一种基于车载网络安全的监测策略研究

钟鑫豪[1,2]，文健峰[1]，王坤俊[1]，郑志敏[1]，汪 帆[1,2]
（1. 中车时代电动汽车股份有限公司，湖南 株洲 412007；2. 中车科技创新有限公司，北京 100080）

摘 要：随着 5G 和人工智能的普及，汽车正朝着更加智能化和网联化的趋势发展，车载网络与通信网络也变得愈加复杂。本文介绍常见的网络攻击形式和风险点，并提出一种基于车载网络安全的监测策略，对车载网络受到的攻击作出相应的监控、分析和处置。

关键词：智能网联汽车；车载网络；安全监测
中图分类号：U463.6；TN915.08 **文献标志码**：A **文章编号**：1006-3331(2024)06-0005-06

Research on a Monitoring Strategy Based on Vehicle Network Safety

ZHONG Xinhao[1,2], WEN Jianfeng[1], WANG Kunjun[1], ZHENG Zhimin[1], WANG Fan[1,2]
(1. CRRC Electric Vehicle Co., Ltd., Zhuzhou 412007, China;
2. CRRC Technology Innovation Co., Ltd., Beijing 100080, China)

Abstract: With the popularity of 5G and artificial intelligence, vehicles are developing toward a more intelligent and networked trend, and the vehicle and communication networks are becoming more complex. This paper introduces the common forms and risk points of network attacks and proposes a monitoring strategy based on vehicle network safety to monitor, analyze, and deal with them.

Key words: intelligent connected vehicle; vehicle network; safety monitoring

ECE R155/R156 法规于 2021 年颁布。其中，ECE R155 是全球首个汽车信息安全强制性法规，其主要内容涉及整车厂在信息安全及其管理体系(CSMS)方面的执行要求，标志着车辆的信息安全已经从符合标准[1-2]的阶段进入到遵从法规的新阶段；ECE R156 则针对软件升级及其管理系统(SUMS)。为此，我国汽车信息安全标准工作组已经开展了 16 项相关标准的制定工作[3-4]，其中 GB 44495—2024《汽车整车信息安全技术要求》[5]和 GB 44496—2024《汽车软件升级通用技术要求》[6]分别参考 ECE R155 和 R156 进行编制，目前已正式发布，预计 2026 年 1 月开始实施。

1 车载网络类型及网络威胁分析

1.1 车载网络架构演变及分类

车载网络，即汽车网络系统，是由汽车内部传感器、控制器和执行器等构成的，采用点对点连接方式的通信网状结构。由于汽车内部的传感器和执行器又与汽车的电子电气架构密切相关，因此车载网络系统和电子电气架构紧密相连，这两者共同构成了汽车的电子控制系统和数据处理系统。本文仅论述车载网络。

电动汽车电子电气架构包括整车控制器、电机控制器、电池管理系统等重要零部件以及 ECU 单元，而车载网络则充当了连接这些零部件和单元的桥梁。因此，车载网络的通信类型和结构取决于汽车电子电气架构中各零部件和各 ECU 单元的带宽时延需求和分域布置。随着汽车技术的不断发展，电气化、智能化、网联化的水平日益提高，汽车所拥有的电子控制单元(ECU)类型和数量越来越多，导致车载网络变得越来越复杂[7]。

行业普遍认为，与车载网络紧密相连的汽车电子

收稿日期：2024-07-18。
第一作者：钟鑫豪(1996—)，男，硕士；助理工程师；主要从事车辆信息安全及电池大数据安全相关工作。E-mail：615508331@qq.com。

电气架构的发展过程包括三个主要阶段，依次为分布式、域集中式和中央集成式。每个主要阶段又细分为两个小阶段，从而形成了六个细分阶段，分别是模块化、集成化、集中化、域融合、车载电脑以及车-云计算。随着汽车功能的集成化和区域化，以及通信网络的高速化，汽车主要控制器的性能不断提升，数量逐渐减少。因此，汽车的电子电气（EE）系统正加速向中央集成式（中央+区域）架构方向发展[8-9]。

