A Survey on Sender Identification Methodologies for the Controller Area Network

Marcel Kneib[1]

Abstract: The connectivity of modern vehicles is constantly increasing and consequently also the amount of attack vectors. Researchers have shown that it is possible to access internal vehicle communication via wireless connections, allowing the manipulation of safety-critical functions such as brakes and steering. If an Electronic Control Unit (ECU) can be compromised and is connected to the internal bus, attacks on the vehicle can be carried out in particular by impersonating other bus participants. Problematic is that the Controller Area Network (CAN), the most commonly used bus technology for internal vehicle communication, does not provide trustworthy information about the sender. Thus ECUs are not able to recognize whether a received message was sent by an authorized sender. Due to the limited applicability of cryptographic measures for CAN, sender identification methods were presented which can determine the sender of a received message based on physical characteristics. Such approaches can increase the security of internal vehicle networks, for instance to limit manipulations to a single bus segment and thus prevent the propagation of attacks. In this paper different methods are presented, which can mainly be divided into the categories time-based and voltage-based. In this context, challenges as well as open questions are identified and the approaches are compared. Thus, the work offers an introduction, identifies possible research fields and enables a quick evaluation of the existing technologies.

Keywords: Sender Identification; CAN Fingerprinting; CAN Security; Automotive Security

1 Introduction

The automotive industry is massively affected by the ongoing digitalization which leads to an increase in the connectivity of vehicles. However, these innovations not only offer advantages in terms of comfort, but also provide completely new possibilities for attackers to manipulate a vehicle without physical access [ZAA14]. Wireless connections such as Bluetooth, WiFi or cellular radio can be used to access the vehicle's internal network [Lu14]. Software vulnerabilities of connected ECUs allow attackers to manipulate the software accordingly, which, depending on the architecture of the vehicle, allows direct access to the internal communication [HKD11; IV13; Ko10; MV13]. If only limited security measures are implemented, vehicle functions can be remotely manipulated or controlled by a compromised ECU. But even with security measures, such attacks cannot be avoided. The severity became particularly apparent by the attack of Miller and Valasek [MV15], who succeeded in manipulating various vehicle functions of a Jeep Cherokee via a remote connection. In addition to various comfort functions, these included safety-critical systems

[1] Robert Bosch GmbH, Mittler Pfad 9, 70499 Stuttgart, Germany, marcel.kneib@de.bosch.com

doi:10.18420/sicherheit2020_07

such as steering, engine and brake, leading to a recall of 1.4 million vehicles. That this is not a single incident shows the vulnerability recently published by Keen Security Lab [Ca19].

The main problem is that no access protection or verification regarding the authenticity of messages is performed or is only possible to a limited extent. This is due to the functionality of the Controller Area Network (CAN) [Ro91], the most commonly used technology for in-vehicle communication. On the basis of a received CAN message, it is not possible to determine which bus participant sent the message, since only the expected sender can be identified via the information contained in the header [Li17; Pa17]. If a message was sent from a compromised ECU, there is no way to detect the misuse of a message. Due to the low bandwidth and payload [GM13; LS12], as well as the limited computing capacities of the ECUs [GM13; JAC18], the use of cryptographic measures for all signals is only possible with restrictions. Besides, digital signatures would be required to ensure non-repudiation, which have much higher requirements [GM13]. Thus, various Intrusion Detection Systems (IDSs) have been developed in the past in order to identify manipulations or anomalies on the basis of a predefined or learned set of rules [Ax00; Du19; Lo19]. Although these systems can enhance the security, the sender of a message provides an essential additional information which can supplement the overall security concept or allows a reliable recognition of different attacks [HKD11; MGF10]. For this reason, several methods have been introduced that use physical characteristics of the communication to either determine the sender of a message or at least use changes in the characteristics to detect anomalies.

This paper provides an overview of the different types of sender identification methods for CAN, which can essentially be divided into two categories, the time- and voltage-based methods. In addition to the presentation of the methods and corresponding approaches including their evaluation, the survey also includes the assessment of the methods with regard to possible applications, challenges and open questions. Thus, the paper facilitates the familiarization with the technology, provides background knowledge and enables a quick assessment for potentially interested manufacturers.

