车载以太网安全分析与多级安全架构设计

赵冬耀
北京理工大学珠海学院，广东 珠海 519088

DOI: 10.61369/SSSD.2025040039

摘　　要： 随着车载以太网的普及及其在智能汽车中应用的重要性，车载以太网安全在车载系统中扮演着关键的角色，车载以太网的安全性不仅关系到车辆的正常运行，还直接影响到驾驶者和乘客的安全与隐私。当前车载以太网面临的主要安全威胁，包括网络攻击、数据泄露、数据篡改、拒绝服务攻击（DoS）和系统入侵等。针对车载以太网网络的物理环境和功能特点本文提出了多级安全架构，形成多层次的安全防护体系，包括不同层级的安全措施，如物理层、数据链路层和应用层的安全防护机制。多级安全架构设计中采用的安全策略和技术手段，如加密、身份验证、机器学习算法建立正常通信基线、入侵检测等。

关 键 词： 车载以太网；安全威胁；多级安全架构；安全策略

Security Analysis of In-Vehicle Ethernet and Multi-level Security Architecture Design

Zhao Dongyao
Beijing Institute of Technology Zhuhai College, Zhuhai, Guangdong 519088

Abstract: With the widespread adoption of automotive Ethernet and its critical role in intelligent vehicles, the security of automotive Ethernet plays a pivotal role in vehicular systems. The safety of automotive Ethernet not only affects the normal operation of vehicles but also directly impacts the security and privacy of drivers and passengers. The primary security threats currently faced by automotive Ethernet include cyberattacks, data breaches, data tampering, denial-of-service (DoS) attacks, and system intrusions. Considering the physical environment and functional characteristics of automotive Ethernet networks, this paper proposes a multi-level security architecture to establish a comprehensive protection system. This architecture incorporates security measures at different layers, such as physical layer, data link layer, and application layer security mechanisms. The design of the multi-level security architecture employs various security strategies and technical approaches, including encryption, authentication, machine learning algorithms for establishing normal communication baselines, and intrusion detection.

Keywords: vehicle-mounted ethernet; security threat; multi-level security architecture; security policy

引言

越来越多的电子控制单元 ECU 和摄像头、激光雷达等设备被应用在智能汽车上，这对车内通信的低延迟和可靠性提出了更高的要求，CAN 总线技术的半双工通信模式和有限的传输速率已经难以满足现代汽车网络对高速、实时、双向数据传输的需求[1]，传统的 CAN、LIN、Flex Ray 等车载网络已经不能满足日益增长的汽车智能化和信息传输交互需求，车载以太网为需要实时传输大量数据的复杂汽车系统提供了一种高速可靠的通信解决方案[2]。随着车载以太网的引入，汽车内部的安全威胁和漏洞正在迅速增加[3]，车载网络安全问题成为了一个日益严重的问题[4]。车载以太网或将成为车载网络的重要通信技术[5]。汽车以太网不仅提供高带宽，最重要的是必须提供可靠和安全的通信。安全性重点关注抵御恶意攻击，涉及可用性、完整性及机密性保护。针对上述挑战，本文提出了一种多级安全架构，通过构建多层次防护体系来保障车载以太网免受恶意攻击，为实现汽车智能化提供至关重要的安全保障。

一、汽车以太网

自1980年问世并于1983年由 IEEE 标准化以来，标准以太网被广泛应用在局域网和广域网中，但由于其对噪声和干扰的敏感性，因此并不适合汽车应用。车载以太网的物理层采用博通公司的 BroadR-Reach 技术[6]。标准以太网与汽车以太网的主要区别在于：汽车以太网采用了不同于标准以太网的单双绞线电缆实现全双工通信，并可选择屏蔽或非屏蔽配置。基于100Base-T1和1000Base-T1标准的汽车以太网相比传统 CAN/LIN 线束减轻30% 的重量，不仅降低了能源消耗，还将连接成本减少了

