# 智能网联车网络安全研究综述

吴武飞[1]，李仁发[2]，曾刚[3]，谢勇[4]，谢国琪[2]

（1. 南昌大学信息工程学院，江西 南昌 330031；2. 湖南大学信息科学与工程学院，湖南 长沙 410082；
3. 名古屋大学工学院，爱知 名古屋 464-8601；4. 厦门理工学院计算机与信息工程学院，福建 厦门 361024）

**摘 要**：针对汽车的网络攻击不仅会造成隐私泄露和经济损失，严重情况下还会危及生命安全，甚至上升为国家公共安全问题，因此智能网联车网络安全问题已成为当前研究的热点。首先，对智能网联车中车载网络的结构现状和特点进行了介绍，阐述了车载网络安全面临的设计约束和挑战。其次，结合车载网络当前面临的功能安全和信息安全问题，综述了近年来车载网络安全方面国内外最新研究进展。最后，从车载网络结构的特点出发，从标准建设、功能安全和信息安全 3 个方面，围绕智能网联车网络信息安全问题指出了一些重要的研究方向和建议。

**关键词**：智能网联车；车载网络；分布式实时系统；网络安全；功能安全关键系统

**中图分类号**：TP393

**文献标识码**：A

**doi:**10.11959/j.issn.1000−436x.2020130

# Survey of the intelligent and connected vehicle cybersecurity

WU Wufei[1], LI Renfa[2], ZENG Gang[3], XIE Yong[4], XIE Guoqi[2]

1. School of Information Engineering, Nanchang University, Nanchang 330031, China
2. College of Computer Science and Electronic Engineering, Hunan University, Changsha 410082, China
3. Graduate School of Engineering, Nagoya University, Nagoya 464-8601, Japan
4. College of Computer and Information Engineering, Xiamen University of Technology, Xiamen 361024, China

**Abstract:** Cyber attacks on vehicles not only cause privacy leaks and economic losses but also endanger human life and even rise to national public safety issues. Therefore, the research on the cybersecurity of intelligent and connected vehicle (ICV) has become a research hot spot. Firstly, the structural status and characteristics of the in-vehicle network (IVN) in ICV were introduced, and the challenges and constraints of cybersecurity enhancement design for IVN were also presented. Secondly, focusing on the current functional safety and cybersecurity issues of IVN, a survey of the current cybersecurity enhancement researches for IVN was conducted. Finally, according to the characteristics of the IVN structure, some important research directions and suggestions about cybersecurity problems of ICV were pointed out from the three aspects of standard construction, functional safety and cybersecurity.

**Key words:** intelligent and connected vehicle, in-vehicle network, distributed real-time system, cybersecurity, functional safety critical system

## 1 引言

随着车联网时代的到来，智能网联车技术在国家社会经济发展中发挥着越来越重要的战略作用[1-2]，并渗透到社会各领域。在车联网不断朝“云–管–端”架构发展的趋势下，作为终端节点[3]，其发展不断显现出智能化、电动化、共享化、网联化——新四化的特征。与此同时，随着新四化的逐步推进，将有更多机械部件逐步被电机控制、动力电池等电动化系统取代[4]。智能网联车电子系统逐步演变为集

**收稿日期**：2019–11–18；**修回日期**：2020–05–22

**基金项目**：国家自然科学基金资助项目（No.61932010, No.61872436）

**Foundation Item:** The National Natural Science Foundation of China (No.61932010, No.61872436)

感知、计算、网络和控制为一体的信息物理融合系统（ACPS, automotive cyber physical system），其中车载网络（IVN, in-vehicle network）变得与感知、计算和控制同等重要[5-6]。

智能网联车在为人们的交通出行带来舒适便捷的同时，系统复杂化和对外通信接口的增加[7]使车载网络更容易受到网络攻击，近年来，不断发生的汽车信息安全召回事件已经引发各界的高度关注[8-9]。鉴于 ACPS 的功能安全关键属性，针对车载网络的攻击，不仅会造成个人隐私泄露和经济损失，严重时还会危及生命安全，甚至上升为国家公共安全问题。因此智能网联车网络安全问题已经成为当前学术界和汽车工业界共同关注的热点[10-11]。

安全一直以来都是人们对汽车的永恒追求，汽车的安全问题同时包含功能安全和信息安全 2 个方面。两者既相互关联，在计算和网络等资源上又存在竞争关系，这使智能网联车的网络安全问题变得更加复杂。一个安全的汽车电子系统至少要满足系统的保密性、完整性及可用性要求，对于 ACPS 而言，数据的真实和完整最关键。然而面对信息安全威胁，现有车载网络协议在设计之初缺乏信息安全考虑，亟待进行信息安全增强。其中车载网络作为构建整个智能网联车的内部网络核心，其协议的设计和应用与汽车安全高度相关，是车联网实现汽车这一终端节点安全防护的重点领域。出于成本和性能的均衡考虑，当前车载网络存在带宽受限、强实时和确定性时延的要求和特点，这导致传统的信息安全增强手段无法直接使用在车载网络环境下。

本文主要综述了智能网联车网络安全方面的相关研究，介绍了车载网络的背景、现状、架构和网络安全技术设计面临的约束。围绕车载网络安全问题，对国内外研究现状进行了综述和比较分析，并对车载网入侵检测技术进行了重点阐述。最后结合车载网络结构的特点，从标准制定、系统功能安全和信息安全 3 个方面提出了智能网联车网络安全相关的 5 点研究建议。

## 2 背景介绍

### 2.1 智能网联车车载网络介绍

如图 1 所示，在网络视角下，作为车联网架构中的移动终端，智能网联车是一个异构分布式实时系统，车载电子控制单元（ECU, electronic control

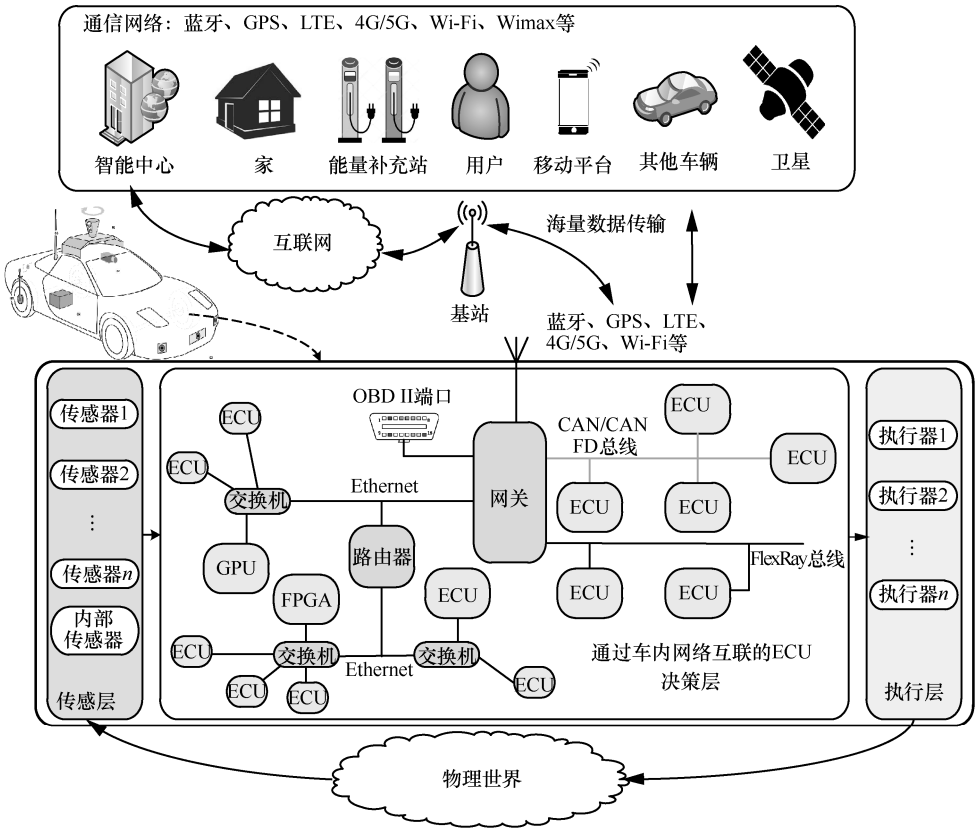



图 1 网络视角下智能网联车电子系统结构

unit）由异构网络（控制器局域网络（CAN, controller area network）、本地互联网络（LIN, local interconnect network）等）连接，不同网络之间通过网关实现信息交互，网络体系结构呈现异构、实时、成本敏感等特点[12]，其主要特征如下。

1) 丰富的对外接口。随着车用无线通信技术（V2X, vehicle to everything）的发展，智能网联车具有互联化特征，即汽车将不再是一个独立的电子系统，而是车联网架构下的一个移动终端，为实现车与 X（例如车、路、人、云等）的信息交换，将配备丰富的对外通信接口（例如蓝牙、GPS、4G/5G、Wi-Fi 等）。与此同时，通信需求增加和对外接口丰富将导致网络攻击入口和形式的多样化。

