Intrusion Detection Systems on CAN Buses for Commercial Vehicles with SAE J1939 Compliant Communication

PhD thesis - Summary
for obtaining the Scientific Title of PhD in Engineering from
Politehnica University Timișoara
in the Field of Computer and Information Technology
by
Eng. Camil-Vasile Jichici
PhD Supervisor: Prof. Dr. Eng. Bogdan Groza
September, 2023

Millions of heavy-duty vehicles travel hundreds of kilometers on highways every day and the likelihood of incidents increases, hence constantly boosting the safety of the traffic participants is crucial. Regarding safety, several improved driver assistance systems, including forward collision warning, lane departure warning, alcohol ignition interlock devices, autonomous emergency braking and blind-spot recognition, have been developed over the past ten years. The ability of vehicles to drive autonomously, without human involvement, is a short-term goal that is especially important in the context of heavy-duty vehicles because of the significantly larger distances they must travel. To fulfill these features, heavy-duty vehicles are also turning into intricate cyber-physical systems with millions of lines of code running through dozens of Electronic Control Units (ECUs) and a variety of sensors, actuators, cameras, and radars. In-vehicle ECUs currently communicate with one another over a variety of communication interfaces, including the traditional Controller Area Network (CAN), FlexRay, and the more recent 100BaseT1 Ethernet, which supports substantially higher communication speeds. However, in spite of recent advancements, CAN is still by far the most widely employed communication medium since it offers a very good cost-performance ratio and a reliable solution for the majority of real-time applications. Two updated versions of it, i.e., CAN-FD [1] as well as CAN-XL [2] enable much higher bit rates and larger payloads, which ensure the longevity of the CAN protocol for the future decades.

On the other hand, due to the increase of software-driven features, connectivity and semi-automated functions, vehicles become vulnerable to cybersecurity attacks. As a result, several attacks were reported by the researchers in various publications, e.g., [3], [4], and [5]. These adversarial interventions may have catastrophic effects for both vehicle occupants and traffic participants alike. Koscher et. al. [3] show that by mounting CAN bus attacks on real world vehicles it is possible to take the control of several critical automotive functions while completely ignoring the driver input. Examples of such actions include disabling the brakes, unlock the car, stopping the engine, etc. Due to the fact that the attacks demonstrated in [3] require a physical connection to the CAN bus, their impact may be more limited. But in addition to this, the same authors proved in a subsequent work [4] that similar attacks can be conducted remotely by establishing a connection with mechanics tools or infotainment units using wireless interfaces such as Bluetooth or WiFi. A comprehensive research on attack surfaces is also provided by Miller and Valasek in [5].

Regardless of the attack access point, the lack of security of the CAN bus, which was introduced by BOSCH in the 80s [6], is the root cause for the previously mentioned attacks. The SAE J1939 standard [7], developed by the Society of Automotive Engineers in the 90s, is dedicated to CAN communication within heavy-duty vehicles and complements the conventional CAN bus protocol by introducing specific features which are detailed in Chapter III. Since the SAE J1939 CAN protocol is built on top of the standard CAN protocol, similar attacks to those previously described can also be mounted on J1939 compliant CAN buses. A first example of such attacks on J1939 CAN buses was proposed in [8]. Burakova et al. [8] demonstrate by practical experiments on two J1939 compliant vehicles (a semi-tractor as well as a school bus), that safety-critical attacks, e.g., truck acceleration while it is moving, turning off the engine brake, can be mounted through J1939 specific diagnostic port. The authors from [9] are the first that address attacks on the SAE J1939 specific transport protocols and demonstrate a DoS attack that targets multi-packet transmissions. A setup in which the adversary is connected to a J1939 compliant CAN bus and has the ability to intercept and inject malicious frames inside a heavy-duty vehicle via the J1939 specific OBD port is depicted in Figure 1.

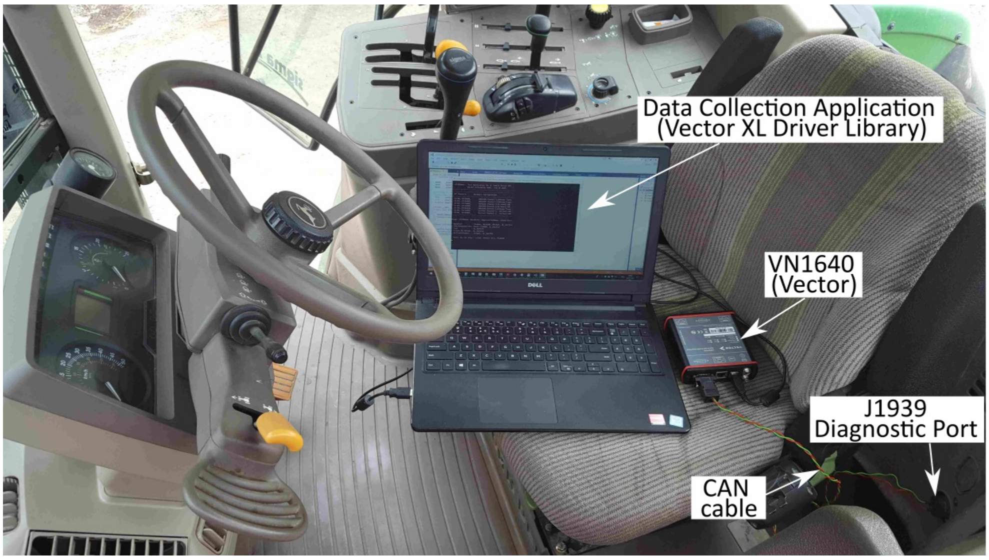


Fig. 1. A typical heavy-duty vehicle implementing the SAE J1939 standard and tools for data collection of the CAN traffic