而车载网络的类型由电子电气架构的排布决定，具体可分为：基于分布式电子电气架构的车载网络类型、基于域集中式电子架构的车载网络类型、基于中央集成式电子电气架构的车载网络类型。本文主要对基于域集中式电子电气架构的车载网络类型进行网络安全监测与分析。

目前，域集中式是行业内常用的一种电子电气架构。基于域集中式电子电气架构的车载网络的通信主要采用总线网络技术，包括车载 CAN 网络、以太网络、CAN-FD 网络、LIN 网络、FlexRay 网络等。随着智能化和娱乐化功能的不断增多，其对应的零部件对通信带宽的要求越来越高，传统的 CAN 网络通信技术已无法满足高带宽的需求，而以太网通信技术因其带宽高、通用性强等优势，已在一些特殊的节点上被广泛采用。目前，域集中式电子电气架构的车载网络总线主要由 CAN 网络和以太网络等网络组成，如图 1 所示。

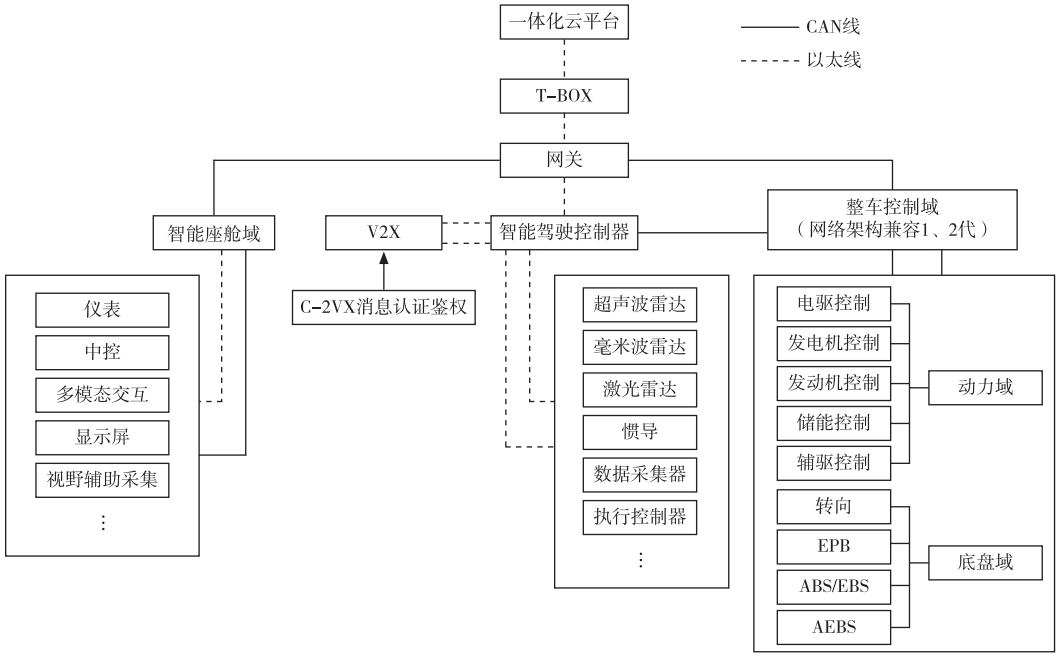

图 1 基于域集中式电子电气架构的车载网络组成图

1.2 车载网络的被攻击风险汇总

图 1 为典型的基于域集中式电子电气架构的车载网络的组成图。从图 1 可以看出，目前智能网联汽车虽然具备了更多功能，但同时也面临着更多的网络安全风险，主要风险来自云端和车端，共包括四个层面，分别是云端层、网络传输层、车载通信层以及外部接口层。这些风险的攻击入口见表 1。

1）云端层。一体化云平台储存并运行着运营车辆的众多信息，能够为相关车辆提供路况信息、车辆调度信息，并具有定位导航、报警以及车辆运营数据上传等功能。云端层虽不属于车载网络，但如果云端平台遭受黑客网络攻击，相关数据被窃取或泄露，也可能会造成严重的影响。本层主要的安全防护技术为网络防火墙和入侵检测防护系统。