2) 大量的实时数据。车载信息娱乐系统（IVI, in-vehicle infotainment）、电子驾驶舱（e-cockpit）、高级辅助系统（ADAS, advanced driving assistant system）、人工智能（AI, artificial intelligence）和传感器（如 LiDAR、Radar、摄像头等）驱动的自动驾驶都会产生大量数据，需要实时传输和处理，然而现有车载网络协议无法满足其带宽要求，通用以太网（Ethernet）又无法提供确定性时延保障。为满足汽车功能不断增长的带宽要求，近年来，具有确定性时延特性的高速车载网络协议得到快速发展，例如时间敏感型车载以太网和 FlexRay[13]、Ethernet TSN（time-sensitive networking）[14]，其中 FlexRay 被应用于线控刹车（drive-by-wire）系统中，这正是利用了其确定性时延的特点。

3) 异构的网络环境。长期以来，出于成本和性能的均衡考虑，汽车电子系统处于多种网络协议共存的状态，不同的网络协议应用于不同功能域（例如骨干网络的 FlexRay[13]、用于动力控制及诊断系统的高速 CAN[15]和应用于车身控制的低成本 LIN[16]），它们之间将通过网关互联以构建整体的车载网络架构。如图 2 所示，车载网络结构具有异构、分布式和实时的特点，其异构不仅体现在硬件平台，同时也包括网络的异构[12]。

4) 信息安全保护机制缺乏。传统汽车是一个相对独立和封闭的个体，因此车载网络设计之初并未考虑外部网络安全威胁问题，即现有的网络协议缺乏基本的安全机制（如认证、加密及接入控制等），随着车联网朝着“云–管–端”架构的发展，智能网联车作为终端节点，亟需开展车联网终端节点的网络安全增强技术研究以提高网络安全性。

综上所述，智能网联车中，车载网络需求呈现高带宽（满足大数据量的通信需求）、信息安全保障和低时延（确保实时通信，保障安全）这三大特征。为避免 ISO 标准 7 层协议带来的过多时间开销，车载网络通常划分为 3 层，即应用层、数据链路层和物理层，其中应用层直接接入数据链路层。当前主流车载网络协议的比较与分析如表 1 所示。

### 2.2　车载网络的分类

根据带宽和功能域的不同，汽车工程师协会（SAE, Society of Automotive Engineer）将网络协议分为 A、B、C、D 这 4 类，其代表协议及主要应用

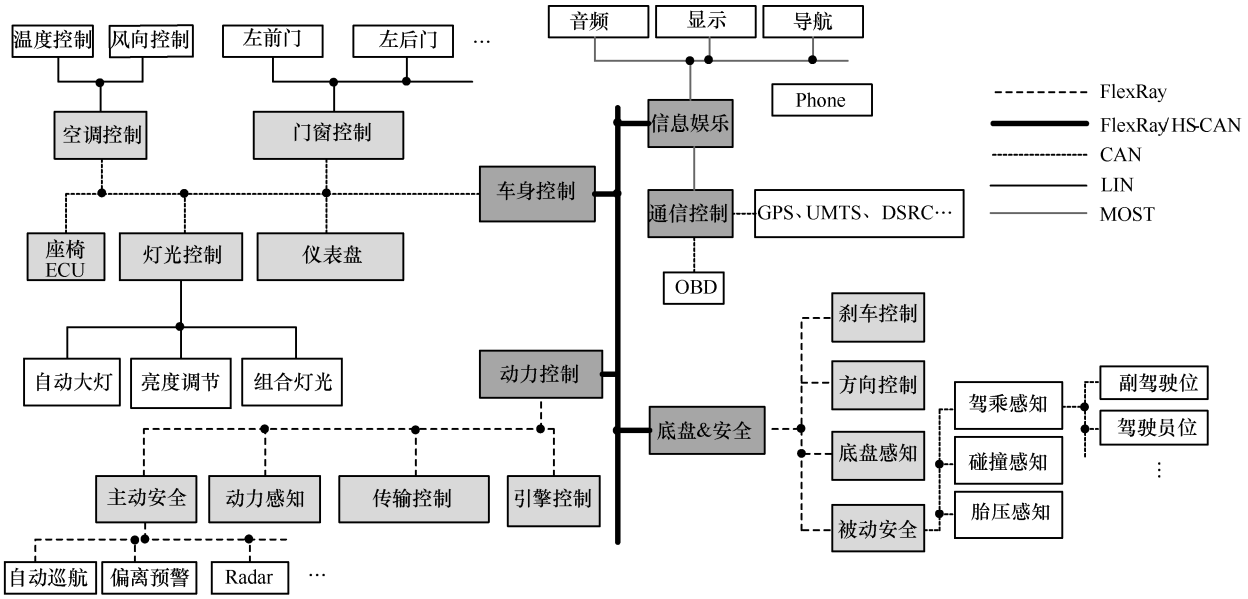



图 2　一种典型的车载网络结构

表 1 面向智能网联汽车的主流车载网络协议比较分析

| 主流车载网络协议 | 最高带宽 | 最大数据负载/B | 最小响应时间 | 实现技术 | 触发方式 | 最长总线/m | 支持节点数/个 | 节点成本 | 可扩展性 | 扩展协议 |
|---|---|---|---|---|---|---|---|---|---|---|
| LIN | 1~20 kbit/s | 8 | 12.8 ms | 主从 | 轮询 | 40 | 16 | 低 | 高 | 无 |
| CAN | 10 kbit/s~1 Mbit/s | 8 | 130 us | CSMA/CR | ET | 40 | 128 | 中等 | 高 | FTT-CAN[17]、TTCAN[18]、CAN-FD[19] |
| FlexRay | 10 Mbit/s | 254 | 65 us | TDMA+CSMA | ET/TT | 未定 | >16 | 中等 | 中等 | 最新规范为 V3.0.1[13] |
| MOST | 150 Mbit/s | 3072 | 333 us | TDMA | TT | 未定 | 64 | 高 | 低 | MOST50[20]、MOST150[21] |
| Ethernet | 1 Gbit/s | 1500 | 12 us（1 GB）、120 us(100 MB) | CSMA | ET/TT | 100 | 无特定 | 低 | 高 | Ethernet AVB[22]、Ethernet TSN[14]、TTEthernet[23] |

表 2 车载网络协议的分类

| 类型 | 代表协议 | 应用领域 | 成本 |
|---|---|---|---|
| A | LIN | 车身，如行李箱开启关闭、车窗控制等数据量小的场合 | 低 |
| B | 低速 CAN(SWC)、CAN2.0、TTP/A | 车身电子，非诊断和安全关键数据 | 低 |
| C | 高速 CAN（HSCAN）、TTP/C、CAN-FD | 传动装置、移动装置、诊断、线控 | 中 |
| D | FlexRay | 动力、底盘等硬实时和高可靠性要求领域 | 高 |
| | Safe-by-wire、Byte-flight | 安全相关的实时和可靠领域 | 高 |
| | MOST、IDB-1394、Ethernet | 多媒体（音频、视频） | 高 |

领域如表 2 所示。由于不同类别网络协议在节点部署成本网络带宽、响应时间和可扩展性不同，各自适用的汽车应用领域也不同[24-25]。

为保障功能安全性，智能网联车要求车载网络在数据链路层上优先保障确定性时延及硬实时的性能，同时在物理层上还要具有较高的抗干扰能力。车载网络可分为时间触发（TT, time triggered）和事件触发（ET, event triggered）2 种。TT 是指以时间点为通信触发条件，一般通过定时和时间同步的方式来实现。ET 是指通信触发条件，即某一事件的发生，例如当汽车安全气囊系统检测到碰撞事件发生后，通过触发传感器所在 ECU 发送包含控制参数的数据帧来引爆气囊。当前车载网络中时间触发型网络主要有 TTCAN[18]、TTEthernet[23]、TTP/C[26]等。TT 型车载网络具有带宽高、传输时延确定的特点，弥补了 ET 型车载网络在确定性时延方面的不足，可应用于线控刹车领域，但同时也存在节点部署成本高、系统可扩展性较差的缺点。在灵活性和扩展性及成本方面，ET 型网络如 LIN、CAN 等又具有明显优势。

## 3 车载网络信息安全问题分析

### 3.1 严峻的信息安全威胁

车载 CAN[15]作为当前车载网络标准协议，在设计之初缺乏消息认证和数据加密机制。随着更多的消费类电子产品可以便捷地接入，智能网联车使汽车成为带轮子的智能移动设备，软件和数据服务的先进性逐渐成为汽车的核心竞争力。如果不及时开展车载网络安全增强研究和部署，就会因潜在的安全漏洞而遭受各方面的恶意攻击[27]。近 10 年来针对汽车的网络供给分析与比较如表 3 所示。从攻击方式来看，近年来针对汽车的信息安全威胁主要可以分为直接物理接入攻击、近距离无线攻击和远程无线攻击 3 种实现方式。直接物理接入攻击主要通过非法接入 CAN、车载诊断系统（OBD, on-board diagnostic）诊断接口等方式；近距离无线攻击主要通过蓝牙和无线传感器信道非法接入的方式；远程无线攻击主要通过 Wi-Fi 和移动数字蜂窝网络端口实现非法接入。

### 3.2 缺乏信息安全保障的车载网络

现有的车载网络协议，例如 CAN 和 FlexRay 等在设计之初均缺乏信息安全机制设计，这使车载网络极易受到嗅探、伪造、修改和重放等类型的攻击。其脆弱性主要体现在以下 3 个方面。

