i||data$
k AUT
+
OBD
id||data
$\{\Delta_1,\Delta_2,\Delta_3,\ldots,\Delta_n\}$
$\{\epsilon_1,\epsilon_2,\epsilon_3,\ldots,\epsilon_n\}$
$id_i||data$
k AUT
+
CAN-H
$k\Delta_i+\epsilon_i+\xi$
id||data
CAN-L

Fig. 4. Structure of the CAN bus and addressed scenario for time-covert authentication using optimized traffic in case of multiple senders

Chapter 5 presents a physical fingerprinting approach for Electronic Control Units (ECUs) that communicate on the Controller Area Networks inside real-world vehicles, as also shown in Figure 5. The first section of this chapter contains details related to existing works that perform either timing-based or voltage-based fingerprinting for nodes connected on CAN buses. The summary of the data collection framework, the data collected by the thesis author as well as a comparison between clock skews and voltage features for ECU fingerprinting are also shown as part of this section. The following section details the theoretical framework for computing clock skews and voltage features that are extracted from the sample data that is collected from several passenger vehicles. There are four voltage features which are determined for each frame identifier. The voltage features that are used in what follows are the mean and maximum voltages from the plateau area of a dominant bit, the bit time and the plateau time. For the separation of IDs from the same ECU or from different ECUs, the intra-distances and inter-distances are also defined using the Euclidian distance. The final section of this chapter details the values that are obtained for each passenger vehicle and emphasizes the limitations in case only one physical characteristic is used. The separation is done based on the feature values determined from the data collected for each frame identifier. The frame identifiers are separated into ECUs based on the voltage features and the resulting clock skews. There are 51 ECUs identified using physical characteristics from 9 passenger vehicles based on data collected for close to 400 frame identifiers. For some vehicles, the clock skew determination was somehow problematic since the variation of reception time was inconsistent. In the dataset collected for Dacia Logan, there are two ECUs separated based on voltage features which have a clock skew difference of only 1ppm (part per million). The inter-distances and intra-distances show separations between IDs from the same ECU or from different ECUs but there are multiple collisions in case only one physical feature is used. When all voltage features are combined, the number of collisions is reduced, and the separation becomes very clear. The environmental influence on physical fingerprinting is the last topic discussed in this chapter. Based on data collected after startup and after 1 hour drive from two vehicles, both timing and voltage-based characteristics are evaluated with respect to changes over time. Since the changes are both positive and negative meaning that the values have either increased or decreased over time, the environmental impact on physical fingerprinting cannot be generalized. This is why updates of fingerprints need to be performed to keep the collected values as close as possible to the expected data.

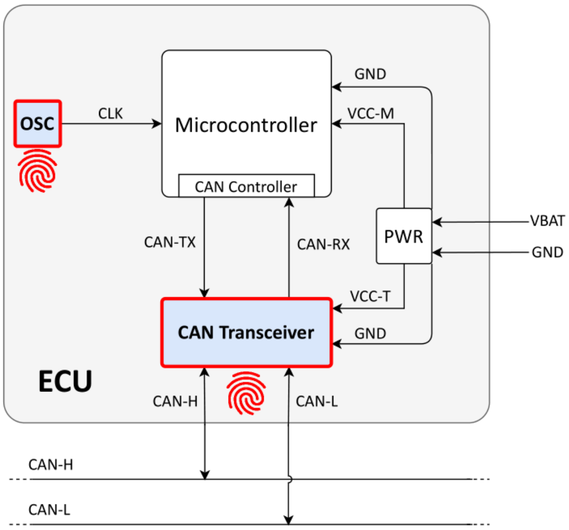

Fig. 5. Internal block diagram of an automotive ECU with architectural components required for CAN communication used for physical fingerprinting

Chapter 6 presents a digital twin for a real-world vehicle Controller Area Network. The first section of this chapter starts with the presentation of the motivation for the design of the digital twin for a CAN bus as well as the related studies. The digital twin is based on ECU models deployed on automotive grade boards that are physically connected to a CAN bus. The

CAN bus is preserved from existing wiring harnesses that were removed from a real-world vehicle. The Electronic Control Units (ECUs) from the real-world vehicle connected to the physical CAN bus were determined from a wiring handbook diagram. The physical wiring from the real-world vehicle is also described with respect to the wiring length and number of stubs. After the physical medium for the CAN bus is described, the design and validation aspects for the ECU models that were performed in MATLAB/Simulink are presented. The ECUs which are modeled and described are the Accessory Protocol Interface Module (APIM), Power Steering Control Module (PSCM), Instrument Panel Cluster (IPC), Remote Function Actuator (RFA), Restraints Control Module (RCM), Anti-lock Brake System (ABS) and Powertrain Control Module (PCM) as also shown in Figure 6.

