专题：智能网联汽车与车联网

车联网安全防护技术综述

陈滢媛[1]，董振江[1]，董建阔[1]，徐敏杰[2]
（1. 南京邮电大学，江苏 南京 210023；2. 中汽创智科技有限公司，江苏 南京 211106）

摘　要：车路云协同的车联网体系已经逐步上升为国家战略，车联网安全关系到行车安全、生命财产安全甚至国家安全，正日益成为行业研究热点。首先介绍了车联网技术架构与安全行业的整体状况；其次，以车联网“车–路–云”技术体系为基准，从车联网终端安全、车联网路侧安全、车联网云端安全 3 个层面，讨论了国内外研究现状，并分析了车联网安全防护领域的问题与挑战；最后，展望了车联网安全防护技术未来的发展与研究重点。

关键词：车联网安全；车路云协同；信息安全
中图分类号：TP393
文献标志码：A
doi: 10.11959/j.issn.1000–0801.2023046

A survey of V2X security protection technologies

CHEN Fuyuan[1], DONG Zhenjiang[1], DONG Jiankuo[1], XU Minjie[2]
1. Nanjing University of Posts and Telecommunications, Nanjing 210023, China
2. China Automotive Innovation Corporation, Nanjing 211106, China

Abstract: The vehicle-road-cloud collaborative V2X system has gradually become a national strategy, and the safety of V2X is related to driving security, life security, property security and even national security, which has increasingly become a hot spot for industry research. Firstly, the overall situation of the V2X security industry and the technology architecture of vehicle-road-cloud collaboration were introduced. Secondly, based on the “vehicle-road-cloud” technology system of V2X, the current status of domestic and international research was discussed, and the remaining problems and challenges in the field of V2X security protection were analyzed from three levels: V2X terminal security, roadside security and cloud security. Finally, the future development and research focus of the V2X security and protection technology were foreseen.

Key words: V2X security, vehicle-road-cloud collaboration, information security

专题策划人：董振江
收稿日期：2023–02–22；**修回日期**：2023–03–15
通信作者：董振江，dongzhenjiangvip@163.com
基金项目：国家重点研发计划项目（No.2021YFB3101100）；江苏省自然科学基金资助项目（No.BK20220388）；江苏省高等学校基础科学（自然科学）研究面上项目（No.22KJB520004）；中国博士后科学基金资助项目（No.2022M711689）
Foundation Items：The National Key Research and Development Program of China (No.2021YFB3101100), The Natural Science Foundation of Jiangsu Province (No.BK20220388), The Natural Science Research Project of Colleges and Universities in Jiangsu Province (No.22KJB520004), The China Postdoctoral Science Foundation (No.2022M711689)

0 引言

近年来，随着新一代互联网+、大数据、云计算、人工智能等新兴技术的发展与渗透，车路云协同的车联网体系已经逐步上升为国家战略。当前，拥有百年历史的汽车行业正在经历颠覆性的变革，随着汽车电动化、网联化、智能化的发展，汽车已经从一个传统的运输工具演变为一个集大数据交互平台、分布式存储单元和运算中心于一体的新时代产物。在新基建与“双碳”目标的推动下，为满足城市智能化交通出行、全局化交通管控、泛在化信息服务的需求，突破单车智能的瓶颈，新一代强调车–路–云协同的车联网技术被提出并受到了广泛关注。

根据中国物联网校企联盟的定义，车联网是由车辆位置、速度和路线等信息构成的巨大交互网络，装载在车辆上的电子标签通过无线射频等识别技术，实现在信息网络平台上对所有车辆的属性信息、静动态信息进行提取和有效利用，并根据不同的功能需求对所有车辆的运行状态进行有效的监管并提供综合服务[1-3]，为人们提供安全、高效、舒适的驾驶体验，为日常出行带来了巨大的便利[4]。

随着车联网技术的迅猛发展，安全问题日渐突出，成为制约车联网技术发展的重要因素。国内外相关研究报告显示，全球智能网联汽车呈现快速增长的趋势，2023 年全球智能网联汽车数量将达到 7.75 亿辆。与此同时，车联网安全事件频发，自 2010 年以来，已公开的汽车及车联网领域安全事件超过 900 起，且攻击规模、频率、复杂程度都呈现指数级增长。2022 年 12 月，蔚来汽车遭勒索致大量用户数据泄露，沃尔沃汽车遭受网络攻击导致大量研发数据被盗；2023 年 1 月，丰田、奔驰、宝马等全球 20 余家知名车企因应用程序接口（application programming interface，API）漏洞泄露车主个人信息；Upstream 发布的《2023 年全球汽车网络安全报告》指出，2022 年车联网引入了新的攻击载体，主要包括汽车应用程序以及充电装置，安全威胁影响面也随之扩大，响应和检测能力亟待调整。2022 年全球汽车主要攻击媒介及其总事件占比如图 1 所示。随着车联网安全事故频发，且安全防护边界的持续扩大，针对车联网的安全攻击呈现出攻击能力智能化、攻击方式多样化、攻击目的逐利化的特征，具有技术含量高、破坏影响力大的特点，使得车联网安全防御难度加大，车联网安全防护技术也受到了越来越多的关注与重视。

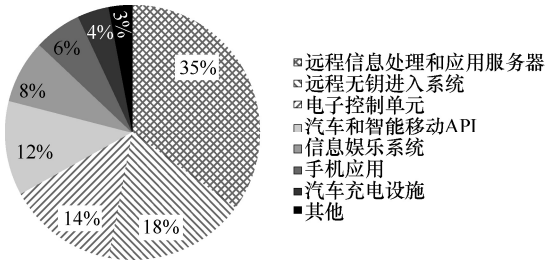

图 1 2022 年全球汽车主要攻击媒介及其总事件占比

车联网安全不仅涉及车辆自身安全，而且关乎个人、社会、国家的安全。近年来，各国政府、国际组织陆续颁布相关安全法规和标准，如以 UNECE/WP.29（R155、R156）和 ISO/SAE 21434 为代表的汽车信息安全国际法规及标准。《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律，以及国家相关政策与指南的发布，对车联网行业的信息安全提出了更严格的要求和更高的标准。2022 年工业和信息化部组织编制了《车联网网络安全和数据安全标准体系建设指南》，用于指导车联网相关标准研制；全国汽车标准化技术委员会、全国信息安全标准化技术委员会、中国通信标准化协会等发布的《汽车信息安全通用技术要求》《信息安全技术操作系统安全评估准则》《车联网信息服务数据安全保护能力评估规范》等标准对车联网信息安全全生命周期过程提出了要求，为车联网行业管理和发展提供了安全保障。

各大车企与信息安全企业依托多年的研发与

研究经验，推出了系列车联网安全防护方案，旨在保障全生命周期的车联网安全。2014 年，360 公司成立了 360 车联网安全实验院（360 Sky-Go），曾全球首次发现特斯拉汽车安全漏洞，并陆续推出了车联网安全运营方案、车联网安全检测平台等，为车联网网络安全合规检测、安全验证等场景提供可靠验证环境；百度公司构建了“AI–云–管–端–数据”的整体安全体系和能力架构，为建设车联网安全综合保障体系提供了可行方案；伊世智能自主研发的车载控制器芯片 HSM（hardware security module）国密算法安全固件，可以实现整车电子控制单元（electronic control unit，ECU）全生命周期安全可信管理；奇安信公司搭建了车联网安全网络靶场，构建了风险评估和产品测试系统，提供了安全评估与测试能力。然而，考虑到当前车联网攻击智能化、多样化的特点，车联网安全防护仍面临诸多风险与挑战。