1) 脆弱的接入控制。车载网络物理层为双绞线或同轴电缆，具有接入简单、缺乏异常接入检测功能的特点，容易被非法接入，无法保障可用性和完整性。

**表 3　　近 10 年来针对汽车的网络攻击分析与比较**

| 攻击方式 | 文献 | 时间 | 攻击入口 | 攻击模型 | 造成影响 | CIA 威胁 |
|---|---|---|---|---|---|---|
| 直接物理接入攻击 | 文献[28] | 2011 年 | CAN 非法接入，OBD 端口 | 帧嗅听，消息重放 | 控制车窗、警示灯开关、安全气囊系统失效等 | 完整性、机密性 |
| | 文献[29] | 2010 年 | OBD 端口 | 帧嗅听，消息重放、伪装，DoS 攻击 | 控制车身、广播、引擎等功能模块，使 CAN 失效 | 完整性、机密性、可用性 |
| | 文献[30] | 2015 年 | OBD 端口 | 帧嗅听，消息重放、伪装，DoS 攻击 | 实现无线接入攻击，控制雨刷、引擎等功能模块 | 完整性、机密性、可用性 |
| | 文献[31] | 2018 年 | USB | 逻辑缺陷 | 车载娱乐系统 | 保密性 |
| 近距离无线攻击 | 文献[32] | 2015 年 | 蓝牙 | 帧嗅听，消息重放、伪装 | 对汽车实现完整控制 | 完整性、机密性 |
| | 文献[33] | 2010 年 | 胎压监测系统（TMPS, tire pressure monitoring system） | 嗅听，消息重放、伪装 | 对汽车造成安全威胁 | 完整性、机密性 |
| 远程无线攻击 | 文献[34] | 2019 年 | 远程无线 | 消息重放、伪装 | 对一辆行驶中的汽车进行了远程控制刹车攻击 | 完整性、机密性 |
| | 文献[35] | 2016 年 | 数字蜂窝、Wi-Fi | 通过安卓手机远程控制 | 实现车身远程非法控制 | 完整性、机密性 |
| | 文献[36] | 2017 年 | Wi-Fi | 通过 Wi-Fi 接入 | 实现了远程对车载CAN的接入，汽车功能控制 | 完整性、机密性 |
| | 文献[37] | 2020 年 | Wi-Fi | Wi-Fi 协议栈漏洞利用 | 用户隐私数据泄露，威胁汽车功能安全系统运行 | 保密性、完整性 |

2) 无数据加密保障。内部消息传输只根据功能进行编码，缺乏信息安全方面的加密保护，容易导致消息被窃取和篡改，无法保障消息的真实性。

3) 无消息认证机制。消息仅通过消息 ID 进行标定和作为接收过滤，容易遭受拒绝服务（DoS, denial of service）、重放、伪造等攻击。例如，当前的 CAN 和 FlexRay 规范仅提供循环冗余校验（CRC, cyclic redundancy check）码用于消息完整性和错误验证功能，缺乏节点认证机制。

### 3.3　丰富的网络安全攻击入口

本文将从网络分层的角度来对智能网联汽车可能受到攻击的外部接口进行归纳和分类，根据攻击来源将不同的攻击划分为不同的层次。如图 3 所示，潜在攻击者往往就是通过这些对外接口对汽车实施不同层次的网络攻击。这些网络攻击的特征如下。

1) 来自传感层（物理层）的攻击。未来汽车将更多地配备激光雷达、毫米波雷达、摄像头和 GPS

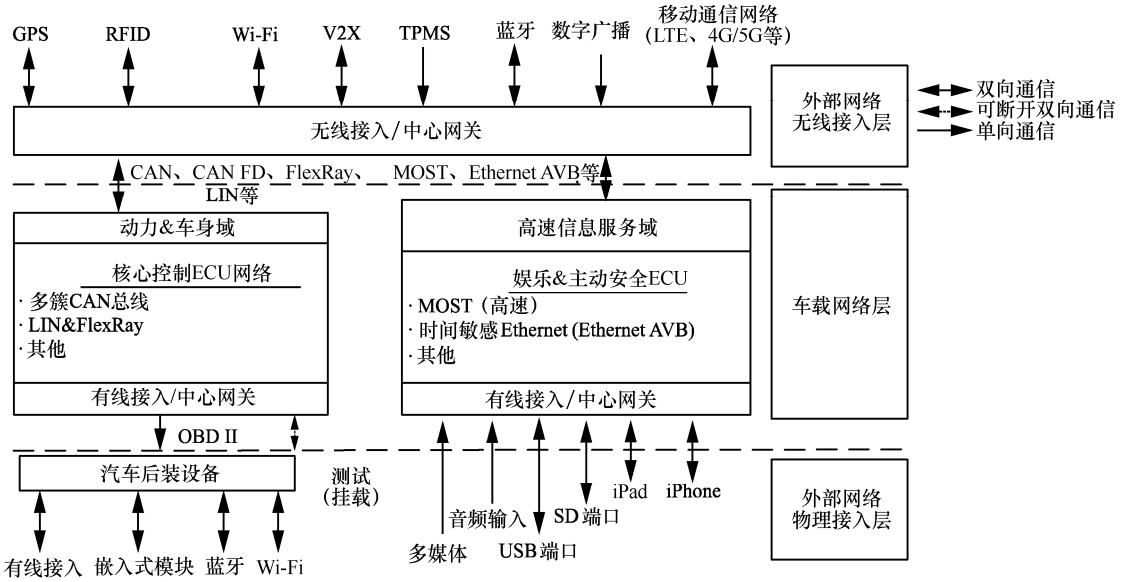



图 3　车载网络对外接口说明

等一系列先进传感器，用于收集外部环境感知信息，为自动驾驶决策提供了感知环境的能力。因此，通过物理层攻击汽车将成为车载网络安全的新威胁。例如，Rouf 等[32]提出一种通过无线电频道对轮胎压力监测系统进行干扰的攻击，使汽车胎压监测系统失效。Tao 等[38]提出通过无线电频道的控制，实现了针对无钥匙启动系统的攻击，对目标汽车实施非法启动。

2) 非法访问（数据链路层）。由于车载网络缺乏数据加密和消息验证机制，攻击者一旦能够访问网络设备，就可以轻松实施攻击。数据链路层的攻击模式有帧注入、帧伪造、帧嗅探、暂停和 DoS 攻击。网络的可用性（availability）将受到严重威胁，例如 Cho 等[39]对车载 CAN 实现了数据链路层的 DoS 攻击，导致整个汽车电子系统功能失效。

3) 来自接口（应用层）的攻击。近年来，有很多关于利用外部网络接口和设备的漏洞对汽车实现远程网络攻击的报告[28,31,40]。攻击入口包括蓝牙、OBD_II、Wi-Fi 等。在网络应用层，攻击者可以进行更有针对性的攻击而不易被发现，例如远程控制或制动车辆[27,29-30]。由于这类攻击没有非法访问节点和明显的数据帧异常，因此更难被检测。针对此类攻击，当前国内外研究者主要集中于基于机器学习的入侵检测方法设计[32-34]，目前主要存在计算资源消耗过大、缺乏测试数据集及模型评估等问题。

### 3.4 功能安全保障下的信息安全问题

功能安全是智能网联汽车发展的前提，围绕汽车安全的传统设计有安全带、被动安全（安全气囊）、主动安全（防抱死制动系统（ABS, anti-lock braking system）、车身电子稳定系统（ESP, electronic stability program）、ADAS 等。功能安全是为避免因电气和电子系统故障行为所带来的不可接受的风险和安全损害。功能安全增强设计既要遵循相应的安全标准（例如 ISO 26262），同时也面临着计算和网络资源、实时性、可靠性等多方面的约束。

在保障汽车功能安全方面，大量研究者在消息可调度性、任务优先级分配等方面开展相应的研究工作[41-43]，其中，Davis 等[43]提出的可调度性分析方法和模型已被 600 多篇论文引用，并通过商业化的 CAN 分析工具的形式转移到工业应用。另外，Xie 等[44-46]针对汽车应用开发问题，在多功能混合关键级的自适应调度方法及多功能混合关键级的高性能实时调度等方面开展了大量研究工作，提出了一系列系统功能关键级自适应的调度算法，在优先保障高关键任务（功能安全性）的同时兼顾了性能与成本的均衡。

车载网络安全问题包括信息安全和功能安全 2 个方面，严重的信息安全将威胁功能安全，但两者在实现过程中又面临系统资源上的竞争。为消解信息安全与功能安全在设计资源上的竞争，在开展车载网络安全研究的同时，需要兼顾系统的功能安全属性和信息安全属性，遵循 ISO 26262 标准和 AUTOSAR 规范。

考虑到车载网络日益紧张的带宽资源，Xie 等[47-48]从车载 CAN 消息封装和带宽利用率优的化角度出发，就 CAN 和 CAN-FD（CAN with flexible data-rate）的信号封装问题，提出了即信息安全增强的信号封装优化模型（即在消息中加载消息认证码（MAC, message authentication code）数据），利用混合整数线性规划（MILP, mimed integer linear programming）得到信号封装最优解。该方案均衡考虑了车载网络的安全性、实时性和带宽开销。

关于车载网络安全与功能安全之间的关系，文献[49-50]均强调网络信息安全威胁会直接影响车内和车外人员的安全。CIA（confidentiality, integrity, availability）原则[51]建立了用于评价网络系统信息安全特性的框架，解释了车载网络安全设计的最重要目标。其中 confidentiality 表示信息的机密性，integrity 表示信息的一致性或者完整性，availability 表示获得授权的用户的可用性。为明确功能安全与信息安全之间的关系和相互影响，本文从设计目标、约束及其相互影响方面出发，总结归纳出两者之间的关系，如图 4 所示。

