车载电子通信安全问题研究

陈树华
浙江零跑科技股份有限公司　浙江　杭州　310000

摘　要：在汽车产业智能化、网联化迅猛发展态势下，车载电子通信系统虽为驾驶体验带来质的飞跃，却也深陷复杂的安全困境。本文旨在分析车载电子通信的系统架构、应用及其发展；系统剖析车载通信所面临的安全威胁因素，并提出多项全方位构筑防护体系的防护措施，期以构建坚实的车载电子通信安全屏障，引领智能交通的稳健发展，提供深入的理论支撑。

关键词：车载电子通信；安全威胁；防护策略；技术革新；产业协同

引言

当前，汽车产业正逐步从传统的出行载具，向集先进电子技术、通信网络于一体的智能移动终端蜕变。车载电子通信系统作为这一转型进程中的核心支柱，整合了信息交互、导航、车辆监控等功能，极大地重塑了驾驶体验。然而，随着其深度应用，安全隐患也如影随形。若车载通信系统被攻破，可能导致车辆失控、隐私信息泄露，威胁车主生命财产安全，更甚影响交通和社会稳定。因此，深入研究车载通信安全问题，对促进汽车产业智能化和保障公众安全至关重要。

1 车载电子通信面临的安全威胁

1.1 网络攻击类型

（1）黑客入侵。黑客利用恶意软件或漏洞，试图非法访问车辆电子通信系统，窃取敏感数据或操控车辆运行。黑客入侵不仅可能导致车辆被盗或被远程控制，还可能造成严重的交通事故，对公共安全构成重大威胁。此类攻击往往具有隐蔽性强、危害性大的特点，是车载电子通信面临的主要安全挑战之一。某国际汽车制造商的车载信息娱乐系统便曾由于设计时忽略输入验证，被黑客远程植入恶意代码，操控车辆行驶和制动系统，引发了极大安全风险和经济损失。（2）恶意软件感染。恶意软件通常伪装成合法的软件更新包，巧妙地绕过车载系统的初级安全检测防线，或深度潜伏于车载娱乐多媒体文件中，利用用户的播放、下载操作触发入侵机制。[1]一旦激活，它们将疯狂篡改车辆核心控制单元（ECU）中的关键数据，例如恶意修改车速传感器脉冲信号频率，导致仪表盘车速显示严重失真，误导驾驶者做出错误的操作判断；同时，通过后台隐秘线程，大量窃取车主通讯、行车轨迹、车内摄像头影像等隐私敏感信息，给车主带来骚扰和诈骗风险，破坏个人隐私。（3）拒绝服务攻击、在车联网核心服务器遭遇分布式拒绝服务（DDoS）攻击的情况下，大量伪造的请求数据包从全球范围内的僵尸网络节点迅速涌来，导致服务器的处理带宽与计算资源被迅速耗尽。这使得车辆与服务器之间的双向通信链路受到严重干扰，实时交通状况信息的更新陷入停滞，驾驶者无法根据精确的路况信息调整行驶路线，从而陷入交通拥堵的困境；同时，远程控制功能完全失效，导致在车辆被盗抢等紧急情况下，车主无法远程执行锁定车辆、启动警报、定位追踪等应急措施，进一步增加了车主的财产损失和安全风险。

1.2 信息泄露风险

（1）用户隐私数据泄露。当前车载应用程序开发中，众多开发团队在追求功能的多样性和用户体验的优化时，信息安全防护架构的设计往往存在显著的缺陷。部分应用程序由于代码漏洞和加密算法的脆弱性，导致车主在登录后其位置信息容易被截获，通过数据收集分析描绘出车主日常出行模式，进而推测泄露包括家庭住址在内的敏感信息。此外，驾驶习惯数据亦可能被商业机构非法获取，构建用户画像并用于定制针对性广告。更有甚者，诈骗分子利用这些信息冒充官方机构，诱骗车主财产，从而造成经济损失。（2）车辆运行数据泄露。车辆内置的传感器网络持续地收集包括车速、加速度、制动频率、发动机转速等在内的多种运行数据。这些数据通过车载通信模块进行传输，若存在加密不足或防护措施不充分，将极易导致数据泄露。不法分子获取数据后，可通过大数据和机器学习分析车主行车模式，选择车辆闲置时以盗窃车内贵重物品。对于物流车、出租车等运营车辆，泄露的载重、路线、载客频次等数据可能被对手利用，进行恶意抢夺客源、优化配送路线以抢占市场份额，从而扰乱商业运营，对企业造成经济损失。

