TECHNISCHE UNIVERSITÄT
CHEMNITZ

# Automotive Communication Buses

## Seminar Report

Chair of Computer Engineering
Dept. of Computer Science

Submitted By: Sachin Bainur
Matrikel Nr.: 610982
Submission Date: 30.08.2020

Supervising Tutor: Prof.Dr. W. Hardt
Prof. Uranchimeg Tudevdagva
Dipl. Inf. Rene Schmidt

# Abstract

This work provides a summary of the automotive bus systems, including current technology and future bus systems. As far as their defense against various attacks is concerned. At present, a broad variety of automobile communication networks have been established due to different car domain requirements. Some of viable attacks and future vulnerabilities for these networks will be presented followed by a brief overview of the best known and current automotive communications systems. Later, a secure automotive communication solution focused on standard encryption mechanisms to overcome most vehicle safety problems, providing confidentiality and authentication will be presented.

# Contents

# List of Figures

# List of Tables

# List of Abbreviations

| | |
|---|---|
| **VDC** | Vehicle Dynamics Control |
| **ECU** | Electronic Control Unit |
| **ACC** | Adaptive Cruise Control |
| **ESP** | Electronic Stability Program |
| **MOST** | Media Oriented Systems Transport |
| **GSM** | Global System for Mobile Communications |
| **CAN** | Controller Area Network |
| **OSI** | Open Systems Interconnection |
| **SOF** | Start Of Frame |
| **RTR** | Remote Transmission Request |
| **IDE** | Integrated Development Environment |
| **DLC** | Data Link Connector |
| **CRC** | Cyclic Redundancy Check |
| **ACK** | Acknowledgment |
| **EOF** | End Of Frame |
| **IFS** | Inter Frame Space |
| **SRR** | Substitute Remote Request |
| **LIN** | Local Interconnect Network |
| **EMI** | Electromagnetic Interference |
| **RFI** | Radio-Frequency Interference |
| **TDMA** | Time-Division Multiple Access |
| **CSMA** | Carrier-Sense Multiple Access |
| **OEM** | Original Equipment Manufacturer |
| **MAC** | Media Access Control Address |

# 1 Introduction

Automotive systems are complex distributed computer systems with diverse networking requirements today. Most car manufacturers share that subcontractors and more subsystems are expected to communicate in a modern automotive system built by various subcontractors. Support for distributed organized behavior requires advanced subsystems features, such as Vehicle Dynamics Control (VDC).The automotive subsystem shall consist of one or more electronic control units ( ECUs). An automotive communication system consisting of a variety of subsystems, up to 80 ECUs, with more than 3000 variables and signals to transmit. In several ways, this complicates the automotive environment, like networking. The automotive industry in recent years has set up many large consortiums to decide on a shared electronic architecture and communication network to address this challenge and to help the automotive systems of tomorrow. The next step is to replace the majority of automotive subsystems such as steering and braking with wires, electrical sensors, and actuators. These new solutions are often referred to as x-by-wire systems[13].

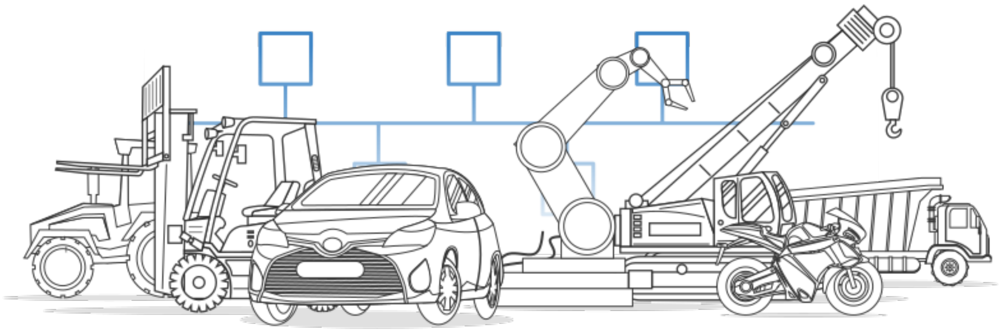


Figure 1.1: Automotive Communication Buses[4]