2）网络传输层。智能网联汽车主要通过无线网络和车辆 OBD 接口与外界进行通信。在此过程中，车辆与云平台、移动端 APP 以及路侧等设备进行信息数据通信，但同时也面临着数据加密、身份认证和协议确认等安全挑战，从而产生了相应的网络安全风险。本层主要的安全防护技术为分级访问机制、分域

管理、基于证书的传输加密和身份认证。

表 1　汽车攻击入口汇总表

攻击入口	安全风险层	访问方式	攻击目标
OBD 接口	外部接口层	物理访问	ECU CAN 网络 以太网络
车载诊断工具	外部接口层 车载通信层	物理访问 短距离无线访问	ECU CAN 网络
USB	外部接口层	物理访问	ECU
传感器	外部接口层 车载通信层 云端层	物理访问 短距离无线访问 长距离无线访问	ECU 以太网络
ECU	网络传输层 外部接口层 云端层	物理访问 短距离无线访问 长距离无线访问	ECU CAN 网络 以太网络
蓝牙	云端层	短距离无线访问	ECU
蜂窝网络	云端层	长距离无线访问	ECU

3）车载通信层。此层是车载网络的主体。随着智能网联汽车功能的增加，其零部件和 ECU 数量也相应增加。由于整车网络内部的通信主要通过 CAN 线和以太网线传输，导致存在大量 CAN 网络和以太网组成的总线。CAN 总线采用非破坏性总线仲裁方式，具有校验简单、一发多读等特点，但安全防护措施相对薄弱，而以太网因其联网的性质，易被无线攻击手段攻击。攻击者若通过总线网络进行报文重放、拒绝服务、篡改、植入恶意软件等手段攻击，可能会导致驾驶控制指令失效或汽车无法正常行驶。本层主要的安全防护技术为加密算法、访问控制和完整性检测。

4）外部接口层。智能网联汽车拥有多个外部接口，如用于整车诊断和刷写的 OBD 接口，以及一些零部件的独立刷写接口。这些通信接口中，有些直接暴露在车辆外部。若黑客对这些接口进行连接、破解或植入攻击代码，将会对整车网络的安全性构成威胁。本层主要的安全防护技术为身份权限管理、访问控制。

2　车载网络攻击者类型及攻击技术分析

2.1　网络安全攻击者分类

汽车已成为万物互联的关键节点之一，而网络安全问题是智能网联汽车所面临的重大安全风险之一。汽车智能网联程度越高，其网络信息安全风险越大。

攻击者按照其身份分类如下：

1）内部攻击者。通常指具有相应权限的内部工作人员。此类攻击者有车辆厂商或者供应商的内部权限，可以轻易地突破智能汽车网络的安全系统，同时能隐蔽自己的攻击记录，难以被发现。

2）外部攻击者。通常指不具有相应权限的攻击人，如渗透测试人员或者黑客。此类攻击者难以获取相应权限，但可以使用系统中存在的漏洞进行攻击。这类攻击往往会在系统中留下记录，可以被入侵监测系统捕捉到。

这些攻击者或以破坏现有系统的正常运行、使其完全瘫痪为目的，或以持续不断地获取利益为目的。前者的攻击通常持续时间较短，具有突发性，难以预测；后者的攻击具有潜伏性和长期性，难以察觉。

2.2　攻击技术分析

车载网络主要遭受的攻击技术分为本地物理访问攻击和线上远程网络攻击两类。

1）本地物理访问攻击。这种攻击主要通过物理连接方式访问整车网络，常见的攻击手段是从影响整车安全的零部件诊断口进行访问攻击。攻击者通常通过 OBD 接口进行数据监听、数据篡改和拒绝服务攻击。由于当前车载网络缺乏身份认证和完整性验证机制，此类攻击方式的破坏性强且操作简便，是最常见的攻击形式。

