Assessment of Current Intrusion Detection System Concepts for Intra-Vehicle Communication

Oleg Schell[1], Jan Peter Reinhard[2], Marcel Kneib[3], Martin Ring[4]

Abstract: Nowadays, vehicles incorporate a lot of electronics, which offer both advanced functionalities but also a great attack surface. Once having access to the communication network, an attacker can control critical functions like accelerating or steering. One possibility to detect these malicious intentions consists in the implementation of Intrusion Detection Systems (IDSs), which will even become mandatory via UN regulations in the future. Therefore, it is important for manufacturers and engineers to understand the opportunities and challenges of IDSs in the automotive environment. Giving an overview on these detection mechanisms is the primary goal of this elaboration. After the current vehicular communication architectures and protocols are outlined, potential attacks on the communication network are addressed. Afterwards, existing IDS concepts are presented, while the general requirements on these systems from an automotive perspective are stated and described next. Following the discussion on how to react to a detection, the elaboration is concluded with an outlook on what has still to be achieved to successfully integrate present IDSs into a vehicle.

Keywords: Automotive Security; Intrusion Detection System; Intra-Vehicle Communication

1 Introduction

With increasing functionality of the vehicular ecosystem, the number of electronic components and interfaces that are indispensable for safety realizations and provided services also increases [LOA19]. As a consequence, these advances widen the surface for the execution of cyber-physical attacks that no longer require physical access to the vehicle due to wireless interfaces like Bluetooth, WiFi or the Global System for Mobile Communication (GSM) [Lu14]. By exploiting these interfaces and the security vulnerabilities in the software of Electronic Control Units (ECUs), an adversary can get access to the internal communication network and remotely control crucial functionalities like steering, accelerating or braking [MV15]. It is evident that these possibilities can have severe consequences for both the driver and its environment. At this point, it must be mentioned that this threat does not only affect a single but several vehicle models, including Jeep [MV15], Tesla [NLD17] and BMW [Ca19], among others.

These circumstances made it quickly apparent that malicious activities on the intra-vehicle communication networks had to be detected and prevented. The latest efforts to realize this

[1] Bosch Engineering GmbH, Robert-Bosch-Allee 1, 74232 Abstatt, Germany, oleg.schell@de.bosch.com
[2] Hochschule RheinMain, Kurt-Schumacher-Ring 18, 65197 Wiesbaden, Germany, janpeterreinhard@gmail.com
[3] Robert Bosch GmbH, Mittlerer Pfad 9, 70499 Stuttgart, Germany, marcel.kneib@de.bosch.com
[4] Bosch Engineering GmbH, Robert-Bosch-Allee 1, 74232 Abstatt, Germany, martin.ring@de.bosch.com

doi:10.18420/inf2020_78

intent include UN regulations [UN20], which propose to implement countermeasures on a mandatory basis. One of the possibilities that they suggest, is the utilization of IDSs to provide a security measure on network basis. Since the demands placed on such systems in the automotive domain are different from those in a classic IT environment, this elaboration will outline different IDS approaches and their requirements for the implementation in vehicles. The presented concepts should serve as a guideline for engineers, while the subsequently addressed inadequacies and open questions regarding the realization should give researchers a direction to advance the topic of automotive IDSs.

Protocol	Rates	Description	Use Case
Linear Interconnected Network (LIN)	11.2 or 19.6 KBit/s	Cheap and simple protocol using a linear bus architecture for small intra-vehicle services.	Battery Monitoring, Window Lifter Control, Temperature Sensors
Media Oriented Systems Transport (MOST)	25, 50 or 150 MBit/s	Relatively expensive protocol, which provides high data rates for infotainment applications.	Audio Module, Navigation System, Infotainment
Controller Area Network (CAN)	125 or 500 KBit/s	Most common protocol for vehicular networks, with new CAN FD and CAN XL standards providing higher data rates.	Engine Control, Electrical Stability Control, Transmission Unit
Ethernet	100 MBit/s	Protocol, which is relatively new in the automotive domain and becomes more popular due to high data rates and cost.	ECU Flash Interface, Cameras, Radar, Network Backbones
FlexRay	5 or 10 MBit/s	Fault tolerant protocol with high bandwidths, which is not often used because of its complexity and high cost.	Steering Angle Sensor, Throttle Control, All-Wheel Drive

Tab. 1: Wired communication protocols for intra-vehicle data exchange based on [Al19; Hu19].

