工程与管理科学
Engineering and Management Science
第 8 卷◆第 2 期◆版本 1.0◆2026 年
文章类型：论文|刊号（ISSN）：2705-0637(P) / 2705-0645(O)

# 车联网通信安全风险分析及隐私保护技术探讨

彭盛晟
广西诺远科技有限公司　530022

DOI：10.32629/ems.v8i2.18514

［摘　要］车联网作为数字经济与交通产业融合的核心载体，其通信开放性与数据密集性特征导致安全隐私风险凸显。通信链路、终端设备、平台系统、数据流转四大维度的安全隐患，不仅威胁车辆行驶安全与用户隐私权益，还制约产业规模化发展。针对上述风险，差分隐私与数据脱敏、混合加密与量子密钥分发、可信执行环境（TEE）、联邦学习等隐私保护技术，从数据源头、传输过程、计算环节、共享场景构建全生命周期防护体系。这些技术通过“安全隔离、加密传输、隐私计算”等核心逻辑，在保障车联网业务连续性的同时，筑牢通信安全与隐私保护防线，为产业高质量发展提供技术支撑。

［关键词］车联网；通信安全；风险分析；隐私保护技术

## 引言

随着人工智能、5G 等技术的深度渗透，车联网已成为衔接制造强国、交通强国建设的关键纽带，推动出行方式与产业格局深刻变革。但车联网多主体协同、多链路通信、多维度数据流转的特性，使其面临复杂的安全隐私挑战：通信链路易遭窃听篡改，终端设备存在漏洞风险，平台系统面临集中式攻击，数据共享过程中隐私泄露隐患突出。这些问题不仅可能引发车辆失控、交通混乱等安全事故，还会侵犯用户信息权益，阻碍产业规模化落地。在此背景下，探讨车联网通信安全风险特征，分析适配产业场景的隐私保护技术路径，对破解产业发展瓶颈、保障公共安全与用户权益具有重要现实意义。

## 一、车联网产业在社会经济中的重要地位

车联网产业作为数字经济与实体经济深度融合的核心载体，在社会经济中占据战略支撑地位。它不仅是全球汽车产业转型升级的关键方向，更成为经济高质量发展的新增长引擎，推动产品形态、产业格局与出行方式发生深刻变革。通过融合人工智能、5G、大数据等前沿技术，车联网构建起涵盖芯片、传感器、网联云控的完整产业体系，带动汽车、电子、通信、新材料等跨行业协同升级，催生万亿级市场规模，预计 2030 年我国“车路云一体化”相关市场规模将超 14 万亿元。作为培育新质生产力的重要力量，车联网加速新技术商业化落地，优化交通调度效率、降低能源消耗与物流成本，同时催生共享出行、无人配送、智能环卫等新业态，拉动消费升级与就业增长。其“车路云一体化”发展路径还推动交通基础设施智能化改造，为智慧城市建设提供重要支撑，强化我国制造业全球竞争力。从政策引领到市场落地，车联网已成为衔接制造强国、网络强国与交通强国建设的关键纽带，为经济可持续增长注入持久动力。

## 二、车联网通信安全风险分析

### （一）通信链路安全风险：开放性导致的多维度攻击暴露

车联网通信依赖蜂窝通信与直连通信链路，其开放性特征成为安全漏洞的核心诱因。蜂窝通信场景下，攻击者可部署伪基站，通过强信号诱导车载终端接入，实现信令窃听、数据篡改或重放攻击，窃取车辆标识、位置等敏感信息，甚至中断网络连接。直连通信场景中，PC5 接口的广播特性让攻击者能假冒合法终端身份，恶意发布虚假路况、交通信号等信息，或篡改合法用户的业务数据，直接干扰车辆驾驶决策。通信协议的安全缺陷进一步放大风险，传统车载网络协议缺乏完善的加密与身份认证机制，仅依赖简单校验手段，难以抵御中间人攻击。在网络覆盖薄弱区域，攻击者可利用链路传输延迟，发起时序攻击，破坏数据新鲜性。这类攻击不仅导致单个车辆失控，还可能通过链路扩散形成区域性交通混乱，将网络空间风险传导至物理交通场景，威胁公共安全。

### （二）终端设备安全风险：接入节点的全生命周期漏洞

车载终端与路侧设备作为车联网的核心接入节点，面临全生命周期的安全隐患。车载终端集成物理接口与无线连接接口，在生产、维修等环节，攻击者可通过暴露的调试端口植入恶意硬件或程序，逆向分析固件获取系统架构，利用权限滥用风险实施后台监听、GPS 跟踪等恶意行为。终端系统

