M. Meier, D. Reinhardt, S. Wendzel (Hrsg.): Sicherheit 2016,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2016 45

Automotive Ethernet: Security opportunity or challenge?

Christopher Corbett[1,2], Elmar Schoch[1], Frank Kargl[2], Preussner Felix[1]

Abstract: The automotive industry's future trends, such as automated driving or advanced driver assistance, require large bandwidths to handle massive data streams and strongly depend on well timed communication. The Ethernet technology is seen as a suitable candidate to cover those needs for vehicle-internal networks; however, Ethernet involves security issues. Thus, by discussing automotive Ethernet attributes with regard to the adaption of existing security mechanisms in contrast to the potential of creating new ones, several challenges and opportunities emerge in consideration of comparatively fewer available resources and the integration into a vehicle environment. Based on these results we derive and propose ideas for manipulation and misuse detection mechanisms.

Keywords: automotive, Ethernet, security, discussion, network, detection, misuse, misbehavior

1 Introduction

Modern automobiles provide drivers with a wide range of safety, comfort and assistance functionalities. The evolution of existing and the integration of additional features in new vehicle generations result in highly complex automotive systems with enhanced hardware and software parts. These systems attract the attention of computer security researchers who challenge themselves to find and exploit flaws in software and hardware implementations. Their goal is to modify, extend, tune or misuse in-vehicle devices beyond their intended purposes or restrictions [VM15]. Any modification can influence the safety state of a vehicle. Hence, it is important to protect an automotive system from any manipulation by third parties through the integration and continuous improvement of security mechanisms.

Future trends like automated driving and advanced driver assistance are seen as key features for further automotive development. They rely on increasing computing power as well as massive data exchange between sensors, actuators and processing devices. The integration of Ethernet into the automotive domain holds opportunities for new or modified security mechanisms to prevent malicious intervention, which could threaten the safety state of a vehicle.

In this paper we discuss the characteristics of automotive and common Ethernet networks within defined criteria and present their differences and potentials for security mechanisms, with focus on vehicle-internal wired networks.

[1] Audi AG, 85045 Ingolstadt, <forename> . <surname>@audi.de
[2] University of Ulm, Institute of Distributed Systems, Albert-Einstein-Allee 11, 89081 Ulm, <forename> . <surname>@uni-ulm.de

2 Criteria for discussion

In reference to the Open System Interconnection (OSI) model, we mainly focus on the physical link, data link, network and transport layers with their protocols Ethernet, Internet Protocol Version 4 (IPv4), Internet Protocol Version 6 (IPv6), Transfer Control Protocol (TCP) and User Datagram Protocol (UDP). We also consider environmental influences and impacts on vehicle parameters as appropriate factors, as the automotive network is part of a large cyber physical system. Regarding the stated premises, the list of criteria shown in Figure 1 will be the base for our discussion of security challenges and opportunities. We assume that the principles of common Ethernet networks and the used protocols are known by the reader, and we only give an introduction to automotive specifics.

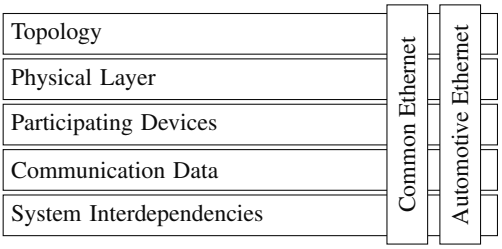
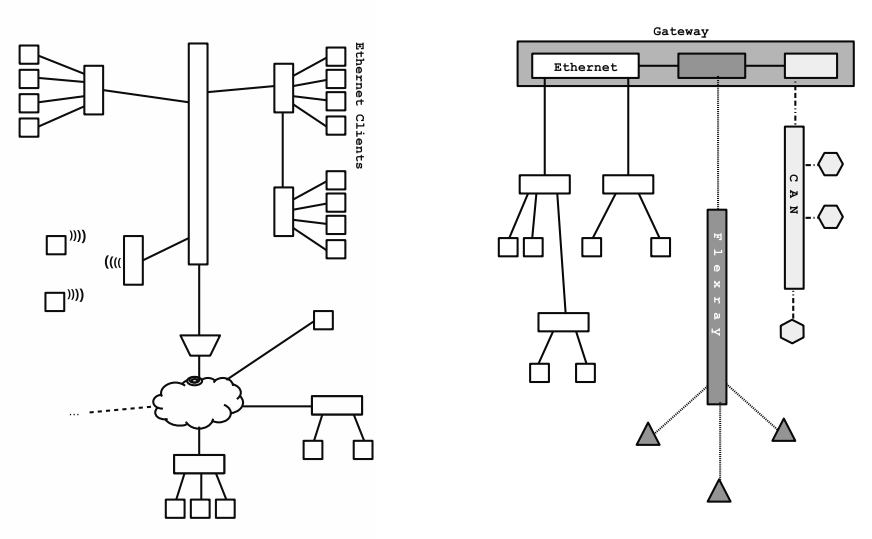