2 Automotive Network Architectures and Protocols

Every vehicle is a distributed system, which is made of ECUs communicating over different protocols. The ECUs represent the computing units of a vehicle and differ in performance, memory capacity and robustness, depending on the intended use. In this context, robustness means how well an ECU is protected against temperature, pressure and humidity changes, as well as its level of failure safety. A single ECU can have multiple network interfaces and thus send data over different media. Wired networks are more common in this regard, for which different protocols exist depending on the area of application as stated in Tab. 1. Besides these, there are also wireless standards like Bluetooth Low Energy or ZigBee which can also be deployed in the vehicle, but have not been widely used to date [Hu19].

The potential topologies, which can be used for these communication protocols, vary widely. Besides the star topology, where each device is connected to a central gateway, repeater or hub to route the data to its destination, each ECU can also be linked to its neighbors to form a ring topology. While furthermore a point-to-point connection is the easiest of

all topologies, communication protocols like LIN, CAN and FlexRay are usually realized in a bus topology, where every device is connected to a single communication line and transfers data in a broadcasting manner. Apart from the aforementioned interconnection methods for individual ECUs, the entire communication architecture is undergoing a transformation [He19]. The trend is shifting from an application-specific communication architecture towards a domain-specific one, where the ECUs in each domain communicate with protocols stated in Tab. 1, while Ethernet is used across domains for fast data exchanges. In the future, it is intended to create a centralized architecture that consists of a few high performance controller, which are connected to most of the ECUs or domains with Ethernet. Although Ethernet may replace protocols like FlexRay and MOST [Rö17], there is still the need to secure the individual communication sections and utilized protocols like CAN.

Requirement	Attack	Description
Authenticity	Spoof & Replay	Impersonating network participants without being noticed or replaying prerecorded messages on their behalf.
Confidentiality	Eavesdrop	Unauthorized access to data and information which is transmitted over the vehicular network.
Availability	Flood & Drop	Preventing operation of network participants by either withholding data or flooding the network with irrelevant messages impeding the transmission of relevant data.
Integrity	Manipulate	Manipulating content of transmitted messages in such a way that it remains hidden from the other network participants.

Tab. 2: Security requirements and potential attacks on intra-vehicle networks.

3 Attacks on Intra-Vehicle Communication

The motivation of an intrusion into the communication network of a vehicle is manifold and includes, among others, altering vehicular characteristics like engine performance or mileage, intruding into the driver's privacy or interfering into the control to cause harm. In order to achieve these goals, access to the communication networks is required first. Before vehicles were equipped with wireless interfaces, access could only be gained in a physical way, either by connecting directly to the communication wires or over the On-board diagnostics (OBD)-II port, which is used by workshops for diagnostic purposes. Nowadays, these wireless interfaces like Bluetooth or Wi-Fi of the telematic control unit represent an additional risk through which unauthorized access is possible. By exploiting security breaches and rewriting the software on this ECU [MV13], data can usually be both read and written by the adversary on the network to which this unit is connected to.

Once having access to the communication network, an adversary can perform different malicious actions due to the lack of security mechanisms. As exemplarily stated in Tab. 2, these attacks can be classified according to the security requirement they violate. For this

reason, appropriate security mechanisms have to be considered already during vehicle design or integrated afterwards to prevent such actions.