尽管各国在政策法规、技术标准、落地应用、商业模式等多方面各有千秋，但基于车路云协同的车联网技术发展目标基本保持一致。车路云协同的车联网体系是利用新一代信息与通信技术，将人、车、路、云的物理层、信息层、应用层连为一体，进行融合感知、协同决策与控制，综合提升交通效率和行驶安全的信息物理系统。本质上，车路云协同的车联网技术是在单车智能的基础上增加了路侧感知，车端、路端数据共同上传至云端形成决策，并返回给车辆，从而解决单车智能长期无法突破的一系列瓶颈。基于车路云协同的车联网技术架构如图 2 所示，由车辆与其他交通参与者、路侧基础设施、云端平台、通信网络以及相关支撑平台组成。车辆与其他交通参与者是车联网体系架构中的重要组成部分，可以利用通信网络或路侧基础设施向云端平台进行动态信息的同步，同时也可以获取和接收来自云端平台的应用服务；路侧基础设施可以获取车辆、道路交通设施的相关数据，并与车辆及其他交通参与者进行同步；云端平台集成了网联汽车赋能类应用、交通管理和控制类应用以及交通数据赋能类应用三大类型的应用服务，基于相关交通数据的采集、存储、处理实现共享应用服务。

本文以车联网“车–路–云”的技术体系为基准，从车联网终端安全、车联网路侧安全、车联网云端安全 3 个层面，就国内外研究现状展开讨论，并针对车联网安全领域尚存的问题与挑战进行分析；最后，展望车联网安全领域的未来发展，为后续研究提供参考。

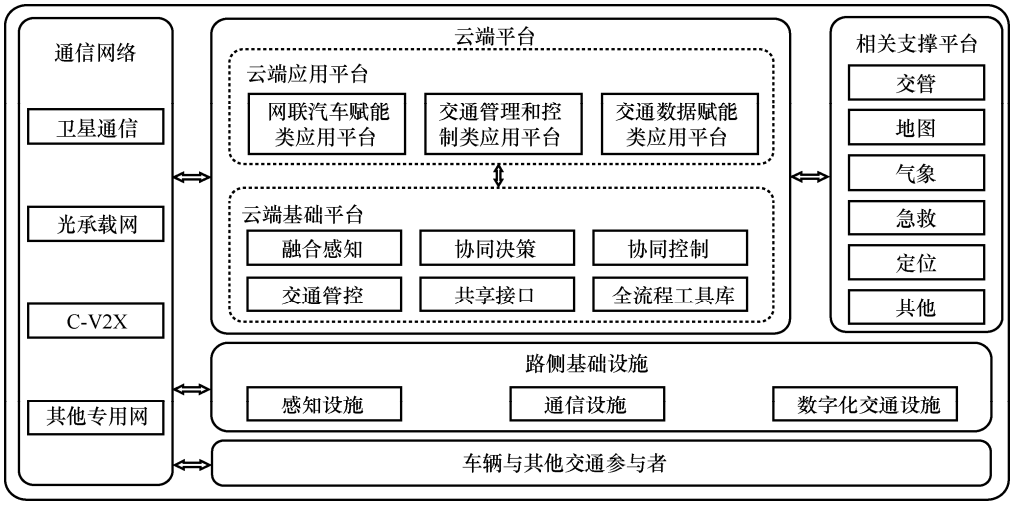

图 2　基于车路云协同的车联网技术架构

1 车联网终端安全

在车路云一体化的车联网技术体系架构中，车侧主要由车辆及其他交通参与者构成，车辆包含具有车–路、车–云网联化能力的网联汽车（包括具备自动驾驶能力的智能汽车与不具备自动驾驶能力的非智能汽车）以及非网联汽车，其他交通参与者主要指道路上参与并且会影响行驶安全与效率的其他对象，主要有非机动车、行人、动物、道路遗撒物等，无法接入车联网的参与者的动态信息将由路侧感知设备及其他网联汽车感知后传送至云端平台。

针对车联网终端的攻击，主要有物理连接和无线网络连接两种方式，利用嗅探攻击、重放攻击、女巫攻击等多种方法，对车载总线与车载系统发动攻击以获取汽车控制权、窃取汽车信息。针对车联网终端的典型攻击方式与业内常见的防御手段见表 1。根据 Upstream 发布的《2023 年全球汽车网络安全报告》，电动智能汽车的普及引入了新的攻击载体，电动汽车充电基础设施也将成为被攻击的目标。

表 1 针对车联网终端的典型攻击方式与业内常见的防御手段

典型攻击方式	常见防御手段
车载僵尸网络	声誉机制、异常检测机制等
植入恶意软件	访问限制等
嗅探攻击	端口访问控制诊断、网络分割、入侵检测防御系统等
黑洞攻击	引入基于信誉的路由等
重放攻击	强加密方法、虚拟专用网络、时延变化等
女巫攻击	公共加密的基于身份和认证的方法等
定时攻击	引入随机变量掩盖时间特征等

本节将从车载系统安全与车载总线安全两个部分，对车路云协同的车联网终端安全的研究现状展开讨论。

1.1 车载系统安全

车载系统作为智能网联汽车的重要车载组件，通过 Wi-Fi、蓝牙、移动互联网等方式与云端服务平台、路侧感知设备、互联网、智能终端等进行通信，实现安全服务、定位导航、辅助驾驶、车身控制、在线娱乐等一系列车载应用，实现人、车和外部环境间的信息交互，提升汽车智能化、网联化水平。车载系统的基本业务功能如图 3 所示。车载系统的基本业务逻辑结构如图 4 所示。车载系统一方面直接物理连接在车载总线网络上，另一方面有许多对外通信接口，增加了车联网终端安全风险[5]。

针对车载系统的安全防护技术，主要有车载加密技术、车载防火墙技术、车载入侵检测技术、车载安全审计技术以及车载网络安全认证技术 5 个方面[6]。

车载加密技术：车载加密技术可以对车辆明文数据信息进行保护，有效防止攻击者利用传输信道窃取或破坏传输信息，进而保证数据传输的完整性和机密性，避免数据泄露的安全风险。Aminifar 等[7]提出了一种基于迭代分组密码的对称加密方法，并设置了机密保护与开销之间的权衡机制，以最大限度地提高机密性，同时保证实时性的要求；Munir 等[8]设计了一种基于车载控制器局域网（controller area network，CAN）线控转向的安全可靠汽车网络物理系统集成方法，利用多核 ECU 通过冗余多线程（redundant multithreading，RMT）提供容错能力，并进一步增强 RMT 以快速检测和纠正错误。

车载防火墙技术：防火墙技术可以对网络流量进行监控，根据事先制定的安全策略对数据流量进行管控。Luo 等[9]为车载网络设计一个安全网关，基于威胁分析定义了车载网关的安全要求，提出将安全通信、密钥主控和防火墙作为保护汽车网关的安全机制，安全通信机制主要包含消息身份验证和数据加密；Rizvi 等[10]提出了一种新型的混合安全系统，使用分布式防火墙过滤放置在每个模块和电子控制单元上的恶意内容（如数据包），保障车载信息系统与安全系统之间的通信安全。