Fig. 1: List of criteria

3 Discussion

3.1 Topology

The design of automotive bus network topologies is mainly driven by functional requirements and cost efficiency. Over the past decades, several network technologies were developed (e.g. Controller Area Network (CAN), Local Interconnect Network (LIN), FlexRay, and Media Oriented Systems Transport (MOST)) in order to satisfy requirements such as time accuracy, low cost, or extensibility. This trend led to very heterogeneous internal networks where protocol conversion between different protocols becomes necessary to enable network-wide data exchange. All of these technologies are either based on arbitration or time slot mechanisms for bus access. The integration of Ethernet adds a packet and point-to-point based technology to the system. Switching and routing components are necessary to enable Ethernet, IPv4 or IPv6 communication between more than two Ethernet devices. Figure 2b shows an abstract example of an heterogeneous automotive network topology with several different bus technologies (CAN, FlexRay, Ethernet) and protocol conversion, via a central device providing gateway functionalities, in contrast to a common network topology shown in Figure 2a. Due to the functional approach, the topology is hierarchically structured, divided into several logical segments and overall considered to be highly static and not extensible.



(a) Abstract example of a common Ethernet network topology

(b) Abstract example of a heterogeneous automotive network topology

Fig. 2: Topology examples

Discussion
One of the primary differences between automotive and common Ethernet networks are the hierarchical structure and the combination of different bus network topologies. With the introduction of Ethernet to vehicle-internal networks, legacy bus technologies will continue to be present and not completely replaced. The easy extensibility and dynamic configuration of common networks must deliberately be avoided to increase controllability and create a solid foundation for safety related requirements. Thus, deliberate limitations of communication are inevitable, and must be applied for example through the use of firewalls, packet filters, network segmentations or Virtual Local Area Networks (VLAN). Major challenges for automotive Ethernet networks are to master the wide functional range of network protocols, as well as to restrict access to configurations of switching and routing components. Furthermore, changes to the topology after the engineering process must be prevented.

3.2 Physical Layer

The physical layer is responsible for transporting digital information via analog electrical signals. The selection of an appropriate transport media strongly depends on physical limitations as well as communication and application requirements. Common demands are bandwidth, unidirectional or bidirectional communication, resistance against electromagnetic influence, cost efficiency, distance to overcome and compatibility.

Modern cars process huge amounts of data provided by many sensors and actuators. Especially image processing units require high bandwidths considering increasing resolutions and a growing number of devices. Data rates of at least 100Mbit/s are necessary to satisfy those needs. Whereas applications with lower bandwidth requirements can be supported by bus technologies like LIN, CAN and FlexRay.

The development of accurate automotive Ethernet technologies is additionally driven by flexible installation and power consumption. Fiber optical cables, which are also used in MOST networks, are not as practicable in comparison to copper based cables. Currently, unshielded twisted pair copper conductors are favored for 100Mbit/s and 1000Mbit/s connections; however, due to different physical characteristics, coaxial copper cables could also be applied for the latter.