1.3 通信干扰因素

通信干扰主要集中表现在电磁干扰和信号遮挡衰减

两方面。电磁干扰是车辆进入在强电磁场源附近的路段时，车载电子通信系统可能遭受高强度的电磁辐射。当电磁场强度超过车载设备的耐受阈值时，便可能会引起通信信号波形畸变、误码率上升。这可能导致仪表盘指针出现无序跳动，车载导航界面出现闪烁，坐标定位出现偏差等现象，使得驾驶者难以准确获取车辆状态与导航指引，增加了判断失误的风险，导致交通事故风险上升，从而对出行安全构成挑战。信号遮挡与衰减表现在车辆在山区、峡谷或城市中行驶时，卫星信号因山体和建筑物遮挡而显著衰减。同时，车载通信设备发出的信号也会因周边环境阻挡而产生多径效应，导致信号质量下降。这使得智能导航系统定位不准确，紧急救援呼叫受限，驾驶者在车辆故障或事故时可能无法及时获得救援，影响生命安全。

2 车载电子通信安全防护措施

2.1 应用加密技术

（1）数据加密算法。在车载通信安全防护体系中，高级加密标准（AES）与非对称加密算法（RSA）共同构筑了坚固的双层防御机制。在关键车辆控制指令的传输过程中，AES算法遵循对称加密原则，以其高效的加密速度，将加速、制动、转向等指令迅速转换为密文。即便黑客通过网络监听截获了传输的数据包，面对复杂的分组加密变换和密钥扩展机制，也难以在有限的时间内破解并还原，从而确保了车辆行驶控制权始终牢牢掌握在驾驶员手中，有效避免了远程操控的风险。对于车主的个人身份信息、通讯录、支付信息等敏感数据，RSA算法基于公钥基础设施（PKI），通过公钥加密和私钥解密的非对称加密机制，为数据传输的保密性提供了双重保障。[2]公钥的广泛分发与私钥的唯一持有，确保了只有授权的接收方能够解密数据，从而全面保护了车主的信息安全。（2）密钥管理系统。车联网生态系统涉及车企、零部件供应商、第三方软件开发商、车主等多元主体，层级复杂，因而分级密钥管理体系应运而生。车企作为根密钥掌控者，基于密码学密钥生成算法，依据车辆生产制造、售后维修、日常使用等不同阶段需求，生成并分发相应层级密钥。在密钥更新环节，借助安全增强型移动宽带（eMBB）5G网络切片技术，开辟专用加密信道，推送新密钥，同时确保旧密钥同步失效，全程采用加密信封、数字签名等防护手段，杜绝密钥泄露风险，保障车载通信加密体系稳健、持续运行，为信息交互筑牢安全根基。

2.2 身份认证机制

一方面，采用车辆与网络身份认证机制。数字证书是车辆合法入网的“电子身份证”，每辆车出厂时，车企基于车辆识别码（VIN）、车型、生产批次等关键信息，为其颁发唯一数字证书，并经权威第三方认证机构数字签名认证。车辆入网时，车联网服务器依据证书链验证逻辑，严格核查证书真伪、有效期及证书吊销状态，确保只有合法车辆方能接入网络，获取各类服务。进而有效阻断非法车辆伪装接入，防范恶意篡改、窃取网络中车辆间交互信息，净化车载通信网络环境，维护通信秩序。另一方面，进行用户身份验证。在传统密码登录基础上，有机融合短信验证码、指纹识别、面部识别等生物特征识别技术。车主启动车辆远程控制功能时，先输入预设密码，系统随即通过短信网关向预留手机发送一次性验证码，车主输入验证码后，若终端设备支持生物识别功能，还需进行指纹或面部识别二次确认。通过多重验证环节层层嵌套、相互校验，即便黑客通过网络攻击窃取密码，亦难以突破后续动态验证码、生物特征识别关卡，进而确保车辆控制权不旁落，切实捍卫车主权益，降低账户被盗用风险。

2.3 入侵检测与防御系统

（1）实时监测异常流量。车载入侵检测系统（IDS）基于深度包检测（DPI）技术与流量特征分析算法，对车载网络流量进行全方位监控。系统内置庞大的攻击特征数据库，包含已识别的黑客攻击模式与恶意软件通信指纹，实时进行车辆与外界通信流量特征的比对分析。一旦检测到流量出现异常波动，例如短时间内向未知IP地址大量发送数据，或接收来自高风险域名、恶意软件常用C&C服务器的数据，系统将立即激活预警机制，并通过车载显示屏、手机APP推送等多种途径，向车主及车企安全运维人员发出警报，为迅速响应和处理争取宝贵时间，将潜在损失遏制在初始阶段。（2）自动防御响应。当IDS准确判断入侵行为确实发生时，车载防御系统迅速激活自动反击机制。一方面，立即中断可疑连接，依据防火墙策略，禁止可疑IP地址和端口的数据包传输，以防止黑客进一步渗透攻击；另一方面，采用网络隔离技术，将受感染区域如车载娱乐系统、车载Wi-Fi模块等与车辆核心控制系统（如发动机控制单元、制动系统）迅速隔离，防止“病毒”扩散至关键部位，确保车辆基本运行安全，最大限度降低入侵危害，保障驾乘人员的生命财产安全。