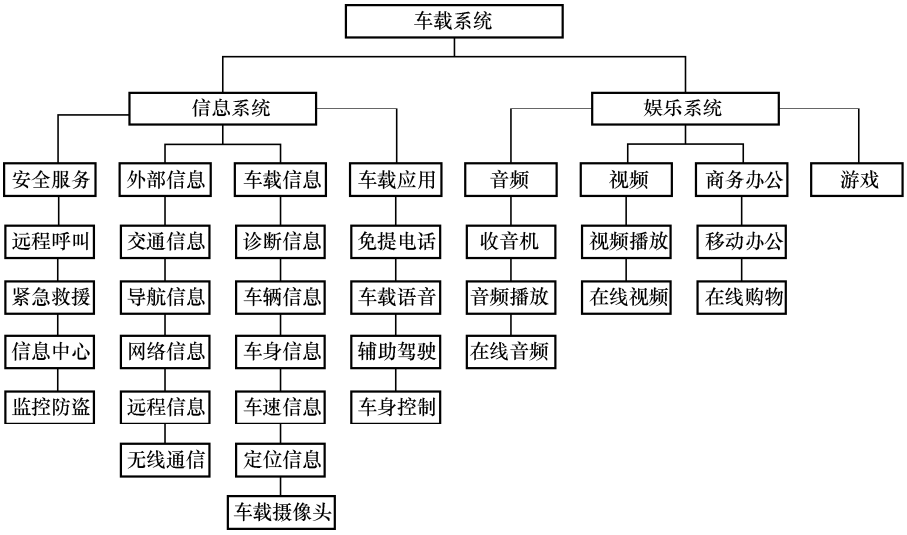

图 3　车载系统的基本业务功能

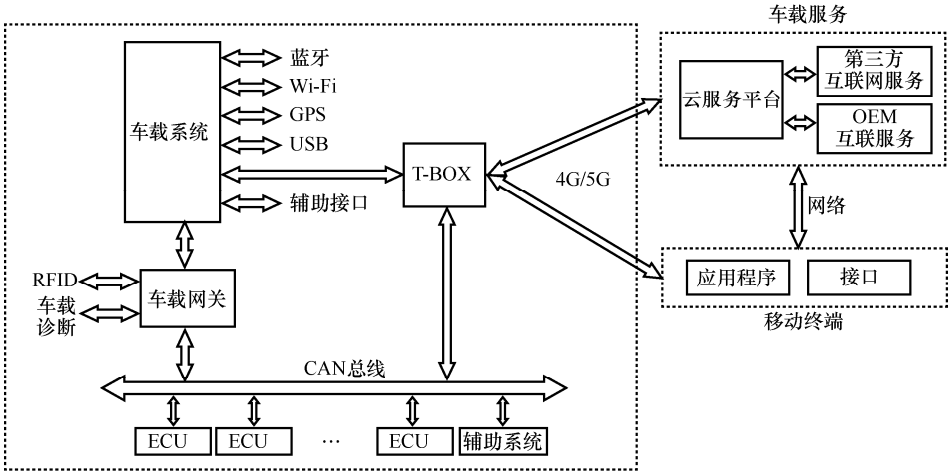

图 4　车载系统的基本业务逻辑结构

车载入侵检测技术：相较于静态的车载入侵防御系统（intrusion prevention system，IPS），车载入侵检测系统（intrusion detection system，IDS）可以对网络流量进行监控，是一种在不影响网络性能前提下的主动防御手段，主要有基于异常 IDS、基于签名 IDS、基于规范 IDS、基于混合 IDS、基于指纹 IDS、基于参数监控 IDS、基于信息熵 IDS 和基于机器学习 IDS。其中，基于异常 IDS 为业内常用的入侵检测方法[11]，将实时数据与正常行为数据进行比对，利用训练好的模型分析结果和常规值的偏差与阈值之间的关系，定位安全风险。

车载安全审计技术：利用车载终端记录的访问日志进行审计和监管，也是车载终端系统安全防护的重要手段之一。Checkoway 等[12]通过实验验证了审计系统会在发现异常或攻击事件时启动处理程序，降低潜在攻击的威胁。常见的安全审计方法有基于数理统计的安全审计、基于特征匹配的安全审计以及基于预测感知的安全审计。

车载网络安全认证技术：车载网络安全认证技术可以增强车载系统的安全性。Jo 等[13]提出了一种 Mauth-CAN 认证方法，利用 ECU 与验证器共享密钥，验证器可以安全有效地为 ECU 分配种子值，进而规避由 ECU 发起伪造攻击的安全风险。

在车载系统安全防护技术中，车载系统的功能需求与安全需求在计算、通信与网络资源等方面存在竞争关系，而安全的车载系统需要同时满足保密性、完整性与可用性的要求，出于成本与性能的综合考量，传统的信息安全手段无法直接作用于车载网络系统。当前针对车载系统的安全防护技术为了减少额外的计算与通信开销，常采用改进硬件模块或优化通信协议的方法，这些方法往往会造成硬件部署成本增加或导致网络协议变得复杂，如何平衡资源开销、运算性能与成本仍需进一步研究。

1.2 车载总线安全

各家汽车制造厂商研发的智能网联汽车所提供的智能决策、辅助驾驶、定位导航以及娱乐服务功能，拥有越来越多的外向型组件，严重违反了车载控制器局域网 CAN 封闭运行环境的初衷[14]。开放的 CAN 总线环境使得智能网联汽车受到了多种破解与攻击威胁。根据车载 CAN 总线的安全防护思路，可以将车载总线安全研究成果分成总线安全防护技术与总线入侵检测技术。

在 CAN 总线攻击方式多样化的同时，各种防护手段陆续被提出。吴尚则等[15]提出了一种基于挑战–应答模式的车载 CAN 总线动态口令身份认证方法，利用身份验证技术保证消息传输的准确性，使用随机动态生成的口令与哈希函数保证消息传输的可信度与完整性；丁山等[16]设计了一种优先级跳变机制，利用分组机制对传输的数据帧进行分段重构，对不同分段采取不同的跳变手段，提升 CAN 总线的安全性；Lin 等[17]针对伪装攻击和重放攻击，设计了一种利用消息 ID 表和消息计数器生成消息认证码的安全策略，在保证 CAN 总线网络通信安全的同时降低通信开销；Kang 等[18]提出了一种基于 CAN 单向哈希链的轻量级认证方法；Geng 等人[19]设计了一种新型汽车网络安全策略，利用软件定义网络（software defined network，SDN）构建汽车的网络架构，针对重放攻击研究一种基于序列号算法与介质访问控制（medium access control，MAC）层完全序列号方法的防御安全方案，将总线安全防护方案嵌入典型安全攻击中，同时满足了不同数据和计算开销的安全要求；Carsten 等[20]对现代车载总线网络的脆弱性进行了分析，总结了 CAN 通信协议作为主要攻击载体的问题，并提出了一系列克服攻击的解决方案。

对 CAN 总线进行入侵检测也是实现车载总线安全的关键技术。于赫[21]提出了一种基于信息熵的 CAN 网络异常检测方法，主要用于对 CAN 总线泛洪、重放等攻击的检测，同时基于决策树的报文异常检测方法也被用于对 CAN 总线通信报文进行异常检测；Bezemskij 等[22]实现了一种针对未知攻击的检测方法，获取实时汽车监控数据并利用机器学习的方法对数据进行训练，实验证明该方法可以有效检测大多数攻击；Levi 等[23]设计了一种适配不同接口的攻击检测系统，通过提取基于事件的相关信息并送入生成模型，检测事件与正常行为的偏差；Olufowobi 等[24]利用基于异常的监督学习方法，提出了基于 CAN 事实模型的检测算法，开发了一套基于规则的入侵检测系统；Studnia 等[25]利用自然语言处理技术，从行为模型中提取攻击特征，设计了一种非侵入式网络入侵检测方法，用于检测通过网络内部传输的恶意消息序列。