2 Controller Area Network

Vehicle architectures are becoming more complex as advances in the automotive industry are mainly achieved through electronic components [Br07; St14]. For these architectures, different bus technologies can be used in parallel, whereby nowadays gateways provide an interface between the individual segments and thus offer an ideal point for the integration of sender identification. Although the architectures will change considerably in the future [Br17], it is expected that Ethernet will be used for high transmission rates and CAN, respectively its developments [CA20], will be retained for lower rates [BSG16]. Accordingly, CAN will also be used in future vehicles, including its security weaknesses.

CAN messages are transmitted via frames, which contain a message identifier, representing the meaning and priority of the message and further is used by only one ECU. As the communication is statically configured, each ECU can receive required messages based on the message identifier. The physical connection consists of a twisted pair cable, one line for CAN high (CANH) and one line for CAN low (CANL), terminated at each end with 120 Ω resistors. If a recessive bit, a logic 1-bit, has to be represented on bus, the voltage of 2.5 V is present on both lines. In case a dominant bit, a logic 0-bit, has to be transmitted, CANH is driven to 3.5 V and CANL to 1.5 V. The actual signal is determined by the differential voltage and thus minimizes potential electromagnetic interference. Since it is possible for several ECUs to access the bus simultaneously, as CAN is a broadcast bus, the arbitration phase ensures that the message with the highest priority is retained. This allows the message with the highest priority to be sent undisturbed, while the ECU that loses arbitration re-queues its message for a later transmission attempt. With regard to sender identification, it should be noted that the physical characteristics of the symbols during the arbitration phase may be distorted.

3 Sender Identification Methodologies

The approaches for sender identification can be divided into two categories. While the time-based approaches use timing differences in CAN communication, the voltage-based approaches analyze differences in the analog signals of received frames. For both methods, models for the observed ECUs are created in an initial learning phase, which are used to analyze subsequent messages for deviations of the expected behavior. If a deviation occurs, the sender of the message can be identified on the basis of the physical parameters.

3.1 Time-based Sender Identification

The approaches in this category use timing differences in CAN communication to identify anomalies or the sender of a present frame.

Clock Skew The Clock-based IDS (CIDS), presented by Cho *et al.* [CS16], exploits the differences in the clocks of the ECUs to detect anomalies within periodically transmitted frames. Each ECU is equipped with its own quartz in order to generate clock frequencies for the microcontroller. One of the applications of these frequencies is the operation of the internal timers, which in turn are responsible for the punctual transmission of periodic messages on the bus. Since the quartzes are subject to natural variations and no synchronization is performed, there are measurable differences between the individual ECUs. By measuring the transmission intervals from an external point, the deviations between the expected and actual periodicity can be observed. On the basis of these deviations, for example, an impersonation attack can be detected.

Specifically, CIDS observes the expected and actual arrival times of each periodically sent message, as illustrated in Figure 1. Here the observed and the expected message flow of two periodically sending ECUs are shown. The messages are sent in statically defined intervals from which, together with the previous arrival time, the arrival time of the following message can be calculated. The deviation between the measured and the expected value specifies the clock offset O. Whenever a predefined number of clock offsets has been measured, an average clock offset is calculated which is then used to estimate an error value indicating the difference between the expected and the actual clock offset of the corresponding ECU. The expected offset is calculated from the cumulative sum of the previous average clock offsets using the Recursive Least Squares algorithm [Ha05]. An increase of the error indicates a deviation of the clock offset and thus an anomaly can be detected if the error rises above a given threshold value. If the forged messages are sent over a longer period of time, the compromised ECU can be identified using the known average clock offsets of all ECUs. CIDS was evaluated on a CAN prototype assembly and three vehicles, whereby missing and additionally transmitted frames and the takeover of a periodically sent signal by a compromised ECU could be reliably detected.

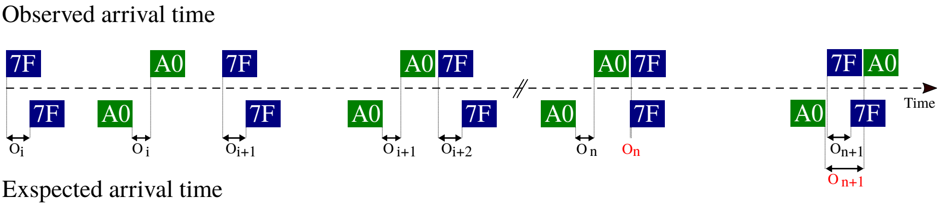

Fig. 1: Expected and observed clock skew from two different ECUs.