Considering the concerns for the protection of numerous passengers (inside buses), or goods (inside heavy-duty trucks), the security solutions employed in the commercial vehicle sector require a special attention. The motivation behind this thesis comes in the light of the above. In this respect, this thesis pursues the deployment of intrusion detection systems tailored to J1939 CAN buses.

Research objectives. The primary research objective is the deployment of intrusion detection systems (IDSs) customized to SAE J1939 protocol, which is built on top of the CAN protocol and defines the upper layers from the communication stack, e.g., data link layer, network management layer, etc., for implementing in-vehicle functionalities over CAN buses. But before moving to J1939 specific solutions, some investigations on intrusion detection mechanism and their integration for regular CAN bus traffic is also necessary. More precisely, the major research objectives of this thesis, can be summed up as follows:

1) Review of the literature on relevant works for intrusion detection on CAN buses;
2) CAN traffic extraction from real-world passenger cars as well as J1939 compliant vehicles for experimental purposes;
3) Performance assessment of machine learning algorithms as candidates for IDS on CAN buses as well as the feasibility of using such detection mechanisms in real-life vehicular applications;
4) Design and implementation of a framework which allows for the simulation of adversarial models and intrusion detection in CANoe;
5) Design and implementation of an intrusion detection and prevention system targeting J1939 CAN buses;
6) Analysis of attacks performed at the control system level on J1939 compliant CAN buses and the design of the appropriate countermeasures.

Major contributions. An overview of the contributions of this thesis is provided in this section. This thesis discusses several IDS approaches for CAN buses, with a focus on J1939 compliant CAN buses in particular. In light of the stated research objectives, the contributions of the author can be summed up as follows:

1) CAN traffic was collected by the author from several vehicles, specifically, 427,660 CAN frames collected from a heavy duty-vehicle in motion that is compliant to SAE J1939 communication [10] and was directly used for the experiments in this thesis;
2) CAN traffic was also collected by the author for several works which he co-authored or partly used in his papers as a first author, specifically, 2,488,248 CAN frames collected from three different Dacia Dusters [11], [12]; 2,783,265 CAN frames and 90,723 voltage bit samples collected from 5 passenger cars [13]; 154,779 CAN frames and 4,021 voltage bit samples collected from a heavy duty vehicle compliant to SAE J1939 communication [13];
3) Evaluation of neural networks in detecting intrusions on CAN as well as their computational performance on automotive embedded platforms [14];
4) Implementation and testing of a framework that allows the integration of adversary models and intrusion detection systems in an industry standard environment, i.e., CANoe [11];
5) Deployment of an intrusion detection and prevention system tailored to meet J1939 specifications. To demonstrate the correctness as well as the feasibility of using the suggested solution in real-world vehicles, a proof-of concept implementation in a laboratory setup is provided [10];
6) A special implementation for decoding the content of CAN frames before the receivers have set the acknowledgment bit. This makes it possible to instantly discard the intrusions with no need for specialized hardware [10];
7) A proposal for a detection mechanism on attacks performed at the control system level that are challenging to be detected by a traditional IDS [15];
8) Development of an experimental setup that connects the two most widely used tools in industry, CANoe for the simulation of in-vehicle networks and MATLAB for control system design, respectively [15].

These contributions are outlined by a number of scientific articles published in different journals and conference proceedings as well. The application of neural networks as possible candidates for IDSs in CAN was explored by the author in [14]. The majority of the experiments were carried on traces from a J1939 simulation and a small part of them were performed on other public datasets. The runtime of the detection algorithm was evaluated on three automotive embedded platforms in order to determine whether the proposed solution could be used in real-world scenarios. One of the platforms represents the low-end device group, while the other two are high-end device candidates. Given the fact that the attacks on J1939 CAN traffic from [14] were generated using a C# script, a more realistic scenario would be to use real-world CAN traffic and to augment it with injections using a CANoe simulation. Because of this, the author analyzes this scenario in [11] where a framework is offered to replay the CAN traffic collected from actual vehicles and permit the integration of adversary models along with detection systems inside a CANoe-based simulation. The k-NN classifier was investigated as a candidate for IDS in this work [11], although the framework was designed to support any other IDS method. The next two papers of the author [10], [15] address IDS in the context of the SAE J1939 CAN buses. In the first one [10], the author proposes a two-stage IDS complemented by a prevention mechanism. In the first stage, the validity of the encrypted addresses is verified. The second stage performs appropriate range checks to identify single bit changes in the payload. Since the payloads of CAN messages are encrypted, the avalanche effect of block ciphers makes it easier to spot adversary interventions. The prevention mechanism requires the decoding of each CAN message (ID and payload) before the receivers confirm the correct reception by overwriting a dominant bit in the ACK slot. Then, if the current CAN frame is regarded as intrusion, it is then discarded by forcing an error frame. To demonstrate the practical applicability of the solution, a proof-of concept implementation on high-end in-vehicle controllers is provided. Last but not least, in [15], the author examines attacks on J1939 CAN buses mounted at control system level and proposes a detection mechanism for such adversarial manipulation. Additionally, this research shows how poorly the machine learning based IDSs performs in identifying these kind of subtle payload alterations and that change detection mechanisms are far more effective.