The most promising technology at the moment for fast Ethernet transceivers (100Mbit/s) is BroadR-Reach® introduced by BroadCom and standardized by the OPEN Alliance Special Interest Group (SIG). With this technology,a pair of twisted unshielded copper conductors can exchange information bidirectional over a guaranteed distance of 15m. In order to provide a bandwidth of 1000Mbit/s over the same type of wiring, 1000Base-T1 is currently the considered standard in automotive Ethernet networks. Being work in progress and because of physical restrictions between the two standards, the bandwidth of Ethernet connections is currently not negotiable at runtime and bound to the used transceivers. Transceivers of the same brand are used, in order to reduce costs and thus maximize their quantity. It is foreseeable that future transceivers will support several standards to increase flexibility in systems engineering by being able to switch between data rates.

Discussion
Cost efficiency and strong requirements on electro magnetic resistance in automotive networks limit the range of possible physical layer technologies compared to common networks. The transfer rates between two connection points are not yet negotiable and are bound to the used transceiver, as well as the used copper conductors. All physical layer attributes are known at the end of the engineering process and will not be changed during its lifetime.

3.3 Network Participants

Participants in any automotive bus network are generally called Electronic Control Units (ECU). A unit is responsible for a certain kind of functionality and specifically designed for that purpose. Environmental influences such as temperature ranges between –40°C and +100°C, humidity or vibrations affect the selection of appropriate components. Peripheral devices must meet all of the specifications and the range of possible parts is limited. Software and hardware components must meet legal and safety requirements and manufacturers are constrained to prove their compliance. Each software part, such as Ethernet stacks, operating systems and application frameworks, are specifically chosen and analyzed in detail during the development process. Some examples for deployed operating systems and frameworks are Qnx, AUTOSAR, VxWorks and Embedded Linux. Figure 3 shows the

different layers of components which can be randomly selected, but have dependencies to each other.

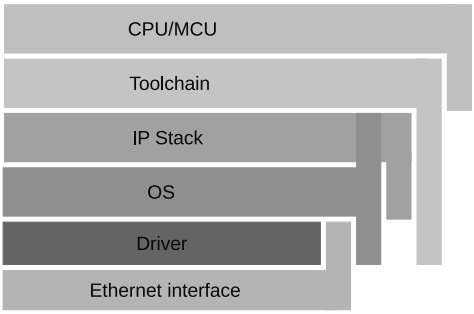


Fig. 3: Dependency overview of hard and software components

The communication within the network is designed, specified, tested and documented for every specific use case, and at the end of the development process knowledge about all network participants exists in detail and will not change after the release of the vehicle.

Discussion
For automotive Ethernet networks it is mandatory that participating devices are reliable, controllable and act strictly according to specification. The misuse of devices, such as modifications of software parts or the replacement of components with third party devices, can lead to undefined behavior and influence the safety of the vehicle. Hence, it is important to ensure the network's consistency by preventing access of unknown network participants, misbehavior of existent devices, as well as any spoofing attempts.

Yet there are no standardized mechanisms for automotive Ethernet networks to restrict access of untrusted devices. The adaption of existing authentication mechanisms (e.g. IEEE 802.1x) to automotive Ethernet networks could be a reasonable approach.

3.4 Communication data

Communication within Ethernet networks is defined by the protocol header, the information in the payload field and their interpretation. In consideration of all possible attributes we think that data structures, message frequencies and the ratio of TCP and UDP connections are promising distinctive parameters for the development of security mechanisms for automotive Ethernet networks. Therefore we focus on these attributes within this section.

Automotive systems must comply with a wide range of safety and reliability specifications. For example, the used protocols and data structures are well chosen, known in every detail and each possible impact on the whole system is considered before the end of the engineering process.

Being a cyber physical system, most of the functionality relies on control loops where sensors, actuators and processing units by design provide or consume data frequently. Events

triggered by user interactions can either result in a single and terminating task or a periodic sequence of tasks, each implicated with data exchange. Considering the use of bandwidth, memory consumption, timeout management and timing for data exchange between one or several participants, UDP connections have a smaller footprint than TCP connections, but limitations in payload size and reliability. A choice strongly depends on the requirements of each application or service and their safety impact. Yet there are no studies on the distribution of TCP and UDP connections in an automotive Ethernet network, and only estimations can be made.
The operability of most functions and eventually the safety state of a vehicle strongly depend on accurate timing, data correctness and authenticity of exchanged information between sensors, actuators and ECUs. Thus protection against manipulation takes priority over preventing eavesdropping of network data. After the market introduction of a vehicle a change or update on used protocols are very unlikely. The domain of information and entertainment (infotainment) systems can be an exception due to the interaction with consumer electronics and common Ethernet network services.

