智能网联汽车安全检测技术综述与未来展望

曲彬 孙倩倩 莫宗维

重庆电讯职业学院，重庆市，402247；

摘要：随着智能网联汽车技术的飞速发展，其安全问题日益凸显，安全检测技术成为保障其可靠运行的关键，并为智能网联汽车的普及提供了坚实的技术支撑。本文以智能网联汽车安全检测技术概述以及智能网联汽车安全检测技术的最新进展进行分析。

关键词：智能网；联汽车安全；检测技术综述；未来展望

DOI:10.69979/3041-0673.24.5.004

引言

随着科技的飞速进步和互联网的深入普及，智能网联汽车（ICV）已成为未来交通出行的革新者。这种融合了先进信息技术与传统汽车工业的新型交通工具，凭借其智能化的驾驶辅助系统、高效的网联通信技术，极大地提升了驾驶安全性和交通效率。然而，随着智能网联汽车技术的广泛应用，其安全问题也日益凸显，引发全球范围内的广泛关注。安全检测，作为保障智能网联汽车可靠运行的关键环节，其重要性和研究价值不言而喻。

1 智能网联汽车安全检测技术概述

1.1 安全检测技术基础

智能网联汽车的安全检测涵盖了从硬件到软件，再到通信协议的各个层面，形成了一套复杂而全面的检测体系。其基础技术主要包括模型验证与确认、形式化方法、数据驱动的测试和新兴技术的应用。

模型验证与确认是早期安全检测的重要手段，它通过对车辆行为的数学模型进行分析，预测和验证系统在不同工况下的行为，从而发现潜在的故障模式和安全漏洞。模型验证通过比较实际运行结果与理论预测，确认设计的正确性，而确认则关注系统的功能是否符合设计规格，两者结合能确保系统设计阶段的安全性。

形式化方法则是一种基于严谨数学逻辑的验证手段，它通过数学模型来描述系统的状态和行为，进而证明系统在所有可能情况下是否满足安全需求。这种方法能有效发现设计阶段的逻辑错误，确保软件和控制算法的正确性，是保证智能网联汽车安全的关键技术之一。

数据驱动的测试是近年来日益受到重视的安全检测方法，它通过收集车辆运行时的大量数据，利用统计和机器学习技术，发现潜在的异常行为和故障模式。这种方法能够适应智能网联汽车的动态环境，及时发现新的安全威胁，是实时保障车辆安全的有效手段。

新兴技术如区块链和人工智能的融入，为安全检测带来了新的机遇。区块链技术通过分布式账本和加密算法，提高了数据的安全性和透明度，有助于防止数据篡改和提升信任度，为数据驱动测试提供了更加可靠的基础。人工智能，特别是深度学习，通过模式识别和预测能力，能更准确地识别潜在的攻击行为和安全漏洞，进一步提升了检测的效率和精度。

1.2 现有安全检测技术综述

智能网联汽车安全检测技术在应对技术变革中扮演着核心角色。现有的安全检测技术主要包括模型验证与确认、形式化方法、数据驱动的测试，以及新兴技术如区块链和人工智能的深度融合。

模型验证与确认是早期安全检测的基础，通过构建数学模型分析汽车行为，用以预测和验证系统在不同情况下的表现，从而识别潜在故障模式和安全漏洞。模型验证侧重于系统设计阶段的正确性确认，而确认则关注功能是否符合设计规格。这些方法在保证系统设计安全方面十分关键，但随着系统规模的扩大，验证与确认的复杂性也随之增加。

形式化方法是基于严格数学逻辑的安全检测手段，它通过数学模型描述系统状态和行为，确保系统在所有可能情况下满足安全需求。这种方法能够有效发现早期设计阶段的逻辑错误，保证软件和控制算法的精确性，是智能网联汽车安全不可或缺的工具。然而，形式化方法的验证过程耗时且需要专业知识，对于复杂系统来说，其应用挑战依然存在。

数据驱动的测试近年来在安全检测领域崭露头角。它依赖于采集的车辆运行数据，通过统计和机器学习技术分析，实时发现异常行为和故障模式，尤其适用于应对智能网联汽车的动态环境。然而，数据隐私保护成为数据驱动测试中的一大挑战，如何在保护用户隐私的同时进行有效的安全检测，是当前研究的重点。

新兴技术如区块链和人工智能已经对安全检测产生了深远影响。区块链技术通过分布式账本和加密算法，提升数据

安全性和透明度，为数据驱动测试提供了更稳定的基础。人工智能，特别是深度学习，凭借其模式识别与预测能力，能够更准确识别和预测潜在威胁，显著提升了检测效率和精度。然而，这些新兴技术的广泛应用也要求建立统一的标准和测试框架，以确保其实际应用的稳定性和一致性。