In addition to the aforementioned research papers, which represent the core of this thesis, the author has been involved in several other research papers, five of which, are also related to automotive cybersecurity and one which addresses mobile device pairing based on the environmental data. Concretely, an efficient approach for localizing the CAN network nodes based on propagation delays of physical CAN signals has been investigated in [16]. Two physical connections, one at either end of the bus, and merely one rising edge are required to examine the propagation delays. In this work, the author has contributed with voltage data collection based on a laboratory setup as well as with the preparation of the data collection setup inside a real vehicle, i.e., Renault Megane. A comparative performance between Android head units and automotive graded controllers for the deployment of several binary classifiers as candidates for IDSs is discussed in [12]. The author's contribution to this work accounts for the CAN traffic collection from a real-world SUV, i.e, Dacia Duster as well as for the augmentation of the collected traffic with specific attacks inside a CANoe based simulation. Another work which is under submission addresses a concept for a cloud-based IDS that makes use of the cloud infrastructure and the computationally powerful Android head units employed in current vehicles. The concept also includes an incident response team that performs additional evaluation of the detection results and the final outcome of this is recorded on the Blockchain as reports that comply with the ISO/SAE 21434 standard [17]. Here the CAN traffic was collected from three different Dacia Duster vehicles in order to demonstrate the transfer learning capability of the proposed IDS. Physical fingerprinting of the electronic control units (ECUs) based on clock skews and voltage data is proposed in [13]. The performed analysis led to the identification of 54 ECU fingerprints. An extensive dataset, including skew and voltage data collected from 9 passenger cars and a J1939 compliant vehicle as well, was used for the evaluation. The data collected from 5 out of 9 passenger cars and from the J1939 heavy-duty vehicle were collected by the author. The author also contributed to a paper where the influence of wiring characteristics on CAN voltage fingerprints is investigated [18]. As a result of this research, it has been determined that CAN networks that rely on commercial or industrial cables have higher noise and slew rates than those that rely on automotive graded cables. Last but not least, the author was a member of the PRESENCE project were he also contributed to a work that addresses the secure device pairing under multi-modal transport based on environmental data, i.e, accelerometer data [19].

Overall, the author has contributed to 10 scientific articles, out of which 9 are focused on automotive security and one is related to secure pairing of mobile devices based on accelerometer data:

1) Camil Jichici, Bogdan Groza, and Pal-Stefan Murvay, “Examining the Use of Neural Networks for Intrusion Detection in Controller Area Networks”, Innovative Security Solutions for Information Technology and Communications: 11th International Conference, SecITC 2018, Bucharest, Romania, November 8–9, 2018, Springer International Publishing, 2019,
2) Camil Jichici, Bogdan Groza, and Pal-Stefan Murvay, “Integrating Adversary Models and Intrusion Detection Systems for In-Vehicle Networks in CANoe”, Innovative Security Solutions for Information Technology and Communications: 12th International Conference, SecITC 2019, Bucharest, Romania, November 14–15, 2019, Springer International Publishing, 2020,
3) Camil Jichici, Bogdan Groza, Radu Ragobete, Pal-Stefan Murvay and Tudor Andreica, “Effective intrusion detection and prevention for the commercial vehicle SAE J1939 CAN bus”, IEEE Transactions on Intelligent Transportation Systems, vol. 13, pp. 17425-17439, 2022,
4) Camil Jichici, Adriana Berdich, Adrian Musuroi, and Bogdan Groza, “Control System Level Intrusion Detection on J1939 Heavy-Duty Vehicle Buses”, IEEE Transactions on Industrial Informatics, 2023,
5) Bogdan Groza, Lucian Popa, Pal-Stefan Murvay and Camil Jichici, “CAN-SQUARE-Decimeter Level Localization of Electronic Control Units on CAN Buses”, Computer Security–ESORICS 2021: 26th European Symposium on Research in Computer Security, Darmstadt, Germany, October 4–8, 2021, Springer International Publishing,
6) Lucian Popa, Bogdan Groza, Camil Jichici, and Pal-Stefan 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,
7) Tudor Andreica, Christian-Daniel Curiac, Camil Jichici, and Bogdan Groza, “Android Head Units vs. In-Vehicle ECUs: Performance Assessment for Deploying In-Vehicle Intrusion Detection Systems for the CAN Bus,” IEEE Access, vol. 10, pp. 95161–95178, 2022,
8) Lucian Popa, Camil Jichici, Tudor Andreica, Pal-Stefan Murvay and Bogdan Groza, “Impact of Wiring Characteristics on Voltage-based Fingerprinting in Controller Area Networks”, IEEE 17th International Symposium on Applied Computational Intelligence and Informatics (SACI 2023), 2023,
9) Tudor Andreica, Adrian Musuroi, Alfred Anistoroaiei, Camil Jichici and Bogdan Groza, “Blockchain Integration for in-Vehicle CAN Bus Intrusion Detection Systems with ISO/SAE

21434 Compliant Reporting", **(under submission)**,

10) Bogdan Groza, Adriana Berdich, Camil Jichici, and Rene Mayrhofer, "Secure Accelerometer-Based Pairing of Mobile Devices in Multi-Modal Transport", IEEE Access, vol. 8, pp. 9246–9259, 2020.