The requirements of the communication network originate from the applications and subsystems it needs to support [2]. Today, numerous networking systems are employed to meet the specific communication criteria set by these subsystems. There is a need for high bandwidth, versatility, and determinism to interconnect these systems. Many subsystems are vital to protection, too. A large number of current network technologies is an important concern for the automotive industry. From a technological point of view, it is also beneficial to use fewer and more general technologies. To minimize the complexity, a set of network technologies should be applied, which are typically found in an automobile framework in most applications.

In order to support tomorrow's automotive systems, these networking technologies need to be interconnected. This interconnection should provide timeliness, composability, and fault-tolerance across the board "Networks of Network"[14].

Further communication networks for vehicles provide access to a range of critical components such as breakage, airbags, and engine control. Cars equipped with driving support systems such as ESP or ACC (Adaptive Cruise Control) allow for a grave operation in-vehicle driving conduct. The underlying automotive data networks are entirely reliant on modern electronics, including vehicle control systems Drive-by-Wire. Present automotive communications networks guarantee protection against much technological interference but are not specifically secured against malicious attacks. The growing connection of unsecured automotive control networks with modern automotive multimedia networks such as MOST, GigaStar, as well as wireless communication integration such as GSM, or Bluetooth entails many additional security risks.

# 2 CAN

## 2.1 Overview

The Controller Area Network (CAN) is a serial communication bus that provides fast, versatile performance, especially in industrial and motor applications. It can withstand rough environments. The model Open Systems Interconnection (OSI) consists of the data link and physical layer, developed by Bosch and later encoded as ISO 11898-1. This provides a low-level networking solution for high-speed communication in vehicles[11]. Moreover, CAN was built to eliminate cord wiring so that one pair of cables could communicate with the separate electronic control units ( ECUs) within a vehicle [12].

## 2.2 CAN Message Frames

There are 4 types of CAN frames namely (1)Data frame, (2)Remote frame, (3)Error frame (4)Overload frame. The data frame is used to transmit data from the transmitter to other nodes on the bus. The transmitter transmits a remote frame to ask for data from a certain node. Any node that detects a bus error can transmit an error frame. For data interruption overload frames are used. Figure 2.1 shows both 2.0A and 2.0B data frames. CAN 2.0B accepts both 11 bits(standard) and 29 bits(extended) identifiers, It is the principal distinction between the two data frames. In general, both standard and extended frames can exist on the same bus and even have the same identifier, in that case, standard frames are prioritized[7].

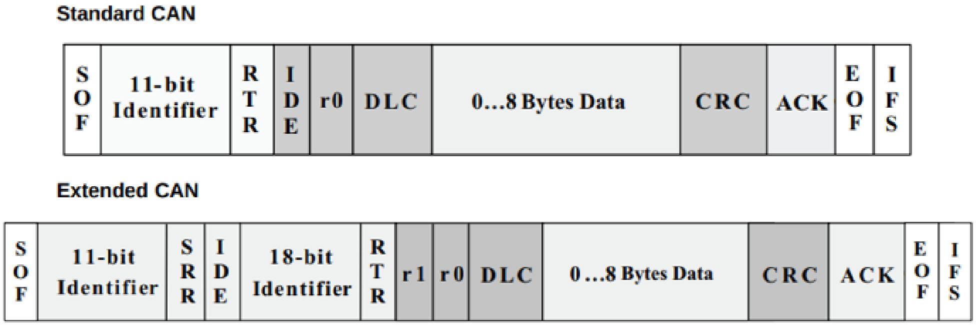


Figure 2.1: CAN Data Frames [3]