漏洞未及时修复、不安全升级等问题，还可能让攻击者通过漏洞提权，关闭安全功能或发起拒绝服务攻击。路侧设备的安全风险同样突出，其通过有线接口与交通基础设施、云平台交互，若缺乏有效防护，易遭非法接入与控制。攻击者可篡改路侧设备的感知数据,发布错误的地图定位或交通指示，导致覆盖区域内交通秩序混乱。同时，路侧设备的部署环境复杂，自然损耗或人为破坏可能暴露通信接口，降低物理防御能力，为远程入侵提供可乘之机，形成“单点突破、全网蔓延”的风险传导链。

（三）平台系统安全风险：中枢节点的集中式攻击威胁

车联网云平台与 OTA 升级平台作为数据交互与控制中枢，已成为网络攻击的重点目标。云平台面临 Web 漏洞、数据库注入、DDoS 攻击等传统风险，攻击者可利用 API 接口安全缺陷，非法获取 AccessKey，篡改升级包或推送恶意程序，实现对车辆的批量远程控制。OTA 升级流程中，云端、通信链路、车端任一环节防护不足，都可能导致升级包被篡改，植入后门程序，引发车辆控制系统失效。平台的多租户架构与第三方应用生态进一步增加风险复杂度。多租户隔离机制薄弱可能导致不同用户数据交叉污染，第三方应用的不安全升级或恶意 SDK 植入，会造成用户隐私数据泄露。这类集中式攻击的危害具有规模化特征，一旦平台被入侵，可能引发大批量车辆失控、海量敏感数据泄露等严重后果，造成巨额经济损失与社会影响[1]。

（四）数据流转安全风险：全生命周期的机密性与完整性威胁

车联网数据在采集、传输、存储、使用的全生命周期中，面临泄露、篡改与滥用的多重风险。数据采集阶段，车载传感器可能过度收集车内对话、周边环境等隐私信息，第三方应用通过权限滥用将数据传输至非授权平台；传输过程中，弱加密或明文传输让攻击者可截获车辆控制指令、用户轨迹等核心数据，通过侧信道攻击推断敏感信息。存储与使用环节的风险同样严峻，云平台数据库若遭受 SQL 注入攻击，或数据脱敏不足，会导致原始数据泄露；攻击者还可篡改车辆健康监测、保险理赔等数据，引发欺诈行为或影响故障诊断准确性。数据跨境传输未符合合规要求、企业数据治理缺失等问题，还可能引发法律风险。而且更为严重的是，车辆控制数据被篡改可能直接导致制动、转向系统异常，将数据安全风险升级为致命的行车安全事故。

## 三、车联网通信隐私保护技术

（一）差分隐私与数据脱敏技术：源头阻断隐私泄露路径

差分隐私与数据脱敏技术聚焦数据采集源头，通过“干扰模糊”与“信息剥离”双重机制，在保障数据可用性的前提下阻断隐私泄露风险。差分隐私保护强度由隐私预算 ε 量化：

公式 1：差分隐私保护强度

$$P\_privacy=-\log(\varepsilon)+C$$

（其中，P_privacy 为保护强度，ε 为隐私预算，C 为技术常数）

ε 值越小保护力度越强，但需平衡模型精度损失。在车联网交通流统计等场景中，ε =1 时可实现 82.3%的模型精度，同时有效屏蔽用户轨迹关联风险[2]。

数据脱敏技术则针对车联网时空关联性强的特点，采用动态脱敏策略：对车辆标识、位置坐标等核心隐私字段，通过替换、截断、加密等方式剥离身份关联属性；对驾驶行为、传感器数据等，通过泛化处理将具体数值转化为区间范围，既保留数据统计价值，又防止逆向推理。该技术可在车载终端本地轻量级部署，针对不同数据类型动态调整脱敏规则，例如对实时控制指令采用加密脱敏，对历史路况数据采用泛化脱敏，确保全场景下的隐私保护与数据效能平衡。两类技术的融合应用，能有效应对过度采集、匿名化失效等问题，为数据全生命周期保护奠定基础。

（二）混合加密与量子密钥分发技术：筑牢通信传输安全防线

混合加密与量子密钥分发技术针对车联网多链路通信特性，构建“经典加密+量子安全”的双层防护体系，保障数据传输的机密性与抗攻击性。混合加密机制结合对称加密的高效性与非对称加密的安全性，在车与云、车与车、车与路侧设备通信中广泛应用：通过 ECC 等非对称算法安全协商临时对称密钥，再利用 AES-256 等对称算法对海量传输数据进行加密，配合 TLS1.2/1.3 协议构建端到端加密通道，确保位置信息、控制指令等敏感数据即使被截获也无法解读。