This thesis investigates various intrusion detection systems for CAN buses with a focus on the SAE J1939 heavy-duty vehicle deployments. The approaches utilized for the deployment of these IDSs range from the use of machine learning algorithms to hindering adversaries by the use of symmetric cryptography or making a fine grained analysis at the control systems level. The majority of the results from this thesis are based on real-world CAN traffic that was collected by the author either from a commercial vehicle (a modern agricultural machinery) or from passenger cars (a sedan or SUV). Part of the results are based on traces generated directly from the CANoe, an industry-standard tool that is widely used in the implementation of in-vehicle networks. To test and demonstrate that the detection mechanisms are suitable for real-world deployment inside vehicles, several measurements on their runtime are performed on automotive devices, i.e., in-vehicle controllers. Moreover, the performance results in detecting intrusions obtained using the proposed solutions are compared with the ones reported by the related works on intrusion detection for CAN buses in order to highlight the advantages offered by them. A brief overview of each chapter follows, also highlighting some of the significant findings.

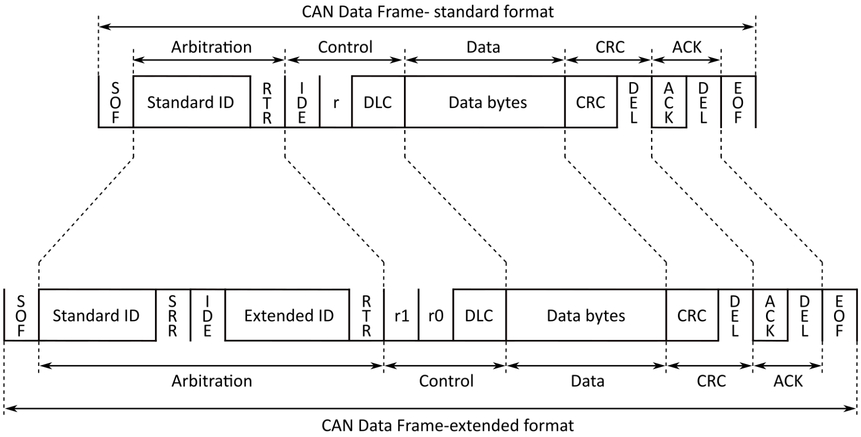


Fig. 2. Standard and extended CAN data frame structure

Chapter II presents a comprehensive literature review on security solutions proposed for the CAN buses, with a focus on intrusion detection systems and J1939 compliant CAN buses. Finally, this chapter introduces the following metrics: true positive rate (TPR), true negative rate (TNR), false positive rate (FPR), false negative rate (FNR), accuracy and precision. These are needed to evaluate the effectiveness of the proposed security solutions in detecting intrusions.

Chapter III provides a brief description of the CAN protocol, focusing on the SAE J1939 compliant CAN buses. An overview of the CAN physical layer, as well as the structure of the data frame, are detailed. The standard and extended formats of a CAN data frame are depicted in Figure 2. This chapter continues with an overview of the SAE J1939 specifics

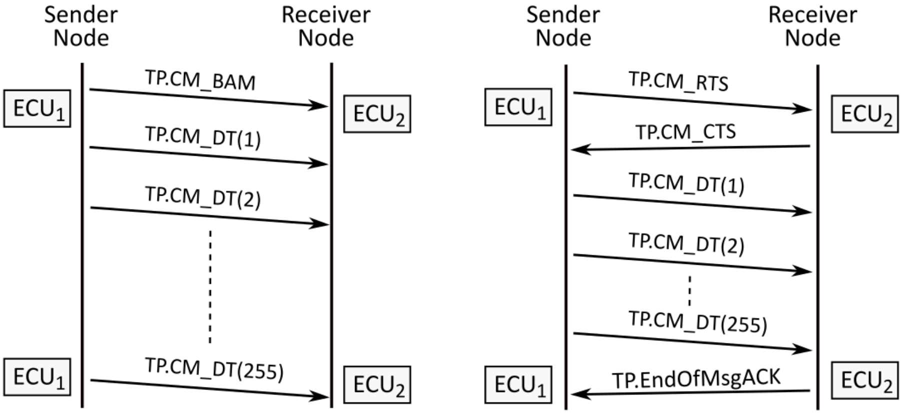


Fig. 3. Broadcast Data Transfer (left) and Connection Mode Data Transfer (right) – transport protocols used in multi-packet transmissions

such as: parameter group numbers, transport protocols, frame identifier breakdown as well as the address claiming procedure. The transport protocols employed in multi-frame message transmissions, i.e., *Broadcast Data Transfer* and *Connection Mode Data Transfer* are depicted in Figure 3. All of these are introduced in order to set room for the deployment of specific intrusion detection systems tailored to meet SAE J1939 specifications that are discussed in the next chapters.