### 2.2.1 Standard CAN Frame

- SOF: Start of frame bit marks the beginning of a message and uses it to coordinate the nodes in a bus.
- Identifier: The 11-bit standard CAN ID sets the message priority.
- RTR: When information from another node is needed, the RTR bit is dominant. All nodes get the message, but the specified node is decided by the identifier.
- IDE: Indicates standard CAN or extended CAN.
- r0: Reserved bit for future modifications.
- DLC: Indicates total amount of data transmitted in bytes.
- Data: 64 bits of data can be transmitted.
- CRC: Cyclic redundancy check is used to provide quality integrity.
- ACK: Each node that receives the correct message overwrites this recessive bit and implies an error-free transmission in the original message.
- EOF: Indicates the end of frame.
- IFS: This 7-bit IFS include the time needed to transfer a frames obtained properly in the message buffer region by the controller.

### 2.2.2 Extended CAN Frame

The extended CAN message is similar to the standard message except that it has 21-bit identifier and some additional fields[3].

- SRR: RTR in standard CAN is replaced by Substitute Remote Request in Extended CAN frame.
- r1: Another reserve bit similar to r0.

# 3 LIN

## 3.1 Overview

In 1998, a group of car companies (Audi, BMW, Daimler Chrysler, Volcano, Volvo and Volkswagen) together with Motorola launched the Local Interconnect Network (LIN)[29]. In 2000 (LIN 1.1) and 2003 (LIN 2.0) LIN was standardized (open standards) and launched in 2001 in the first production car set. It now has a good role in the field of automotive applications where it coexists well with CAN. LIN is a cheap network that provides network speeds of up to 20 KBps. LIN is usually used for monitoring of systems such as seat monitoring, light sensors and temperature control in the body and comfort subsystems. For instance, a subsystem can be a car door with all its functions such as window lifts, door locks, etc. Such subsystems are then interconnected (usually) through a LIN / CAN gateway via the CAN network. LIN is also used in conjunction with CAN, as LIN complements CAN by providing much cheaper and easier communication with traditional automotive subsystems that are not linked to safety[13].

## 3.2 LIN Bus Working

LIN bus is fairly easy at its core.A master node iterates through each and every slave nodes in bus system requesting for data. Slave node response with data whenever it is polled otherwise master moves to next slave[5]. Nevertheless, new features have been introduced to the LIN specification with each specification update-making it more complicated[15].

## 3.3 LIN Bus Fames

A header and a response is the LIN bus message frame. A header block is normally sent by the LIN master to the LIN bus. This induces a slave with up to 8 bytes of data responses. This LIN frame can be seen as follows:

- Break: The break is at least 13 + 1 bits long (and normally 18 + 2 bits in practice). The Break field serves as a ”start of the frame” for all LIN nodes on the bus.

- Sync: The field Sync 8 bit is pre-defined by 0x55(01010101). The LIN nodes will set the baud rate by determining time between rise and fall of edges.

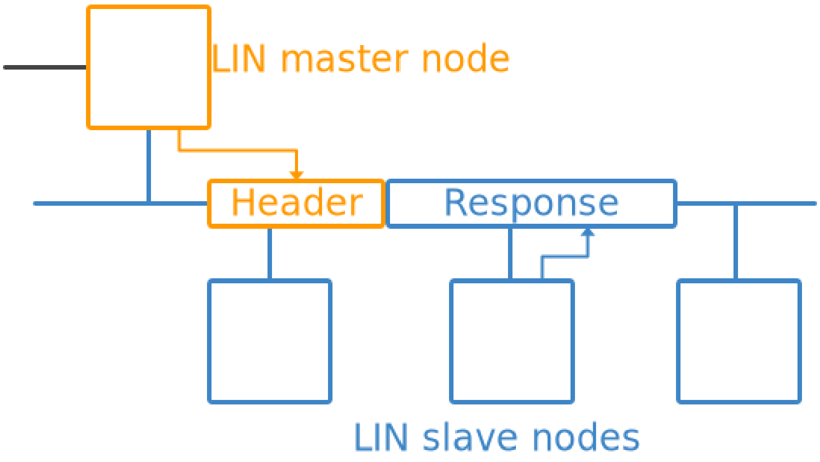


Figure 3.1: LIN Bus Working Principle[5]