Propagation Time Until a transmitted signal arrives at the receiver, a certain period of time expires, which mainly depends on the distance between both nodes. More precise, a signal propagates on the bus medium in the direction of both bus ends, whereby the time of reaching both ends depends on the position of the sender. The TCAN approach of Biham *et al.* [BBG18] is based on these time spans in order to determine the location of an ECU and thus to distinguish between the senders. For this purpose, a measuring unit and a repeater are attached to the opposite ends of the bus. The function of the repeater is to analyze the signals of the messages in order to send an echo to the bus when the first falling edge, i.e. the change from a dominant to a recessive state, is detected after the arbitration phase. However, the CAN communication must not be disturbed by the echo signal and it must be recognizable by the measuring unit, which is also responsible for the determination of the time spans. Therefore, it also has to recognize the first falling edge of the message after the arbitration phase and the echo signal of the repeater. Subsequently, the time interval t_s between these two points is considered for the calculation of the position of the sender. For this purpose, the distance between the measurement unit and the sender of the message is calculated. For the assignment of the ECU to a measured distance, an authentication table is created before operation, for whose initialization the authors specify several options. The process is illustrated in Figure 2 for two different senders. Biham *et al.* [BBG18] also mentions that repeater and measuring unit could be housed in one device, eliminating the need for the echo signal, which corresponds to the approach of Moreno *et al.* [MF19]. Their approach was additionally evaluated on a vehicle bus with four ECUs. Altogether, the position of the ECUs at a sampling rate of 100 MS/s could be determined with an accuracy between 20 and 30 cm. The distinction was reliable, since there was a sufficiently large distance between the two closest ECUs so that the probability of a misclassification was negligible.

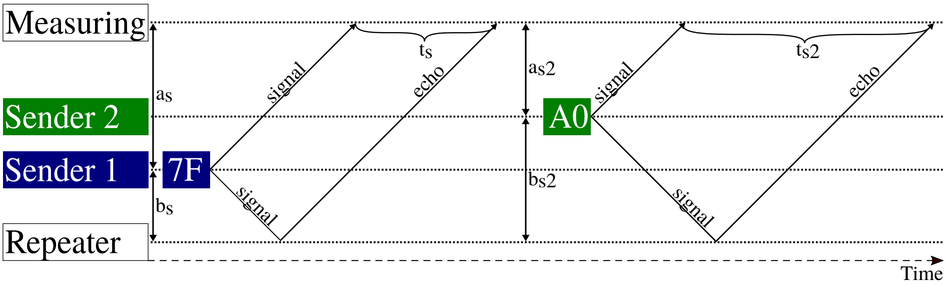

Fig. 2: Propagation delay for two different ECUs using an echo signal.

3.2 Voltage-based Sender Identification

Existing differences in the analog signals, caused by manufacturer-related imperfections of electronic components and the structure of the present CAN topology, can be utilized to identify the sender of received frames. As an example, Figure 3 shows a segment of the signals of six ECUs from a Fiat 500.

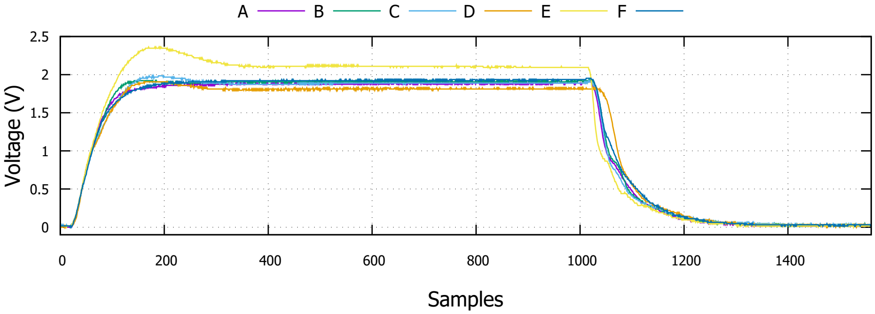

Fig. 3: CAN signals of several ECUs from a Fiat 500.