2 智能网联汽车安全检测技术的最新进展

2.1 数据安全检测技术

数据安全检测技术在智能网联汽车的安全检测中扮演着至关重要的角色，尤其是随着车辆智能化程度的提升，数据的流动和处理变得更为频繁和复杂，数据安全的威胁也随之增加。数据安全检测主要涉及数据的完整性、机密性和可用性，旨在确保数据在传输、存储和处理过程中不被未经授权的访问、修改或泄露。

数据完整性检测关注的是数据在传输过程中是否被篡改。在智能网联汽车中，数据完整性检测技术通常结合加密算法，如哈希函数，用于验证数据在传输后是否与原始数据保持一致。一旦检测到数据完整性遭到破坏，系统可以采取措施，如终止通信或者启动故障恢复机制，保证汽车系统的正常运行。

数据机密性检测旨在保护敏感信息不被非法获取。这通常通过加密技术实现，如 SSL/TLS 协议，为数据传输建立安全通道。随着量子计算等技术的发展，研究人员正在开发更高级别的加密算法，如基于量子密钥分发的加密，以应对未来的安全挑战。

数据可用性检测着重于确保数据在需要时能够被正确获取，防止数据被恶意拒绝服务攻击（DoS）或分布式拒绝服务攻击（DDoS）所影响。智能网联汽车中的数据可用性检测通常结合了冗余数据存储和网络流量管理策略，以优化数据传输和确保在潜在攻击下的数据可访问性。

数据隐私保护是数据安全检测中的另一个重要方面。车辆收集的大量用户数据，如行驶路线、驾驶习惯等，需要在进行安全检测的同时，确保这些信息不被滥用。这需要开发更高级的隐私保护技术，如差分隐私和同态加密，以在数据分析过程中保护个人隐私，同时允许必要的安全检测和故障诊断。

近年来，数据驱动的测试技术结合机器学习和人工智能，开始在数据安全检测中发挥作用。这些技术可以识别异常行为模式，如异常数据流、恶意软件活动，以及潜在的入侵，提前预警可能的安全威胁。然而，这同样带来了新的挑战，如如何平衡数据模型的训练与隐私保护之间的关系，以及如何处理模型解释性与隐私保护的矛盾。

随着智能网联汽车的生态系统日益复杂，数据安全检测技术将需要与车辆控制、通信技术紧密结合，以形成更全面的防护体系。同时，制定统一的数据安全检测标准和评估框架，加强产业、学术界和政策制定者的合作，将有助于提升整个行业的数据安全性。未来，随着深度学习在安全检测中的应用进一步深化，智能网联汽车的数据安全检测将更加自动化和精准，有效应对不断变化的数据安全威胁，确保驾驶者的隐私和行车安全。

2.2 网络安全检测技术

网络安全检测技术在智能网联汽车安全检测中扮演着举足轻重的角色，它主要关注车辆与外界通信网络的交互，确保数据的完整性和系统不受恶意攻击。随着网络技术的快速发展和智能网联汽车的广泛应用，网络安全威胁日益复杂，对检测技术提出了更高的要求。

网络安全检测技术涉及对通信协议的分析与验证。通过对车辆与外界通信数据的包头、包体、协议结构进行深度解析，可以识别出潜在的协议漏洞，如是否存在容易被操纵的字段、是否存在过时的或者不安全的协议版本。通过协议分析，可以防止攻击者利用这些漏洞进行中间人攻击、数据篡改或拒绝服务攻击。

入侵检测系统（IDS）和入侵防御系统（IPS）在网络安全检测中发挥了关键作用。IDS 通过监控网络流量，通过模式匹配、统计分析和机器学习算法，识别出异常的网络行为，如不寻常的数据包频率、未知的通信源等，及时预警潜在的攻击。而 IPS 则在检测到威胁时，能够实时采取行动，如阻断通信、记录事件或自动修复，以防止攻击的发生。

同时，网络安全检测技术也关注对车载软件和系统的安全扫描。这包括对操作系统、应用程序、通信模块等进行漏洞扫描，识别并修补可能被利用的软件漏洞。此过程通常涉及静态分析、动态分析以及模糊测试等方法，确保软件的安全性和健壮性。

随着区块链技术的兴起，其在网络安全检测中的应用也日益受到关注。区块链的分布式账本特性提供了数据的透明性和不可篡改性，使得网络活动能够被追踪和审计，有助于检测和防止数据盗窃、欺诈及恶意软件。通过将区块链技术与网络安全检测系统结合，可以构建更为安全的通信架构，提高数据的信任度。

然而，网络安全检测技术目前也面临一些挑战。例如，随着网络攻击手段的不断升级，需要持续更新和优化检测模型以应对新型威胁。同时，如何在保护数据隐私和提供安全检测之间找到平衡，防止无端的数据泄露，也是网络安全检测技术需要解决的问题。