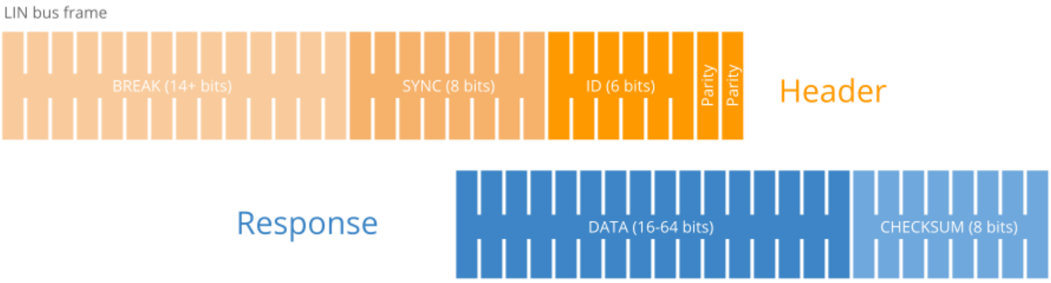


Figure 3.2: LIN Bus Frame[5]

- Identifier: 6 bits are defined followed by 2 bits. For each LIN packet sent, the ID is used as an identifier, which nodes respond to the header.
- Data: If the master intercoms a LIN slave it can reply by two, four or eight bytes of data.
- Checksum: As with CAN, the integrity of the LIN frame is ensured by an checksum field.

# 4 FlexRay

## 4.1 Overview

BMW and Daimler-Chrysler evaluated existing automotive network systems (e.g., May, TTP, MOST) in 1998 and found that none of these technologies meet the future requirements of next-generation car systems, especially when the automotive industry is going to take the next step towards x-by-wire.

The FlexRay consortium[9] was formed in response to this to create a new protocol. FlexRay offers up to 10 MBps of network bandwidth. This new protocol will be the solution for implementing the x-by-wire systems as well as replacing some of the existing field buses, decreasing the total number of in-car networking technologies. Today, virtually all car manufacturers have joined this group and the specifications for the protocol were made public in the middle of 2004.

For high-speed automotive control applications connecting ECUs in the future automotive network, FlexRay is expected to be the de-facto communication standard. High-speed safety-critical vehicle technologies like x-by-wire and advanced powertrain applications would be of particular interest.

## 4.2 FlexRay Schedule

Bus interaction is structured in accordance with a cyclically stable, four-segmented structure

- Static: Automatically defined transmission time. Consisting of set slots in constant length.
- Dynamic: Dynamic time, time transmission can be different.
- Symbol Window(optional).
- Network Idle Time.

The cycles and segments begin at the same time in dual channel systems however, time can be different on both networks.

## 4.3 FlexRay Frame Structure

- The header has 5 initial bits (a)Reserved bit, (b)Payload preamble indicator, (c)Null frame indicator, (d)Sync frame indicator and (e)Startup frame indicator.
- Frame ID: Indicates where the frame should be transmitted.
- Payload Length: Indicates the number of data bytes.
- Header CRC: It is checksum for the header.
- Cycle Count: This is according to the transmitter.

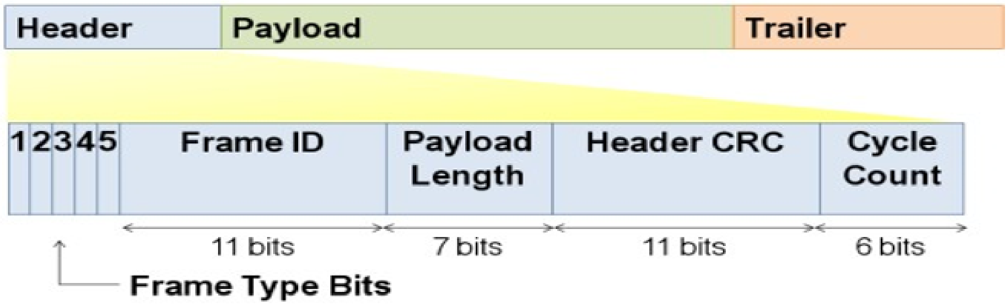


Figure 4.1: FlexRay Frame Format[1]