2）线上远程网络攻击。这种攻击主要通过智能网联车辆暴露的远程接口进行，如 T-BOX 通信接口、蓝牙、蜂窝网络等。攻击者利用这些远程网络接口渗透到整车网络中，远程对整车进行攻击和控制[10-12]。此类攻击方式具有高隐蔽性、高破坏性，但操作难度较高。

车载网络中，容易受到攻击的目标、采用的攻击技术和方法[13-14]分类见表 2。

表 2 车载网络被攻击分类

攻击目标	攻击技术	具体攻击方法
ECU	ECU 伪装攻击	冒充正常的 ECU 发送消息
	重刷攻击	通过物理连接或者 OTA 方式重复刷写 ECU 上的固件或软件
	CAN 重放攻击	重放车载网络的指令
CAN 网络	CAN 通信漏洞	CAN 通信漏洞
	CAN 消息篡改攻击	冒充正常的 ECU 发送消息
	CAN 消息注入攻击	通过发送恶意或虚假的 CAN 帧,干扰或破坏正常的通信过程
以太网络	拒绝服务攻击	通过发送过多合法请求,超出服务系统的处理能力
	病毒软件攻击	通过注入病毒攻击通信接口的漏洞

3 监测策略设计

本文设计一种针对智能网联汽车的安全监测、风险分析及上报的策略模型,模型架构如图 2 所示。该策略分为三个阶段:数据接收阶段、威胁检测阶段以及威胁分析处置阶段,其中最重要的是威胁检测阶段的模型库分析。

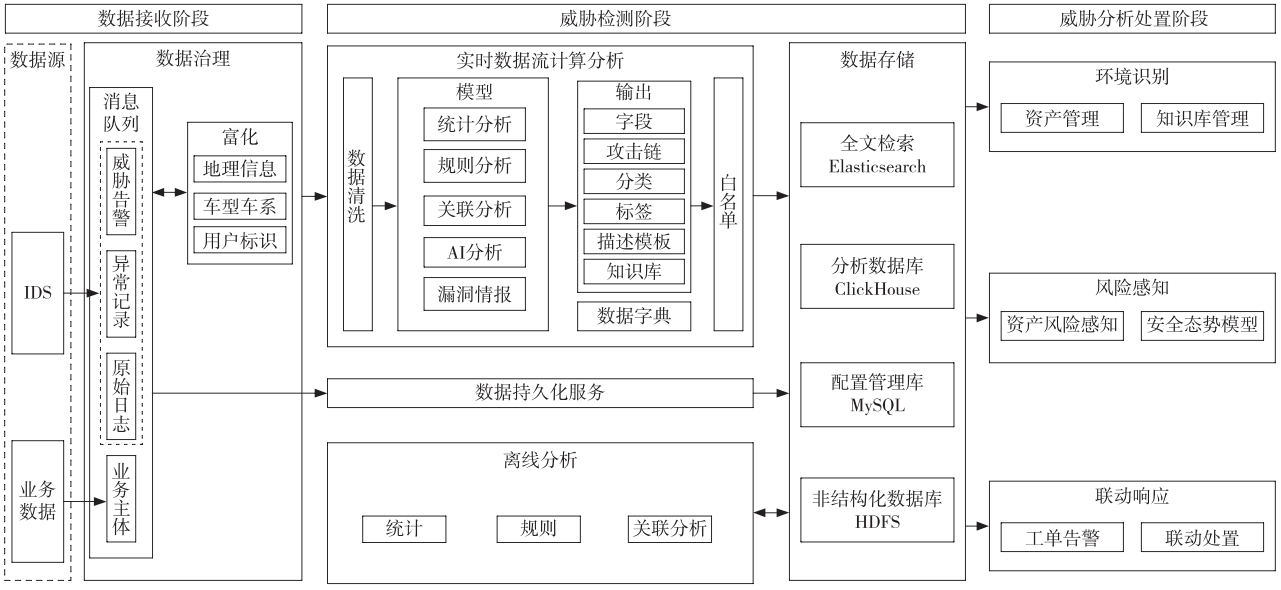

图 2 车载网络监测策略模型架构

3.1 数据接收阶段

该阶段的作用为记录车载网络被攻击时的相关数据。当车辆受到威胁警告、异常记录、原始日志、漏洞警告等消息队列时,进行关键字(包含车型、零部件、用户标识等)匹配,将匹配到的相关数据输入威胁检测阶段。