Discussion
Communication in vehicle-internal networks rests upon specifications, and once released changes are unlikely. Compared to common networks, the user of a vehicle is limited to triggering machine-to-machine interactions (e.g. data exchange, remote function calls). A user is supposed to only change predefined payload values via existing Human Machine Interfaces (HMI) (e.g. steering wheel buttons, infotainment controls), but can not alter existing protocol structures or introduce protocols of their own.
The exchange rates of information are rather high. Complete data encryption, to prevent eavesdropping and guaranty message authenticity, would cause heavy use of resources and can lead to large latencies which contradicts with timing requirements. Applying integrity and authentication mechanisms, such as Message Authentication Codes (MAC), could be a more efficient approach for such use cases.

3.5 System interdependencies

As a cyber physical system, a vehicle is exposed to different environmental factors (e.g. physical forces, traffic participants, temperature changes) with impacts on the driver, sensors, actuators and finally the overall system state. Actions taken by the driver result in transitions between different system states and can lead to changes of environmental factors, which again influence inputs to control loops. The Ethernet network and all of its devices, being part of the vehicle, are also influenced by system state transitions.

Discussion
Devices in automotive networks are not geographically spread and are clustered in a superior system, i.e. a vehicle, controlled by a driver and partly by passengers. Compared to common networks, protocols and data structures are strictly specified and user interaction via control interfaces explicitly limited. Environmental factors and user actions trigger dedicated functions and change the vehicle system state as well as the exchanged data streams.

4 Security challenges and opportunities

Based on the previous discussion, we derive numerous challenges and opportunities for automotive Ethernet networks and briefly describe them in the following section.

4.1 Challenges

Increasing number of potential attackers
Ethernet is a well-known technology, which is extensively described in literature and many people have experience with this technology through day-to-day use both at work and at home. Therefore the number of capable potential attackers is considered greater than compared to other automotive bus technologies. Due to the availability of cheap compliant devices, the technical barrier for interested persons is also rather low. In combination with todays social media platforms (e.g. Youtube, Forums) it is possible to quickly share information and provide simple instructions for carrying out exploits.

Fewer resources
In comparison to systems using common Ethernet, resources (e.g. computing power, memory) are more restricted due to financial and vehicle power boundaries. As such it is not possible to run full-fledged security appliances, such as Intrusion Detection Systems (IDS) or high performance network traffic inspection.

Gained attention
Ethernet will be the key technology for future automotive trends to fulfill necessary requirements in vehicle-internal networks. Being a daily used object, and with a total of 44.4 million registered vehicles [Kr15] alone in Germany, cars are commercially attractive to numerous interest groups. We defined a list of stakeholders, shown in table 1, with their main intentions on exploiting software and hardware flaws.

Tuner/Modder	**Criminals**	**Third party manufacturers**	**Hackers**
- Modifying funct.	- Theft	- Providing alteration	- Sell Knowledge
- Extending funct.	- Selling used parts	- Provide spare parts	- Personal satisfaction
- Tuning of components	- Life threatening manipulation		- Searching for flaws

Tab. 1: List of interest groups for exploits

Accessibility
All network components are clustered inside a vehicle and not physically distributed among different geographical locations, like in most common networks. Who ever is in control of the automobile has full access to the whole network ecosystem.

Security diversity
An automobile is a very heterogeneous system. Each distributed communication technology was designed for a specified purpose, provides certain features and has furthermore limitations. It is difficult to apply a mutual security mechanism to the system, e.g. MAC, due to differences in computing resources of ECUs and payload sizes of protocol frames (e.g. CAN (8 Byte), Controller Area Network with Flexible Datarate (CAN-FD) (64 Byte), FlexRay (255 Byte) and Ethernet (1500 Byte)).

Safety compliance
Safety related functions in automotive systems must meet certain requirements, such as high availability, strong reliability, exact timing and low latency in communication. Hence, it is important that applied security mechanisms do not have impact on the safety state of a vehicle, as safety is prior to security in vehicular systems.