Chapter IV explores the use of neural networks as candidates for intrusion detection in Controller Area Networks. The first section of this chapter starts with a presentation of the scenarios that can be exploited by an adversary to gain access to the CAN bus via the OBD port and injects adversarial CAN frames. The same section details the types of attacks that are subject for the evaluation of the IDS. The following section describes the development environments employed for the implementation of neural network based intrusion detection. Two different deployments are done, one using the Neural Network Toolbox made available by the MATLAB platform while the other is based on a C++ implementation. The first approach is preferred since the neural network toolkit offered by MATLAB is well-known for its performance, while the second is used since the C++ code can be easily ported on automotive-graded controllers. Nevertheless, a verification is done to make sure that identical detection results are produced using both deployments, and indeed this is the case. Then, this section briefly discusses the stopping conditions (for the training stage), the neural network architecture, which is depicted in Figure 4, as well as the features extracted from the CAN traffic, which serve as inputs for the neural network. The experimental results in terms of detection and runtime performance for the proposed IDS are detailed in the next section from this chapter. The experiments are performed on a J1939 compliant CAN traffic, recorded using a CANoe simulation and on a public CAN dataset. For each type of attack (replay or injections with random data inside the payload), several scenarios are tested depending on how the CAN traffic is split between training, validation and testing as well as on how the attacks are performed, either on a single ID or on full trace (all IDs). Moreover, in order to emphasize the trade-off between the accuracy of the detection results and the runtime performance, the evaluation is carried out using three different sizes for the neural network. The runtime performance of the detection algorithm is

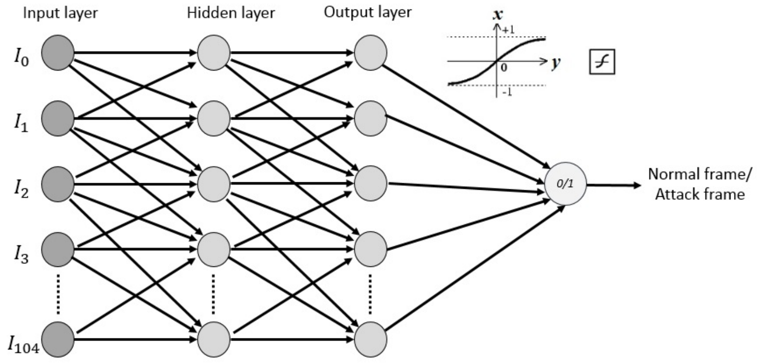
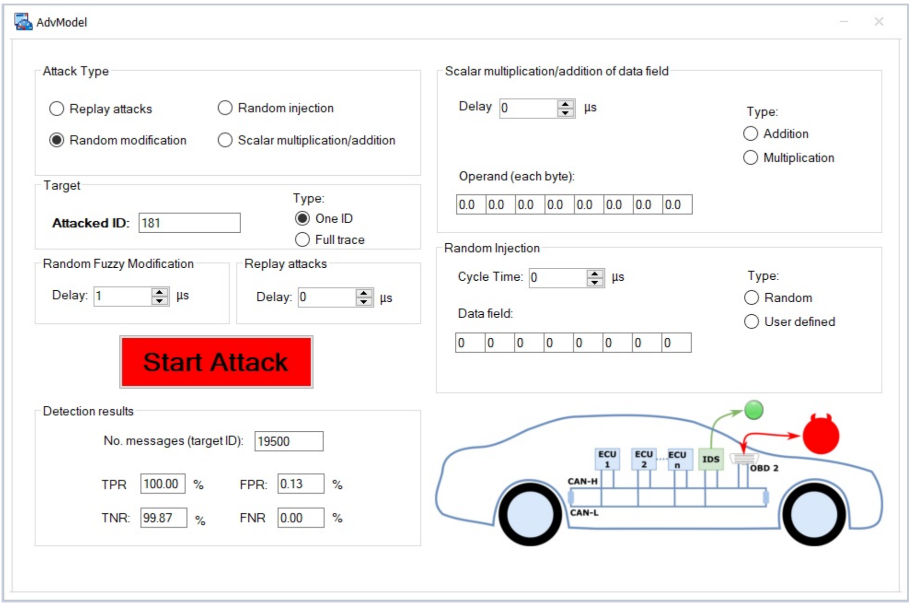


Fig. 4. Neural network architecture

measured on three automotive graded controllers, one regarded as candidate for the low-end device group and the other two for the high-end device group. The proposed IDS has a poorer accuracy in detecting replay attacks since the content of the injected frames is the same to the one of the genuine frames (the arrival time of the CAN frames is the sole way to identify such attacks). Overall, the experiments show that despite the good results in detecting intrusions, the usage of such a solution for the real-time filtering of the CAN traffic is debatable at least on microcontrollers from the low-end device group, since the time required to classify a CAN frame is in order of dozens milliseconds. This can be regarded as an important aspect since most of the related papers do not present such results, or use a PC based environment with powerful resources, which does not reflect the reality at microcontroller level.