入侵检测技术具有占用带宽资源少、部署便捷的特点，相较于被动的总线安全防护技术，入侵检测更适合资源与成本受限的车载终端部署与应用。近年来，相关实验表明基于信息熵的车载 CAN 总线网络异常检测方法可以有效检测重放、泛洪等攻击，但这种方法不具备良好的稳健性，易受汽车状态变化造成的信息熵抖动影响。基于机器学习的检测技术虽然在未知攻击检测方面表现出了良好的效果，但受限于车载网络的计算、存储与通信资源限制，基于机器学习的方法在车

载终端系统中难以呈现理想的效果。因此，如何降低计算复杂度与通信带宽的需求，提高检测精度，缩短响应时延，提升检测的稳健性是进一步研究的方向。

2　车联网路侧安全

在车路云协同的车联网架构中，路侧基础设施包括感知设备、通信设备以及数字化交通设施，其中感知设备主要包括摄像头、毫米波雷达、激光雷达等传感器，融合数字化交通设施的数据信息（如交通信号灯等），依托路侧多接入边缘计算（multi-access edge computing，MEC）形成结构化的感知数据，利用路侧单元（road side unit，RSU）向其他交通参与者进行广播，实现车–路、路–云信息共享[26]。车路云协同信息交互模型如图 5 所示。路侧单元的业务功能架构如图 6 所示，主要由交通信息收发、交通设备接入、交通场景分析、定位和授时、边缘计算与云平台整合构成。

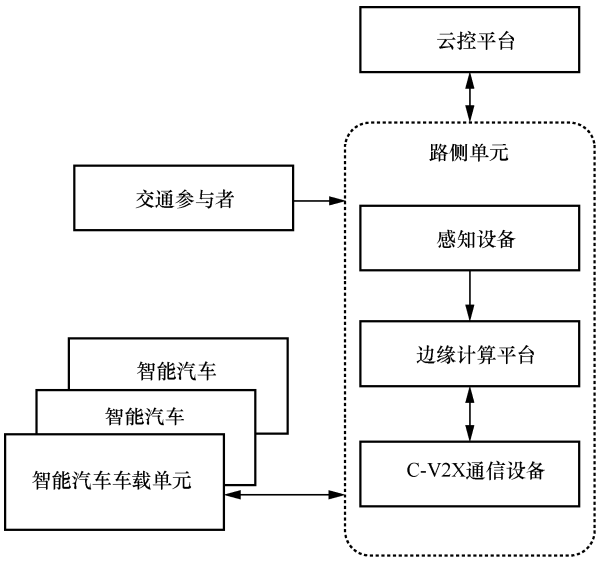

图 5　车路云协同信息交互模型

路侧基础设施的建设一方面可以为网联汽车提供超视距感知，弥补单车感知的局限性，另一方面可以完成交通数据的全量汇聚，支撑并实现精细化、实时化的交通管控与监测。针对路侧基础设施

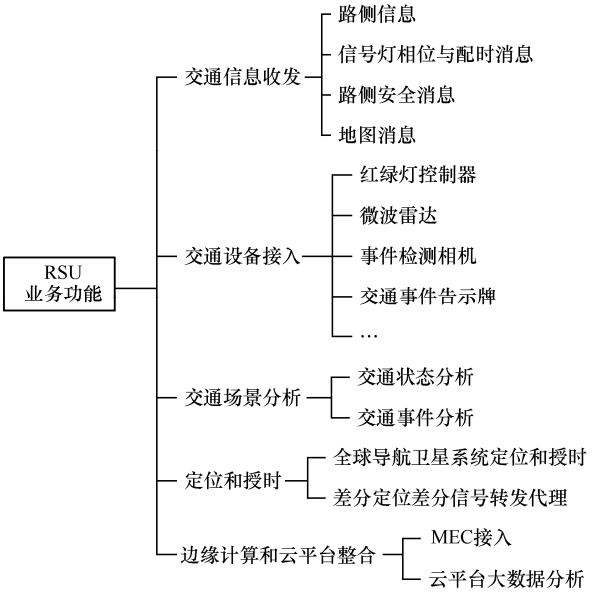

图 6　路侧单元的业务功能架构

的攻击主要利用通信传输或接口漏洞等进行恶意攻击，截获、修改、泄露交通信息，危害汽车安全、人身安全甚至国家安全。针对车联网路侧单元的典型攻击方式与常见防御手段表 2。

表 2　针对车联网路侧单元的典型攻击方式与常见防御手段

典型攻击方式	常见防御手段
伪造数字签名攻击	强加密方法、区块链技术等
自动驾驶算法攻击	增强神经网络鲁棒性、标记样本、数据预处理等
域名系统劫持攻击	通信模组升级、增加安全芯片、嵌入式入侵检测防御模块等

车路云协同中，路侧所面临的安全问题主要有如下几个方面。

- 路侧设备自身具有较高价值，易诱发失窃或非法占用等风险。以激光雷达为代表的感知设备由于缺乏完善的保护措施，硬件容易遭窃；以边缘计算设备为代表的硬件设施的算力可能存在被非法占用的风险。
- 路侧设施由于安装分散且缺乏完善的管理方案，容易遭受攻击。攻击者利用社会工程学的方法很容易接触到相关路侧设施，例如安装在信号灯杆中的设备，大大增加了接口暴露的风险。此外，考虑通用性，

路侧设施通常采用通用计算硬件与通用操作系统，使得车路云协同体系下的路侧基础设施具备通用系统的安全漏洞，攻击者可以通过以太网、通用串行总线（universal serial bus，USB）装置等方式接入，实施攻击。

- 路侧单元需要在车联网特殊传输要求下满足高精度、实时化的车–路、路–云、路–路通信，网络通信安全是车路云协同落地的关键问题之一。
- 车路云协同体系下的路侧单元汇聚了全量交通信息，包括车辆信息、交通信息、云端信息等，数据安全与隐私保护也是路侧所面临的问题。
- 路侧边缘计算单元 MEC 作为边缘节点承载了大量计算任务，完成对大容量、大连接数据的本地化处理，以达到降低通信时延、节省网络带宽的目的。通常 MEC 利用 AI 算法对数据进行处理，智能算法所面临的后门攻击、数据投毒攻击等脆弱性问题，也是车联网路侧安全防护待解决的问题之一。

就防护对象而言，车路云协同下的路侧安全防护技术有 3 个主要方向：网络通信安全防护技术、身份与认证技术、数据隐私保护技术。

（1）网络通信安全防护技术

当前，人工智能算法在车联网通信安全方面有着广泛的应用。

俞建业等[27]提出了一种基于 Spark 的车联网分布式组合深度学习入侵监测方法，利用 Spark 集群框架将卷积神经网络和长短期记忆网络进行组合，对车联网的入侵特征进行提取和数据检测，满足车联网场景下对入侵检测实时性和精准性的要求，这一方案同样适用于车联网的通信安全入侵检测；吴茂强等[28]研究发现攻击者可以通过训练反卷积网络的方式对车路云协同中的数据发起图像还原攻击，研究了 3 种基于差分隐私的防御方法，通过加入扰动参数破坏还原攻击；李明磊等[29]设计了一种基于多智能体强化学习算法，提升基于委托权益证明的共识算法在车联网中的安全性；Zhang 等[30]提出了一种基于信任的互联网车辆通信对抗深度强化学习方法，将对抗网络架构部署到 SDN 的逻辑集中控制器中，将 SDN 控制器作为代理，通过车载自组网中的深度神经网络学习最受信任的路由路径，从而缓解恶意节点的攻击；Yoon 等[31]提出了一个基于深度强化学习的资源分配与移动目标防御部署框架，设计了基于强化学习的主动防御机制和弹性强化学习方法，允许代理在存在对抗性干扰的情况下运行，并使用基于多智能体深度强化学习的网络切片技术，使得这一框架在存在干扰的情况下也可以进行鲁棒性学习，增强了网络通信的安全性。