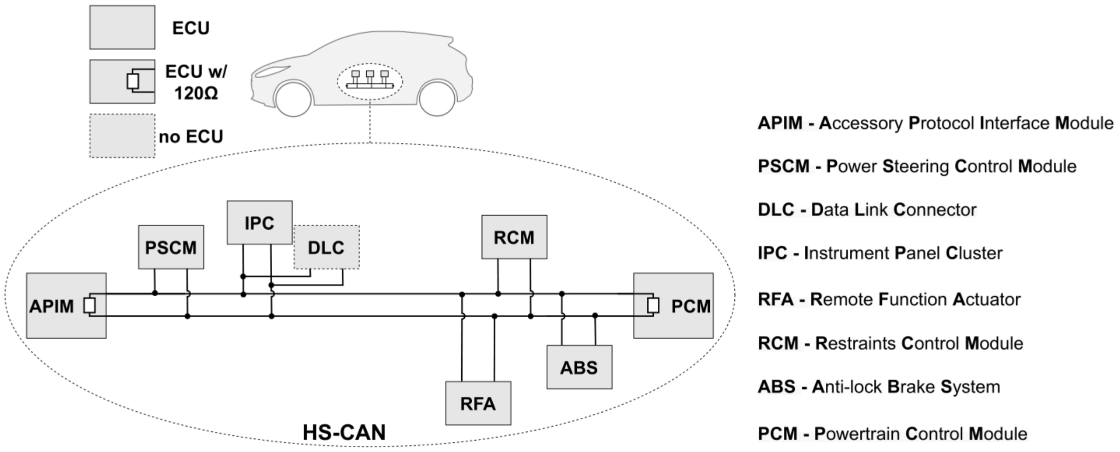
ECU
ECU w/ 120Ω
no ECU
PSCM
IPC
DLC
RCM
APIM
PCM
ABS
RFA
HS-CAN
APIM - Accessory Protocol Interface Module
PSCM - Power Steering Control Module
DLC - Data Link Connector
IPC - Instrument Panel Cluster
RFA - Remote Function Actuator
RCM - Restraints Control Module
ABS - Anti-lock Brake System
PCM - Powertrain Control Module

Fig. 6. Schematic view of the in-vehicle high-speed CAN bus that are used for the digital twin network

The ECU models were afterwards deployed on automotive-grade microcontrollers from the AURIX family that are produced by Infineon. The development of a C#-based tool that provides specific vehicle level signals required by some of the ECU models is also described in this section. The integration of the models on the embedded devices was done by verifying the outputs from the CAN bus with those from the modelling tool having the same input arrays provided for both. Afterwards, the vehicle speed and engine speed provided by the digital twin models are compared with the vehicle speed and engine speed from a real-world vehicle. The input that is provided to the digital twin model is the brake status that reduces the vehicle speed and engine speed, if applied. There are two driving conditions which are compared, the local roads and the highway. A statistical comparison is performed by showing the differences and correlation coefficients for vehicle speed from the model and the vehicle trace. Possible applications for the digital twin model as well as a brief comparison with related works are shown in what follows. The second section addresses the wiring impacts on voltage fingerprints performed on Controller Area Networks. Several related works are presented before the data collection tool configuration is described. The wiring impacts are evaluated using datasets from three experimental setups with different wirings and a dataset collected from a real-world vehicle. The characteristics which are evaluated are the slew rate for a rising edge, for a dominant bit, the peak-to-peak value on the bit plateau area and the peak-to-root mean square value on the same area. Considering the differences between the wirings used in experimental setups and the real-world vehicle, it seems that automotive cables are highly recommended to be used for testbeds where the intention is to collect voltage samples for fingerprinting the nodes that communicate on the CAN bus. If other wiring types are used, additional noise that may be induced by the cables would have a negative impact on the fingerprinting results.

To summarize, this thesis presents various methods for securing the Controller Area Network that can be implemented on automotive-grade embedded devices, from time-covert authentication protocols, which benefit from frame scheduling optimization to physical device fingerprinting using time and voltage characteristics. An experimental setup which is realized as a digital twin for a real-world vehicle Controller Area Network is also described. The wiring impact from this experimental setup is evaluated in the context of voltage-based fingerprinting, a relevant topic for transmitter identification and intrusion detection in Controller Area Networks. There are still many open questions regarding the use of physical layer security on CAN buses which can serve as future works. With regards to time-covert authentication channels, an open research topic is related to the maximum data-rate that can be retrieved from such channels. If voltage or timing characteristics are used as fingerprints for CAN transmitters, their stability over time and the impact of the ECUs' voltage supply are future research directions. Since digital twins are an emerging topic in the automotive areas, they can be further used for studies of CAN safety and cybersecurity in the automotive context. Automotive digital twins clearly need much more exploration at the current time since only a few papers about them were published so far.

REFERENCES

[1] K. Koscher, A. Czeskis, F. Roesner, S. Patel, T. Kohno, S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham et al., “Experimental Security Analysis of a Modern Automobile,” in *2010 IEEE Symposium on Security and Privacy*. IEEE, 2010, pp. 447–462.