A framework that enables the integration of various CAN bus attacks as well as intrusion detection systems inside a CANoe based simulation and provides a realistic testbed for them, is presented in Chapter V. The first section of this chapter begins with a description of the data collection procedure used by the author for extracting the CAN traffic from the two passenger cars. Then, this section presents the setup employed for the data extraction inside vehicles as well as the format of the recorded CAN messages. The CAN network structure from the CANoe simulation and how the collected CAN traffic is used inside it, are detailed at the end of this section. The second section introduces various types of adversarial manipulations that were integrated into the CANoe simulation. These attacks include replays, injections with randomly generated data inside the payload, injections with scalar addition or multiplication of the payload content as well as arbitrary injections. Then, this section proceeds with a presentation of how the designed graphical interface, illustrated in Figure 5, can be used. This interface permits to configure various adversary parameters. In the following section an overview of the *Statistics and Machine Learning Toolbox* offered by MATLAB platform as well as of the k-NN algorithm, a candidate for IDS, are presented. This section ends with a description of the input sample for the k-NN algorithm, which contains the following features extracted from the CAN frames: the time interval elapsed between consecutive arrivals of CAN messages that share the same identifier as well as the data field content. Last but not least, the experimental section discussed the detection results obtained for several scenarios. The experiments are conducted to cover all the previously defined types of attacks. The tested scenarios depend on the attack delay, on what the adversary targets (one ID or full CAN traffic), on how many neighbors and which



AdvModel

Attack Type
○ Replay attacks ○ Random injection
● Random modification ○ Scalar multiplication/addition

Target
Attacked ID: 181
Type:
● One ID
○ Full trace

Random Fuzzy Modification
Delay: 1 µs

Replay attacks
Delay: 0 µs

Start Attack

Detection results
No. messages (target ID): 19500
TPR 100.00 % FPR: 0.13 %
TNR: 99.87 % FNR 0.00 %

Scalar multiplication/addition of data field
Delay 0 µs
Type:
○ Addition
○ Multiplication
Operand (each byte):
0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 | 0.0

Random Injection
Cycle Time: 0 µs
Type:
○ Random
○ User defined
Data field:
0 | 0 | 0 | 0 | 0 | 0 | 0 | 0

Fig. 5. Graphical user interface for the CANoe simulation

distance metric are used by the k-NN algorithm as well as on the scalar values utilized for the addition and multiplication of payload bytes. As far as the author is aware, this is the first framework that allows the simulation of both the CAN bus attacks and the IDS inside a unified environment. At the same time, using a simulated environment is safer because it prevents any potential danger to drivers or cars.

In Chapter VI, a targeted intrusion detection and prevention system for securing the SAE J1939 heavy-duty CAN buses is evaluated. The first section summarizes how the J1939 compliant CAN traffic is collected by the author through the J1939 specific diagnostic port from an agricultural machinery (a tractor). Following that, this section continues with an inspection of the J1939 compliant features that are present inside the collected traffic. The recorded traffic contains 51 frame identifiers and it is transmitted by three different ECUs that are determined by investigating the unique source addresses that are embed inside the IDs. According to J1939 standardization, the function of each ECU from the network becomes apparent as follows: engine control module, body control module and transmission control module, respectively. A quantitative analysis focusing on the periodicity accounted for each CAN ID from the recorded CAN messages, is discussed at the end of this section. The next section introduces the adversary model which includes both replays and modification attacks. Nevertheless, the modification attacks follow a different approach from the one used in Chapters IV and V in that they are mounted at parameter level, not on the complete payload. This section then presents the two-stage IDS that was designed to protect J1939 CAN buses. The first stage relies on the *encrypted addresses*, i.e., the source as well as the destination addresses from each frame ID are encrypted using AES. The rationale behind embedding security elements into CAN identifiers is as follows. According to J1939 standardization, the payload of the J1939 CAN frames is fully allocated with specific J1939 parameters, which are assigned to a parameter group. Security elements are therefore packed in the IDs rather than the payload because doing otherwise would have been in contrast with J1939 specifications. This stage is complemented by the second one, which is based on the encrypted payload. This enables the detection even when single bits are tampered, due to the avalanche effect resulted from the decryption of the payload and subsequent plausibility checks applied for each J1939 parameter carried by the frame. Subsequently, this section discusses how these encrypted addresses will be generated and stored using an ordered binary tree as well as circular lists. Since these addresses must be generated cyclically the section ends with a formalisation on the trade-off between the periodicity of address tree generation and resources (computational power and storage capacity). Last but not least, the experimental section gives a presentation of runtimes measured on automotive development boards for the symmetric encryption operations as well as for the generation of the address tree. Then, the section gives an overview of the active defense mechanism, which acts like a prevention system. This mechanism permits the decoding of the CAN frame content (ID and payload) before the ACK slot becomes overwritten by receivers in case of a correct reception. Moreover, if the decoded frame is classified as an intrusion, then the destroying procedure of it with error flag is triggered. To test and prove the frame destruction capabilities of the prevention mechanism the laboratory setup depicted in Figure 6 is used. Lastly, this section shows the detection results obtained for attacks mounted on different J1939 parameters and provides an analogy between the security level accounted for the proposed solution and one that meets AUTOSAR SecOC requirements [20]. Overall, the proposed solution, which was specifically designed to meet J1939 specifications, proved to be a cost-effective method for both real-time detection and

