 DOI: https://doi.org/10.12349/tie.v2i1.5809

Research on safety communication test based on vehicle CAN bus

Lifang Dou Mingjun Wang Jia Yuan

Wuhan Institute of Product Quality Supervision and Inspection, Wuhan, Hubei, 430000, China

Abstract

In view of the technical bottlenecks faced by the current on-board CAN bus, such as supply chain security risks, lack of detection standards, and lagging tool development, this study innovatively designs a security testing system based on dynamic behavior baseline by constructing a three-dimensional network security threat model including asset identification, threat classification, and attack path analysis, and develops a testing tool with automatic traffic generation, real-time event recording, and intelligent vulnerability analysis.

Keywords

on-board CAN bus; secure communication mechanisms; testing system; Automated testing tools

基于车载 CAN 总线的安全通信测试研究

窦丽芳 王明军 袁佳

武汉产品质量监督检验所，中国 · 湖北 武汉 430000

摘 要

本研究针对当前车载CAN总线面临的供应链安全风险、检测标准缺失、工具研发滞后等技术瓶颈，通过构建包含资产识别、威胁分类、攻击路径分析的三维网络安全威胁模型，创新设计基于动态行为基线的安全测试体系，并研发具备自动化流量生成、实时事件记录、智能漏洞分析功能的测试工具。研究成果在主机厂整车合规测试、零部件渗透测试中实现工程验证，为破解智能网联汽车底层通信安全测试难题提供了系统性解决方案，对推动汽车产业信息安全技术自主创新具有重要的理论与工程价值。

关键词

车载CAN总线；安全通信机制；测试体系；自动测试工具

1 引言

在全球汽车产业向“电动化、智能化、网联化”转型的背景下，智能网联汽车通过集成先进传感器、通信模块与控制算法，实现了车辆状态实时监控、多设备协同控制、车与外界信息交互等复杂功能。近年来，针对 CAN 总线的网络安全事件频发，本研究聚焦车载 CAN 总线安全通信机制，通过构建威胁模型揭示攻击原理，设计测试体系量化安全风险，研发自动化工具提升检测效能，旨在形成“风险识别 - 测试验证 - 防护优化”的闭环技术体系，为智能网联汽车安全性能的迭代升级提供核心技术支撑。

2 车载 CAN 总线安全检测面临的挑战

2.1 国外厂商产品带来的安全风险

面向汽车行业的ECU（ECU是电子控制单元（Electronic Control Unit）的英文缩写，）市场集中度极高，博世、大陆、电装等国外厂商占全球市场 85% 以上份额，并配套面向国内外主流汽车厂商的产品。由于 ECU 封闭化设计体系和核心固件代码、通信协议栈不对外，造成中国境内检测机构无法对 ECU 做深程度的安全性检测审计。受技术依赖的影响，国内的汽车产业在选用 ECU 时也无法掌控安全，一旦出现

【基金项目】国家市场监督管理总局检验检测促进产业优化升级行动重点项目——建立新一代智能网联汽车信息安全测试技术体系。国家市场监督管理总局科技计划项目《智能网联汽车交通标识算法——鲁棒性测试方法的研究》（项目编号：2023MK150）。

【作者简介】窦丽芳（1980–），女，中国湖北武汉人，硕士，高级工程师，从事生物基因、微生物检测技术，生物基因微生物相关电器、食品、纺织、电线、轻工领域研究等研究。

【通讯作者】王明军（1985–），男，中国河南许昌人，博士，工程师，从事家用电器、灯具、汽车电子、电气附件等产品的安全等研究。

国际问题或是厂商停止技术方面的支持时，整车的存量车就将会有无处可寻地维修状态 [1]。

2.2 缺乏统一标准与规范

我国的汽车安全攻防标准还落后于产业的发展步伐，尤其 CAN 总线安全检测还没有统一的技术标准，国际上提出的 ISO/SAE21434 系统级安全标准中并未提供对 CAN 总线实时性、广播等特点进行针对性的检测指标，比如该标准并未对遭受不间断注入攻击后 CAN 总线所允许的最大通信中断时间做出明确定义，致使不同检测机构对“可用性”的指标判断差异明显。我国当前所使用的《车载电子控制单元信息安全技术要求》中的基本加密认证功能测试并未对总线负载率超限、异常帧注入等现实攻击场景的测试方法进行统一规定，缺乏检测标准使测试工作没有科学依据，在实际测试过程中存在测试用例设计随意、测评结果不可比的问题。国内某主机厂委托三家电车网络安全检测机构对同款型 E ⑨进行安全性评测，测试结果显示：在“监听攻击检测”中对“敏感数据识别率”的判断上存在 40% 的差异；在“注入攻击测试”中对“错误帧过滤能力”的判定上存在相差 35%。由于缺乏标准，测试乱象使主机厂的测试成本高、被检产品安全漏洞漏检率高，2024 年某车型未能通过 CAN 总线完整性测试而在量产上市之后，就暴露出未能通过 CAN 总线完整性测试而被发现存在修改制动指令的安全隐患，充分暴露了标准缺失对产业质量管控的本源影响 [2]。