2.4 安全通信协议

（1）现行协议。控制器局域网（CAN）协议通过仲裁机制和差分信号技术，支持关键系统如发动机控制的数据交换，而本地互联网络（LIN）协议适用于车身辅助

设备通信，如车窗升降、座椅调节、雨刮器控制等[3]。二者基本确保了车内各电子控制单元（ECU）之间的高效协同工作，实现了实时且可靠的通信。然而，两者虽都注重实时性和成本效益，但安全性的考虑相对不足，导致通信数据多以未加密的形式传输，容易受到安全威胁，为车载电子通信系统带来潜在安全隐患，威胁车辆运行安全。（2）新兴协议。基于区块链的车联网通信协议正在兴起，有望重塑车载通信的安全性。该协议采用去中心化的分布式账本，建立了一个点对点（P2P）的对等网络，避免了单点故障的风险。利用区块链的特性，数据一旦记录就不可篡改，使每辆车都成为可信节点，并记录交互历史，确保信息可追溯。同时在车辆传输关键数据时，区块链网络广播能够验证信息真实性，提高通信的可信度和安全性，从而为智能交通系统的信息交互提供安全保障。

3 车载电子通信安全的发展展望

3.1 技术发展趋势

（1）引入量子加密技术。随着量子计算技术的蓬勃发展，传统加密算法所依赖的基于数学难题求解的安全性正面临严峻挑战。量子加密技术利用量子态的奇异特性，例如量子纠缠的超距关联和量子不可克隆定理，实现了无条件的安全通信。在车载领域，量子密钥分发（QKD）技术利用单光子的偏振态、相位等量子特性，确保了密钥传输的绝对安全。使得车辆之间以及车辆与基础设施之间的加密通信更加坚固，为智能交通网络提供了深度加密保护。（2）人工智能与安全的融合。人工智能将成为车载电子通信安全的智能“守护者”。通过深度学习算法，AI系统能够实时分析海量的车载网络数据，构建复杂的威胁识别模型，精准地识别潜在的安全威胁。[4]它能够从正常的通信流量中敏锐地捕捉到细微的异常，并运用异常检测、行为分析等技术预测未知的攻击模式，提前进行防御；还能根据车辆的实时状态和周边环境，智能地优化安全策略，例如在电磁干扰高发区，自动强化信号加密与纠错能力，动态提升车载通信应对复杂环境的安全韧性，以智能化手段为车载电子通信安全赋能。

3.2 法规与标准的完善

法规与标准构成了车载电子通信安全的坚实基础。当前，频繁发生的与安全相关的事件深刻揭示了立法的不足和标准的缺失。迫切需要通过立法明确汽车制造商、软件开发企业、通信运营商等各方的安全责任，建立严格的产品安全准入制度。发生安全事故时依法进行严厉的惩处，形成强大的威慑力。此外，统一车载电子通信安全标准，全面覆盖硬件安全设计规范、软件加密强度要求、网络防护能力指标等多个维度，使消费者在购车和用车时有明确的规范可依，促进行业的规范化发展，进而推动整个产业的健康和有序发展。

3.3 产业协同合作

产业协同合作是解决车载电子通信安全问题的关键手段。汽车制造商、通信服务提供商以及科研机构必须共同构建一个协同发展的生态系统。汽车制造商应将先进的防护技术整合至车辆设计之中；通信服务提供商需对网络基础设施进行优化，并发展多样化的通信技术；科研机构则应致力于研究和创新安全技术。如量子加密技术的实用化和新型入侵检测算法的开发。并建立信息共享平台，使各方能够共享威胁情报，联合攻克技术难题，从而形成协同效应，进而提升车载电子通信安全技术的整体水平。

结束语

车载电子通信安全问题与每位驾驶者及乘客的生命财产安全息息相关，对智能交通产业的发展趋势具有深远影响。回顾过往，频繁发生的安全事故不断向我们发出严峻警告；审视当前，相关实践研究已取得一定进展，车载电子通信安全有所保障。未来随着相关技术进步，要进一步加强产业合作，持续创新，积极应对新挑战，确保汽车智能网联化稳健发展，为社会带来福祉。

参考文献

[1]陈艺晖.车载电子通信系统的安全技术分析[J].电子技术,2021,50(11):38-39.

[2]王敏.一种低成本的安全车载通信实现[J].电子世界,2021,(11):114-117.

[3]范晶晶,刘壮,陈超,等.基于动态密钥的车载以太网安全通信方法[J].江苏大学学报(自然科学版),2024,45(03):302-308.

[4]宁娟桂,董国芳.基于区块链的车载自组网车与基础设施快速切换认证方案[J].计算机应用,2024,44(01):252-260.