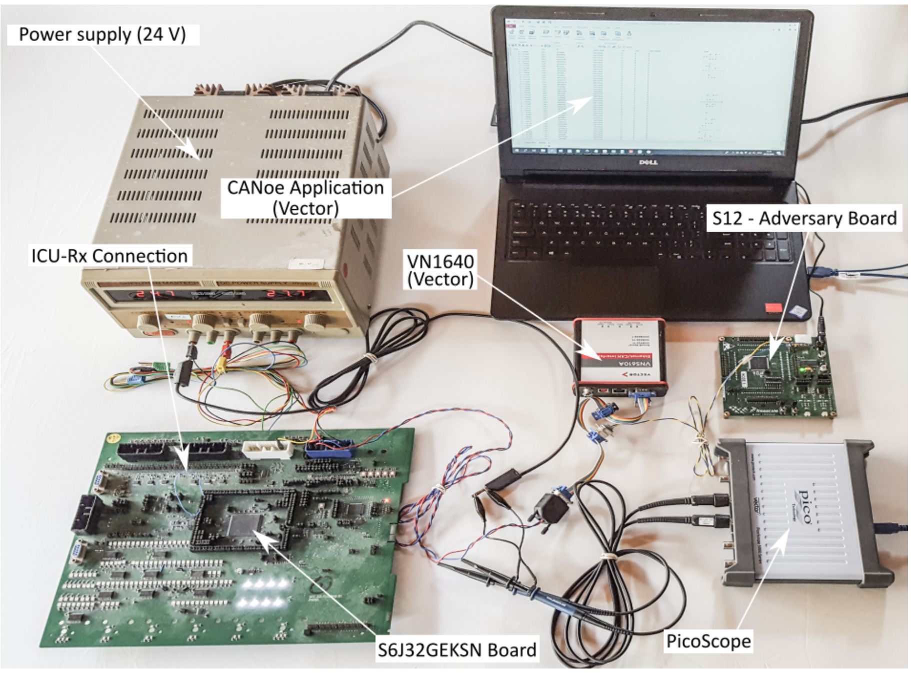
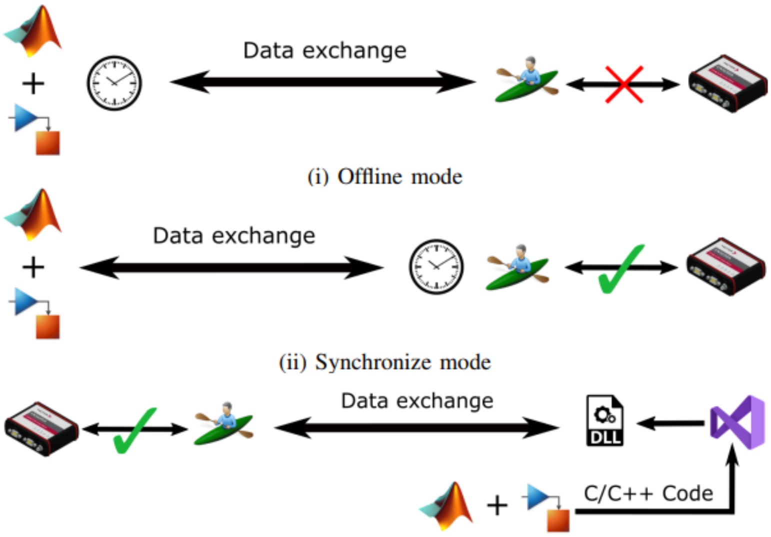


Fig. 6. Experimental setup with the VN1640 device, S6J32GEKSN and S12 boards, Power Supply as well as the PicoScope for monitoring the CAN communication

the elimination of attack frames. Moreover, to the best of author's knowledge this is the first intrusion detection and prevention system tailored for SAE J1939 heavy-duty vehicle buses. The innovative approach for decoding the CAN frame using ICU is another significant development of this chapter.

Chapter VII presents an intrusion detection system at control system level tailored to meet J1939 specifications. An overview on the connection between Simulink and CANoe as well as their combined operation modes is presented in the first section from this chapter and is also depicted in Figure 7. The next section proceeds with a brief description of the J1939 CANoe Simulation, the employed Simulink models as well as the adversary model. The Simulink models are integrated into the CANoe simulation and allow the prediction of the following signals: vehicle speed, trip distance, engine speed and torque. The adversary model accounts for specific attacks mounted at the control system level such as: surge attacks, bias attacks and geometric attack, which have not been considered by others works on CAN bus intrusion detection until now. Beside these three attack types, also a more common type of attack is taken into consideration, i.e., fuzzing attacks. The first part of the experimental section points out the behavior of the J1939 parameters when such attacks are mounted. Then, this section presents the performance results in detecting intrusion accounted for both the machine learning based approaches and change detection mechanisms. A significant finding from this section shows that, in spite of rising efforts to deploy machine learning approaches as candidates for IDS, such algorithms are unable to spot minor changes in the data field. On the other hand, as demonstrated by the experiments, the change detection mechanism seems to be more effective in detecting such attacks. For each J1939 signal, several attack scenarios are tested with regard to short simulations (1000 CAN frames) and long simulations (1 hour). For each signal, regardless of the attack type, the same bias and threshold values are maintained. This was done to cover the more realistic scenarios. The last part of this section discussed the