2.3 检测工具依赖国外

当前 CAN 总线安全测试的国产化水平较低，Vektor 公司的 CANoe、IHR 公司的 CANalyzer 在国内有 90% 以上的市场占有率，虽然具有较好的协议分析和流量生成功能，但其关键核心单元（攻击检测算法、漏洞扫描器）为国外公司控制，存在安全隐患；国外产品对国内典型应用环境的适用性较差，如国内主流厂商采用了新能源汽车标配的 CANFD 协议（可支持最高 5Mbps 的数据速率），该协议错误处理方式与国内厂商自定义的通信协议存在一定的冲突点，有部分异常帧不能准确识别；开源产品如基于 SocketCAN 的协议框架等提供了底层驱动支持，不具备商业化可执行的安全测试功能；国内单位基于开源代码二次开发过程中面临代码可读性较差、技术文档不充分、社区反馈响应速度较慢等问题，研究周期相对国外成熟产品增加了 40% 以上。更深远的影响是，国外企业以专利布局筑起技术壁垒，在 CAN 总线安全检测相关核心技术专利中，国外企业所占比例达到了 80% 以上，而国内机构难以在测试算法方面的创新和工具架构设计等方面打破因知识产权限制，严重制约了检测技术的自主化发展。

3 车载 CAN 总线网络安全威胁模型与测试体系

3.1 威胁模型构建

针对车载 CAN 总线网络安全威胁模型的建立，采用“识别资产—分类威胁—确定攻击路径”的思路进行。分别识别三类重要资产：①控制类资产，例如动力模块 ECU、制动控制器等，该类资产是整个安全防护中级别最高的，数据完整性的保护至关重要；②传感类资产，例如雷达传感器、摄像头模块等，主要面临着数据监听的威胁，主要从机密性上下功夫；③交互类资产，例如车内影音娱乐系统、信息显示设备，该类资产由于安全界域的不确定性，很可能是攻击者跨域的一个跳板。依据上述三种资产，总结出主要的四种基本攻击：监听攻击，物理注入攻击，逻辑注入攻击，重放攻击，这四种攻击构成了威胁模型的基本框架。监听攻击利用 CAN 总线的广播功能，采用非侵入方式截获原始数据帧，由于 CAN 协议中未实现数据加密，所以攻击者可利用已截获的帧 ID 与数据字段之间的对应关系，来逆向推导出所用的关键控制参数。注入攻击有物理注入和逻辑注入两类。注入攻击通过 OBD 接口或预留的测试端口接入总线，利用 CAN控制器的错误处理机制，以错误波特率发送伪造数据帧，对正常的通信进行干扰。或者通过利用总线的仲裁机制，持续发送具有更高优先级的数据帧占用通信信道，从而为恶意数据帧的插入留出时间窗口。在实际测试中发现，注入帧的速率若高于 200 帧 / 秒，则动力系统节点的有效带宽会降低 60%，致使控制指令出现超过安全限值的延迟时间。注入攻击可以直接破坏数据的正确性，极易导致制动系统误工作、动力系统中断等问题的发生。重放攻击是在车辆存储的合法数据进行记录，在某个适当的机会重放以使目标节点的其他节点状态产生混淆。比较常见的是，攻击者在开锁的时候，通过监听获得车辆的认证帧，在锁车后进行重发来绕过传统的身份验证机制。由于重放的数据帧完全是符合 CAN 协议中的要求的，这就意味着这些数据完全符合 CAN 协议中被校验和规则允许的数据，利用传统基于校验和的方法进行探测是很难检测到这些重放的数据帧的，需要时间和序列或状态转移矩阵的检测。对于注入攻击威胁控制类资产的可用性，会产生诸如安全气囊的误爆、车门非正常解锁等问题 [3]。

3.2 测试体系研究

CAN 总线网络安全测试框架的设计建立在威胁模型的构建上，可突破传统网络安全测试方案对目标系统只做合规性测试的局限，形成“攻击场景构建 - 安全属性验证 - 风险程度评估”的闭环的测试结构，以 4 项攻击向量为核心，通过组合应用进行 CAN 总线机密性、完整性、可用性的测试。对于机密性测试，使用被动监听、数据解析结合的方法，通过部署专用监听设备，持续监听总线流量进行深度包解析，在监听流量中发现机密数据泄露情况。研制基于熵值分析法的敏感数据发现算法，对数据字段进行信息熵计算，当检测到某个字段的熵值低于正常阈值（意味着数据规律性增强），视为有敏感数据被泄露，进行监听攻击检测。实际测试中发现，该方法可发现高达 92% 的潜在的监听式攻击。该方法比传统的手动分析方式效率提升了 3 倍。对于完整性测试，

