

车联网通信中 V2X 技术的安全性挑战与应对措施

许春玉

北京移动系统集成有限公司 北京

【摘要】车联网通信中的 V2X 技术作为智能交通的核心，其安全性至关重要。本文分析了 V2X 技术面临的安全性挑战，包括身份认证风险、数据隐私泄露、网络攻击威胁等。针对这些挑战，提出了基于区块链的身份认证机制、数据加密与匿名化处理、强化网络安全防护等应对措施。通过这些措施，能够有效提升 V2X 技术的安全性，为智能交通系统的稳定运行提供保障。研究结果表明，综合运用多种技术手段是应对 V2X 安全挑战的关键，未来需进一步探索技术优化与协同合作，推动车联网通信的安全发展。

【关键词】车联网；V2X 技术；安全性；身份认证；数据隐私

【收稿日期】2025 年 3 月 5 日

【出刊日期】2025 年 4 月 6 日

【DOI】10.12208/j.jer.20250157

Security challenges and countermeasures of V2X technology in internet of vehicles communication

Chunyu Xu

Beijing Mobile System Integration Co., Ltd, Beijing

【Abstract】As the core of intelligent transportation, V2X technology in Internet of Vehicles communication is crucial. This paper analyzes the security challenges of V2X technology, including identity authentication risk, data privacy leakage, network attack threat and so on. In response to these challenges, blockchain-based identity authentication mechanism, data encryption and anonymity processing, strengthening network security protection and other measures are proposed. Through these measures, the safety of V2X technology can be effectively improved to guarantee the stable operation of the intelligent transportation system. The research results show that the comprehensive use of a variety of technical means is the key to cope with the V2X security challenges, and the future technology optimization and cooperation are needed to promote the security development of Internet of Vehicles communication.

【Keywords】Internet of vehicles; V2X technology; Security; Identity authentication; Data privacy

引言

车联网通信是智能交通系统的重要组成部分，而 V2X（Vehicle to Everything）技术作为其核心，通过车辆与车辆（V2V）、车辆与基础设施（V2I）、车辆与行人（V2P）等的通信，实现了交通信息的实时共享与协同决策，极大地提升了交通安全与效率。研究 V2X 技术的安全性挑战及其应对措施具有重要的现实意义，本文将深入探讨这一问题，为车联网的安全发展提供参考。

1 V2X 技术的安全性挑战

在车联网通信中，车辆与设备之间的身份认证是确保通信安全的基石。当前的身份认证机制存在诸多漏洞，这些问题严重威胁着车联网的安全性。伪造身份的问题日益突出。攻击者可以通过技术手段伪造车辆

或设备的身份信息，伪装成合法用户接入系统。这种伪造行为不仅会干扰正常的通信秩序，还可能导致错误的信息被传递和使用，进而引发交通事故^[1]。身份冒用也是身份认证环节的一大隐患。攻击者可能通过窃取合法用户的认证信息，冒充其身份进行恶意操作。攻击者可以伪装成车辆向交通信号灯发送错误的请求，或者伪装成基础设施设备向车辆发送虚假的路况信息，从而误导车辆行驶，甚至造成严重的交通拥堵或事故。

V2X 通信过程中涉及大量的敏感数据，包括车辆的行驶速度、位置信息、驾驶习惯，以及用户的个人信息等。这些数据在传输、存储和共享的各个环节都面临着隐私泄露的风险。在传输过程中，数据可能被网络攻击者截获，尤其是在无线通信环境中，数据的传输链路更容易被监听和篡改。一旦数据被截获，用户的隐私信

作者简介：许春玉（1984-）女，汉，天津，本科，研究方向为信息与通信工程。

息将暴露无遗,可能导致用户遭受骚扰、诈骗等安全威胁。在存储环节,数据通常存储在车辆的本地系统或云端服务器中。如果存储系统存在安全漏洞,攻击者可能通过入侵获取大量用户数据。在数据共享过程中,数据可能被未经授权的第三方获取和使用。车辆制造商或服务提供商可能与第三方合作,共享用户数据用于商业目的,但如果没有严格的安全措施,这些数据可能会被滥用,从而侵犯用户的隐私权益。