# 5 MOST

## 5.1 Overview

MOST are widely used to provide communications for multimedia applications. MOST was introduced in 1997, primarily for automotive media communications, and has many sponsors such as Volkswagen, BMW, and Daimler-Chrysler. MOST applications are typical for multimedia and infotainment interconnections, such as video displays, GPS, active speakers, and digital radios.Typical MOST system is shown in figure 5.1.

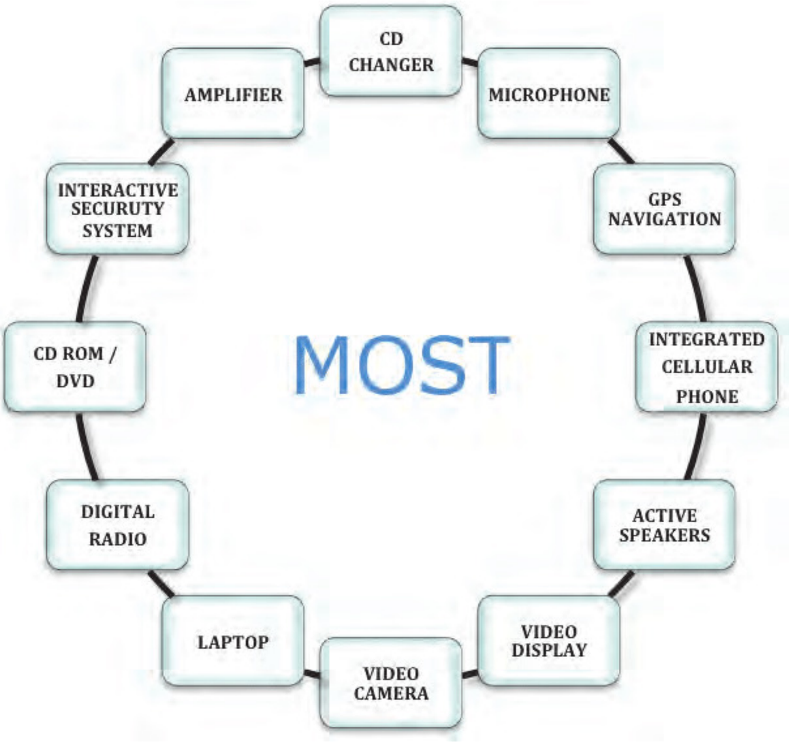


Figure 5.1: MOST Bus System[6]