（2）安全认证技术

根据应用场景的不同，车路云协同下的车联网安全认证可以分为匿名认证、群组认证、跨域认证和基于区块链的认证 4 种[6]，如图 7 所示。

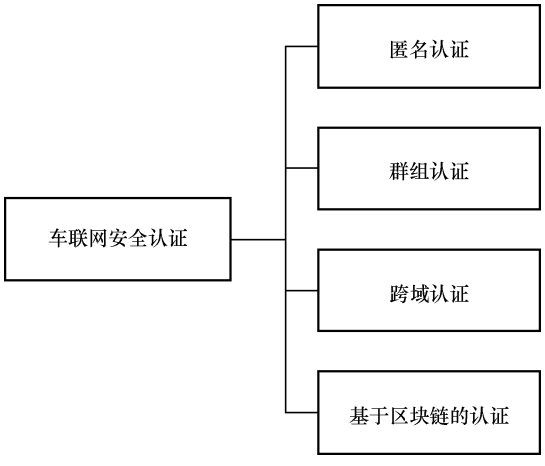

图 7　车联网安全认证技术

Wang 等[32]提出了一种基于本地身份的匿名消息身份验证协议，每个车辆和路边单元在注册阶段被分配来自证书颁发机构的唯一长期认证，车辆可以从当前 RSU 获取本地密钥以生成本地化

的匿名身份，在实际通信中车辆随机选择匿名身份对相关消息进行签名，可以通过单次或批量认证方式进行有效验证，在保证匿名性的同时提高了效率；Wasef 等[33]提出了一种可以同时支持位置隐私保护与身份认证的基于公开密钥基础设施（public key infrastructure，PKI）的机制，并设计了一种可以降低拒绝服务（denial of service，DoS）攻击影响的方案，有效保障车联网安全。基于 PKI 的方案通常需要第三方证书颁发机构（certificate authority，CA）提供证书并管理身份与公钥，不仅增大存储负担，也暗含安全风险。

Zhang 等[34]提出了一种基于身份的聚合签名认证方案，支持分层聚合和批量验证，使得在车联网中可以以极低的时延和快速响应验证接收到的消息；Zhang 等[35]设计了一种分布式聚合隐私保护身份验证机制，依赖聚合签名技术，可以实现多个消息的同时验证，并且它们的签名可以压缩成单个消息，从而大大减少车辆和数据收集器所需的存储空间。

由于汽车往往会频繁地进行跨域行驶，在这一应用场景下跨域认证的方案实现也会影响车联网安全。Xu 等[36]通过提出一种高效安全的基于 ID 的车载网络消息认证方案改善车载网络的安全功能；李晓伟等[37]提出了一个基于口令无服务器参与的跨域车辆与车辆之间的认证与密钥协商协议，采用分发认证凭证的方式实现跨越认证，通过将智能卡与口令结合的方式增强口令的安全性，由于没有服务器的参与，该协议可以避免服务器并发能力不足带来的时延。

传统的安全认证技术都基于可信第三方，存在单点崩溃的安全风险，基于区块链的技术可以有效规避这一安全威胁。Jiang 等[38]提出了一种采用私有信息检索思想的隐私保护轻节点认证方案，使轻节点能够像全节点用户一样在正常运行的同时保护节点隐私；Gabay 等[39]利用区块链和智能合约的分布式应用程序解决车载网络的隐私保护认证问题，将零知识证明与区块链技术结合，实现隐私保护下的身份验证，同时消除对集中式服务器的需求。

（3）数据隐私保护技术

数据隐私保护技术主要分为身份隐私保护、位置隐私保护和基于区块链的隐私保护技术三大类，如图 8 所示。

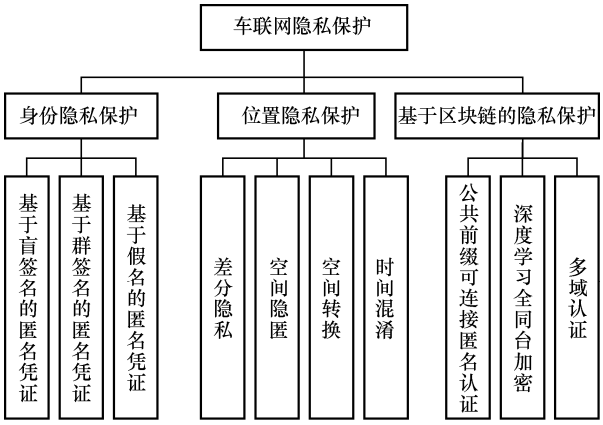

图 8　数据隐私保护技术

匿名凭证是身份隐私保护的通用手段。Sun 等[40]提出了一种基于盲签名的隐私保护防御技术，这一方法不需要证书进行身份验证；Xu 等[41]提出一种基于模糊系统的车载网络安全高效的群认证和隐私保护方案，利用群认证和隐私保护级别的设置提高车载网络的安全性；Park 等[42]设计了一种基于假名的车路云访问管理系统，利用车辆的假名服务访问令牌和 RSU 本地撤销机制，防止车辆信息被追踪。

差分隐私是位置隐私保护的主要实现手段。Zhou 等[43]设计了一种部署在边缘节点上的基于位置的差异隐私保护框架，包括基于位置的差分隐私保护机制和隐私级别调整机制，可以实现隐私级别的动态调整，保证隐私安全。

Baza 等[44]利用区块链技术，提出了一种基于隐私保护的充电站到车辆的能源交易方案，使用了一个通用的前缀可链接匿名身份验证机制，保证汽车信息的隐私安全；Chen 等[45]将深度学习、区块链和全同态加密技术融合应用于车联网安

全，提出了一种去中心化隐私保护深度学习模型，为车-路信息传输搭建安全可信的通信环境；Yang等[46]提出了一种多域车辆认证架构，通过引入区块链技术构建分布式信任，并在多个管理域之间共享跨域信息，保证了匿名性和可追溯性。

车联网这一特殊应用场景对信息传输的毫秒级时延和超高可靠要求远超一般场景，并且将直接影响用户的生命财产安全，这也为路侧感知与计算系统带来了部署、多源异构数据事件同步、处理等一系列的难题与挑战。对于网络通信安全防护技术，基于强化学习的方法虽然可以适用于多种攻击防御场景，但在传输时延与算法鲁棒性方面仍有提升空间；基于区块链的隐私保护与认证技术是当前的研究热点，可以提供安全可靠的身份验证、数据存储与隐私保护，但需要大量的存储与计算资源，如何合理部署并调度资源以满足车联网的应用需求尚待进一步研究。

3 车联网云端安全

如图 2 所示，车路云协同的车联网体系架构下，云端平台由云端基础平台与云端应用平台构成，云端基础平台以车侧与路侧传回的车辆、道路、交通实时动态数据为核心，为相关产业部门提供标准化的通用基础服务；云端应用平台主要包括网联汽车赋能类应用平台、交通管理与控制类应用平台以及交通数据赋能类应用平台。车联网云服务拥有强大的存储、计算、分析和运维能力，可以为车辆运行、人车交互、车车交互以及交通管理提供全方位的服务，同时也作为“中枢神经”增强车联网信息安全和驾驶安全。

车联网云端具有通用云平台的安全问题，同时由于车联网应用场景的特殊性，在保证低时延的条件下仍需满足计算的准确性以及数据的安全性要求。针对车联网云平台的典型攻击方式与常见防御手段见表 3。当前，企业普遍通过分布式拒绝服务（distributed denial of service，DDoS）、防火墙、云安全中心等技术或产品，为车联网云端服务系统提供纵深防御，防护手段逐步从事后被动防御转变为事前主动防御。