80%，同时具备更强的抗干扰能力，能够更好地应对汽车环境中的各种挑战，可以实现高速传输，包括100Mb/s甚至1Gb/s速度等级[7]。

二、车载以太网面临的网络安全威胁

车载以太网是一种基于以太网技术的网络系统，在车辆内部用于连接各种车载设备和控制单元，实现数据传输和通信。随着涉及安全和隐私的数据（如车辆自动驾驶、车联网和多媒体系统）通过车载以太网传输，潜在的网络攻击和未经授权的访问风险成为一个重大安全问题。重放攻击、中间人攻击、拒绝服务攻击这些传统以太网的攻击手段对于车载以太网一样是成立的。随着车载外部接口增多，车载通信过程中的ECU固件的安全隐患、数据传输过程中的安全隐患也在不断提升。确保其安全性成为一个关键问题。车辆内部传输和交换的大量数据存在未经授权访问、数据泄露和网络攻击的潜在风险。汽车以太网安全方面的任何薄弱环节都可能造成严重的安全或隐私泄露后果。因此，必须实施严格的安全措施，以保护通过汽车以太网总线传输的数据的完整性和机密性。

针对汽车以太网的攻击类型有四种：网络访问、流量机密性、流量完整性和DoS攻击[8-9]。在网络访问攻击中，黑客首先通过交换机的不安全端口建立连接，进而尝试入侵以车载以太网网络。攻击者的最终目标是取得网络控制权，实现对多个节点的操控或远程接管整个网络。当实施流量机密性攻击时，攻击者先渗透进入网络，通过监听窃取网络中的通信内容。流量完整性攻击则类似于中间人攻击方式，通过将数据流量重定向至被感染的节点来篡改信息，具体可分为会话劫持和重放攻击两种形式。车载以太网中的DoS攻击，主要分为两种类型：第一种是攻击者直接破坏以太网基础设施，通过物理手段损毁链路或硬件使其完全瘫痪；第二种则被称为资源耗尽攻击或基于协议的DoS攻击，攻击者通过消耗系统关键资源来达成破坏目的。

三、车载以太网的多层安全架构

随着汽车网络面临的内外部通信安全风险日益严峻，恶意篡改的ECU不仅会引发车辆安全隐患，更可能导致整车控制权被远程接管，严重威胁驾乘人员生命安全。为应对这一挑战，ISO与SAE联合制定并发布了ISO/SAE 21434标准，为行业提供网络安全规范指导。在此背景下，网络安全措施已成为汽车设计的核心要素。2021年1月，欧盟正式实施两项新法规：UN-R155（网络安全管理体系及车辆型式认证）和UN-R156（车辆软件升级管理体系及车辆型式认证）[10]，进一步强化了汽车网络安全监管要求。要求个人汽车，货车，公共汽车能够有效的针对黑客攻击的防护。我国制订的国家标准GB/T 38628-2020《信息安全技术—汽车电子系统网络安全指南》，该标准规定了系统性地构建了汽车电子系统网络安全的整体架构。该标准适用于指导整车厂、零部件供应商、软件供应商、芯片供应商以及各种服务提供商等汽车电子供应链上各组织机构开展网络安全活动，指导相关人员在从事汽车电子系统的设计开发、生产、运行和服务等过程中满足基本的网络安全需求[11]。

针对车载以太网面临的安全挑战，需要构建一个系统化、分层次的纵深防御体系。本文提出的四级安全防护架构采用递进式保护策略，通过层层设防的方式有效抵御各类网络安全威胁。

第一级“网络访问控制”作为防护体系的基础，通过严格的网络边界管控和访问限制，构筑起第一道安全屏障。该层级采用物理隔离、VLAN划分等技术手段，最大限度阻止攻击者渗透进入车载网络系统。禁止ECU直接访问外部网络，而是统一通过中心网关对外网访问。实践表明，仅这一级防护就能阻断90%以上的常规网络攻击。