车联网系统作为复杂的网络环境,面临着多种网络攻击的威胁。其中,拒绝服务攻击(DoS)是常见的攻击方式之一。攻击者通过向车联网系统发送大量的虚假请求,使系统资源被耗尽,从而导致合法用户无法正常访问服务。在交通高峰时段,攻击者对交通信号灯控制系统发起 DoS 攻击,可能导致信号灯无法正常工作,造成交通瘫痪。中间人攻击也是车联网系统面临的重要威胁。攻击者可以插入到车辆与基础设施之间的通信链路中,窃取或篡改传输中的数据。攻击者可能篡改车辆接收的路况信息,误导车辆行驶方向,甚至导致车辆碰撞^[2]。这些网络攻击不仅会中断正常的通信,还可能导致数据被篡改或伪造,严重破坏车联网系统的完整性和可靠性。

2 V2X 技术的安全性应对措施

区块链技术以其独特的去中心化、不可篡改和透明性等特点,为解决 V2X 通信中的身份认证问题提供了新的思路。在传统的身份认证系统中,车辆和设备的身份信息通常存储在中心化的服务器中,容易受到攻击和篡改^[3]。而区块链通过分布式账本技术,将车辆的身份信息以区块的形式存储在多个节点上,每个区块都包含前一个区块的哈希值,从而形成了一个不可篡改的链式结构。

数据加密是保护 V2X 通信中数据安全的重要手段。在车联网环境中,车辆行驶数据、用户个人信息等敏感数据在传输和存储过程中面临着被窃取和篡改的风险。通过采用先进的加密技术,如对称加密和非对称加密算法,可以将数据转换为无法被轻易解读的密文,只有持有正确密钥的接收方才能解密并读取数据内容。这不仅确保了数据在传输过程中的安全性,还防止了数据在存储时被非法访问。除了加密技术外,匿名化处理也是保护用户隐私的关键措施。通过匿名化技术,可以隐藏用户的身份信息,避免用户在 V2X 通信中被识别和跟踪。可以采用差分隐私技术,在数据中添加噪声,从而在不泄露用户隐私的情况下实现数据的共享和分析。

为了应对车联网系统面临的多种网络攻击威胁,必须采取综合的网络安全防护措施。部署防火墙和入侵检测系统(IDS)是网络安全防护的基础。防火墙可以有效地阻止未经授权的访问,防止外部攻击者进入系统内部。而入侵检测系统则能够实时监测网络流量,检测到异常行为时及时发出警报并采取相应的措施。通过防火墙和 IDS 的协同工作,可以及时发现并阻止网络攻击,保护车联网系统的安全。采用安全协议和加密算法也是提升通信链路安全性的重要手段^[4]。使用 TLS/SSL 协议对通信链路进行加密,可以防止数据在传输过程中被窃取或篡改。定期更新和升级安全协议和加密算法,以应对不断变化的网络攻击手段,也是确保车联网系统安全运行的关键。

3 V2X 技术安全性措施的实施效果

通过一系列针对性的安全措施的实施,V2X 通信的安全性得到了显著的提升。在身份认证方面,引入了先进的技术手段,如区块链技术,极大地增强了身份认证的可靠性和安全性。区块链的去中心化和不可篡改特性,使得车辆和设备的身份信息更加可信,有效防止了伪造身份和身份冒用等问题的发生^[5]。这不仅保障了通信的合法性,还为车联网的稳定运行奠定了坚实的基础。在数据隐私保护方面,通过采用先进的加密技术和匿名化处理,数据在传输和存储过程中的安全性得到了有效保障。

在网络安全防护方面,通过部署防火墙、入侵检测系统等安全设备,以及采用安全协议和加密算法,车联网系统对网络攻击的抵御能力得到了显著增强。拒绝服务攻击(DoS)和中间人攻击等常见网络攻击的威胁大幅降低。系统能够更有效地检测和防御恶意攻击行为,保障通信链路的完整性和可靠性。这些措施的实施,不仅减少了网络攻击对车联网系统的直接影响,还提升了系统的整体稳定性,为智能交通系统的正常运行提供了有力支持。

尽管当前的安全措施已经取得了初步成效,但为了应对日益复杂的网络安全环境,这些措施仍需不断优化和完善。一方面,技术的更新换代需要持续投入,以确保安全机制能够适应新的威胁和挑战。随着量子计算技术的发展,现有的加密算法可能面临被破解的风险,因此需要提前研究和部署更加先进的加密技术。另一方面,安全措施的协同合作也至关重要^[6]。车联网涉及多个领域和行业,需要政府、企业、研究机构等各方共同努力,形成全方位的安全防护体系。用户的安全意识也需要进一步提高,以减少因用户操作不当导致