未来，网络安全检测技术将更侧重于深度学习和人工智能的应用，通过智能分析网络行为，实现对未知威胁的自适

应检测和防御。跨领域的协同研究，如将网络安全与车辆控制、通信技术相结合，将提高整个系统的安全性能。此外，建立统一的网络安全检测标准和评估体系，以及政策制定者的参与，将是推动智能网联汽车网络安全检测技术持续进步的重要驱动力。

2.3 隐私保护检测技术

隐私保护检测技术在智能网联汽车安全检测中占据了至关重要的地位。随着车辆成为移动的数据采集和处理中心，个人隐私保护成为了与数据安全同样重要的考量。这些技术的目的是在收集、传输和处理用户数据时，确保数据的匿名性、不可链接性以及用户的控制权，防止未经授权的访问、滥用或泄露。

一种主要的隐私保护检测技术是差分隐私（DifferentialPrivacy）。这种技术通过向数据中添加随机噪声，使得单个用户的数据无法被准确识别，同时保证数据的统计特性尽可能不受影响。差分隐私在智能网联汽车中，例如在车辆位置信息的共享中，可以确保即使数据被分析，攻击者也无法确定特定车辆的精确位置信息。

同态加密（HomomorphicEncryption）是另一种重要的隐私保护技术，它允许数据在加密状态下进行计算，而无需先解密。在智能网联汽车中，同态加密可以用于实时分析加密的车辆数据，如检测异常驾驶行为，同时确保原始数据的隐私性。

差分隐私和同态加密的结合使用在数据驱动的测试中展现出巨大潜力。通过差分隐私保护数据的个体隐私，同态加密则允许在加密数据上进行分析，两者的结合确保了数据的安全分析，同时保护了用户的隐私，为智能网联汽车的安全检测提供了强有力的支持。

然而，隐私保护检测技术也面临着挑战。例如，差分隐私中的噪声添加会一定程度上影响数据的准确性，而同态加密的计算效率相对较低，可能会对实时性要求高的应用产生影响。此外，如何在保护隐私的同时保持数据的有效性和实用性，以及如何在法律法规框架内合法合规地应用这些技术，都是研究者和工程师需要解决的问题。

未来，隐私保护检测技术将在智能网联汽车中实现更深度的应用。这包括开发新的隐私保护算法，如基于多方计算的隐私保护方案，以及探索隐私保护与数据价值之间的最优平衡。同时，跨领域的合作，如与法律专家、伦理学家的交流，将有助于建立适应新技术的隐私保护标准和规范，确保智能网联汽车在保障用户隐私的同时，实现技术的创新与进步。

2.4 车载系统安全检测技术

车载系统安全检测是智能网联汽车安全检测的重要组成部分，它着眼于汽车内部电子系统和软件的防护，避免恶意攻击者通过软件漏洞获取对车辆的控制权，或者泄露车内敏感信息。随着车辆电子系统复杂性的增加，车载软件的测试和验证变得尤为关键。传统的静态代码分析和动态测试方法，在车载系统安全检测中仍然占有重要地位。静态代码分析通过检查源代码，发现潜在的安全漏洞，如未初始化的变量、缓冲区溢出等，确保软件设计阶段的安全。动态测试则关注软件在运行时的行为，通过模拟各种输入和环境条件，发现运行时的错误和安全问题。

近年来，随着软件工程的进化，车载系统安全检测方法也在不断进步。其中，形式化方法的应用日益广泛，它通过数学模型的形式化描述，对软件行为进行严格证明，确保其满足安全需求。这种方法能有效发现复杂的逻辑错误，对于保障车载软件的正确性和安全性具有显著优势。然而，形式化方法的高昂成本和对专业知识的高要求限制了其在大规模软件系统中的应用。

3 结语

智能网联汽车安全检测技术的未来将是一场创新、融合与合作的盛宴。通过深度学习、自动化、跨领域协同、标准化以及隐私保护技术的结合，智能网联汽车将能够应对日益复杂的威胁，为用户提供更安全、更高效的出行体验。在这个过程中，政策制定者、产业界和学术界都将在推动技术进步和保障公共安全上发挥关键作用。

参考文献

[1]袁豪杰.智能网联汽车网络架构分析及安全检测[J].《信息安全与通信保密》,2024 年第 1 期 60-69,共 10 页
[2]陈桂银.智能网联汽车协同生态驾驶策略综述[J].《大众汽车》,2024 年第 7 期 0001-0003,共 3 页
[3]王鹏.智能网联汽车车载网络异常检测技术研究[J].《信息通信技术》,2023 年第 4 期 39-48,共 10 页
[4]于静.“双智”协同与智能网联汽车的发展现状与建议[J].《中外建筑》,2024 年第 7 期 70-74,共 5 页