表 3 针对车联网云平台的典型攻击方式与常见防御手段

典型攻击方式	常见防御手段
DDoS 攻击	隐藏服务器或端口、接入限制技术、质询–响应协议、资源限制等
侧信道攻击	缓存擦除、插入随机时延等
中间人攻击	黑盒、对抗测试等
云中间人攻击	物理不可克隆功能（physically unclonable function，PUF）、认证安全互联网服务机制、云中间人（man in the cloud，MITC）卫士等

当前，车联网云端安全防护技术主要考虑云服务安全与智能算法安全两个方向。

（1）云服务安全

在云平台架构安全方面，由于车联网场景下对数据传输实时性的要求，传统云平台架构存在通信慢、数据集中、需要多次通信等问题，许多学者就车联网场景下的云平台架构进行了设计与研发。Wang 等[47]对车载云架构发展现状以及面临的挑战进行了讨论，并且提出了一种基于云的软件定义车载网络，解决传统云在车联网场景下的系列弊端；当下信息安全企业通常利用基于平台即服务（platform as a service，PaaS）的云平台架构，牛雅丽等[48]搭建并研发了基于 PaaS 的车联网云平台，实现了以容器为运行单元，以 Kubernetes 为集群调度的新一代轻量化车联网 PaaS 平台。

在云计算的隐私安全方面，为了解决资源分配与隐私安全的冲突，一些学者就车联网场景下的云计算隐私安全性进行了研究分析。Arain 等[49]发现现有的位置隐私保护技术无法适用于车联网场景，因此针对路云协同的移动车辆地图服务，设计了一种多混区位置隐私保护综合方法，使移动车辆用户能够查询地图上两个端点之间的路径，而不会泄露任何敏感位置和查询信息；王瑞锦等[50]提出了一种基于同态加密和区块链技术的车联网隐私保护方案，设计了一种基于同态加密

的数据结构，将隐私数据加密后由获得记账权的网关节点写入区块链网络，通过同态加密技术和区块链技术的结合，实现隐私数据以密文状态分发、共享和计算，有效保护用户隐私。

业内各大信息安全企业就车联网场景下的云服务安全问题研发了各具优势的车联网云安全管理平台。云盾慧御云安全管理平台是首批通过车联网服务平台安全能力测试评价并获得“五星级平台”车联网云服务安全平台，集成了丰富的云安全资源（如主机安全、智慧防火墙、数据库审计等），并通过策略组合满足云计算等级保护扩展要求的合规性；利用开放协议采集来自不同部件的安全事件数据，提供分析与安全决策的数据依据；通过集中管理多个分布式部署的安全资源池保障多云融合场景下的安全。华为提出的车联网平台支持亿级海量联接和百万级高并发，可以满足高峰时期的通信需求；提供支持传输层安全（transport layer security，TLS）双向证书认证，保障车辆接入安全；支持车联网系统基于策略弹性、平滑扩容，缓解车辆高峰期对平台的冲击。360Sky-Go 研发了 360 车联网安全检测平台，为智能网联汽车提供网络安全验证基础设施，搭载了车载系统测试、硬件安全测试、车载网络测试、App 安全测试等多个测试工具，可以以场景的形式对测试用例进行组合以满足安全测试需求，实现自动化检测。

车联网云端安全相较于传统云平台对精准性、实时性、高并发提出了更高的需求，以保证车路云数据交换在应用层可以满足自动驾驶控制可用性与信息安全的实际要求，同时保证互操作性和易用性。当前的相关技术主要包括：指定统一的数据交互标准、开发数据共享接口、优化数据存储模型、采用轻量级的基础设施、虚拟化管理平台、分布式边缘云部署架构、通信链路性能优化等。但实时的远程控制、安全可靠的计算下沉、高效的跨域数据交互通信、计算–存储–通信资源优化等一系列难题，仍有待进一步探究。

（2）智能算法安全

车路云协同下的车联网云平台，利用人工智能算法对大量交通数据进行处理，进而为用户提供相应的服务。然而，人工智能算法存在潜在的安全问题，如不可解释性、逆向攻击、后门攻击、投毒攻击、对抗样本攻击等，增加了车联网云端安全风险。彭长根等[51]聚焦人工智能技术存在的潜在安全风险，从隐私保护、算法鲁棒性、算法安全性几个角度，分析归纳了常见人工智能算法安全问题的解决对策，可以为车联网云平台的人工智能算法安全提供研究思路和方向；Zhu 等[52]提出了一种新的对抗训练算法，通过在词嵌入中添加对抗扰动，最小化输入样本周围不同区域内产生的对抗风险，提升嵌入空间的鲁棒性；Vilone 等[53]就 AI 缺乏可解释性的问题，从综述文章、理论、概念、方法及其评估几个角度，阐述了可解释 AI 的最新技术，并提出了未来研究的发展方向。

4　展望

近年来，国家发展和改革委员会、工业和信息化部、交通运输部等发布了一系列政策意见来指导和规范车联网行业发展，对车联网技术创新和产品研发提出了创新发展需求。《汽车整车信息安全技术要求》《智能网联汽车自动驾驶数据记录系统》与《汽车软件升级通用技术要求》3 项推荐标准转化为国家强制标准，意味着针对车联网信息安全、车联网数据安全以及车联网通用要求的相关标准将得到进一步的发展与细化。

车–路–云协同一体化是当前车联网的主要发展方向，为了应对当前智能化、复杂化的安全攻击，搭建贯通“端管云”3 个层面的车联网主动防御防护体系具有必要性。当前防御手段大多通过搭建或加固安全防护边界，对网内与网外的南北

向流量进行阻隔，但网内东西向流量缺乏一定的安全防护措施。零信任代表新一代的网络安全防护理念，不信任任何设备、用户、网络以及系统，通过基于身份的认证和授权对每一个访问请求进行验证。通过“持续验证，永不信任”的防御原则，保障系统内的身份可信、设备可信、应用可信以及链路可信。搭建基于零信任原则的网络安全防护架构，可以对车联网网内资源实施细粒度的主动安全防护。

为确保数据要素在车联网内的流通安全，隐私计算仍是车联网安全防护架构中的重要组成部分。车联网内交互数据呈现出数据量大、结构复杂、敏感信息多等特征，为保障在不泄露原始数据的情况下对数据进行分析计算，当前隐私计算的实现路径包括联邦学习、安全多方计算、可信计算和区块链技术等。同态加密技术是当前隐私计算的热门研究方向，可以使得数据在密文的状态下进行传输和计算，进而有效保障车辆、用户、交通以及道路信息的数据隐私安全。但当前同态加密技术尚存性能瓶颈，如何有效提升同态加密算法的运算速度，满足车联网应用场景下对计算以及通信时延的需求，是相关技术能否落地实现的关键。

密码算法作为安全领域的底层技术，加密算法的安全系数在车联网安全防护技术架构中起着决定性作用。棱镜门事件后国密算法进入了高速发展时期，国密算法的研究也将带动车联网安全技术的发展。不断提升国密算法的安全性，突破加密解密运算的性能瓶颈，降低实际运算所需的计算开销，将有利于提升车联网这一特殊应用场景下的数据与信息安全。

车路云协同下的车联网上层应用依赖于人工智能算法，人工智能的内生安全以及衍生安全问题将是车联网安全防护亟须解决的关键问题。在车联网应用场景下，数据集对算法鲁棒性有着重要影响，数据投毒以及对抗样本攻击都将直接威胁自动驾驶安全。对人工智能算法进行精准高效的安全检测，将能从很大程度上保证车联网服务的安全性、准确性与高效性。

5 结束语

本文主要讨论了当前车路云协同体系架构下的车联网安全问题以及对应的研究现状。首先介绍了车联网行业整体情况以及面临的安全风险，并对车路云协同体系进行了概述，将车联网安全防护技术分为车联网终端安全、车联网路侧安全以及车联网云端安全 3 个方面。同时，针对当前聚焦的安全问题研究现状进行了分析总结，回顾了相关威胁的解决方法，并指出了现有研究方案的局限性以及未来研究的重点。本文给出了车联网安全的未来发展趋势与研究展望，为进一步的研究工作奠定了基础。

参考文献：

[1] 陈山枝, 时岩, 胡金玲. 蜂窝车联网(C-V2X)综述[J]. 中国科学基金, 2020, 34(2): 179-185.
CHEN S Z, SHI Y, HU J L. Cellular vehicle to everything (C-V2X): a review[J]. Bulletin of National Natural Science Foundation of China, 2020, 34(2): 179-185.