经本文总结，得出以下 4 点功能安全保障下的车载网络信息安全设计面临的挑战和约束。

1) 计算、存储及通信带宽资源的约束，使汽车内部硬件资源约束主要表现为计算、存储、带宽和能量约束。

2) 复杂异构的软硬件结构，汽车内部由大量异构复杂的软件和硬件部件组成，它们通过异构的车载网络协议和网关进行通信。系统复杂性和异构性不仅给功能安全和信息安全增加了不确定性因素，也给系统功能安全保障测试和验证增加

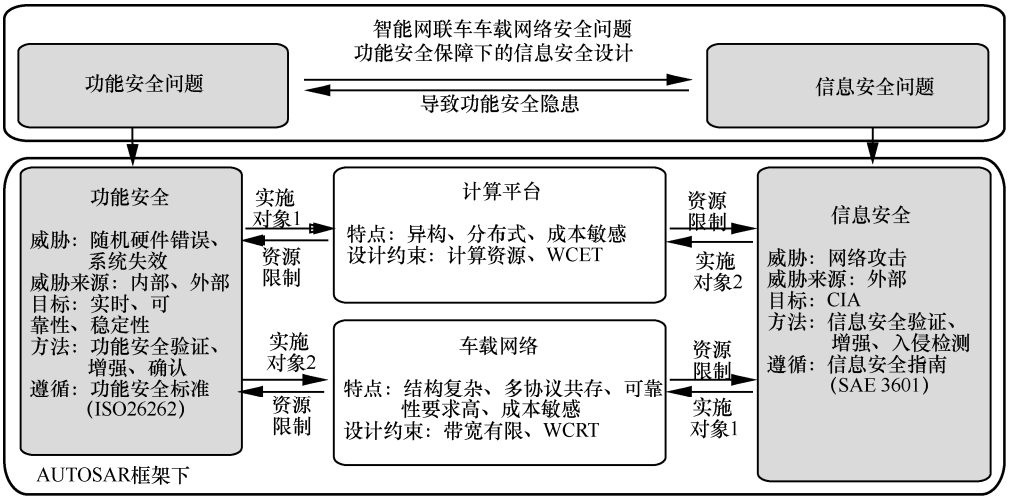



图 4　智能网联车中功能安全与信息安全之间的关系

了难度。

3) 处于成本和性能的均衡考虑，ACPS 中 ECU 的计算和存储资源往往有限，而部署的高成本可能导致网络安全部署被给予低优先级，车载网络安全设计受到严格的成本约束，这也导致传统信息的网络信息安全增强方案往往无法部署于汽车环境。

4) 车载网络对功能安全设计的约束主要表现为消息传输的实时性、端到端时延边界、系统任务可调度性等，这些都将影响到系统的可靠性和稳定性。当前针对车载网络消息可调度性分析的研究工作主要集中在探索通信时延的上界[52-54]、网络消息可调度性分析[55-56]、满足确定性时延分析等方面[57]。

## 4　车载网络信息安全增强技术研究进展

本文重点关注车载网络在智能网联汽车环境下的信息安全威胁问题，分别从车载网络数据加密技术、车载网络消息认证技术和车载网络异常入侵检测技术 3 个方面进行综述。

### 4.1　车载网络数据加密技术

加密和认证被广泛应用于通信信道的安全领域，这一技术也被大量应用于车载网络环境（其中 MAC 技术已经被纳入 AUTOSAR 协议规范）。然而传统的消息加密与认证技术在车载网络环境下，面临着体系结构异构、带宽和计算资源受限等问题。因此为减少加密运算带来的额外时间开销，车载网络中消息认证和加密通常采用轻量化、硬件加速等方式，例如利用可编程逻辑期间进行高级加密标准（AES, advanced encryption standard）、椭圆曲线密码编码学（ECC, elliptic curves cryptography）运算加速[58]、通过即现场可编程门阵列（PFGA, field programmable gate array）实现裁剪版的哈希算法[59]、将多个消息传输一个 MAC 等[60]。

针对车载网络环境中计算资源紧张和消息加密对网络通信带来的额外时间开销的问题，Wang 等[61]采用添加硬件模块的方式来解决加密算法计算时间的问题，有效降低了消息加密对网络性能的影响，其缺点是会增加硬件部署的成本。

为应对多种车载 ECU 的漏洞和攻击模型，Siddiqui 等[62]提出了一种基于硬件的安全可信框架，在车载 CAN 上实现了基于轻量级物理不可克隆函数（PUF, physical unclonable function）的双向认证和在非安全通信信道上的安全加密，实验结果表明，在 1 Mbit/s 的车载 CAN 发送一个加密数据帧的时间开销为 108 μs。Gu 等[63]从消息封装和调度的层面将数字签名和认证码等信息通过消息分配层的优化，将任务分配到汽车 ECU 中，以降低消息加密认证对网络时间性能带来的影响，同时不产生额外的硬件成本开销，其缺点是导致网络协议异常复杂。

### 4.2　车载网络消息认证技术

近年来，车载 CAN 的多种轻量级消息认证协议被提出，以保护车辆免受伪装攻击。该协议最初由 Herrewege 等[64]提出。近年来，Jo 等[65]提出了一种新的认证协议——MAuth-CAN，可以在不修改 CAN 硬件控制器的情况下，实现网络带宽消耗与防止伪装攻击之间的均衡。另外，Kang[66]提出一种在 CAN 中使用单向哈希链的轻量级源认证协议，具有攻击弹性树算法，可以通过 ECU 的固件更新实现

部署。分析表明，该协议具有较高的安全性。通过在虚拟 ECU（CANoe 实现）和 FreescaleS12XF 结合的实验表明，该协议在认证时间、响应时间、服务时延等方面均具有明显优势。

轻量级消息认证协议设计可解决 CAN 协议缺乏安全认证设计的问题，保障车载网络通信的真实性，考虑到目前车载网络带宽资源及消息响应时间的要求，现有消息认证协议设计存在的问题及挑战主要在于如何在提高消息认证安全性的同时避免因通信带宽消耗而导致消息可调度引起的功能可靠和实时问题。

### 4.3 车载网络异常入侵检测技术

相比于消息加密、访问控制、协议认证等信息安全增强手段，入侵检测具有占用带宽资源小、便于现有车辆部署的特点，更适合资源和成本受限的车载网络。入侵检测根据数据源可分为基于主机的 IDS 和基于网络的 IDS；根据检测技术又可分为基于特征观察的检测方法、基于信息理论和统计分析的检测方法、基于机器学习的检测方法等，如图 5 所示。下面将对现有相关的研究工作从以下几个方面进行总结和分析。

1) 基于特征观察的检测方法

特征观察是常用的入侵检测手段之一，被广泛应用于车载网入侵检测研究中[50]。通过对车载网络体系结构及网络协议的分析发现，可用于入侵检测观察的网络特征主要有设备指纹（通过时域和频域信息提取）[67]、时钟偏移[68]、频率观察[69]、远程帧[70]等。例如，曾凡[71]在对 CAN 字节和位级别特征充分解析的基础上，提出了基于 Snort 规则的车载 CAN 入侵检测技术，设计实现了完整的车载网络入侵检测系统，并通过实验验证了其对异常规则检测的有效性。李飞等[72]提出了一种基于时钟偏移的车载网络入侵检测方法，通过挖掘各 ECU 之间的关联规律，构建了时钟累计偏移模型，提出累计算法用于发现入侵行为，对轻微偏离目标具有较好的检测效果。

2019 年，关亚东[73]提出了基于报文周期特性的自适应入侵检测算法，并以 BP 神经网络作为该算法的分类模型。针对数据类别不平衡的问题提出一种欠采样的数据选择方法，实现了对 Bus-off 攻击的入侵检测。秦洪懋等[74]提出一种基于报文序列预测的车载网络入侵检测方法，通过学习攻击类型的报文来实现对攻击行为的检测。

近年来，利用 ECU 电气特征的唯一性建立设备指纹信息成为一种热门车载网络攻击溯源方法，被广泛用于车载网络入侵检测研究，该方法由 Cho 等[75]首次提出。随后，Song 等[76]通过对网络信号特征的提取和统计来实现入侵检测。Lee 等[70]利用 CAN 周期消息的返回值时延、时间间隔等作为设备指纹信息来源并取得良好的检测效果，这为入侵检测提供了新的数据来源。Yang 等[77]利用 RNN-LSTM 分类器在频域特征构建 ECU 指纹信号，实验表明该方法可有效检测泛洪攻击。Ning 等[78]提出了一种基于局部异常因子（LOF, local outlier factor）的攻击检测方案，该方案利用 CAN 帧的电压物理特性来判断消息是否由合法的 ECU 发送，所提算法具有较低的时间和空间复杂度，在真实车载网络环境数据下的实验表明，针对特定攻击模型识别精度可达到 98%以上。

基于特征观察的检测方法针对特定攻击模型往往能够取得高的检测精度，具有响应时间短、网络带宽开销小的特点[67]。然而考虑到汽车长生命周期（20 年左右）、网络环境动态变化的特点，现有研究中主要存在 3 个方面的问题。① 检测方法往