## 5.2 MOST Layer Architecture

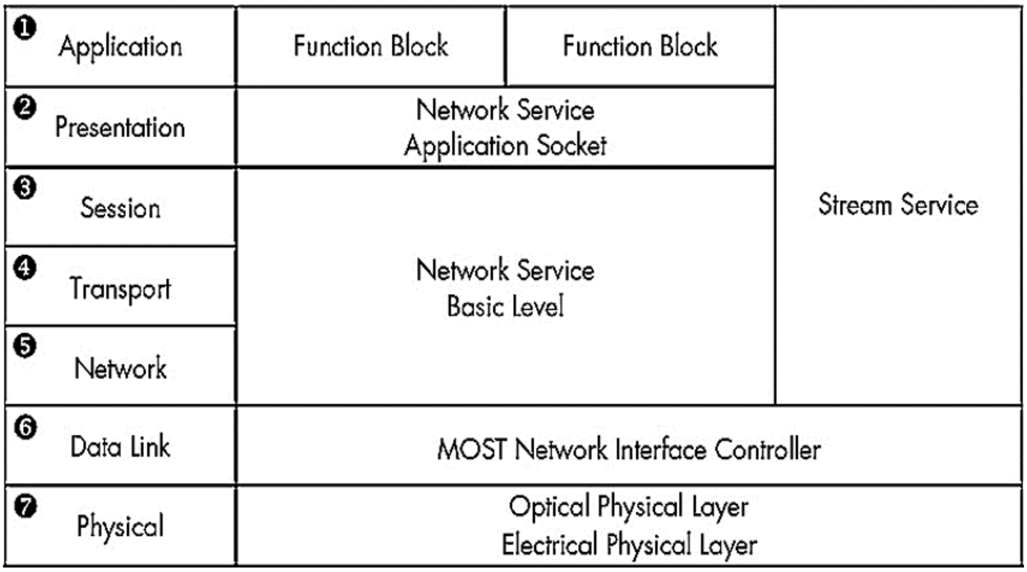
With the introduction of the MOST system, car manufacturers had two fundamental demands on the design of the infotainment bus system:

1. A basic device concept based on a practical perspective.

2. Transmission of streaming and packet data along with control information.

The first demand led to the creation of the MOST architecture with function blocks. It contains all the MOST software properties and methods ( e.g., CD changer) needed to operate the system. The application protocol, which is a self-declaring notation without the requirement of the MOST device address, transmits certain feature blocks. It is therefore possible to design the infotainment domain easily and quickly with a high level of abstraction. The functional blocks form the application interface and thus are included in layer 7 of the ISO / OSI model(as in figure 5.2).

The second demand with the frame structure was achieved. This transmits multimedia data synchronously and can transmit asynchronously large amounts of data, offering a control channel for controller commands and status messages without disrupting the synchronous transmission. The message is used in the program protocol[6]. According to the above mentioned second request, the data link layer is based on the asynchronous transfer of data frames. Apart from a more regular optical bit transmission layer, an electrical physical layer is also available i.e MOST Network Interface Controller.



| | | | |
|---|---|---|---|
| ❶ Application | Function Block | Function Block | Stream Service |
| ❷ Presentation | Network Service<br>Application Socket | | |
| ❸ Session | Network Service<br>Basic Level | | |
| ❹ Transport | | | |
| ❺ Network | | | |
| ❻ Data Link | MOST Network Interface Controller | | |
| ❼ Physical | Optical Physical Layer<br>Electrical Physical Layer | | |

Figure 5.2: MOST Layer Architecture[6]

# 6 Comparison of Bus Systems

| **Bus** | **Adapted for** | **Target Applications** | **Transfer Modes** | **Data Rate** | **Physical Layer** |
|---|---|---|---|---|---|
| LIN | Low-level Subnets | Door locking, power windows, rain sensor, lights | Synchronous | 20 kBit/s | Single-Wire |
| CAN | Soft Real-Time | Antilock break system, Driving assistants, Engine control, Electronic gear box | Asynchronous | 1 MBit/s | Dual-Wire |
| FlexRay | Hard Real-Time | Break-by-Wire, Steer-by-Wire, Shift-by-Wire, Emergency systems | Synchronous & Asynchronous | 10 MBit/s | Optical Fiber or Dual-Wire |
| MOST | Multimedia Telematics | Entertainment, Navigation, Information services, Mobile Office | Synchronous & Asynchronous | 24 MBit/s | Optical Fiber |

Table 6.1: Comparison of Bus Systems[16]

# 7 Other Technologies

## 7.1 Ethernet

Automotive Ethernet is a physical network that is used to link components within a vehicle using a wired network. It has been adapted for the automotive sector, including electrical requirements, sensitivities, frequency and latency (EMI / RFI) requirements. To completely satisfy the automotive requirements, several new standards and updates to standards are being performed in the IEEE 802.3 and 802.1 classes.

