新形势下车联网网络安全挑战与应对探究

巩金亮，周光涛，阮红阳，王亚东，韩涛
联通智网科技股份有限公司，北京 101599

DOI: 10.61369/TACS.2025100018

摘　　要： 随着信息技术与汽车产业的深度融合，车联网已成为汽车产业转型升级的核心方向，其在提升出行效率、改善驾驶体验的同时，也因多终端互联、多场景交互的特性，面临着日益严峻的网络安全风险。本文从新形势下车联网的发展特征出发，系统梳理车联网在终端设备、通信传输、数据管理以及应用服务等层面存在的网络安全挑战，并从技术防护、管理规范、生态构建三个维度提出针对性的应对策略，为保障车联网产业的安全、健康发展提供理论参考。

关 键 词： 车联网；网络安全；安全挑战；应对策略

Research on Cybersecurity Challenges and Countermeasures of Internet of Vehicles Under the New Situation

Gong Jinliang, Zhou Guangtao, Ruan Hongyang, Wang Yadong, Han Tao
China Unicom Smart Network Technology Co., Ltd., Beijing 101599

Abstract: With the in-depth integration of information technology and the automotive industry, the Internet of Vehicles (IoV) has become the core direction of the transformation and upgrading of the automotive industry. While improving travel efficiency and driving experience, it also faces increasingly severe cybersecurity risks due to the characteristics of multi-terminal interconnection and multi-scenario interaction. Starting from the development characteristics of IoV under the new situation, this paper systematically sorts out the cybersecurity challenges existing in IoV at the levels of terminal equipment, communication transmission, data management and application services. Corresponding countermeasures are proposed from three dimensions: technical protection, management norms and ecological construction, providing theoretical reference for ensuring the safe and healthy development of the IoV industry.

Keywords: internet of vehicles (IoV); cybersecurity; security challenges; countermeasures; industrial ecology

随着互联网、智能化技术的发展，汽车已成为“交通工具”的升级版，即所谓的“移动智能终端”，车联网作为“终端”的体现成为这一升级的关键[1]。它实现了车与车、车与路侧设备、车与云、车与用户的全面连接。与互联网相比，车联网具有异构终端、通信实时性、场景相关性以及后果严重的安全特点。互联网常见的安全威胁仅仅造成数据泄露或者服务不响应，但对于车联网来讲，严重的安全风险会导致人身财产安全的威胁，可能导致人车数据交换发生错误而带来严重的后果，例如大量的交通堵塞等。因此，系统分析车联网的网络安全威胁，提出切实可行的防范措施，对于促进车联网安全发展，保障社会公共利益等方面意义重大。

一、新形势下车联网的发展特征

车联网的技术架构从传统分布式架构向“云－边－端”一体化架构扩展，传统车联网以车辆的控制及数据处理依赖车载终端的算力支持，和外界交互不频繁[2]。“云－边－端”一体化架构通过基于车辆的“端”，边缘节点的“边”以及云端平台的“云”所构建的智能控制计算与处理一体化平台，车载终端起到数据采集和实时控制的作用，边缘节点完成附近数据的处理和短时响应需求，云端平台则完成数据分析、信息存储、云端决策等功能，大大提高了车联网的计算与服务效率；但也因此导致车联网的网络边界不确定性增强，安全防护相对困难。

应用层面上，车联网的应用场景由单一导航、娱乐等基本应用，向自动驾驶、智能交通管理、车路协同等复杂应用场景拓展。自动驾驶作为车联网关键场景，必须实时获取自身周边的环境数据、交通信号数据以及其他车辆的行驶数据，实现高精度的计算决策和控制。智能交通管理必须依赖车联网实现交通流量监测调度与优化，实现路网通达能力提升[3]。

在产业生态层面，车联网已发展形成汽车制造企业、信息技术企业、通信运营业务企业、零部件提供商等多个主体多方参与的复杂生态。汽车制造企业开展车辆生产制造、信息技术企业提供人工智能、大数据等技术支撑、通信运营业务企业提供车联网通信网络支持、零部件提供企业供应车载芯片、传感器等关键部

件。多元主体协同开展车联网活动，但不同主体间的技术标准不规范、数据开放共享体系不健全、安全责任不清等问题，又为车联网网络安全风险的传导和扩散提供了方便渠道[4]。