[2] S. Checkoway, D. McCoy, B. Kantor, D. Anderson, H. Shacham, S. Savage, K. Koscher, A. Czeskis, F. Roesner, T. Kohno et al., “Comprehensive Experimental Analyses of Automotive Attack Surfaces.” in *USENIX Security Symposium*, San Francisco, 2011.

[3] *Specification of Secure Onboard Communication*, 4.2.2 edition, AUTOSAR, 2014.

[4] M. Wille, “Automotive security—an overview of standardization in AUTOSAR,” *VDI/VW-Gemeinschaftstagung Automotive Security*, 2015.

[5] A. Hazem and H. Fahmy, “LCAP - A Lightweight CAN Authentication Protocol for Securing In-Vehicle Networks,” in *10th escar Embedded Security in Cars Conference*, Berlin, Germany, vol. 6, 2012, p. 172.

[6] B. Groza, P.-S. Murvay, A. Van Herrewege, and I. Verbauwhede, “LiBrA-CAN: a Lightweight Broadcast Authentication protocol for Controller Area Networks,” in *11th International Conference on Cryptology and Network Security, CANS 2012*, Springer-Verlag, LNCS, 2012.

[7] A.-I. Radu and F. D. Garcia, “LeiA: a lightweight authentication protocol for CAN,” in *European Symposium on Research in Computer Security*. Springer, 2016, pp. 283–300.

[8] B. Groza, L. Popa, and P.-S. Murvay, “Highly Efficient Authentication for CAN by Identifier Reallocation with Ordered CMACs,” *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 6129–6140, 2020.

[9] K. Han, A. Weimerskirch, and K. G. Shin, “A practical solution to achieve real-time performance in the automotive network by randomizing frame identifier,” *Proc. Eur. Embedded Secur. Cars (ESCAR)*, pp. 13–29, 2015.

[10] A. Humayed and B. Luo, “Using ID-hopping to defend against targeted DoS on CAN,” in *Proceedings of the 1st International Workshop on Safe Control of Connected and Autonomous Vehicles*. ACM, 2017, pp. 19–26.

[11] “CAN Injection: keyless car theft,” https://kentindell.github.io/2023/04/03/can-injection/, 2023

[12] L. Popa, B. Groza, and P.-S. Murvay, “Performance Evaluation of Elliptic Curve Libraries on Automotive-Grade Microcontrollers,” in *Proceedings of the 14th International Conference on Availability, Reliability and Security*, 2019, pp. 1–7.

[13] B. Groza, L. Popa, and P.-S. Murvay, “TRICKS—Time TRIggered Covert Key Sharing for Controller Area Networks,” *IEEE Access*, vol. 7, pp. 104294–104307, 2019.

[14] B. Groza, L. Popa, and P.-S. Murvay, “CANTO-Covert AutheNtication with Timing channels over Optimized traffic flows for CAN,” *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 601–616, 2020.

[15] L. Popa, B. Groza, C. Jichici, and P.-S. Murvay, "ECUPrint—Physical Fingerprinting Electronic Control Units on CAN Buses Inside Cars and SAE J1939 Compliant Vehicles", *IEEE Transactions on Information Forensics and Security*, vol. 17, pp. 1185–1200, 2022

[16] L. Popa, A. Berdich, and B. Groza, “CarTwin—Development of a digital twin for a real-world in-vehicle CAN network,” *Applied Sciences*, vol. 13, no. 1, p. 445, 2022.

[17] L. Popa, C. Jichici, T. Andreica, P.-S. Murvay, and B. Groza, “Impact of Wiring Characteristics on Voltage-based Fingerprinting in Controller Area Networks,” May 2023, *IEEE 17th International Symposium on Applied Computational Intelligence and Informatics (SACI 2023)*.

[18] B. Groza, L. Popa, and P.-S. Murvay, “INCANTA – Intrusion detection in Controller Area Networks with Time-covert Cryptographic Authentication,” in *Security and Safety Interplay of Intelligent Software Systems: ESORICS 2018 International Workshops, ISSA 2018 and CSITS 2018, Barcelona, Spain, September 6–7, 2018, Revised Selected Papers*. Springer, 2019, pp. 94–110.

[19] P.-S. Murvay and B. Groza, “TIDAL-CAN: Differential Timing based Intrusion Detection And Localization for Controller Area Network,” *IEEE Access*, vol. 8, pp. 68895–68912, 2020.

[20] B. Groza, P.-S. Murvay, L. Popa, and C. Jichici, “CAN-SQUARE - Decimeter Level Localization of Electronic Control Units on CAN Buses,” in *Computer Security–ESORICS 2021: 26th European Symposium on Research in Computer Security, Darmstadt, Germany, October 4–8, 2021, Proceedings, Part I 26*. Springer, 2021, pp. 668–690.