By 2022, it is projected that 40 percent of the cost of a vehicle will be in electronics (up from about 32 percent today). New security, infotainment, and communication features and technologies will drive this increase[8]. By 2025, auto wires would switch from heterogeneous proprietary protocol networks to hierarchically homogeneous car networks like Ethernet networks. In the latest model, switched 1GE automotive Ethernet will interconnect all the domains in the car.

## 7.2 TT-CAN

Initiated in 1999 as a time-triggered session layer on the top of the CAN. TT-CAN is a TDMA hybrid on top of CSMA that enables both time-controlled and event-controlled traffic[10]. TT-CAN is ISO standardized and x-by-wire controlled. It does not, however, have the same fault tolerance as the other x-by-wire applicants like FlexRay. TT-CAN strong points help coexisting events and time-consuming traffic along with ISO standardization. The standard CAN with a simple change can be converted to TT CAN. Also, TT-CAN controllers exist off-the-shelf.

# 8 Security in Automotive Bus Systems

## 8.1 Overview

Since electronic devices are integrated into vehicles, the target for malicious attacks or handling was also often feasible. The use of miles, unauthorized chip tuning, or tachometer spoofing [An98], even more, straightforward examples, has already become popular. Additional future automated vehicle technologies such as electronic tachographs, e-tolls and electronic license plates, or paid information services (Location-based Services) increase risks. In particular, the drivers' protection of their car and all the surrounding road users could be threatened by unauthorized vehicle modifications.

Figure 8.1: Automotive Security

Some traditional features of current vehicle bus systems make access fairly convenient to unauthorized users. The publicly accessible documents for most vehicle cars describe the potential bus messages and their respective mechanisms and contact procedures. Besides, controllers cannot check whether an incoming message is from an authorized sender.

The key threat, however, is that all automotive bus systems are interconnected. The net-spanning data sharing across various gateway systems enable access from any current bus network to any other bus. Each control will generally send messages to other existing car controllers on each LIN, CAN, or MOST controller. A single constructed bus system without practical preventive steps thus compromises the entire vehicle communication network. The consequences of active attacks vary from moderate comfort constraints to the possibility of an accident. The probability of an attack and the degree of safety of a particular bus system depends on the potential consequences of failure or exploitation.

## 8.2 Possible Threats

- Using the reliance of the LIN slave on the master and attacking this single failure point.
- In CAN jamming the communication channel by regularly introduced higher priority useless message.
- In FlexRay attacks on the standard time base, which would make the FlexRay network completely in-operative.
- Introducing malicious timing frames can interrupt the MOST synchronization mechanism.
- Wireless interfaces can be an easy target for viruses and malware.

## 8.3 Approaches to Security

The high-end communication protection is needed as an enabling environment for most future vehicular applications. In general, it is critical that all the transmitted information can be displayed and obtained only by the parties concerned, that no possible modifications can be hidden and non-authorized parties can not participate in the communication. Most vehicle safety problems are solved by modern communication security mechanisms, confidentiality, protection, and authentication based on cryptographic algorithms and protocols. A series of measurements can avoid unregulated interference in-vehicle communication networks. Below are three basic practices in order to ensure the safety of vehicle bus communication.

### 8.3.1 Authentication of Controller

Both sender and receiver must be authenticated to ensure the bus network only contains legitimate controllers. Any communications not approved can then be handled either separately or canceled immediately. Each controller, therefore, requires a certificate to be authenticated as a legitimate sender against the gateway. The certificate shall contain the controller identifier, the public key, and the respective controller's authorizations. The gateway currently holds the public keys of all OEMs, which are licensed by the respective vehicle manufacturer. With its respective secret key, each controller certificate is signed by the OEM digitally.