Comprehensive Signal Characteristics This subcategory considers approaches which are based on the complete or a segment of the analog signal. The idea itself was introduced by Murvay and Groza [MG14] and further developed by Choi *et al.* [Ch18a] by using machine learning for identification. The two most advanced approaches are VoltageIDS [Ch18b] and Scission [KH18], which consist basically of three phases. In the first phase, the analog CAN signals are recorded and preprocessed. By using the differential signal, potential electromagnetic interferences are compensated, necessary to provide a robust identification. While the sampling rate of VoltageIDS is between 250 and 2500 MS/s, Scission operates with a lower sampling rate of 20 MS/s. In order to provide data-independence, utilizable voltage level changes of the recorded signals are then divided into individual sets. In the second phase, the feature extraction, different characteristics are extracted from the prepared signals, which represent the fingerprint of the sending ECU. Here, the approaches differ with regard to the selected features. Subsequently, the fingerprint is processed in the third phase, the identification and intrusion detection. Here, machine learning algorithms are used in order to determine the sender, resulting in a probability per ECU. The VoltageIDS makes use of Support Vector Machines and Bagged Decision Trees, while Scission uses Logistic Regression for classification. Whereas VoltageIDS marks the ECU with the highest probability as the sender, Scission uses a two-stage threshold procedure to reduce the number of false positives. Only if the probability of the expected sender undercuts a first threshold, the probabilities of the remaining ECUs are calculated. In case one of these probabilities exceeds a second threshold value, the corresponding ECU is labeled as unauthorized sender and the frame is determined to be malicious. The use of comprehensive signal characteristics was analyzed on various prototype structures and four vehicles, whereby Scission shows an identification rate of 99.85 % while all false alarms were prevented.

Voltage Level Compared to the previous category, the approach considered here, Viden [CS17], uses only isolated points of the signal. First, the dominant voltages of CANH and CANL are measured separately with a low sampling rate of 50 kS/s. A voltage instance is then derived from a defined number of measurements, consisting of the most common voltages and various percentiles. Thereby, the deviations of the measured voltages from the expected standardized voltages are calculated and summed up in order to compensate transient deviations as much as possible. This value, which remains approximately constant during operation, is then cumulatively summed up. Using Recursive Least Squares, a voltage profile can be calculated per message identifier, which allows the identification of the sending ECU. Since Viden is designed to complement higher-level IDSs, Viden is used after an attack has been detected in order to identify the attacking ECU. For this purpose, an attacker voltage profile is created for the unauthorized used identifier. As soon as sufficient voltage values have been measured for its calculation, the ECU with the most similar voltage profile is marked as the sender. Since ECUs may have similar profiles, or an attacker may has adjusted his profile to imitate a specific ECU, a further step is taken for identification. For this purpose Viden utilizes a 200 Random Forest classifier, which receives the voltage instance as input. The approach was also evaluated on a prototype structure and two vehicles with an attacker identification of up to 99.8 %.

4 Evaluation

This section assesses the different approaches in terms of purpose, resource needs and unresolved issues. An overview of the assessment can be seen in Table 1.

Tab. 1: Assessment of the sender identification methodologies.

	Maturity level	**Hardware Requirements**	**Computational Requirements**	**Robustness**	**Security**	**Restrictions Architecture**	**Aperiodic Frames**
Clock Skew	+	+	○	○	-	+	-
Propagation Time	-	-	+	+	+	-	+
Signal Characteristics	+	-	-	+	+	+	+
Voltage Level	+	○	○	○	○	+	○

4.1 Time-based Sender Identification

Clock Skew The most significant disadvantage of the procedure is that due to the manner of the clock skew extraction, counterfeiting cannot be completely excluded as demonstrated by the attack of Ying *et al.* [Yi19]. Since the skew can also be observed via a compromised ECU and the transmission frequency can be adjusted via software, the CIDS can be circumvented. Thus the system can only reliably detect missing or additional frames, which can also be achieved by analyzing the transmission schedule [MGF10]. Another disadvantage of the offset extraction is the exclusive consideration of periodic frames as well as a possible shift of frames, shown in the right part of Figure 1, which can lead to fluctuations. However, the software-based approach and especially the methodology is a good demonstration that the clock skew can be used for anomaly detection. Should an alternative source for the extraction of the clock skew be found, the system offers a good and cost-effective way to detect attacks. A method that makes it independent of aperiodic frames would be ideal in order to extend the scope of detection. Furthermore, more detailed investigations are necessary here with regard to changes in the clock skew in fluctuating environmental conditions, such as temperature.