3.2 威胁检测阶段

此阶段将输入的相关威胁数据进行数据清洗,然后把主要的异常信息输入到已搭建好的模型云平台中,并进行数据对比分析,以确定该异常信息是否为黑客攻击的信号。已搭建好的模型分为以下五类:

1) 统计分析模型。该模型对安全事件、安全行为的特征进行统计分析,量化各类事件和行为的状态、频次、发生周期等数据特征,从而揭示事件数据的分布状况、主要特征、时间序列的趋势性,以及是否存在异常值。此外,统计分析还能汇总事件结果,并通

过阈值过滤识别异常指标，以发现暴力破解、端口扫描等恶意行为。因此，统计分析可直接用于事件性质的判定、解释和决策。

2）规则分析模型。该模型基于规则进行安全威胁检测，通过配置触发规则来筛选日志数据中的异常记录。数据源可以是原始日志也可以是异常记录，规则表达式支持多级嵌套，确保严格限定触发条件。规则分析应输出安全告警的名称、威胁等级、告警类型、攻击链阶段等信息。

3）关联分析模型。该模型通过对多源数据和历史数据进行字段关联和逻辑关联，揭示隐藏在相关事件中的高级威胁和安全风险。这有助于排除安全事件的误报、推论事件源，并重新定义安全事件级别。此外，该模型支持安全事件的横向和纵向关联分析：横向关联分析通过多源数据的关联，结合多设备告警数据和原始数据，发现单点检测无法识别的潜伏性高级威胁；纵向关联分析则通过历史数据的关联，揭示持续性的潜伏威胁。

4）AI 分析模型。AI 学习建模内置时序算法、分类算法、聚类算法等多种集群学习算法原型，能够对任意指标数据进行学习和分析，持续构建并更新基线信息，模型能够通过自适应算法发现异常和偏离，从而增强对未知威胁的检测能力。

5）漏洞情报模型。漏洞信息更新和获取主要通过设置若干个持续更新的漏洞库网址。每两周做一次漏洞库网址的漏洞情报收集，获取到车载网络相关的最新漏洞后，更新此模型，以关键词触发的形式记录未知的威胁及攻击信息。

3.3　威胁分析处置阶段

在完成威胁检测阶段后，策略进入威胁分析处置阶段。该阶段包括环境识别、风险感知以及联动响应三个过程。

1）环境识别过程。该过程实际上是对车载网络中的电子电气架构上的每个 ECU 进行资产评估（指 ECU 包含的数据、系统、网络等各种信息资产的价值）。首先，分析 EE 架构上每个 CAN 线路上的 ECU（如 BMS、EVCC、EBS 等），以确定它们具有被网络攻击的价值，即攻击后可能会造成个人信息的泄露和硬件资产的损失。其次，分析每个 ECU 可能遭受攻击的路径，并将其输出为各自的相关项定义。结合常见的网络安全损害场景以及攻击路径的难易程度和风险值，估算出每个 ECU 的风险等级，这一过程即为威胁分析与风险评估。因此，该过程能有效地判定整个车载网络上 ECU 风险值的高低，为后续的响应和处置方式提供优先级和紧急程度的计划安排。

2）风险感知过程。将经过危险检测阶段识别、匹配和对比后的异常信息，输出至整车网络进行资产（数据、系统、网络和软硬件等）和知识库的环境对比来判断该资产是否有被攻击的风险。若判断为肯定，则对该安全事故进行风险评级，评级过程参照环境识别阶段的风险评估方法进行判定。