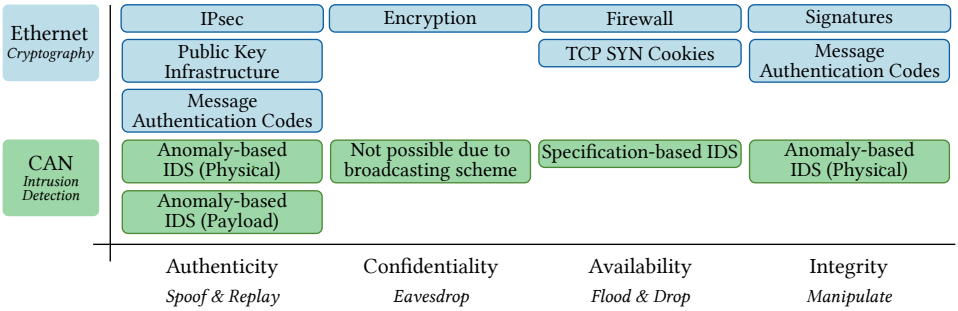

Fig. 1: Possible security mechanisms for vehicular Ethernet and CAN.

4 Intrusion Detection System Concepts

Compared to the remaining communication protocols from Tab. 1 which have been in use for several years, Ethernet is currently finding more and more its way into the vehicle, enhancing communication networks with a high bandwidth and low cost [Rö17]. Here, Ethernet does not provide security mechanisms by itself, they are mainly obtained by using higher level protocols like Transmission Control Protocol/Internet Protocol (TCP/IP). Since these have long been used in classical IT systems such as home computers, server applications or corporate networks, usual security mechanisms, some of which are listed in Fig. 1, can theoretically be applied in the automotive sector [HKD09]. Although the bandwidth allows the transmission of additional data for the proper operation of these security mechanisms, the real-time requirements must still be considered for their implementation [Rö17].

Taking CAN into consideration, the limited hardware resources and communication bandwidths commonly available, exacerbate the implementation of cryptography-based approaches [GM13]. Furthermore, the fact that CAN is already used in almost every vehicle renders a subsequent security provision for existing networks more difficult. This is especially critical, since CAN does not deploy any security mechanisms and can therefore be attacked successfully with ease [Al19]. To remedy this issue, the utilization of IDSs can be considered, which can retrofit basic security aspects into existing and future CAN networks. Since IDSs can be realized in various ways, the most prominent concepts are discussed in more detail, mentioning their merits and shortcomings. At this point it should be noted that the mentioned IDS concepts represent general methodologies and can therefore also be utilized for different communication protocols like Ethernet.

Signature-based IDS Using signature-based detection, the ongoing communication is continuously compared to known attack patterns in the IDS database like the sequence of

transmitted data or malicious instructions. Although usually used in anti-virus software for IT systems, the pattern matching procedure is a resource demanding process for vehicular ECUs. Further, the attack database has to be kept updated and distributed to the individual vehicles, while there is no possibility to recognize novel attacks. This is particularly critical as such patterns have not yet been extensively established for attacks on vehicles, which however are constantly increasing in number. At last, unlike classical IT systems where patterns can be shared, a manufacturer-specific signature cannot be used by another vendor, as other digital platforms are usually implemented. On the other hand, once these patterns are developed, this approach reliably detects known attacks with a low false alarm rate.

Specification-based IDS Communication properties like transmission schedules, communication partner or which ECU is eligible to transmit which messages on the respective network segment, are mostly specified during the design phase of a vehicle and usually do not change after deployment. The same applies to the static communication architectures which are not altered after establishment [Hu17]. An IDS can take advantage of this by considering the specification and establishing rules which are checked during the ongoing communication. For example, in this way it is possible to implement a firewall in units which interconnect several networks and which then are able to block transmissions not complying to the rules. Be it the deviation of data values from a predefined range or the propagation of unauthorized messages in a network, the specification-based approach is able to detect these easily and efficiently. Big disadvantages are that these rules have to be manually created by experts, which is error-prone and thus can lead to a high number of false alarms, while an adversary can circumvent the rules if he acts within acceptable limits.

Anomaly-based IDS Anomaly-based approaches work similarly to specification-based procedures in that they detect deviations from predefined behavior. The difference here is that the predefined behavior is learned by the system itself in the case of anomaly detection. This not only eliminates the need to set up rules but also enables the detection of unknown and novel attacks. Generally, the normal behavior can be learned based on different communication characteristics, which are briefly described in the following.