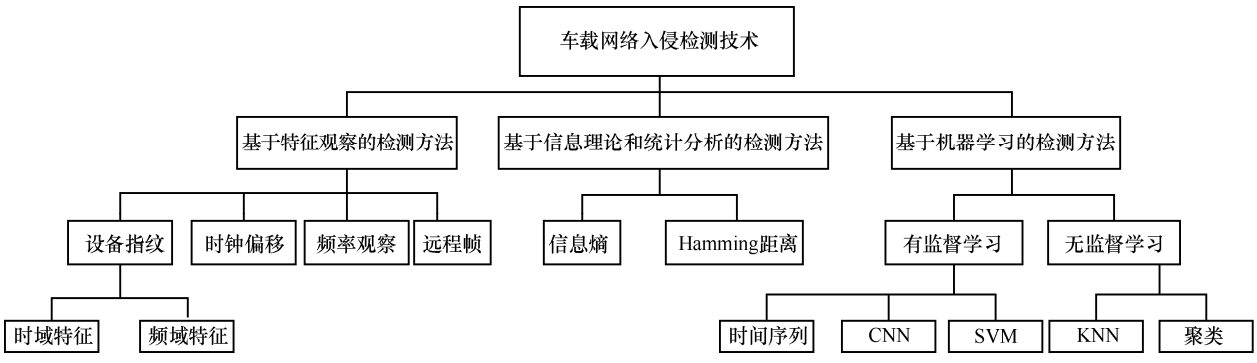



图 5 车载网络的入侵检测技术分类

往对应特定的攻击模型；② 检测效果的稳健性不强（有诸多前提条件，缺乏对汽车状态的感知）；③ 缺乏检对检测响应时间的评估及对功能安全保障的影响。考虑到 ACPS 功能安全关键属性，亟待通过入侵检测模型和算法的优化研究来解决上诉问题，以避免因网络安全问题导致严重的智能网联车功能安全危机。

2) 基于信息理论和统计分析的检测方法

通过对 6.673 亿条 CAN 消息进行信息熵的分析发现，车载 CAN 中信息熵均值为 11.436[79]。而当发生恶意攻击时（如 DoS、重放等），车载 CAN 的信息熵会显著降低，这一特性被广泛应用于资源受限的车载网络入侵检测研究中[80-82]。例如， Marchetti 等[81]评估了基于信息理论的车载网络入侵检测算法，研究发现，在车载网络入侵检测评估中，利用单一的信息理论模型只能针对单一的泛洪攻击有效。Muter 等[82]首次将信息熵的概念用于车载网络的入侵检测，并将信息熵的评估范围限制在 CAN 消息 ID，利用这一特性，可快速对入侵状态进行识别，具有检测响应时间短（最快可在 0.01 ms 内发现入侵攻击）的特点。在此基础上，Wu 等[83]提出一种基于固定消息数量的滑动窗口策略，相比于传统的固定时间窗口的滑动窗口策略，该方案可有效避免因车载 CAN 非周期性消息带来的信息熵抖动问题。实验表明，该方案可有效提高基于信息熵的车载网络入侵检测应对泛洪和重放攻击的检测精度，并进行了检测响应时间的评估。

近年来，秦贵和团队[84-86]利用信息理论的方法针对车载网络异常检测开展了一系列研究工作，首先在文献[84]中，通过理论分析及实验表明了使用信息熵的车载 CAN 总线网络异常检测方法对重放、泛洪等攻击检测的有效性。随后在文献[85]中，指导学生提出了基于 Renyi 信息熵的改进型 CAN 总线异常检测方法，有效提高了检测精度，但依然局限在对重放、泛洪攻击模型的检测。在文献[86]中，还提出一种基于随机森林模型的 CAN 报文异常检测方法，并利用真实车辆采集的大量数据在构造随机森林分类算法时进行了多次调整。实验表明，合适的网络特征参数对提高车载网络异常的检测有效性具有显著影响。

现有基于信息理论的车载网络入侵检测方法研究往往忽略了汽车不同状态带来的车载网络信息熵抖动对检测结果的影响，其检测模型在有限的汽车状态下具有较高的检测精度，但对不同汽车状态的稳健性有待提高。这些问题导致此类方法无法满足当前汽车安全完整性等级（AISL, automotive safety integration level）中的高等级安全要求，因此本文拟通过对汽车状态的感知，开展状态感知的车载网入侵检测算法优化研究。

3) 基于机器学习的检测方法

机器学习、神经网络等理论也已成为研究车载网络入侵检测技术的热门方向[87-89]。Andreas[90]提出使用具有径向基函数（RBF, radial basis function）内核的一类支持向量机（SVM, support vector machine）来学习基线正常行为，并将偏差归类为异常，生成的分类器适用于消息时间序列。后来，Kang 等[91]提出了一种使用深度神经网络（DNN, deep neural network）的车载网入侵检测技术，通过训练 ECU 之间交换的车载网分组消息以提取低维特征并用于区分正常和黑客分组。文献[92]采用贝叶斯网络方法来快速识别 CAN 上的恶意消息攻击，利用汽车城市驾驶环境模拟器（CARLA, car learning to act）[93]来模拟真实汽车各种运行状态下的 CAN 消息，存在的不足在于其检测精度无法满足功能安全等级保障要求。

以上各个方法的实验结果表明，机器学习对于车载网络未知攻击模型的入侵检测具有较好的效果。然而在车载网中，由于计算、存储和通信带宽资源的限制，现有基于机器学习的入侵检测方法在如何降低计算复杂度和对车载网络通信带宽的消耗上是一个有待进一步解决的问题，同时提高检测精度、降低误报率、缩短响应时间和提高稳健性也是该类方法需要进一步改善的方向。而且，对于 ACPS 而言，鉴于其功能安全关键属性，网络的真实和可靠是最重要的信息安全诉求，因此亟需开展车载网络入侵检测模型与算法设计研究，以解决上述问题。

车载网具有异构的特征，呈现出多个功能域通过车载网关实现消息通信的异构结构，因此不同网络层入口的攻击针对的车载网络安全漏洞不同，可实现的攻击模型也不同，可用于入侵检测的观察特征也不同。对此，本文通过文献调研，建立了车载网络的攻击入口、安全漏洞、攻击模型和可利用特征之间的关系，如图 6 所示。

结合前文所述，本文对 3 类信息安全增强手段结合智能网联车环境，遴选了具有代表性的工作，

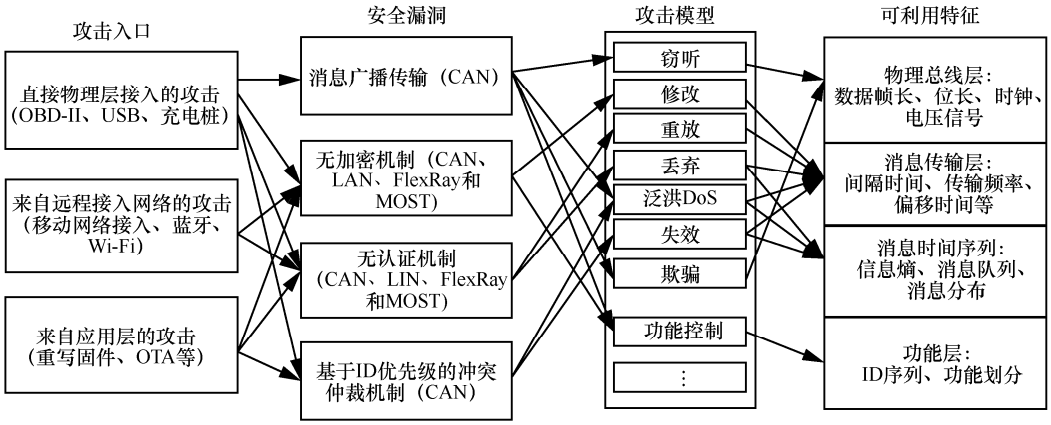



图 6 车载网络的攻击入口、安全漏洞和入侵检测可利用特征之间的关系

**表 4 车载网络安全增强技术比较与分析**

| 技术 | 应用范围 | 代表性文献及技术 | 信息安全性保障 | 特点及挑战 |
|---|---|---|---|---|
| 数据加密 | 数据链路层 | 轻量级 AES[58]、硬件密码加速模块[59]、MAC 分解传输[60] | 安全性、完整性、正确性 | 对网络消息传输安全性和完整性、正确性的增强，主要面临安全性与计算资源之间的平衡问题 |
| 消息认证 | 物理层、数据链路层 | TESLA[64]、MAuth-CAN[65]、单向哈希链表[66] | 正确性 | 对网络消息传输的正确性的增强保护，主要面临网络带宽带来的设计约束问题 |
| 入侵检测 | 物理层、数据链路层、应用层 | 一类 SVM[90]、深度神经网络[91]、贝叶斯网络[92]、RNN-LSTM[77] | 可用性、完整性 | 对网络可用性和完整性的增强保护，当前主要挑战是提高检测精准度和稳健性，降低误报率和检测响应时间 |

并对其进行了比较分析，如表 4 所示。车载网络异常入侵检测系统具有扩展性强、成本低和向下兼容的特点，可应用于资源受限的传统车载网络环境，是一种可有效保障智能网联车车载网络消息真实性和可用性的信息安全技术。因此相比于数据加密和消息认证技术，车载网络入侵检测技术更适合于功能安全关键、资源受限和成本敏感的智能网联车车载网络环境，可有效弥补加密和认证机制带来的计算和通信开销，可以预见，车载网络入侵检测仍是今后较长时期的智能网联车信息安全增强研究的一个重要发展方向。