第二级“安全通信保障”通过加密算法、访问控制和完整性检测[12]等机制保证所有安全关键信息的保密性和真实性。当攻击者突破第一级防护时立即发挥作用。基于国密算法的车载以太网控制器身份认证方法[15]和硬件安全模块(HSM)的加密体系，能够有效防止通信数据被窃取或篡改。例如采用范晶晶[13]等设计的基于动态密钥的车载以太网安全通信方法。

第三级“数据应用管控”则从业务逻辑层面提供防护。通过基于上下文的数据验证和使用策略，确保敏感操作只能在特定条件下执行。例如，关键ECU的固件更新必须满足车速为零、点火开关处于特定状态等多重条件才能进行。

第四级“异常监测处置”作为安全体系的最后防线，通过实时监测网络流量和行为模式，利用深度学习算法的入侵检测系统[14]，一旦发现攻击迹象，系统将自动触发防御机制，包括隔离攻击源、重置安全会话、告警通知等响应措施，同时修复前三级防护可能存在的安全漏洞。

级别1：限制对网络的访问

车载网络应采用集中式安全网关架构，限制对外链接ECU的数量，通过统一的网关节点管理所有内外网通信。该网关集成防火墙、入侵检测、协议转换等核心安全功能。不仅要限制内部和外部的通信，并且内部的通信也要限制访问，例如车载信息娱乐系统和动力总成间的通信也是要被隔离起来的。外部同内部、内部间的数据通信都通过车载网关，因此要防范交换机被攻击，针对交换网络的攻击方式主要有Mac层攻击、Vlan攻击、欺骗攻击等。例如防范地址泛洪攻击在数据链路层采用静态的以太交换表转发表和ARP表。内部设备也需要进行身份验证和授权管理，关闭限制或未授权的端口[15]。

表1安全措施

安全策略		具体措施	
网络分区隔离	关键系统实施物理隔离	按功能域划分安全区域	采用VLAN技术实现逻辑隔离
通信管控策略	通信方严格限制跨域通信	信息娱乐系统与动力系统强制隔离	所有通信必须经网关审查
交换网络安全防护	防范MAC欺骗、VLAN跳跃等攻击	配置静态ARP表和MAC地址绑定	实施端口安全管理和访问控制

级别2：安全的机载通信

运用密码学来保证数据的完整性、保密性。主要涉及到密码的生成，存储，会话密钥的分发，密钥生命周期管理。针对车载设备的计算能力和带宽的限制，采用高效的混合加密体系。采用加解密速度快优势的 AES 等对称加密算法处理业务数据，满足车载设备的快速响应的要求。对称秘钥的密钥分发对安全性至关重要，需要利用 ECC 椭圆曲线机密算法或国密 SM2算法的非对称密钥技术对对称密钥加密，具有计算速度快、资源消耗低的优点。密钥的设计应用原则要遵循不同的功能使用不同密钥，并且密钥要有一定的有效期，从而减小收到损害的风险面。通过 HSM 硬件安全模块保障密钥安全。采用动态密钥更新策略，定期轮换会话密钥，单点泄露不影响其它节点通信安全，通信完整性通过 HMAC 消息认证，并且采用时间戳防重放攻击。

级别3：应用数据使用策略

车载系统需要建立严格的数据使用策略，通过多重验证确保安全性。系统会对车辆状态（如车速、挡位）和传感器数据进行实时检测，只有符合条件的数据才会被处理。关键操作设有执行门槛，仅在特定应用程序状态下接受控制命令，比如 ECU 升级必须满足停车、电压稳定等条件。系统还会评估数据可信度和有效性，对可疑数据采取警告、限制或阻断等分级措施。以 ADAS 系统为例，必须同时满足行驶状态、传感器数据一致等条件才会处理数据。这种策略既防范了攻击，又保证了系统正常运行，实现了安全与性能的平衡。