Propagation Time Even though a detailed evaluation of this variant has not yet been carried out, Moreno's [MF19] work indicates that the propagation time is a robust quantity. Especially since the propagation time should be less affected by fluctuations, it might be suitable to falsify malicious frames, however, requiring a much deeper analysis. Since this characteristic is defined by the cable lengths respectively the topology, there is no possibility for a remote attacker to adjust the characteristics of the compromised ECU according to the device to be impersonated. Accordingly, neither complex calculations nor a full update of the time models are necessary, as long as the hardware has not been changed. In addition, the propagation time is not limited to periodically transmitted messages. However, the implementation is not trivial in terms of hardware. For the timely transmission of the echo signal used by Biham *et al.* [BBG18], the measuring unit and the repeater must reliably recognize and analyze the individual edges within a frame, which exceeds the capabilities of standard CAN devices. Besides, the echo signal must be viewed critically with regard to the CAN specification. Basically, a high clock frequency respectively a high sampling rate is necessary for the accurate measurement of the timings, which represents a high demand on the measuring unit. For example, Biham *et al.* [BBG18] specify a resolution of 1 GHz for an accuracy of 15 cm and 100 MHz for 1.5 m, respectively. If a low frequency is used, only longer distances can be distinguished, which limits the electrical/electronic architecture of the vehicles. However, Moreno *et al.* [MF19] show that even with a low resolution it is possible to make precise predictions. Another limitation is that the location of the implementing devices is restricted. This means that either a device must be placed at both ends of the bus or, if implemented in a single ECU, the already large wiring harness will be further enlarged.

4.2 Voltage-based Sender Identification

Comprehensive Signal Characteristics Although there has been progress in these approaches in the last years and reliable identification has been demonstrated, they still require a considerable amount of resources due to the high sample rates. Accordingly, high demands are placed on the processing ECU with regard to computing performance for the processing of large amounts of data, the calculation of machine learning algorithms and the recording of signals. This is illustrated by the fact that no demonstration has yet been shown on a resource-limited platform. Basically, for a CAN with 500 kB data rate, a payload of 8 bytes and a maximum bus utilization, it can be assumed that the entire classification must be completed in roughly 200 μs in order to be able to react in real time and prevent a buffering of the fingerprints. Although high identification rates have already been achieved in production vehicles, longer investigations are necessary for a reliable assessment. This also includes more concrete information regarding the life cycle of the models, i.e. how to react to possible variations in the signals. In particular, training a classifier is very computationally intensive, which is why it must be shown that this is feasible on the target platform.

Voltage Level Viden is designed for attacker identification only and therefore requires a high-level IDS for the detection of attacks. Only when an attack has been detected, the approach is used to identify the compromised ECU. Due to the methodology and the low sample rate, Viden is designed for periodic messages. Thus, several messages are necessary per iteration, i.e. per creation of a voltage instance. Accordingly, the applicability could be extended to aperiodic messages by increasing the sampling rate to perform the necessary measurements within a single frame. However, just as with the approaches of the previous section, further investigations would be necessary to assess the suitability of Viden as an IDS. At the same time, the assumption made about the equal changes in the voltage levels among all ECUs should be evaluated, as our measurements show different fluctuations for different ECUs. The deviations of two ECUs during a drive are shown in Figure 4, whereas A has a deviation of 12.2 mV and B of 4.8 mV on average. If it is not possible to simply adjust the voltage signal on the basis of a single value, the model must be regularly retrained, for which the integrity of the vehicle must be ensured. Although the main part of the approach requires few resources, a 200 Random Forest classifier is used for the verification and thus has comparable requirements to the approaches of the previous chapter. In order to benefit from the performance advantage, a solution is required which makes the verification step obsolete.