## 5 分析和总结

近年来，智能网联车网络安全问题引起了产业界和学术界的广泛关注，其中焦点之一是围绕车载网络开发具有抗攻击能力的算法和体系结构。结合前文所述智能网联车发展趋势及当前车载网络安全方面的最新研究进展，本文进一步提出了智能网联车网络安全领域的一些开放性问题。

### 5.1 如何提高入侵检测精度、降低响应时间

针对车载网的恶意攻击检测不及时带来的严重的功能安全威胁，将入侵检测作为重要的智能网联车网络安全增强手段，提高检测精度、降低误报率、缩短检测响应时间和提高系统稳健性是未来车载网络入侵检测技术研究中最迫切需要解决的问题之一。

### 5.2 如何实现精准的网络安全测试评估

由于未来智能网联车中使用的异构软件和硬件组件的复杂性日益增加，针对车载网络的新攻击将不断出现。这些新组件和车载系统的复杂性在为开发高效和可适应的车载网络安全机制带来更多的挑战的同时，也给网络安全的测试和验证带来困难。例如，为验证一个入侵检测模型及算法，需要模拟真实车载网络环境中遭受网络攻击情况下的车载网络信息流，测试数据的获取和生成将进一步影响检测的精度和效果，如何实现精准的车载网络安全测试评估是当前还未得到有效解决的问题。

### 5.3 如何应对未知的智能网联车网络攻击

考虑到汽车长生命周期（20 年左右）和网络环境动态变化的特点，现有研究中主要存在 3 个方面的问题。1) 检测方法往往对应特定的攻击模型；2) 检测效果的稳健性不强（有诸多前提条件，缺乏对汽车状态的感知）；3) 缺乏检对检测响应时间的评估及对功能安全保障的影响。考虑到 ACPS 功能安全关键属性，亟待通过入侵检测模型和算法的优化研究来解决上述问题，以避免因网络安全问

题导致严重的智能网联车功能安全危机。

### 5.4　如何实现网络安全增强与资源消耗的均衡

智能网联车环境下计算和通信带宽等资源的限制带来功能安全和信息安全设计在资源上的竞争博弈。现有的基于机器学习的入侵检测方法存在计算和带宽资源消耗大的问题，如何降低计算复杂度和对车载网络通信带宽的消耗。实现网络安全增强与资源消耗均衡是当前智能网联车信息安全增强研究有待进一步解决的问题。

### 5.5　如何制定及时有效的智能网联车信息安全标准

标准化建设是有效提高汽车产品开发协同效率、降低开发和维护成本的有效措施，同样，智能网联车网络安全问题设计也需要遵循一系列的标准和指南。当前针对汽车功能安全的有 ISO 26262[94]、面向信息安全的 SAE J3061[95]等。面向智能网联车的功能安全标准、规范及信息安全指南的主要还有 OSEK[96]、AUTOSAR[97]、Automotive SPICE[98]等。

然而，由于法律和监管框架往往落后于技术发展的速度，汽车分散的业务生态系统和全球供应链使法规遵循变得更困难，这将导致未来汽车遭受更多的信息安全威胁，同时，也给制定相关标准带来挑战，当前针对智能网联车网络安全的标准建设存在滞后现象。例如，ISO 正在开发一个新的标准（道路车辆–预期功能的安全性 ISO 21448[99]），该标准关注的不是系统出现故障时的安全性，而是系统正常运行时的安全性（包括信息安全危险导致的安全问题）。与此同时，全国信息安全标准化技术委员会也于 2018 年提出汽车电子网络安全标准化白皮书[100]。因此如何制定及时有效的智能网联车信息安全标准是未来需要解决的重要问题。

## 6　结束语

智能网联车作为车联网朝“云–管–端”架构发展下的终端节点，面临着日益严重的信息安全威胁。在此背景下，本文首先介绍了智能网联车中车载网络协议现状及分类情况。随后总结了当前车载网络安全问题，对比分析了车载网络安全增强技术现状。最后对未来车载网络安全技术的发展和研究进行了总结和展望。本文可以帮助车载网络安全相关的研究者快速全面地了解和掌握车载网络安全的基本现状和研究进展，并对未来一段时间内车载网络相关研究给出了参考方向。

## 参考文献：


[1] 郄广, 张岩. 智能车与网联技术分析[J]. 移动通信, 2020, 44(1): 80-85.
QIE G, ZHANG Y. Intelligent connected vehicle: a survey of the technical analysis[J]. Mobile Communications, 2020, 44(1): 80-85.

[2] 方凯正, 朱成, 刘頔. 5G 技术在汽车产业中的创新应用研究[J]. 科技与创新, 2020(6): 148-149.
FANG K Z, ZHU C, LIU D. Research on the innovative application of 5G technology in automobile industry[J]. Science and Technology & Innovation, 2020(6): 148-149.

[3] 李克强, 戴一凡, 李升波, 等. 智能网联汽车(ICV)技术的发展现状及趋势[J]. 汽车安全与节能学报, 2017, 8(1): 1-14.
LI K Q, DAI Y F, LI S B, et al. State-of-the-art and technical trends of intelligent and connected vehicles[J]. Journal of Automotive Safety and Energy, 2017, 8(1): 1-14.

[4] 中国汽车工程学会. 智能网联汽车信息安全白皮书[R]. (2017-10-17)[2019-11-18].
China Society of Automotive Engineering. White paper on intelligent network automobile information security[R]. (2017-10-17) [2019-11-18].

[5] 荀毅杰, 刘家佳, 赵静. 智能网联汽车的安全威胁研究[J]. 物联网学报, 2019, 3(4): 72-81.
XUN Y J, LIU J J, ZHAO J. Research on security threat of intelligent connected vehicle[J]. Chinese Journal on Internet of Things, 2019, 3(4): 72-81.

[6] 李岩松. 复杂网络环境下智能网联汽车安全威胁分析与远程入侵研究[D]. 西安: 西安电子科技大学, 2019.
LI Y S. Analysis of safety threats and remote invasion of intelligent and connected vehicle in complex network environment[D]. Xi'an: Xidian University, 2019.

[7] JADHAV S, KSHIRSAGAR D. A survey on security in automotive networks[C]//International Conference on Computing Communication Control and Automation. Piscataway: IEEE Press, 2018: 1324-1330.

[8] YANG D, JIANG K, ZHAO D, et al. Intelligent and connected vehicles: Current status and future perspectives[J]. Science China-Technological Sciences, 2018, 61(10): 1446-1471.

[9] ALNABULSI H，ISLAM R. Protecting code injection attacks in intelligent transportation system[C]//Trust Security and Privacy in Computing and Communications. Piscataway: IEEE Press, 2019: 799-806.

[10] 苗圩. 苗圩: 发展智能网联汽车的六大重点工作[J]. 汽车纵横, 2017(7): 21-23.
MIAO W. Miao wei: the development of intelligent network car six key work[J]. Automotive crossbar, 2017(7): 21-23.

[11] DIBAEI M, ZHENG X, JIANG K, et al. An overview of attacks and defences on intelligent connected vehicles[J]. arXiv Preprint, arXiv:1907.07455, 2019.

[12] 吴武飞. 新一代汽车网络入侵检测及安全增强设计研究[D]. 长沙: 湖南大学, 2018.
WU W F. Research on intrusion detection and cybersecurity enhancement design for new in-vehicle network environment[D]. Changsha: Hunan University, 2018.

[13] SHAW R, JACKMAN B. An introduction to FlexRay as an industrial network[C]//International Symposium on Industrial Electronics. Pis-

cataway: IEEE Press, 2008: 1849-1854.

[14] THIELE D, ERNST R. Formal worst-case timing analysis of ethernet TSN's burst-limiting shaper[C]//Conference on Design, Automation & Test in Europe. Piscataway: IEEE Press, 2016: 187-192.

[15] ISO. Road vehicle-interchange of digital information-controller area network (CAN) for high-speed communication[S]. ISO 11898, (2015-12-01)[2019-11-18].

[16] RUFF M. Evolution of local interconnect network (LIN) solutions[C]//Vehicular Technology Conference. Piscataway: IEEE Press, 2003: 3382-3389.

[17] ALMEIDA L, PEDREIRAS P, FONSECA J A G. The FTT-CAN protocol: why and how[J]. IEEE Transactions on Industrial Electronics, 2002, 49(6): 1189-1201.

[18] FIJAKOWSKI B T. Time triggered controller area networking[M]. Netherlands: Springer, 2011: 69-72.

[19] WOO S, JO H J, KIM I S, et al. A practical security architecture for in-vehicle CAN-FD[J]. IEEE Transactions on Intelligent Transportation Systems, 2016, 17(8): 2248-2261.

[20] ALDERISI G, IANNIZZOTTO G, PATTI G, et al. Prioritization-based bandwidth allocation for MOST networks[C]//Emerging Technologies and Factory Automation. Piscataway: IEEE Press, 2013: 1-4.

[21] POFERL S, BECHT M, DE P, et al. 150 Mbit/s MOST, the next generation automotive infotainment system[C]//International Conference on Transparent Optical Networks. Piscataway: IEEE Press, 2010: 1-2.