1. **Payload**: Mainly utilizing machine learning algorithms, IDSs of this category strive to establish a model of the message content and attempt to detect unusual data sequences that can be traced back to attacks. This approach would represent a promising option to detect different types of intrusions, if only the interrelationships were not so complex, the need for data not so high and the computational power not so demanding.
2. **Physical**: ECUs and their electronic components are subject to manufacturing imperfections, leading to small differences in the physical properties like clock timings and voltages. IDSs can utilize these small differences and implement sender identification mechanisms, with which unauthorized transmissions can be detected and the malicious ECU pinpointed. However, since the properties refer to the respective ECUs, an adversary can send unnoticed authorized messages with malicious content

from the compromised ECU. Further, in most cases, high performance analog-to-digital converters (ADCs) or timers are required to record even small differences.

Regardless of which characteristic is selected, anomaly-based approaches necessarily require trustworthy data to learn the normal behavior, whereby the time and data amounts required for this learning should not be neglected. Furthermore, one of the main reasons why this type of IDS has not yet been widely used is that it has a high false alarm rate [Al19], which is especially important when the driver is not to be distracted unnecessarily and when intrusions are not only to be detected but also actively prevented.

As shown in Fig. 1, different IDS concepts provide varying security measures for protocols like CAN. To establish a holistic security system, it is therefore essential to implement a combination of these concepts. For instance, specification-based methods could provide the first line of defense against rudimentary attacks, while anomaly-based procedures detect the presence of more sophisticated attackers. These *hybrid* IDSs allow the incorporation of both digital and physical characteristics making the resulting system more robust and reliable.

5 Requirements

For the design of an intrusion detection approach, different requirements play a major role in the automotive domain. While standards like ISO/SAE DIS 21434 [IS20] and UN regulations [UN20] mandate the realization of security management processes and name best practices, the criteria mentioned here represent a non-formal set of requirements. These are mainly derived from the challenges of implementing IDSs in the automotive sector stated by literature such as [LOA19] or [Al19] and make no claim to completeness.

The most significant difference of automotive systems compared to classical IT is the high importance of *Safety*. Therefore, an IDS is not allowed to affect data by delaying or removing it which may lead to the loss of safety relevant information. This also includes the fact that a restriction of the information availability by an IDS must not take place. Safety comes along with the requirement on *Performance*. In order to not delay data and to be able to analyze all exchanges messages even at high bandwidths, the IDS must have a certain computing performance. Furthermore, it requires a high detection performance to detect all attacks, while not generating false alarms. Although an IDS is a security measure by itself, it also has to meet different *Security* requirements. In this context, it is important that the system is not reducing the functionality and effectiveness of other security concepts such as firewalls or encryption, while not creating new exploits and critical security gaps. Other important requirements relate to the *Privacy* of the driver and other passengers. Because of the high connectivity of modern automotive systems, it is important that an IDS does not leak private data without permission to other systems. Especially, if the IDS uses a cloud-based back-end for incident analysis and transmits sensitive data. Finally, the *Update* of an IDS plays a crucial part for the requirements. In contrast to IDSs for classical IT systems which can be

updated almost at any time via the Internet, with vehicular IDSs it must be ensured that, for example, the rule update procedure of a specification-based approach does not open new security breaches and is not corrupted. If the update takes place over-the-air, short connections to road side infrastructures and disconnections must further be expected.

6 Post Detection and Outlook

An important question that has not yet been clarified in this elaboration is how to deal with intrusion detections in the automotive environment. In the literature a distinction is made between passive and active measures [LOA19], under which logging, notifying and preventing fall. Each of these three methods can be more or less beneficial in individual aspects. Logging, for example, stores information about the potential intrusion, which can then be read out in case of an incident to patch the security gap in the remaining fleet. Although logging does not distract or hinder the driver, the large amount of information must first be stored and subsequently analyzed in time-consuming manual work. Considering to notify the driver in case of an intrusion, the danger is immediately apparent and actions can be carried out. False alarms play a crucial part here, because even with transmission rates of several tens of milliseconds and a low false alarm rate, the driver could be mistakenly warned several times a minute. These false alarms become even more serious if active prevention is taken into account. If safety-relevant data is incorrectly recognized as an attack and on this basis prevented, it becomes apparent that such actions can have far-reaching consequences for the passengers and their environment.