(i) Offline mode

(ii) Synchronize mode

(iii) Hardware in the loop mode

Fig. 7. CANoe-Simulink interraction – operation modes

runtime performance of the proposed IDS algorithms. The obtained results clearly show that the runtime of the change detection mechanisms is 2-65 times smaller than the one required for the execution of the machine learning algorithms. Moreover, not only from the perspective of computational efficiency does the change detection mechanism performs better, but also from the storage capacity point of view – since it requires just several lines of codes, while the machine learning based algorithms have a footprint of 10-30 KB.

Chapter VIII holds the conclusion of this thesis. All in all, this thesis investigates various security solutions that target SAE J1939 heavy-duty vehicle CAN buses, some of which could also be applied to regular CAN deployments, e.g., from passenger cars. Their practical application has been tested in various laboratory setups using equipment designed specifically for the automotive industry (microcontrollers, VN1640, CAN cables, etc.). As a major result, this thesis accounts for a realistic platform for testing in-vehicle CAN bus attacks and IDS as well, an intrusion detection and prevention systems tailored to meet J1939 specifications, a novel method to interpret the content of the CAN frames (ID and payload) before their correct reception as well as an IDS designed at control system level. The results of this thesis were published in relevant journals and conferences in the field of security, automotive, and industry applications. Overall, the results indicate that the intrusion detection systems are essential in boosting the security of in-vehicle networks and such mechanism can be efficiently deployed.

References

[1] "ISO11898-1. Road vehicles — Controller area network (CAN) —Part 1: Data link layer and physical signalling," International Organization for Standardization, Standard, 2nd edition, Dec 2015.

[2] F. Hartwich and R. Bosch, "Introducing CAN XL into CAN Networks," *future*, vol. 11898, p. 1, 2015.

[3] 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 *Security and Privacy (SP), 2010 IEEE Symposium on*. IEEE, 2010, pp. 447–462.

[4] 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.

[5] C. Miller and C. Valasek, "A survey of remote automotive attack surfaces," *Black Hat USA*, 2014.

[6] *CAN Specification Version 2.0.*, Robert BOSCH GmbH, 1991.

[7] "J1939 - Serial Control and Communications Heavy-Duty Vehicle Network," SAE International, Standard, June. 2023.

[8] Y. Burakova, B. Hass, L. Millar, and A. Weimerskirch, "Truck Hacking: An Experimental Analysis of the SAE J1939 Standard," in *10th USENIX Workshop on Offensive Technologies (WOOT 16)*, 2016.

[9] S. Mukherjee, H. Shirazi, I. Ray, J. Daily, and R. Gamble, "Practical DoS Attacks on Embedded Networks in Commercial Vehicles," in *Information Systems Security*, I. Ray, M. S. Gaur, M. Conti, D. Sanghi, and V. Kamakoti, Eds. Cham: Springer International Publishing, 2016, pp. 23–42.

[10] C. Jichici, B. Groza, R. Ragobete, P.-S. Murvay, and T. Andreica, "Effective Intrusion Detection and Prevention for the Commercial Vehicle SAE J1939 CAN Bus," *IEEE Transactions on Intelligent Transportation Systems*, 2022.

[11] C. Jichici, B. Groza, and P.-S. Murvay, "Integrating Adversary Models and Intrusion Detection Systems for In-vehicle Networks in CANoe," in *International Conference on Information Technology and Communications Security*. Springer, 2020, pp. 241–256.

[12] T. Andreica, C.-D. Curiac, C. Jichici, and B. Groza, "Android Head Units vs. In-Vehicle ECUs: Performance Assessment for Deploying In-Vehicle Intrusion Detection Systems for the CAN Bus," *IEEE Access*, vol. 10, pp. 95 161–95 178, 2022.

[13] 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.

[14] C. Jichici, B. Groza, and P.-S. Murvay, "Examining the Use of Neural Networks for Intrusion Detection in Controller Area Networks," in *International Conference on Security for Information Technology and Communications*. Springer, 2019, pp. 109–125.

[15] 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*, pp. 1–13, 2023.

[16] 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.

[17] “ISO/SAE 21434:2021 Road vehicles — Cybersecurity engineering,” International Organization for Standardization, Standard, 1st edition, Aug 2021.

[18] L. Popa, C. Jichici, T. Andreica, P.-S. Murvay, and B. Groza, “Impact of Wiring Characteristics on Voltage-based Fingerprinting in Controller Area Networks,” in *2023 IEEE 17th International Symposium on Applied Computational Intelligence and Informatics (SACI)*. IEEE, 2023, pp. 000 231–000 236.

[19] B. Groza, A. Berdich, C. Jichici, and R. Mayrhofer, “Secure Accelerometer-Based Pairing of Mobile Devices in Multi-Modal Transport,” *IEEE Access*, vol. 8, pp. 9246–9259, 2020.

[20] *Specification of Secure Onboard Communication*, R20-11 ed., AUTOSAR, November 2020, no. 654.