[22] CAO J, CUIJPERS P J L, BRIL R J, et al. Tight worst-case response-time analysis for ethernet AVB using eligible intervals[C]//IEEE World Conference on Factory Communication Systems. Piscataway: IEEE Press, 2016: 1-8.

[23] KERMIA O. Schedulability analysis and efficient scheduling of rate constrained messages in the TTEthernet protocol[J]. Software Practice & Experience, 2017: 1485-1499.

[24] 魏学哲, 孙泽昌, 陈觉晓. 汽车网络分类方法及其主流协议发展趋势[J]. 同济大学学报(自然科学版), 2004(6): 762-766.
WE X Z, SUN Z C, CHEN J X. Automobile network classification method and its mainstream protocol development trend[J]. Journal of Tongji University (Natural Science Edition), 2004(6): 762-766.

[25] 罗峰, 苏剑, 袁大宏. 汽车网络与总线标准[J]. 汽车工程, 2003(4): 372-376.
LUO F, SU J, YUAN D H. Automotive network and bus standard[J]. Automotive Engineering, 2003(4): 372-376.

[26] 刘冬冬, 张天宏, 陈建, 等. TTP/C 协议的关键特性研究[J]. 计算机测量与控制, 2012, 20(10): 2769-2772.
LIU D D, ZHANG T H, CHEN J, et al. TTP/C protocol key features study[J]. Computer Measurement & Control, 2012, 20(10): 2769-2772.

[27] 车联网网络安全委员会. 车联网网络安全白皮书[R]. (2017-09-02)[2019-11-18].
Internet of Vehicles Network Security Committee. White paper on Internet of vehicles network security[R]. (2017-09-02)[2019-11-18].

[28] CHECKOWAY S, MCCOY D, KANTOR B, et al. Comprehensive experimental analyses of automotive attack surfaces[C]//Usenix Conference on Security. Berkeley: USENIX Association, 2011: 6.

[29] KOSCHER K, CZESKIS A, ROESNER F, et al. Experimental security analysis of a modern automobile[C]//2010 IEEE Symposium on Security and Privacy. Piscataway: IEEE Press, 2010: 447-462.

[30] WOO S, JO H J, DONG H L. A practical wireless attack on the connected car and security protocol for in-vehicle CAN[J]. IEEE Transactions on Intelligent Transportation Systems, 2015, 16(2): 993-1006.

[31] KEENLAB. A review of safety studies on multiple BMW models[R]. (2018-05-22)[2019-11-18].

[32] FOSTER I, PRUDHOMME A, KOSCHER K, et al. Fast and vulnerable: a story of telematic failures[C]//Usenix Conference on Offensive Technologies. Berkeley: USENIX Association, 2015: 1-9.

[33] ROUF I, MILLER R, MUSTAFA H, et al. Security and privacy vulnerabilities of in-car wireless networks: a tire pressure monitoring system case study[C]//19th Usenix Security Symposium. Berkeley: USENIX Association, 2010: 11-13.

[34] KHAN Z, CHOWDHURY M, ISLAM M, et al. In-vehicle false information attack detection and mitigation framework using machine learning and software defined networking[J]. arXiv Preprint, arXiv: 1906.10203, 2019.

[35] TAYLOR A, LEBLANC S, JAPKOWICZ N, et al. Anomaly detection in automobile control network data with long short-term memory networks[C]//IEEE International Conference on Data Science & Advanced Analytics. Piscataway: IEEE Press, 2016: 130-139.

[36] KEENLAB. CAR hacking research: remote attack tesla motors[R]. (2016-09-19)[2019-11-18].

[37] KEENLAB. The exploitation of Wi-Fi protocol stack vulnerability on Tesla model S[R]. (2020-01-02)[2020-05-22].

[38] TAO Y, KONG L, WEI X, et al. Resisting relay attacks on vehicular passive keyless entry and start systems[C]//International Conference on Fuzzy Systems & Knowledge Discovery. Piscataway: IEEE Press, 2012: 2232-2236.

[39] CHO K T, KANG G S. Error handling of in-vehicle networks makes them vulnerable[C]//ACM Sigsac Conference on Computer and Communications Security. New York: ACM Press, 2016: 1044-1055.

[40] SUN J, IQBAL S, ARABI N S, et al. A classification of attacks to in-vehicle components (IVCs)[J]. Vehicular Communications, 2020(25): 1-16.

[41] POP T, ELES P, PENG Z. Schedulability analysis for distributed heterogeneous time/event triggered real-time systems[C]//Euromicro Conference on Real-Time Systems. Piscataway: IEEE Press, 2003: 257-266.

[42] DAVIS R I, CUCU G L, BERTOGNA M, et al. A review of priority assignment in real-time systems[J]. Journal of Systems Architecture, 2016(65): 64-82.

[43] DAVIS R I, BURNS A, BRIL R J, et al. Controller area network (CAN) schedulability analysis: refuted, revisited and revised[J]. Real-Time Systems, 2007, 35(3): 239-272.

[44] XIE G, ZENG G, LI Z, et al. Adaptive dynamic scheduling on multifunctional mixed-criticality automotive cyber-physical systems[J]. IEEE Transactions on Vehicular Technology, 2017, 66(8): 6676-6692.

[45] XIE G, CHEN Y, LIU Y, et al. Minimizing development cost with reliability goal for automotive functional safety during design phase[J]. IEEE Transactions on Reliability, 2017, PP(99): 1.

[46] XIE G, ZENG G, LIU Y, et al. Fast functional safety verification for distributed automotive applications during early design phase[J]. IEEE Transactions on Industrial Electronics, 2017, PP(99): 1.

[47] XIE Y, LIU L, LI R, et al. Security-aware signal packing algorithm for CAN-based automotive cyber-physical systems[J]. IEEE/CAA Journal of Automatica Sinica, 2015, 2(4): 422-430.

[48] XIE Y, ZENG G, KURACHI R, et al. Security/timing-aware design space exploration of CAN FD for automotive cyber-physical systems[J]. IEEE Transactions on Industrial Informatics, 2018, 15(2): 1094-1104.

[49] PIRYADARSHINI I. Introduction on cyber security[M]. New York: John Wiley & Sons, 2019.

[50] WI W, LI R, XIE G, et al. A survey of intrusion detection for in-vehicle networks[J]. IEEE Transactions on Intelligent Transportation Systems, 2020, 21(3): 919-933.

[51] LEE H, GEUM Y. Development of the scenario-based technology roadmap considering layer heterogeneity: an approach using CIA and AHP[J]. Technological Forecasting and Social Change, 2017: 12-24.

[52] PENG C, ZENG H. Response time analysis of digraph real-time tasks scheduled with static priority: generalization, approximation, and improvement[J]. Real-Time Systems, 2017(1): 1-41.

[53] CHEN G, GUAN N, LIU D, et al. Utilization-based scheduling of flexible mixed-criticality real-time tasks[J]. IEEE Transactions on Computers, 2018, PP(99): 1.

[54] XIE G, ZENG G, KURACHI R, et al. WCRT analysis of CAN messages in gateway-integrated in-vehicle networks[J]. IEEE Transactions on Vehicular Technology, 2017, 66(11): 9623-9637.

[55] DAVIS R I, ALTMEYER S, REINEKE J, et al. Response-time analysis for fixed-priority systems with a write-back cache[J]. Real-Time Systems, 2018, 54(4): 912-963.

[56] CHANG W, SAMARJIT C. Resource-aware automotive control systems design: a cyber-physical systems approach[J]. Foundations & Trends® in Electronic Design Automation, 2016, 10(4): 249-369.

[57] VATANPAVAR K, FARUAUE M A. ACQUA: adaptive and cooperative quality-aware control for automotive cyber-physical systems[C]//2017 IEEE/ACM International Conference on Computer Aided Design. Piscataway: IEEE Press, 2017: 193-200.

[58] LUO F, HOU S. Cyberattacks and countermeasures for intelligent and connected vehicles[J]. SAE International Journal of Passenger Cars-Electronic and Electrical Systems, 2019, 12(1): 55-66.

[59] GURGENS S, ZELLE D. A hardware based solution for freshness of secure onboard communication in vehicles[C]//Computer Security. Berlin: Springer, 2018: 53-68.

[60] SARPM. Secure message authentication protocol for CAN[D]. Ankar: Middle East Technical University, 2020.

[61] WANG E, XU W, SASTRY S, et al. Hardware module-based message authentication in intra-vehicle networks[C]//2017 ACM/IEEE 8th International Conference on Cyber-Physical Systems. Piscataway: IEEE Press, 2017: 207-216.

[62] SIDDIQUI A S, PLUSQUELLIC Y G, SAQIB F, et al. Secure communication over CANbus[C]//International Midwest Symposium on Circuits and Systems. Piscataway: IEEE Press, 2017: 1264-1267.

[63] GU Z, HAN G, ZENG H, et al. Security-aware mapping and scheduling with hardware co-processors for FlexRay-based distributed embedded systems[J]. IEEE Transactions on Parallel & Distributed Systems, 2016, 27(10): 3044-3057.

[64] HERREWEGE A V, SINGELEE D, VERBAUWHEDE I. CANAuth-a simple, backward compatible broadcast authentication protocol for CAN bus[C]//ECRYPT Workshop on Lightweight Cryptography. [S.n.:s.l.], 2011: 299-235.