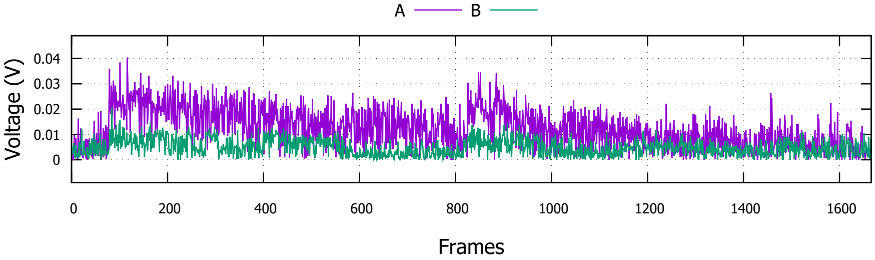

Fig. 4: Plateau voltage fluctuation of two ECUs from a Fiat 500.

5 Comparison and Challenges

Overall, the voltage-based approaches have been evaluated more fully and comprehensively, but further investigations are necessary, particularly regarding robustness. Further vehicles and a longer observation period have to be considered, ideally with different climatic conditions. Even if the evaluations of Scission and Viden show a robustness against fluctuations, the performance of VoltageIDS decreases considerably with temperature changes, unless the models are continuously updated. Considering that the temperature ranges depend on the positioning of ECUs, the performance must be evaluated at least between −40°C and 85°C [Au07]. Furthermore, due to the high production volumes it is essential that especially the methods based on comprehensive signal characteristics are optimized with regard to hardware requirements. Considering available automotive microcontrollers, e.g. STM SPC [ST17] or Infineon TriCore [In19], the implementation of one of these approaches is not realizable due to their high data rates. In terms of reliability, however, these methods offer an advantage over voltage level methods due to the use of numerous characteristics.

In comparison, the time-based procedures require a more extensive evaluation, modification and optimization. The clock skew procedure can be considered broken and therefore requires rework or a new and immutable way to extract clock skews. In addition, an optimization for the monitoring of aperiodic messages would be desirable. Also the temperature dependence of the clock skew has to be examined in detail, as fluctuations affect the clock rate of the ECUs. In comparison, the propagation time can be assumed to be less fluctuating, since the speed of a signal is assume to vary less. Furthermore, it must be clarified how the positioning of the monitored ECUs, the resolution or sampling rate and potential fluctuations interact in order to be able to configure the system accordingly. Here, questions regarding the implementation on automotive hardware are still open, as the evaluation of the existing approach was carried out offline. However, in view of the current results, the propagation time is also a promising method for implementing sender identification.

Furthermore, it has not yet been clearly elaborated how IDSs should be used in general, i.e. how they can react in the event of a detected intrusion. An interesting possibility for the sender identification systems is that a detection is possible during the actual transmission, which, with a correspondingly fast calculation, allows the invalidation of the message, e.g. by overlaying with the dominant state. Here, extensive research as well as enhancements in robustness and detection rates are necessary, so that wrong reactions are compliant with safety requirements. The reduction of false alarms is particularly important due to the high number of messages, as otherwise, depending on the reactions, the usability of the vehicle could be restricted. Therefore, especially the propagation time approaches and Scission show potential, due to the lack of false alarms.

6 Conclusion

This paper presents the methods for sender identification using physical characteristics for CAN. They provide a reliable detection of impersonation attacks and complement existing IDSs, but still require further research. Open questions have been identified in this paper, representing a starting point for future work. The methods were also compared in order to show the respective advantages and disadvantages, which allows a fast assessment. Generally, the hardware requirements must be further reduced and the robustness must be analyzed in greater detail by extending the evaluation to several vehicles while observing them for a longer duration. In addition, a suitable method for updating the models must be found, especially for the voltage-based methods, as changes of the signal characteristics during the life time of a vehicle are expected. In summary, sender identification offers a considerable benefit with regard to the security of connected vehicles, if the open challenges can be solved.

References

[Au07] Automotive Electronics Council: AEC-Q100 Failure Mechanism Based Stress Test Qualification for Integrated Circuits. 2007.

[Ax00] Axelsson, S.: Intrusion detection systems: A survey and taxonomy, Technical report, 2000.

[BBG18] Biham, E.; Bitan, S.; Gavril, E.: TCAN: Authentication Without Cryptography on a CAN Bus Based on Nodes Location on the Bus. In: Proceedings of the 2018 Workshop on Embedded Security in Cars (ESCAR). 16, Nov. 14, 2018.

[Br07] Broy, M.; Kruger, I. H.; Pretschner, A.; Salzmann, C.: Engineering Automotive Software. Proceedings of the IEEE 95/2, pp. 356–373, Feb. 2007, ISSN: 0018-9219.