### 8.3.2 Encrypted Communication

The encryption of all automotive data transmissions is a crucial step to strengthen the protection of automotive bus communication. The combination of symmetric and asymmetric encryption meets the requirements of adequate security[16]. Although fast, efficient symmetric encryption ensures internal communication of bus transmission, asymmetrical encryption is used for the safe distribution of the key required[16]. Throughout this case, all local bus system controllers use the same symmetrical, frequently modified key to encrypt the internal bus communication. Asymmetric encryption provides the acquisition for newly added approved controllers of the symmetrical key and the periodic updating of the symmetric key as well as the required authentication procedure.

### 8.3.3 Gateway Firewalls

Gateways have to implement capable firewalls to complete automobile bus communication security, where the vehicle controllers are able to execute digital signatures or MACs, the firewall rules are based on permissions issued by the certificates of each controller. Therefore, valid messages can only be transmitted to bus systems by approved controllers. If digital signatures or MACs can not be used by the vehicle controls, firewall rules can only be set on the authorizations of each subnet [16]. In general, however, controllers with less restrictable networks such as LIN or MOST do not send messages to high-security bus systems such as CAN or FlexRay.

# 9 Conclusion

An overview of the current automotive networking technologies has been presented in this report, which describes conventional and modern automotive bus systems and identifies various safety issues. The report addressed the following measures in automotive communications and concentrated on x-by-wire systems. It has also identified an approach using current communication safety mechanisms to overcome most of the safety problems in vehicles. One of the greatest challenges today is to link up a new car architecture with probably heterogeneous networks. This can be done by designing highly secured and structured middleware technologies.

# Bibliography

[1] Overview of the flexray automotive communication bus - ni. https://www.ni.com/de-de/innovations/white-papers/06/flexray-automotive-communication-bus-overview.html (May 2019), (Accessed on 08/29/2020)

[2] AREA, B.S.A.: Automotive bus systems

[3] Cook, J., Freudenberg, J.: Controller area network (can). EECS 461, 1–5 (2007)

[4] CSSElectronics: Can bus explained - a simple intro. https://www.csselectronics.com/screen/page/simple-intro-to-can-bus/language/en (2020), (Accessed on 08/29/2020)

[5] CSSElectronics: Lin bus explained - a simple intro. https://www.csselectronics.com/screen/page/lin-bus-protocol-intro-basics/language/en (2020), (Accessed on 08/29/2020)

[6] Grzemba, I.A.: MOST: the automotive multimedia network. Franzis Verlag (2012)

[7] HPL, S.C.: Introduction to the controller area network (can). Application Report SLOA101 pp. 1–17 (2002)

[8] Ixia, T.: Automotive-ethernet-ltr.indd. https://support.ixiacom.com/sites/default/files/resources/whitepaper/ixia-automotive-ethernet-primer-whitepaper_1.pdf (May 2014), (Accessed on 08/29/2020)

[9] Koopman, P.: The flexray protocol. Electrical and Computer Engineering, Carnegie Mellon University (2004)

[10] Leen, G., Heffernan, D.: Time-triggered controller area network. Computing & Control Engineering Journal 12(6), 245–256 (2001)

[11] Liu, H., AN, J.p., YANG, J.: Vehicle network communication protocols—comparison and case study

[12] Michael, S.S.: Introduction to can (controller area network) - technical articles. https://www.allaboutcircuits.com/technical-articles/introduction-to-can-controller-area-network (Feb 2019), (Accessed on 08/29/2020)

[13] Nolte, T., Hansson, H., Bello, L.L.: Automotive communications-past, current and future. In: 2005 IEEE Conference on Emerging Technologies and Factory Automation. vol. 1, pp. 8–pp. IEEE (2005)

[14] Poledna, S., Ettlmayr, W., Novak, M.: Communication bus for automotive applications. In: Proceedings of the 27th European Solid-State Circuits Conference. pp. 482–485. IEEE (2001)

[15] von der Wense, H.C.: Introduction to local interconnect network. Tech. rep., SAE Technical Paper (2000)

[16] Wolf, M., Weimerskirch, A., Paar, C.: Security in automotive bus systems. In: Workshop on Embedded Security in Cars. pp. 1–13. Bochum (2004)