[2] 陈山枝, 葛雨明, 时岩. 蜂窝车联网(C-V2X)技术发展、应用及展望[J]. 电信科学, 2022, 38(1): 1-12.
CHEN S Z, GE Y M, SHI Y. Technology development, application and prospect of cellular vehicle-to-everything (C-V2X)[J]. Telecommunications Science, 2022, 38(1): 1-12.

[3] AHMED E, GHARAVI H. Cooperative vehicular networking: a survey[J]. IEEE Transactions on Intelligent Transportation Systems: a Publication of the IEEE Intelligent Transportation Systems Council, 2018, 19(3): 996-1014.

[4] CAVALCANTI E R, DE SOUZA J A R, SPOHN M A, et al. VANETs’ research over the past decade[J]. ACM SIGCOMM Computer Communication Review, 2018, 48(2): 31-39.

[5] 张宏涛. 车载信息娱乐系统安全研究[D]. 郑州: 战略支援部队信息工程大学, 2021.
ZHANG H T. Research on security of In-vehicle infotainment system[D]. Zhengzhou: Information Engineering University, 2021.

[6] 周建华, 侯英哲, 吕臣臣, 等. 智能网联汽车安全防护技术研究综述[J]. 武汉大学学报(理学版), 2022: 10.14188/j.1671-8836.2022.0191.

ZHOU J H, HOU Y Z, LYU C C, et al. A review on security and defense technologies for intelligent connected vehicle[J]. Journal of Wuhan University (Natural Science Edition), 2022: 10.14188/j.1671-8836.2022.0191.

[7] AMINIFAR A, ELES P, PENG Z B. Optimization of message encryption for real-time applications in embedded systems[J]. IEEE Transactions on Computers, 2018, 67(5): 748-754.

[8] MUNIR A, KOUSHANFAR F. Design and analysis of secure and dependable automotive CPS: a steer-by-wire case study[J]. IEEE Transactions on Dependable and Secure Computing, 2020, 17(4): 813-827.

[9] LUO F, HU Q. Security mechanisms design for in-vehicle network gateway[C]//Proceedings of SAE Technical Paper Series. Warrendale: SAE International, 2018.

[10] RIZVI S, WILLETT J, PERINO D, et al. Protecting an automobile network using distributed firewall system[C]//Proceedings of the 2nd International Conference on Internet of Things, Data and Cloud Computing. New York: ACM Press, 2017: 1-6.

[11] TAYLOR A, JAPKOWICZ N, LEBLANC S. Frequency-based anomaly detection for the automotive CAN bus[C]//Proceedings of 2015 World Congress on Industrial Control Systems Security (WCICSS). Piscataway: IEEE Press, 2016: 45-49.

[12] CHECKOWAY S, MCCOY D, KANTOR B, et al. Comprehensive experimental analyses of automotive attack surfaces[C]//Proceedings of the 20th USENIX Conference on Security. New York: ACM Press, 2011: 6.

[13] 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.

[14] BOZDAL M, SAMIE M, ASLAM S, et al. Evaluation of CAN bus security challenges[J]. Sensors (Basel, Switzerland), 2020, 20(8): 2364.

[15] 吴尚则, 秦贵和, 刘毅, 等. 车载控制器局域网络总线的动态口令身份认证方法[J]. 西安交通大学学报, 2017, 51(6): 97-102.
WU S Z, QIN G H, LIU Y, et al. A method for identifying authentication of dynamic passwords for In-vehicle controller area network buses[J]. Journal of Xi'an Jiaotong University, 2017, 51(6): 97-102.

[16] 丁山, 臧仕义, 曹殿明, 等. 基于动态ID跳变的CAN总线安全调度算法[J]. 东北大学学报(自然科学版), 2022, 43(3): 350-358.
DING S, ZANG S Y, CAO D M, et al. Security scheduling algorithm of CAN bus based on dynamic ID hopping[J]. Journal of Northeastern University (Natural Science), 2022, 43(3): 350-358.

[17] LIN C W, SANGIOVANNI-VINCENTELLI A. Cyber-security for the controller area network (CAN) communication protocol[C]//Proceedings of 2012 International Conference on Cyber Security. Piscataway: IEEE Press, 2013: 1-7.

[18] KANG K D, BAEK Y, LEE S, et al. Lightweight authentication method for controller area network[C]//Proceedings of 2016 IEEE 22nd International Conference on Embedded and Real-Time Computing Systems and Applications (RTCSA). Piscataway: IEEE Press, 2016: 101.

[19] GENG R, WANG X J, LIU J. A software defined networking-oriented security scheme for vehicle networks[J]. IEEE Access, 2018(6): 58195-58203.

[20] CARSTEN P, ANDEL T R, YAMPOLSKIY M, et al. In-vehicle networks: attacks, vulnerabilities, and proposed solutions[C]//Proceedings of the 10th Annual Cyber and Information Security Research Conference. New York: ACM Press, 2015: 1-8.

[21] 于赫. 网联汽车信息安全问题及 CAN 总线异常检测技术研究[D]. 长春: 吉林大学, 2016.
YU H. Research on connected vehicle cyber security and anomaly detection technology for In-vehicle CAN bus[D]. Changchun: Jilin University, 2016.

[22] BEZEMSKIJ A, LOUKAS G, ANTHONY R J, et al. Behaviour-based anomaly detection of cyber-physical attacks on a robotic vehicle[C]//Proceedings of 2016 15th International Conference on Ubiquitous Computing and Communications and 2016 International Symposium on Cyberspace and Security (IUCC-CSS). Piscataway: IEEE Press, 2017: 61-68.

[23] LEVI M, ALLOUCHE Y, KONTOROVICH A. Advanced analytics for connected car cybersecurity[C]//Proceedings of 2018 IEEE 87th Vehicular Technology Conference (VTC Spring). Piscataway: IEEE Press, 2018: 1-7.

[24] OLUFOWOBI H, BLOOM G, YOUNG C, et al. Work-in-progress: real-time modeling for intrusion detection in automotive controller area network[C]//Proceedings of 2018 IEEE Real-Time Systems Symposium (RTSS). Piscataway: IEEE Press, 2019: 161-164.

[25] STUDNIA I, ALATA E, NICOMETTE V, et al. A language-based intrusion detection approach for automotive embedded networks[J]. International Journal of Embedded Systems, 2018, 10(1): 1-12.

[26] 董振江, 古永承, 梁健, 等. C-V2X 车联网关键技术与方案概述[J]. 电信科学, 2020, 36(4): 3-14.
DONG Z J, GU Y C, LIANG J, et al. Overview on key technology and solution of C-V2X for Internet of vehicles[J]. Telecommunications Science, 2020, 36(4): 3-14.