[Br17] Brunner, S.; Roder, J.; Kucera, M.; Waas, T.: Automotive E/E-architecture enhancements by usage of ethernet TSN. In: 2017 13th Workshop on Intelligent Solutions in Embedded Systems (WISES). Pp. 9–13, June 2017.

[BSG16] Braun, L.; Sax, E.; Gauterin, F.: Abschlussbericht: Experteninterview zur Anforderungsanalyse heutiger und zukünftiger E/E Architekturen im Kraftfahrzeug. DOI: 10.5445/IR/1000054216, 2016.

[Ca19] Cai, Z.; Wang, A.; Zhang, W.; Gruffke, M.; Schweppe, H.: 0-days & Mitigations: Roadways to Exploit and Secure Connected BMW Cars. Black Hat USA 2019/, p. 39, 2019.

[CA20] CAN in Automation: CAN XL is knocking at the door./, Jan. 3, 2020, URL: https://www.can-cia.org/news/cia-in-action/view/can-xl-is-knocking-at-the-door/2020/1/3/, visited on: 01/03/2020.

[Ch18a] Choi, W.; Jo, H. J.; Woo, S.; Chun, J. Y.; Park, J.; Lee, D. H.: Identifying ECUs Using Inimitable Characteristics of Signals in Controller Area Networks. IEEE Transactions on Vehicular Technology 67/6, pp. 4757–4770, June 2018, ISSN: 0018-9545.

[Ch18b] Choi, W.; Joo, K.; Jo, H. J.; Park, M. C.; Lee, D. H.: VoltageIDS: Low-Level Communication Characteristics for Automotive Intrusion Detection System. IEEE Transactions on Information Forensics and Security 13/8, pp. 2114–2129, Aug. 2018, ISSN: 1556-6013.

[CS16] Cho, K.-T.; Shin, K. G.: Fingerprinting Electronic Control Units for Vehicle Intrusion Detection. In: Proceedings of the 25th USENIX Conference on Security Symposium. SEC'16, USENIX Association, Berkeley, CA, USA, pp. 911–927, 2016, ISBN: 978-1-931971-32-4, URL: http://dl.acm.org/citation.cfm?id=3241094.3241165.

[CS17] Cho, K.-T.; Shin, K. G.: Viden: Attacker Identification on In-Vehicle Networks. In: Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security. CCS '17, ACM, New York, NY, USA, pp. 1109–1123, 2017, ISBN: 978-1-4503-4946-8, URL: http://doi.acm.org/10.1145/3133956.3134001.

[Du19] Dupont, G.; Hartog, J. d.; Etalle, S.; Lekidis, A.: Network intrusion detection systems for in-vehicle network-Technical report. arXiv preprint arXiv:1905.11587/, 2019.

[GM13] Groza, B.; Murvay, S.: Efficient Protocols for Secure Broadcast in Controller Area Networks. IEEE Transactions on Industrial Informatics 9/4, pp. 2034–2042, Nov. 2013, ISSN: 1551-3203.

[Ha05] Haykin, S. S.: Adaptive filter theory. Pearson Education India, 2005.

[HKD11] Hoppe, T.; Kiltz, S.; Dittmann, J.: Security threats to automotive CAN networks—Practical examples and selected short-term countermeasures. Reliability Engineering & System Safety 96/1, pp. 11–25, 2011, ISSN: 0951-8320, URL: http://www.sciencedirect.com/science/article/pii/S0951832010001602.

[In19] Infineon Technologies: AURIX^{TM} 32-bit microcontrollers for automotive and industrial applications. 2019.

[IV13] Illera, A.; Vidal, J.: Dude, WTF In My Car. DEFCON 21, 2013.

[JAC18] Junior, E. A. S.; Araujo-Filho, P. F. d.; Campelo, D. R.: Experimental Evaluation of Cryptography Overhead in Automotive Safety-Critical Communication. In: 2018 IEEE 87th Vehicular Technology Conference (VTC Spring). Pp. 1–5, June 2018.

[KH18] Kneib, M.; Huth, C.: Scission: Signal Characteristic-Based Sender Identification and Intrusion Detection in Automotive Networks. In: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security. CCS '18, ACM, New York, NY, USA, pp. 787–800, 2018, ISBN: 978-1-4503-5693-0, URL: http://doi.acm.org/10.1145/3243734.3243751.