[65] JO H J, KIM J H, CHOI H Y, et al. MAuth-CAN: masquerade-attack-proof authentication for in-vehicle networks[J]. IEEE Transactions on Vehicular Technology, 2020, 69(2): 2204-2218.

[66] KANG K D. A practical and lightweight source authentication protocol using one-way hash chain in can[D]. Daegu: Daegu Gyeongbuk Institute of Science & Technology, 2017.

[67] CHO K, SHIN K G. Fingerprinting electronic control units for vehicle intrusion detection[C]//Usenix Security Symposium. Berkely: USENIX Association, 2016: 911-927.

[68] HALDER S, CONTI M, DAS S K, et al. COIDS: a clock offset based intrusion detection system for controller area networks[C]//International Conference of Distributed Computing and Networking. New York: ACM Press, 2020: 1-10.

[69] 李飞, 王超. 基于关联规则挖掘的车载网络入侵检测技术研究[J]. 数据挖掘, 2017, 7(3): 65-69.
LI F, WANG C. Research on vehicle network intrusion detection technology based on association rule mining[J]. Data Mining, 2017, 7(3): 65-69.

[70] LEE H, JEONG S, KIM H K, et al. OTIDS: a novel intrusion detection system for in-vehicle network by using remote frame[C]//Conference on Privacy Security and Trust. Piscataway: IEEE Press, 2017: 57-66.

[71] 曾凡. 网联汽车入侵检测系统的研究与实现[D]. 成都: 电子科技大学, 2018.
ZENG F. Research and implementation of networked vehicle intrusion detection system[D]. Chengdu: University of Electronic Science and Technology, 2018.

[72] 李飞, 廖租奇, 张鹏飞. 一种基于时钟偏移的车载网络入侵检测方法及系统: CN201811137466.0[P]. (2019-01-22)[2019-11-18].
LI F, LIAO Z Q, ZHANG P F. A method and system of on-board network intrusion detection based on clock offset: CN201811137466.0[P]. (2019-01-22)[2019-11-18].

[73] 关亚东. 车内 CAN 总线入侵检测算法研究[D]. 黑龙江: 哈尔滨工业大学, 2019.
GUAN Y D. Research on incar CAN bus intrusion detection algorithm[D]. Heilongjiang: Harbin Institute of Technology, 2019.

[74] 秦洪懋, 闫梦如, 冀浩杰, 等. 一种基于报文序列预测的车载网络入侵检测方法: CN201910499446.6[P]. (2019-08-20)[2019-11-18].
QIN H M, YAN M R, JI H J, et al. A vehicle-mounted network intrusion detection method based on message sequence prediction: CN201910499446.6[P]. (2019-08-20)[2019-11-18].

[75] CHO K, SHIN K G. Viden: attacker identification on in-vehicle networks[C]//Computer and Communications Security. New York: ACM Press, 2017: 1109-1123.

[76] SONG H M, KIM H R, KIM H K. Intrusion detection system based on the analysis of time intervals of CAN messages for in-vehicle network[C]//International Conference on Information Networking. Piscataway: IEEE Press, 2016: 63-68.

[77] YANG Y, DUAN Z, TEHRANIPOOR M. Identify a spoofing attack on an in-vehicle CAN bus based on the deep features of an ECU fingerprint signal[J]. Smart Cities, 2020, 3(1): 17-30.

[78] NING J, LIU J. An experimental study towards attacker identification in automotive networks[C]//2019 IEEE Global Communications Conference. Piscataway: IEEE Press, 2019: 1-6.

[79] WANG E, XU W, SASTRY S, et al. Hardware module-based message authentication in intra-vehicle networks[C]//2017 ACM/IEEE 8th International Conference on Cyber-Physical Systems. Piscataway: IEEE Press, 2017: 207-216.

[80] VAN W F, WANG Y, KHOJANDI A, et al. Real-time sensor anomaly

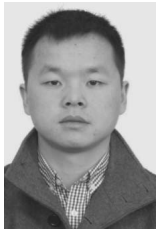
detection and identification in automated vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2020, 21(3): 1264-1276.
[81] MARCHETTI M, STABILI D, GUIDO A, et al. Evaluation of anomaly detection for in-vehicle networks through information-theoretic algorithms[C]//IEEE International Forum on Research and Technologies for Society and Industry Leveraging a Better Tomorrow. Piscataway: IEEE Press, 2016: 1-6.
[82] MUTER M, ASAJ N. Entropy-based anomaly detection for in-vehicle networks[C]//IEEE Intelligent Vehicles Symposium. Piscataway: IEEE Press, 2011: 1110-1115.
[83] WU W F, HUANG Y, KURACHI R, et al. Sliding window optimized information entropy analysis method for intrusion detection on in-vehicle networks[J]. IEEE Access, 2018(6): 45233-45245.
[84] 于赫, 秦贵和, 孙铭会, 等. 车载CAN总线网络安全问题及异常检测方法[J]. 吉林大学学报(工学版), 2016, 46(4): 1246-1253.
YU H, QIN G H, SUN M H, et al. Cyber security and anomaly detection method for in-vehicle CAN[J]. Journal of Jilin University (Engineering Edition), 2016, 46(4): 1246-1253.
[85] 闫鑫. 基于 Renyi 信息熵的 CAN 总线异常检测方法[D]. 吉林: 吉林大学, 2017.
YAN X. CAN bus anomaly detection method based on Renyi information entropy [D]. Jilin: Jilin University, 2017.
[86] 吴玲云, 秦贵和, 于赫. 基于随机森林的车载 CAN 总线异常检测方法[J]. 吉林大学学报(理学版), 2018, 56(3): 663-668.
WU L Y, QIN G H, YU H. Random forest based vehicle CAN bus anomaly detection method[J]. Journal of Jilin University (Science Edition), 2018, 56(3): 663-668.
[87] JEON B, JU H, JUNG B, et al. A study on traffic characteristics for anomaly detection of Ethernet-based IVN[C]//International Conference on Information and Communication Technology Convergence. Piscataway: IEEE Press, 2019: 951-953.
[88] MOUSAVINEJAD E, YANG F, HAN Q, et al. Distributed cyber attacks detection and recovery mechanism for vehicle platooning[J]. IEEE Transactions on Intelligent Transportation Systems, 2019, PP(99): 1-14.
[89] TAYLOR A, LEBLANC S, JAPKOWICZ N, et al. Anomaly detection in automobile control network data with long short-term memory networks[C]//IEEE International Conference on Data Science and Advanced Analytics. Piscataway: IEEE Press, 2016: 130-139.
[90] ANDREAS T. Anomaly detection in recordings from in-vehicle networks[J]. Big Data and Applications, 2014(3): 23-29.
[91] KANG M, KANG J. A novel intrusion detection method using deep neural network for in-vehicle network security[C]//Vehicular Technology Conference. Piscataway: IEEE Press, 2016: 1-5.
[92] CASILLO M, COPPOLA S, DE S M, et al. Embedded intrusion detection system for detecting attacks over CAN-BUS[C]//2019 4th International Conference on System Reliability and Safety. Piscataway: IEEE Press, 2019:136-141.
[93] DOSOVITSKIY A, ROS G, CODEVILLA F, et al. CARLA: an open urban driving simulator[J]. arXiv Preprint, arXiv: 1711.03938, 2017.
[94] ISO. Road vehicles-functional safety: ISO 26262[S]. (2018-12-01)[2019-11-18].
[95] SAE. Cybersecurity guidebook for cyber-physical vehicle systems, standard: J3061_201601[S]. (2016-01-01)[2019-11-18].
[96] VU D H, AOKI T. Faithfully formalizing OSEK/VDX operating system specification[C]//Symposium on Information & Communication Technology. New York: ACM Press, 2012: 13-20.
[97] AUTOSAR. Specification of operating system, release 4.1. technical report[R]. (2017-12-03)[2019-11-18].
[98] AUTOMOTIVE SIG. The SPICE user group, automotive SPICE process assessment model v2.5 and process reference model v4.5[R]. (2010-09-05)[2019-11-18].
[99] ISO. Road vehicles-safety of the intended functionality: PD ISO/PAS 21448[S]. (2019-02-15)[2019-11-18].
[100] 全国信息安全标准化技术委员会. 汽车电子网络安全标准化白皮书[R]. (2018-04-16)[2019-11-18].
National Information Security Standardization Technical Committee. White paper on automotive electronic network security standardization[R]. (2018-04-16)[2019-11-18].

[作者简介]

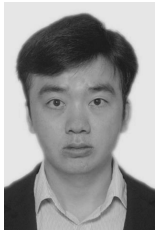
**吴武飞**（1986– ），男，江西安义人，博士，南昌大学讲师，主要研究方向为嵌入式计算、CPS、车载网络安全技术。

**李仁发**（1957– ），男，湖南郴州人，博士，湖南大学教授、博士生导师，主要研究方向为计算机体系结构、嵌入式计算、CPS、物联网。

**曾刚**（1970– ），男，湖南常德人，博士，名古屋大学助理教授，主要研究方向为能耗计算、实时嵌入系统设计。



**谢勇**（1985– ），男，湖南衡阳人，博士，厦门理工学院副教授，主要研究方向为嵌入式系统、CPS、车内网络的设计和优化。



**谢国琪**（1983– ），男，湖南宁乡人，博士，湖南大学副教授，主要研究方向为嵌入式与信息物理系统、并行与分布式系统、安全关键系统。