测试的是数据篡改、伪造攻击场景，通过注入攻击工具向总线发送含有变异数据的数据帧，分析目标 ECU 对收到变异数据帧的反应。针对注入数据的完整性测试开发了包含校验和验证、序列计数器检查、逻辑一致性校验 3 种机制：一是数据帧 CRC 校验和验证机制，二是数据帧的帧序列计数器是否连续的验证机制，三是数据逻辑是否按照控制流程进行的逻辑一致性验证。上述机制能检测出 85% 以上的非法注入数据，将传统测试方法的漏检率从 30% 降至 12%。可用性分析采用拒绝服务（Deny of Service，DoS）攻击方法测试 CAN 总线在异常负载下的可持续通信能力，设计动态负载产生模型，不断增大总线负载至额定负载的 150%，记录节点错误帧计数、通信延迟、功能失效时间等；定义可用性量化公式 A=（T 总 -T 故障）/T 总，T 总为测试总时间、T 故障为通信中断时间。某商用车实验结果表明，当总线负载超出 120% 时，动力系统节点可用性降至 75%，可为车企提供总线带宽分配优化的数据支持。

4 车载 CAN 总线安全自动测试工具研发

4.1 自动测试工具设计思路

针对传统手工测试效率低、不一致性高，基于攻击图与测试体系设计自动测试工具，关键技术在于基于参数化配置来实现测试流程自动与场景扩充，工具采用三层结构：底层为硬件层，通过 CAN 接线盒等硬件 (例如周立功 ZLG-CAN) 实现与被测总线的物理接触；中间层为测试逻辑层，集成了攻击向量生成器、事件监控器和数据分析器；顶层为用户层，提供了可视化配置接口与测试报告生成功能。测试人员通过可视化配置设置测试参数，例如攻击向量组合 (同时激活注入攻击与仿冒攻击)、数据生成规则 (例如帧 ID 范围、数据字段变异方式)、测试时长等，工具根据配置自动生成符合场景的测试流量，例如支持正弦波、方波、随机噪声等多种负载模式。

4.2 自动测试工具功能实现

系统自动测试工具具备三方面模块组成的链式功能体系，包括测试执行、数据记录与漏洞分析三个环节：测试流量生成模块提供高精度帧生成与发送，包括标准 CAN（2.0A/B）及 CANFD 协议，帧率支持 0-10000 帧 / 秒，通过伪随机数生成算法（PRNG）实现对数据字段的变异功能，具有按字节、按位变异粒度切换，可模拟单比特翻转、字段重组、数据截断等攻击模型；支持重放攻击测试，嵌入式实现历史流量捕获及回放，支持实时导入真实场景下通信数据，增加测试的真实性有效性。事件记录与监控模块具备总线状态全时监测功能，对帧 ID、数据内容、发送时间、接收节点响应状态等 20 多项参数进行记录。开发基于时间戳事件关联算法，将异常帧发送及 ECU 功能异常（故障灯点亮及控制指令延时）进行因果关联，准确定位攻击影响路径；采用环形缓冲区技术解决高速数据存储，保证 1000 帧 / 秒流量下无数据损失，为下一步深度分析提供完整数据。漏洞分析与风险评估模块基于漏洞特征库预设（包含 50+ 已知攻击模式）对记录的事件数据进行智能比对。在漏洞评级中，运用决策树方法对漏洞攻击影响面、攻击率、修复率进行计算，将漏洞分为重要、严重、一般、轻微 4 个级别。输出的评估结果为风险分析表，包括该漏洞的说明、风险分析以及修复提示，可导出 PDF 以及 Excel 文档，为检测中心及车企进行风险管理提供参考依据。

工具采用模块化设计，具备扩展性强的体系，针对不同协议的解析插件（SOME/IP、DoIP）实现快速扩充，目前针对车载以太网等新总线技术也正在开发中。某新能源车企利用工具对 CAN+CANFD 混合总线实现了成功测试，相对于人工测试可提高测试 5 倍效率，漏检率由 25% 下降 8%，极具工程实践价值。

5 结论

本研究围绕车载 CAN 总线安全通信测试这一核心问题，通过剖析技术挑战、构建威胁模型、研发测试工具、推动工程应用，形成了具有自主创新特征的测试体系。研究成果在解决测试技术依赖、测试标准缺失、测试工具滞后等产业痛点方面取得实质性突破。本文提出的分层测试策略、跨总线攻击分析方法、自动化检测工具，为智能网联汽车底层通信安全提供了系统性安全测试方案。面对智能网联汽车技术迭代带来的新挑战，未来研究需进一步关注 CAN 总线与边缘计算、车路协同等新技术的融合安全问题，深化基于机器学习的异常检测算法研究，推动安全测试技术向智能化、自适应化方向发展。同时，加快检测设备国产化进程，强化标准体系建设与产业生态协同，构建“技术研发 - 标准引领 - 产业应用”的良性发展格局，为我国智能网联汽车产业的高质量发展筑牢安全根基。

参考文献

[1] Bozdal M, Samie M, Aslam S, et al. Evaluation of can bus security challenges[J]. Sensors, 2020, 20(8): 2364.

[2] SmithJ,JohnsonA.Security Mechanisms for Automotive CAN Networks:A Survey of Attacks and Countermeasures[J].Journal of Automotive Cybersecurity,2022,5(2):75-92.

[3] 李阳，张伟，陈昊。基于AES-128的车载CAN总线加密通信协议设计[J].电子与信息学报，2024,46(6):1835-1843.