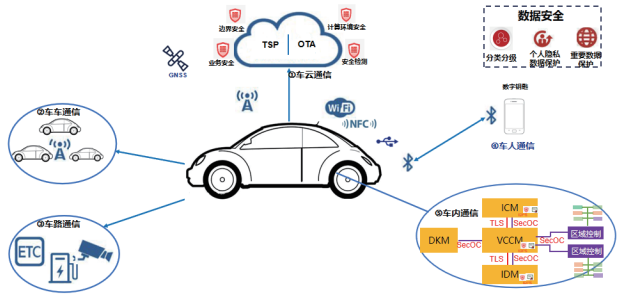


图1：智能网联汽车结构示意图

二、近年车路云与车联网漏洞信息总结

车路云一体化与车联网快速发展的同时，安全漏洞风险持续攀升，核心隐患集中分布在车载终端、路侧单元及云端平台三大关键环节，远程攻击已成为主流威胁形式。

车载终端漏洞主要表现为功能模块缺陷，其中车载信息娱乐系统是漏洞高发区域。常见漏洞类型包括命令注入、“释放后重用”以及数值检查缺陷等，部分高危漏洞可实现对终端的“零交互”远程控制，对车辆行驶安全构成直接威胁。

路侧单元因普遍存在部署分散、无人值守的特点，安全风险尤为突出。弱口令、固件后门等问题较为常见，攻击者可借此入侵系统，不仅可能导致交通信号等基础设施异常，还可通过伪造路况信息引发安全事故，暴露供应链及固件安全管理短板。

云端平台的漏洞主要源于配置管理疏漏，易引发大规模数据泄露事件。此外，云端系统也成为勒索软件攻击的重点目标，攻击者通过加密系统等方式实施勒索，同时数据存储与传输过程中的防护不足，进一步加剧了信息安全风险。

三、新形势下车联网面临的网络安全挑战

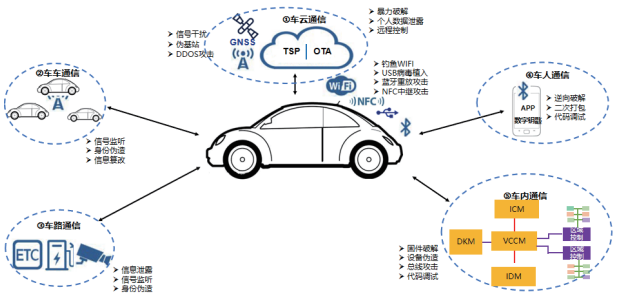


图2：车联网安全风险示意图

（一）终端设备层面：异构终端漏洞凸显，防护能力参差不齐

车联网数据采集与控制的实施载体是车载终端设备，车联网的安全性最终由车载终端的安全水平决定[5]。车联网新技术背景下车载终端设备呈现明显的异构特征，除了传统的车载信息娱乐设备、发动机控制器外，还增加了大量的智能终端设备，包括激光雷达、毫米波雷达、摄像头、自动驾驶控制器等。智能终端设备的种类繁多，由多家供应商提供，存在不同的硬件和操作系统架构，面临各类安全问题。另外终端设备在设计时追求功能实现而忽视安全性设计，如出现缓冲区溢出漏洞、权限管理不足、固件升级漏洞等问题，攻击者可以通过远程或者与主机直接接触方式对终端进行攻击，从而获取车辆的控制权，对汽车的转向、制动等核心部件进行控制。另一方面，终端设备的安全防护参差不齐，传统的车载终端硬件能力有限，使得传统车载终端很难安装复杂的安全防护软件，新添加的智能终端在安全保障方面有所提高，但毕竟技术迭代的速度极快，漏洞也会随之增加。

（二）数据管理层面：数据体量庞大且敏感，全生命周期安全存在隐患

在车联网运行过程中将产生大体量数据，包括车辆自身运行状态数据、驾乘人员个人信息数据、道路环境数据、交通流量数据等，不仅数据体量庞大，而且包含诸多敏感信息，涉及大数据生命周期诸环节的安全威胁。一些车联网设备在进行数据采集时具有采集范围大、未征得用户同意就采集了个人信息等特点，使用户隐私信息泄露的危险性进一步提升。数据传输。数据在传输链路中通过不安全的传输通道被窃听、篡改、丢失的概率增大，因此数据的安全性受到威胁，数据的保密性受到损害。数据存储。云端平台和边缘节点存储了车联网中大量的数据，一旦存储系统存在漏洞将会造成大数据泄露。由于车联网中各个主体之间的数据共享机制不健全，在数据进行共享时也缺少有效的安全管控措施，从而造成数据泄露和窃取等。