4.2 Opportunities

Detection capabilities
Attributes of automotive networks, regarding running applications, services, architecture and topology design, are very static. The combination of this static design with environmental factors and vehicle states enables further detection capabilities of contrary behavior in Ethernet networks after the manufacturing process.

Extended bandwidth
With the introduction of Ethernet to the vehicle-internal networks the bandwidth compared to legacy bus systems is increased and gives leeway to better authentication or encryption mechanisms (e.g. Media Access Control (MAC)). Also software or configuration updates can be distributed faster.

Stricter separation
Due to the point-to-point characteristics of Ethernet a stricter separation into and within functional domains can be achieved compared to bus technologies like CAN. Through the use of switches in combination with the IEEE 802.1Q specification of VLAN and Quality of Service (QoS), as well as firewall concepts, communication paths inside the network can be restricted and priorities for packets considered.

4.3 Approaches for security mechanisms

The previously stated challenges and opportunities hold potential for different approaches to security mechanisms for automotive Ethernet networks. In this section we propose our ideas regarding applicable mechanisms with focus on the detection of network manipulation and misuse.

Physical Layer security mechanism
Security mechanisms for common networks based on layer 1 attributes are not reasonable due to a large variety of available transceivers, cable types, range extenders and negotiable transfer rates. Through the massive restrictions in automotive Ethernet networks we think of physical layer security mechanisms to verify the identity of physically to each other connected devices by searching for distinct characteristics as electric resistance, impedance or changes of signal modulations, frequencies and amplitudes to build a distinct fingerprint. Also the introduction of a light-weight encryption mechanism could be possible to prevent the addition of new or the replacement of existing devices.

Meta information based mechanism
Through the restricted design of ECUs and the detailed knowledge about all network related parameters and attributes, meta information (e.g. stack auditing, packet statistics, used parameters) could be used to detect misbehavior or spoofing of devices in vehicle-internal networks.

Specification based misuse detection mechanism
Considering the stated communication data characteristics the introduction of an anomalous behavior detection system (or Misuse Detection System (MDS)) based on specifications could be used to uncover possible manipulations or injection of malicious network data.

Misbehavior detection mechanism through vehicle state mapping
By mapping certain identified system states to exchanged data streams, atypical behavior either by the system or the network could be detected.

5 Conclusion

In this paper we briefly discussed common and automotive Ethernet networks within defined criteria to identify challenges and opportunities for security mechanisms in vehicle-internal networks. Overall we see potential for network manipulation and misuse detection mechanisms in future automotive Ethernet networks. We consider the combination of several mechanisms as a chance to increase the security of future vehicular Ethernet networks, with a sensible use of resources. The elaboration, simulation and evaluation of all ideas are topics for future research.

References

[Co14] Corporation, Broadcom: . BroadR-Reach Physical Layer Transceiver Specification for Automotive Applications., May 2014.

[Kr15] Kraftfahrt Bundesamt: , Gesamtbestand an PKW zum 1. Januar 2015 in Deutschland, January 2015.

[PH12] Peter Hank, Thomas Suermann, Steffen Mueller: Automotive Ethernet, a Holistic Approach for a Next Generation In-Vehicle Networking Standard. Advanced Microsystems for Automotive Applications, pp. 79–89, 2012.

[Ta96] Tanenbaum, Andrew S.: Computer Networks. 1996.

[VM15] Valasek, Chris; Miller, Charlie: Remote Exploitation of an Unaltered Passenger Vehicle. Black Hat Conference, 2015.

[We05] Werner, Martin: Netze, Protokolle, Schnittstellen und Nachrichtenverkehr. 2005.

[Wi13] Wilfried, Plassmann: Handbuch Elektrotechnik. Springer Vieweg, 6 edition, 2013.

[Zi07] Zimmermann, Schmidgall: Bussysteme in der Fahrzeugtechnik. Vieweg, 2nd edition, 2007.

[ZMC09] Zhang Min, Dusi Maurizio, John Wolfgang; Changjia, Chen: Analysis of UDP Traffic Usage on Internet Backbone Links. Applications and the Internet, 2009. SAINT '09. Ninth Annual International Symposium on, 2009.