[27] 俞建业, 戚湧, 王宝茁. 基于 Spark 的车联网分布式组合深度学习入侵检测方法[J]. 计算机科学, 2021, 48(S1): 518-523.
YU J Y, QI Y, WANG B Z. Distributed combination deep learning intrusion detection method for Internet of vehicles based on spark[J]. Computer Science, 2021, 48(S1): 518-523.

[28] 吴茂强, 黄旭民, 康嘉文, 等. 面向车路协同推断的差分隐私保护研究[J]. 计算机工程, 2022, 48(7): 29-35.

WU M Q, HUANG X M, KANG J W, et al. Research on differential privacy protection for collaborative vehicle-road inference[J]. Computer Engineering, 2022, 48(7): 29-35.

[29] 李明磊, 章阳, 康嘉文, 等. 基于多智能体强化学习的区块链赋能车联网中的安全数据共享[J]. 广东工业大学学报, 2021, 38(6): 62-69.
LI M L, ZHANG Y, KANG J W, et al. Multi-agent reinforcement learning for secure data sharing in blockchain-empowered vehicular networks[J]. Journal of Guangdong University of Technology, 2021, 38(6): 62-69.

[30] ZHANG D J, YANG R Z, et al. A deep reinforcement learning-based trust management scheme for software-defined vehicular networks[C]//Proceedings of the 8th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications. New York: ACM, 2018: 1-7.

[31] YOON S, CHO J H, KIM D S, et al. DESOLATER: deep reinforcement learning-based resource allocation and moving target defense deployment framework[J]. IEEE Access, 2021(9): 70700-70714.

[32] WANG S B, YAO N M. LIAP: a local identity-based anonymous message authentication protocol in VANETs[J]. Computer Communications, 2017, 112: 154-164.

[33] WASEF A, LU R X, LIN X D, et al. Complementing public key infrastructure to secure vehicular ad hoc networks[security and privacy in emerging wireless networks][J]. IEEE Wireless Communications, 2010, 17(5): 22-28.

[34] ZHANG L, HU C Y, WU Q H, et al. Privacy-preserving vehicular communication authentication with hierarchical aggregation and fast response[J]. IEEE Transactions on Computers, 2016, 65(8): 2562-2574.

[35] ZHANG L, WU Q H, DOMINGO-FERRER J, et al. Distributed aggregate privacy-preserving authentication in VANETs[J]. IEEE Transactions on Intelligent Transportation Systems, 2017, 18(3): 516-526.

[36] XU C, HUANG X H, MA M D, et al. A secure and efficient message authentication scheme for vehicular networks based on LTE-V[J]. KSII Transactions on Internet and Information Systems, 2018, 12(6): 2841-2860.

[37] 李晓伟, 杨邓奇, 曾新, 等. 车联网环境下跨域间认证与密钥协商协议[J]. 西安电子科技大学学报, 2021, 48(1): 141-148.
LI X W, YANG D Q, ZENG X, et al. Cross-domain authentication and the key agreement protocol in VANETs[J]. Journal of Xidian University, 2021, 48(1): 141-148.

[38] JIANG W B, LI H W, XU G W, et al. PTAS: privacy-preserving thin-client authentication scheme in blockchain-based PKI[J]. Future Generation Computer Systems, 2019, 96: 185-195.

[39] GABAY D, AKKAYA K, CEBE M. Privacy-preserving authentication scheme for connected electric vehicles using blockchain and zero knowledge proofs[J]. IEEE Transactions on Vehicular Technology, 2020, 69(6): 5760-5772.

[40] SUN J Y, ZHANG C, ZHANG Y C, et al. An identity-based security system for user privacy in vehicular ad hoc networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2010, 21(9): 1227-1239.

[41] XU C, LIU H Z, PAN Z H, et al. A group authentication and privacy-preserving level for vehicular networks based on fuzzy system[J]. Journal of Intelligent & Fuzzy Systems: Applications in Engineering and Technology, 2020, 39(2): 1547-1562.

[42] PARK Y, SUR C, RHEE K H. Pseudonymous authentication for secure V2I services in cloud-based vehicular networks[J]. Journal of Ambient Intelligence and Humanized Computing, 2016, 7(5): 661-671.

[43] ZHOU L, YU L, DU S G, et al. Achieving differentially private location privacy in edge-assistant connected vehicles[J]. IEEE Internet of Things Journal, 2019, 6(3): 4472-4481.

[44] BAZA M, SHERIF A, MAHMOUD M M E A, et al. Privacy-preserving blockchain-based energy trading schemes for electric vehicles[J]. IEEE Transactions on Vehicular Technology, 2021, 70(9): 9369-9384.

[45] CHEN J G, LI K L, YU P S. Privacy-preserving deep learning model for decentralized VANETs using fully homomorphic encryption and blockchain[J]. IEEE Transactions on Intelligent Transportation Systems, 2022, 23(8): 11633-11642.

[46] YANG Y H, WEI L J, WU J, et al. A blockchain-based multi-domain authentication scheme for conditional privacy preserving in vehicular ad-hoc network[J]. IEEE Internet of Things Journal, 2022, 9(11): 8078-8090.

[47] WANG Q P, GAO D Y, ZHU W T. Cloud-enabled software-defined vehicular networks: architecture, applications and challenges[J]. Journal of Internet Technology, 2019, 20(6): 1819-1828.

[48] 牛雅丽, 屈光洪. 基于 PaaS 的车联网云平台开发探究[J]. 汽车实用技术, 2020(9): 47-48, 76.
NIU Y L, QU G H. Research on development of vehicle networking cloud platform based on PaaS cloud platform[J]. Automobile Applied Technology, 2020(9): 47-48, 76.

[49] ARAIN Q A, DENG Z L, MEMON I, et al. Map services based on multiple mix-zones with location privacy protection over road network[J]. Wireless Personal Communications, 2017, 97(2): 2617-2632.

[50] 王瑞锦, 唐榆程, 张巍琦, 等. 基于同态加密和区块链技术的车联网隐私保护方案[J]. 网络与信息安全学报, 2020, 6(1): 46-53.
WANG R J, TANG Y C, ZHANG W Q, et al. Privacy protec-

tion scheme for Internet of vehicles based on homomorphic encryption and block chain technology[J]. Chinese Journal of Network and Information Security, 2020, 6(1): 46-53.
[51] 彭长根, 何兴, 谭伟杰, 等. 人工智能算法安全研究现状与对策[J]. 贵州师范大学学报(自然科学版), 2022, 40(6): 1-16, 134.
PENG C G, HE X, TAN W J, et al. Research status and countermeasures of artificial intelligence algorithm security[J]. Journal of Guizhou Normal University (Natural Sciences), 2022, 40(6): 1-16, 134.
[52] ZHU C, CHENG Y, GAN Z, et al. FreeLB: enhanced adversarial training for natural language understanding[J]. arXiv preprint, 2019, arXiv: 1909.11764.
[53] VILONE G, LONGO L. Explainable artificial intelligence: a systematic review[J]. arXiv preprint, 2020, arXiv: 2006.00093.

[作者简介]

陈滢媛（2000– ），女，南京邮电大学博士生，主要研究方向为车联网安全、网络空间安全与密码工程。

董振江（1970– ），男，博士，南京邮电大学教授、博士生导师，国务院政府特殊津贴专家，中国人工智能学会常务理事，主要研究方向为人工智能与车联网。

董建阔（1992– ），男，博士，南京邮电大学讲师，主要研究方向为隐私计算、密码工程、并行计算与物联网。

徐敏杰（1987– ），男，中汽创智科技有限公司高级工程师，主要研究方向为智能网联汽车信息安全。