（三）应用服务层面：场景复杂导致风险传导，安全责任界定模糊

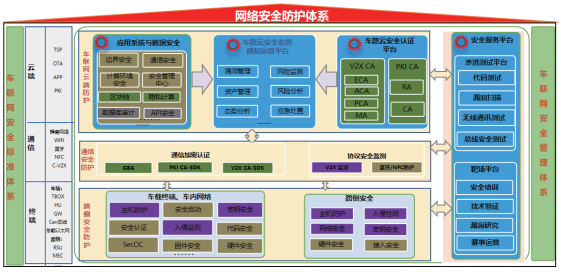
应用服务是车联网应用场景范围扩展之后的风险面的延伸与延续。车联网应用服务场景覆盖了车辆控制、交通管控、娱乐社交等多个领域，在不同应用层之间存在相互数据流动和业务关联等复杂情况，各类安全风险会在不同车联网服务场景之间实现“多米诺”式影响。例如通过车载信息娱乐系统存在的安全漏洞，攻击者入侵车辆信息娱乐系统后通过信息娱乐系统与其他车载系统的接口进入车辆自动驾驶系统，由此造成自动驾驶事故等安全问题；智能交通管理平台的安全漏洞可造成管理平台与路网中交通信号的数据被篡改，从而影响路网整体交通秩序，甚至造成大范围交通拥堵或事故等[6]。

（四）人工智能应用层面：技术赋能下的新型安全风险凸显

人工智能在车联网自动驾驶决策、智能调度等场景的深度应用，既提升了系统智能化水平，也带来了独特安全挑战。自动驾驶依赖的 AI 模型易受对抗性样本攻击，攻击者通过篡改路况图像、干扰传感器数据等方式，可误导模型做出错误决策，如将停止标识识别为通行信号。同时，AI 训练数据可能存在偏见或污染，导致模型决策偏差，引发行驶安全隐患；模型部署后的 “黑箱” 特性，又使得安全故障溯源和责任认定难度加大。此外，AI 算法的快速迭代与车联网硬件适配不同步，部分老旧终端难以支撑安全防护型 AI 应用，进一步放大了安全风险。

四、新形势下车联网网络安全的应对策略

（一）技术层面：构建四轮驱动的安全技术体系



首先，从终端设备方面加强车载终端的安全设计，实现车联网终端设备安全的全生命周期应用，在开发设计阶段，应用安全的硬件架构和操作系统，对安全漏洞进行检测和漏洞渗透测试，从根源降低安全漏洞数量[7]；在制造阶段，落实产品安全准入制度，对终端产品进行安全加锁和身份认证；在运用阶段，形成健全的固件更新机制，及时补修终端设备安全漏洞。其次，研发车载终端设备的安全防御软件，增强车联网终端设备自我防护能力。

通信传输方面，需要考虑提升通信协议安全性，提升各类通信场景下的通信安全。对于车载总线通信，部署身份鉴权和数据加密的方式防范攻击者修改总线数据的行为；对于无线通信部署加密传输、动态身份鉴权等安全控制方式防范身份冒充、数据窃听等攻击行为。进一步研发低时延的安全防护技术，实现低时延与通信实时性提升的双赢，同时提升通信网络实时监测能力，及早防范异常通信事件[8]。

数据管理方面，构建车联网数据全生命周期数据安全管理机制。在数据采集环节，界定数据采集范围，经过用户授权，防止恶意数据过度采集；在数据传输环节，进行传输加密，在数据传输环节保证数据的完整性与机密性；在数据存储环节，数据安全存储，进行存储系统的访问权限控制及安全防护，定期进行备份数据的恢复演练；在数据使用环节，进行数据使用权限管理，防止数据被使用及泄露。