[Ko10] Koscher, K.; Czeskis, A.; Roesner, F.; Patel, S.; Kohno, T.; Checkoway, S.; McCoy, D.; Kantor, B.; Anderson, D.; Shacham, H.; Savage, S.: Experimental Security Analysis of a Modern Automobile. In: 2010 IEEE Symposium on Security and Privacy. Pp. 447–462, May 2010.

[Li17] Liu, J.; Zhang, S.; Sun, W.; Shi, Y.: In-Vehicle Network Attacks and Countermeasures: Challenges and Future Directions. IEEE Network 31/5, pp. 50–58, 2017, ISSN: 0890-8044.

[Lo19] Loukas, G.; Karapistoli, E.; Panaousis, E.; Sarigiannidis, P.; Bezemskij, A.; Vuong, T.: A taxonomy and survey of cyber-physical intrusion detection approaches for vehicles. Ad Hoc Networks 84/, pp. 124–147, 2019.

[LS12] Lin, C.; Sangiovanni-Vincentelli, A.: Cyber-Security for the Controller Area Network (CAN) Communication Protocol. In: 2012 International Conference on Cyber Security. Pp. 1–7, Dec. 2012.

[Lu14] Lu, N.; Cheng, N.; Zhang, N.; Shen, X.; Mark, J. W.: Connected Vehicles: Solutions and Challenges. IEEE Internet of Things Journal 1/4, pp. 289–299, Aug. 2014, ISSN: 2327-4662.

[MF19] Moreno, C.; Fischmeister, S.: Sender Authentication for Automotive In-Vehicle Networks through Dual Analog Measurements to Determine the Location of the Transmitter. In: Proceedings of the 5th International Conference on Information Systems Security and Privacy - Volume 1: ICISSP, SciTePress, pp. 596–605, 2019, ISBN: 978-989-758-359-9.

[MG14] Murvay, P.; Groza, B.: Source Identification Using Signal Characteristics in Controller Area Networks. IEEE Signal Processing Letters 21/4, pp. 395–399, Apr. 2014, ISSN: 1070-9908.

[MGF10] Müter, M.; Groll, A.; Freiling, F. C.: A structured approach to anomaly detection for in-vehicle networks. In: 2010 Sixth International Conference on Information Assurance and Security. Pp. 92–98, Aug. 2010.

[MV13] Miller, C.; Valasek, C.: Adventures in automotive networks and control units. Def Con 21/, pp. 260–264, 2013.

[MV15] Miller, C.; Valasek, C.: Remote exploitation of an unaltered passenger vehicle. Black Hat USA 2015/, p. 91, 2015.

[Pa17] Pan, L.; Zheng, X.; Chen, H.; Luan, T.; Bootwala, H.; Batten, L.: Cyber Security Attacks to Modern Vehicular Systems. J. Inf. Secur. Appl. 36/, pp. 90–100, Oct. 2017, ISSN: 2214-2126, URL: https://doi.org/10.1016/j.jisa.2017.08.005.

[Ro91] Robert Bosch GmbH: CAN Specification. 1991.

[St14] Staa, P. v.: How KETs can contribute to the reindustrialisation of Europe, European Technology Congress, Wrocław, June 12, 2014, URL: http://docplayer.net/21724658-Date-2012-how-kets-can-contribute-to-the-re-industrialisation-of-europe.html, visited on: 06/27/2019.

[ST17] STMicroelectronics: SPC58EEx, SPC58NEx 32-bit Power Architecture\textsuperscript® microcontroller for automotive ASIL-D applications. 2017.

[Yi19] Ying, X.; Sagong, S. U.; Clark, A.; Bushnell, L.; Poovendran, R.: Shape of the Cloak: Formal Analysis of Clock Skew-Based Intrusion Detection System in Controller Area Networks. IEEE Transactions on Information Forensics and Security 14/9, pp. 2300–2314, Sept. 2019, ISSN: 1556-6013.

[ZAA14] Zhang, T.; Antunes, H.; Aggarwal, S.: Defending Connected Vehicles Against Malware: Challenges and a Solution Framework. IEEE Internet of Things Journal 1/1, pp. 10–21, Feb. 2014, ISSN: 2327-4662.