量子密钥分发技术则依托量子力学“不确定性原理”与“不可克隆定理”，提供无条件安全的密钥共享方案，抵御量

子计算对传统加密算法的破解威胁。针对车联网高移动性、信道复杂的场景，QKD 技术通过协议轻量化、抗多普勒频移优化，实现密钥分发时延≤50ms、生成率≥1Mbps 的性能指标，满足 V2X 实时通信需求。结合密钥管理系统的动态轮换与审计功能，可实现密钥全生命周期安全管控，配合边缘计算节点的就近加密转发，在降低传输延迟的同时，形成“密钥安全+传输加密+链路防护”的全链条通信安全保障[3]。

（三）可信执行环境与安全飞地技术：硬件级隔离敏感计算

可信执行环境与安全飞地技术通过硬件级隔离构建隐私计算“安全特区”，确保敏感数据处理与核心操作不被恶意篡改或窃取。TEE 依托 IntelSGX、ARM TrustZone 等专用硬件模块，在车载处理器中划分独立的隔离空间，通过内存加密、指令流混淆等技术，实现代码与数据的机密性保护 —— 即使车载主系统（REE）被入侵，隔离空间内的敏感信息仍无法被访问。

AutoCrypt IVS-TEE 等车载专用方案已实现对 ADAS、车载娱乐系统的全覆盖，仅允许执行经验证的可信应用（TA），保障 OTA 升级包校验、密钥存储等核心操作的安全性。安全飞地则针对车载终端资源受限特点，采用轻量级虚拟化方案划分独立计算单元,在 200KB 内存占用下即可实现隐私计算功能。两者通过“双因子认证”协同工作：TEE 提供硬件安全模块（HSM）级别的根信任，安全飞地负责动态资源分配与轻量级加密计算，使车载终端在降低 37%功耗的同时，保持 95%以上的隐私保护强度。该技术组合可有效防护侧信道攻击、权限滥用等风险，将攻击面缩小至 0.03%，既满足 ISO/SAE 21434 汽车安全标准，又为驾驶行为分析、生物特征验证等敏感场景提供安全计算底座[4]。

（四）联邦学习与隐私计算融合技术：破解数据共享隐私困境

联邦学习与隐私计算融合技术通过“数据可用不可见”的核心逻辑，破解车联网数据共享与隐私保护的矛盾。联邦学习采用分布式训练架构，车辆本地数据无需上传至云端，仅将训练后的模型参数加密传输至聚合节点，由云平台或边缘服务器完成全局模型更新，从根本上避免原始数据泄露。在自动驾驶环境感知等精度敏感场景中，联邦学习可将模型精度损失控制在 5%以内，10 节点协同训练时仍能保持 28FPS 的实时性，远超同态加密等技术的性能表现。

为强化防护效果，该技术常与同态加密、群签名等技术融合：采用改进的 CKKS 同态加密算法对模型梯度进行加密处理，支持密文直接计算，确保参数传输过程中不泄露敏感信息；结合 BLS 动态短群签名技术，实现车辆身份匿名化与行为可追溯，既能防止恶意节点注入虚假参数，又能在争议发生时定位责任主体。针对车联网节点动态性强的特点，通过边缘服务器协同与强化学习优化参数权重分配，可降低 30-50%的通信开销，支持部分车辆掉线时的模型稳定更新。这种融合方案既打破了“数据孤岛”，又构建了“分布式训练+加密传输+可追溯验证”的全流程隐私保护体系，成为车联网多主体数据协同的核心技术支撑[5]。

## 结语

综上所述，车联网通信安全与隐私保护是技术创新与风险防控的动态平衡过程，其核心在于实现“安全可控”与“业务赋能”的协同推进。通信链路、终端、平台、数据层面的风险相互交织，决定了隐私保护需采用多技术融合的全链条防护思路。差分隐私、混合加密、TEE、联邦学习等技术的应用，为风险防控提供了有效解决方案，但技术落地仍需适配车联网高移动性、低时延等场景需求。未来，随着技术迭代与标准完善，隐私保护技术将向“轻量化、智能化、协同化”方向发展，通过技术创新与产业实践深度融合，持续筑牢车联网安全隐私屏障，为产业可持续发展注入持久动力。

## [参考文献]

[1]林美玉.5G 网络赋能物联网安全[J].中兴通讯技术，2022（10）：1－7.

[2]张富琴. 5G 网络在物联网中的应用研究[J]. 产业创新研究，2022（18）：61－63.

[3]包力泰. 5G 通信技术背景下物联网应用发展[J]. 中国传媒科技，2022（8）：92－94.

[4]谢广耀. 5G 通信技术与物联网的融合与发展[J]. 网络安全和信息化，2022（8）：4－6.

[5]李湛.车联网网络安全存在的问题及防范策略[J].网络安全技术与应用，2020（2）：1-2.