云端平台层面：构建车联网安全运营平台和车联网安全认证平台。对整车进行全生命周期的网络安全风险监测预警，及时发现网络中存在的安全风险和问题。基于身份认证技术实现车联网各要素之间实现的身份识别，建立安全通信信道。

（二）生态层面：推动多主体协同与构建信任体系

保障车联网网络安全，需充分发挥车联网产业生态圈各主体优势，推动多主体协同合作，形成车联网网络安全防护合力。建立车联网产业安全协同机制，由政府牵头，携手汽车企业、信息企业、通信企业、科研院所等主体联合搭建建设车联网安全靶场，实现安全信息共享平台，实现安全漏洞、安全事件等安全信息的实时共享，开展联合技术研发工作，共同破解车联网安全防护关键技术难关，提升车联网产业安全技术水平[9]。

车联网产业信任体系建设是推动各参与主体实现协同合作的重要保障，应当建立国家级的统一的身份认证体系，为车联网各主体设备、用户、企业等进行统一身份认证，确保各主体身份的真实与合法；应当建立信用评价体系，评价车联网各主体安全防护能力、信用记录等，并公示评价结果，引导各主体重视安全防护工作；应当推动建立数据共享安全机制，在数据保障数据安全的情况下，规范数据的共享流程与共享方式，促进数据资源的开发与利用，提高车联网服务质量与服务水平。

（三）管理层面：完善制度规范与强化执行力度

完善的规范是车联网网络安全的重要保障，需要加快建立健全车联网网络安全相关的法律法规标准体系。建议由政府牵头制定车联网网络安全专门法律法规，将车联网网络安全中涉及主体的安全责任、义务和违法处罚标准规定明确，为车联网网络安全提供必要的保障。

在完善制度规范的基础上，加强制度执行。企业作为车联网网络安全的直接责任主体，完善企业内部安全管理制度体系，明确企业内部安全管理机构及人员的权责，定期组织网络安全风险评估、漏洞扫描和安全培训，对检查发现的安全漏洞及时进行整改。政府有关部门组织对企业的安全工作监督检查，对未落实安全制度规范的企业要严肃处罚，督促企业履行安全主体责任[10]。

五、结论

车联网作为融合汽车和信息两个行业新技术的新兴产业，在促进智能出行发展的同时，也面临着终端漏洞、通信传输威胁、数据隐私安全以及应用服务威胁等方面的风险。车联网网络安全风险问题产生的原因包括技术演进与安全保障脱节、法规标准缺失与落实不到位以及产业生态协同不足与信任体系缺失等。研究车联网网络安全防护、落实车联网风险防控、促进车联网安全发展是新时代的必要需求。随着时间推移，车联网技术不断发展，车联网产业生态不断优化和拓展，车联网网络安全风险在不断变化，加强车联网网络安全研究、健全车联网网络安全防护策略仍是必然趋势。

参考文献

[1] 万紫骞，刘凯，黄灶星. 智能网联汽车攻击面分析与安全防护策略 [J]. 电子质量，2024,(09):68-73.
[2] 徐国进. 面向车联网安全通信的异常检测算法研究 [D]. 杭州电子科技大学，2025.
[3] 涂江健. 基于集成学习的车联网入侵检测算法研究 [D]. 广州大学，2025.
[4] 胡斌，王文卓. 车联网技术的安全风险与立法完善 [J]. 保密科学技术，2025,(04):56-59.
[5] 王运付，刘霞，姜元山，等. 基于5G的工业物联网网络安全威胁识别及消减建议 [J]. 物联网技术，2024,15(08):51-54.
[6] 刘灵，朱厚友，张艺舰. 基于车联网技术的智能网联汽车网络安全研究 [J]. 农机使用与维修，2024,(04):87-90.
[7] 吴昊，董琛，刘晓曼. 车联网环境下车辆网络安全检测技术研究 [J]. 保密科学技术，2023,(03):56-62.
[8] 徐享希，李炯彬，郭志远. 车联网网络安全挑战与评估技术分析 [J]. 质量与认证，2024,(02):83-86+91.
[9] 秦博阳，刘晓曼. 车联网数据安全进展与未来展望 [J]. 保密科学技术，2025,(01):51-54.
[10] 胡月. 信息安全风险管理在网络安全保险中的应用研究 [J]. 网络安全技术与应用，2024,(12):138-140.