的安全风险。

4 结论与展望

V2X 技术作为车联网通信的核心,正在迅速改变交通系统的运作方式。通过车辆与车辆(V2V)、车辆与基础设施(V2I)、车辆与行人(V2P)等多种通信方式,V2X 技术能够实现交通信息的实时共享与协同决策,极大地提升交通安全与效率^[7]。车辆可以提前获取前方道路的拥堵情况,从而选择更优的行驶路线;交通信号灯可以根据实时车流调整信号时长,减少等待时间。随着 V2X 技术的广泛应用,其安全性问题也日益凸显。身份认证漏洞、数据隐私泄露以及网络攻击等安全威胁,不仅会干扰正常的通信秩序,还可能引发严重的交通事故,甚至危及公共安全。保障 V2X 通信的安全性,是推动车联网技术健康发展的关键。

为了应对 V2X 技术的安全挑战,多种技术手段被提出并应用于实际场景中。基于区块链的身份认证机制为解决身份认证问题提供了新的思路。区块链的去中心化和不可篡改特性,能够有效防止身份伪造和冒用,确保通信双方身份的可信性。数据加密与匿名化处理技术在保护用户隐私方面发挥了重要作用。通过加密技术,敏感数据在传输和存储过程中能够得到充分保护,防止被窃取或篡改;匿名化处理则隐藏了用户的身份信息,进一步降低了隐私泄露的风险。强化网络安全防护也是保障 V2X 通信安全的重要措施。部署防火墙、入侵检测系统等网络安全设备,能够有效抵御外部攻击,确保通信链路的稳定性和可靠性。这些技术手段的综合应用,为 V2X 通信的安全性提供了有力保障,使其能够在复杂的网络环境中稳定运行。

尽管当前的技术措施已经在一定程度上缓解了 V2X 技术的安全问题,但随着技术的不断发展和应用场景的日益复杂,新的挑战也在不断涌现。未来,我们需要进一步探索新技术的应用与协同合作,以推动车联网通信的安全发展。人工智能和机器学习技术可以用于实时监测和分析网络流量,及时发现异常行为并采取措施;物联网安全标准的不断完善,将为 V2X 通信提供更明确的安全规范和指导。跨领域的合作也至关重要^[8]。汽车制造商、通信设备供应商、网络安全专

家以及政府部门需要共同努力,形成合力,从技术、标准、政策等多个层面推动车联网通信的安全发展。

5 结语

V2X 技术作为车联网通信的核心,虽面临身份认证、数据隐私及网络攻击等安全挑战,但通过区块链身份认证、数据加密与匿名化处理以及强化网络安全防护等措施,其安全性已显著提升。未来,随着技术的持续创新与跨领域合作的深化,需进一步探索新技术应用,完善安全标准与政策,推动车联网通信的安全发展。这将为智能交通系统的稳定运行提供坚实保障,助力车联网技术在提升交通安全与效率方面发挥更大作用。

参考文献

- [1] 张雯,郑浩. V2X 通信系统中信号同步技术的优化策略[J]. 数字通信世界, 2025, (02): 30-32+35.
- [2] 李颖. 车路协同 C-V2X 关键技术演进发展研究 [J]. 产业科技创新, 2024, 6 (05): 116-120.
- [3] 孟超. 应用 V2X 技术实现交叉路口碰撞预警的功能测试方案 [J]. 汽车知识, 2024, 24 (09): 127-131.
- [4] 李育勇. 基于专利分析的 V2X 车辆碰撞预警技术发展趋势 [J]. 汽车周刊, 2024, (10): 7-9.
- [5] 刘茗铄,陈满,王志承. MQTT 技术构建 V2X 数据传输平台研究 [J]. 福建电脑, 2024, 40 (09): 26-32.
- [6] 李育勇. 基于专利分析的 V2X 车辆碰撞预警技术发展趋势 [J]. 中国汽车市场, 2024, (04): 85-86.
- [7] 郝波,冯东. 基于 V2X 技术的无线车车直连通信系统研究 [J]. 控制与信息技术, 2024, (04): 123-129.
- [8] 苑广勇. 基于 5G 的 V2X 车联网通信模组技术应用 [J]. 电子技术, 2023, 52 (07): 56-57.

版权声明: ©2025 作者与开放获取期刊研究中心(OAJRC)所有。本文章按照知识共享署名许可条款发表。

<https://creativecommons.org/licenses/by/4.0/>