Only after it is clarified how to deal with these detections, IDSs can be effectively put into utilization, whereby further challenges have to be taken into account. Up to now, the throughout implementation of security in a vehicle is regarded as a matter of course by the customer [Hu17]. Therefore, manufacturers keep the available resources for IDSs as low as possible, which stands in contradiction to increasing data amounts and complexity. Achieving lower latencies and real-time capability, which are particularly relevant for safety-critical tasks, ECUs require more hardware resources and computing power. These requirements are especially true for anomaly-based IDSs, which currently receive the greatest focus, as they are most promising to detect sophisticated attacks [LOA19]. For the evaluation of anomaly-based approaches, individually recorded data from test vehicles are often used. Yet, to ensure a better comparability of existing approaches, a publicly available data set with respective communication characteristics is required. In the end, knowledge of different disciplines like artificial intelligence, automotive systems and electrical engineering are crucial for the design and consolidation of different security concepts. Only if this knowledge comes together, a holistic security system can be developed which is able to recognize or prevent not only rudimentary but also the presence of advanced attackers. For this purpose, different concepts have to be employed in a joint approach to realize the essential security requirements. In doing so, the non-formal criteria like safety, performance or privacy must be considered for both current and future communication architectures.

References

[Al19] Al-Jarrah, O. Y.; Maple, C.; Dianati, M.; Oxtoby, D.; Mouzakitis, A.: Intrusion Detection Systems for Intra-Vehicle Networks: A Review. IEEE Access 7/, pp. 21266–21289, 2019, ISSN: 2169-3536.

[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.

[GM13] Groza, B.; Murvay, S.: Efficient Protocols for Secure Broadcast in Controller Area Networks. IEEE Transactions on Industrial Informatics 9/4, 2013.

[He19] Helge Zinner Julian Brand, D. H.: Automotive E/E Architecture evolution and the impact on the network. IEEE802 Plenary, March 2019, 802.1 TSN/, 2019.

[HKD09] Hoppe, T.; Kiltz, S.; Dittmann, J.: Applying intrusion detection to automotive IT-early insights and remaining challenges. Journal of Information Assurance and Security (JIAS) 4/, pp. 226–235, Jan. 2009.

[Hu17] Humayed, A.; Lin, J.; Li, F.; Luo, B.: Cyber-physical systems security—A survey. IEEE Internet of Things Journal 4/6, pp. 1802–1831, 2017.

[Hu19] Huang, J.; Zhao, M.; Zhou, Y.; Xing, C.: In-Vehicle Networking: Protocols, Challenges, and Solutions. IEEE Network 33/1, pp. 92–98, Jan. 2019.

[IS20] ISO/SAE DIS 21434: Road Vehicles – Cybersecurity engineering, Standard, Geneva, CH: International Organization for Standardization, 2020.

[LOA19] Lokman, S.-F.; Othman, A. T.; Abu-Bakar, M.-H.: Intrusion detection system for automotive Controller Area Network (CAN) bus system: a review. EURASIP Journal on Wireless Communications and Networking 2019/1, p. 184, 2019.

[Lu14] Lu, N.; Cheng, N.; Zhang, N.; Shen, X.; Mark, J. W.: Connected Vehicles: Solutions and Challenges. IEEE Internet of Things Journal 1/4, 2014.

[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.

[NLD17] Nie, S.; Liu, L.; Du, Y.: Free-fall: Hacking tesla from wireless to can bus. Briefing, Black Hat USA/, pp. 1–16, 2017.

[Rö17] Röder, J.: Automotive Ethernet - Die Zukunft der vernetzten Fahrzeugarchitektur - The future of in-vehicle data Management./, July 2017, URL: https://www.vdi-wissensforum.de/news/automotive-ethernet/.

[UN20] UN Task Force on Cyber Security and Over-The-Air issues: Proposal for the 01 series of amendments to the new UN Regulation on uniform provisions concerning the approval of vehicles with regard to cyber security and of cybersecurity management systems. 2020.