第4级：检测异常并防御

第四级防护采用实时监测与动态防御机制，持续分析网络通信行为特征。系统通过机器学习算法建立正常通信基线，实时检测报文周期异常、认证失败激增等异常模式，能够有效识别 DoS 攻击等威胁行为。当检测到安全事件时，系统启动分级响应机制。针对网络层攻击，自动阻断恶意端口并实施流量控制；在系统层面，立即更新加密密钥并强化认证流程；对于应用层风险，则采取功能降级等保护措施。系统根据威胁等级实施差异化响应：记录初级异常事件，限制中级威胁访问权限，对严重攻击执行完全隔离。防御体系包含自动恢复功能，可快速修复网络配置、重建安全会话。这种智能化的主动防护系统通过持续监控、实时分析和自动处置，形成完整的安全闭环，显著提升车载网络的抗攻击能力，确保关键业务持续可用。

表2多级安全架构提供的保护有效性

级别	可用性	完整性	保密性
1	Yes	Yes	Yes
2	No（DoS攻击）	Yes	Yes
3	No（DoS攻击）		No(窃听)
4	Yes	Yes	No(窃听)

四、总结

针对车载以太网的安全威胁分析，通过这种层层递进的多级防护架构，通过防御纵深的构建，为车载以太网提供了可用性、完整性和机密性的全面保障。各级防护既相对独立又协同配合，即使某级防护被突破，后续层级仍能提供有效保护，显著提升了车载网络系统的整体安全性。

参考文献

[1] 安富利 . 车载网络的新趋势——车载以太网 [J]. 软件和集成电路 ,2024,(08):15-17.DOI:10.19609/j.cnki.cn10-1339/tn.2024.08.003..

[2] 呼布钦，秦贵和，刘颖，等. 下一代汽车网络：车载以太网技术现状与发展 [J]. 计算机工程与应用，2016,52(24):28-36.

[3] 邬江兴 . 智能网联汽车内生安全问题与对策 [J]. 重庆邮电大学学报 (自然科学版),2023,35(03):383-390.

[4] 李玉峰，陆肖元，等 . 智能网联汽车网络安全浅析 [J]. 电信科学 ,2020,36(4):36-45.

[5] 安富利 . 车载网络的新趋势——车载以太网 [J]. 软件和集成电路 ,2024,(08):15-17.DOI:10.19609/j.cnki.cn10-1339/tn.2024.08.003.

[6] 孟祥坤，张起朋，张宏伟 . 车载以太网技术发展与测试方法研究 [J]. 汽车电器 ,2019,(05):40-44.DOI:10.13273/j.cnki.qcdq.2019.05.012.

[7] 李志涛 . 车载以太网系统测试的研究与分析 [J]. 汽车电器，2019(10):9-12.

[8] 李泽华 . 汽车车载网络信息安全风险评估与防护策略 [J]. 汽车测试报告 ,2024,(11):89-91.

[9] 郗来乐，林声浩，王震，等 . 智能网联汽车自动驾驶安全：威胁、攻击与防护 [J]. 软件学报 ,2025,36(04):1859-1880.DOI:10.13328/j.cnki.jos.007272.

[10] 丁宜 .T ü V 莱茵获邀出席中国国际汽车零部件大会 [N]. 机电商报 ,2023-12-25(A03).DOI:10.28408/n.cnki.njdsb.2023.000579.

[11] 全国信息安全标准化技术委员会 (SAC/TC 260). 信息安全技术　汽车电子系统网络安全指南 :GB/T 38628-2020[S]. 中国标准出版社 ,2020.

[12] 钟鑫豪，文健峰，王坤俊，等 . 一种基于车载网络安全的监测策略研究 [J]. 客车技术与研究 ,2024,46(06):5-10.DOI:10.15917/j.cnki.1006-3331.2024.06.002.

[13] 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.

[14] 章意 .AUTOSAR 框架下车载系统入侵检测研究 [D]. 成都信息工程大学 ,2023.DOI:10.27716/d.cnki.gcdxx.2023.000006.

[15] 郭辉，罗勇，郭晓潞 . 基于国密算法的车载以太网控制器身份认证方法 [J]. 网络与信息安全学报 ,2022,8(06):20-28.