3）联动响应过程。在确定了被攻击对象和攻击方法后，对攻击风险等级进行评估，并据此制定响应策略。该过程我司主要参考企标《网络安全持续活动》，针对不同风险等级的网络安全事件，采取相应的对应措施，并对发生的次级安全事故进行评分和风险等级划分。同时制定相应的联动处理机制。评分标准主要参考网络安全保障等级（表 3），对不同风险值的响应紧急程度进行区分。

表 3　网络安全事件响应时间

风险值	响应时间
4-5	24 h 内响应主机厂并完成分析团队组建，48 h 内完成漏洞分析，7 天内完成修复。
2-3	48 h 内响应主机厂并完成分析团队组建，5 天内完成漏洞分析，14 天内完成修复。
1	72 h 内响应主机厂并完成分析团队组建，14 天内完成漏洞分析，90 天内完成修复（如决定修复）。

4　结束语

本文分析了汽车车载网络架构的类型及其网络安全面临的攻击风险及技术，提出了一种基于数据模型库的智能网联汽车的网络安全监测策略。随着汽车智能网络技术的不断进步和车载功能的日益丰富，车载 ECU 和网络接口数量的增加意味着整车将面临更高的网络安全攻击风险。因此，车辆网络安全的检测、防护和处理技术需要不断更新和迭代，以推动汽车网络安全水平不断提升。

参考文献：

[1] 中华人民共和国工业和信息化部. 汽车信息安全通用技术要求：GB/T 40861—2021[S]. 北京：中国标准出版社，2021：2-3.

[2] 中华人民共和国工业和信息化部. 汽车网关信息安全技术要求及试验方法：GB/T 40857—2021[S]. 北京：中国标准出版社，2021：6-7.

[3] 安晖. 加强网络安全保障能力促进智能网联汽车产业健康发展[J]. 智能网联汽车，2021(5)：20-21.

[4] 刘国平，林可春. 智能网联汽车技术与标准发展研究[J]. 内燃机与配件，2024 (9)：132-134.

[5] 中华人民共和国工业和信息化部. 汽车整车信息安全技术要求：GB 44495—2024[S]. 北京：中国标准出版社，2024：4-5.

[6] 中华人民共和国工业和信息化部. 汽车软件升级通用技术要求：GB 44496—2024[S]. 北京：中国标准出版社，2024：3.

[7] 蔡方博，李钰莹. 智能网联汽车信息安全风险研究[J]. 智能网联汽车，2024(2)：72-74.

[8] 袁豪杰，唐刚. 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(1)：60-69.

[9] 李楠. 智能汽车网络安全监控技术的研究与实现[D]. 成都：电子科技大学，2019.

[10] 陈博言，沈晴霓，张晓磊，等. 智能网联汽车的车载网络攻防技术研究进展[J/OL]. 软件学报：1-30[2024-07-17]. https://doi.org/10.13328/j.cnki.jos.007196.

[11] 唐诗华，刘冲，唐旭. 智能网联汽车网络安全与防护方案研究[J]. 汽车测试报告，2023(23)：85-87.

[12] 吴尚则. 基于车载 CAN 总线网络的身份认证方法研究[D]. 长春：吉林大学，2018.

[13] KIM Kyounggon, KIM Jun Seok, JEONG Seonghoon, et al. Cybersecurity for autonomous vehicles: Review of attacks and defense[J]. Computers &Security, 2021(103): 102150.

[14] ALIWA E, RANA O, PERERA C, et al. Cyberattacks and countermeasures for in-vehicle networks[J]. ACM Computing Surveys, 2020(54): 1-37.

(上接第 4 页)

[7] 张聪. 基于鱼眼镜头的车载全景环视系统[D]. 杭州：浙江大学，2015.

[8] 江龙. 360°泊车辅助系统全景成像的研究[D]. 哈尔滨：哈尔滨工业大学，2016.

[9] 许毅立. 基于嵌入式 GPU 全景环视拼接系统的研究[D]. 哈尔滨：哈尔滨工程大学，2018.

[10] 李广云，范百兴. 精密工程测量技术及其发展[J]. 测绘学报，2017，46(10)：1742-1751.

[11] GAO Xiaoshan, HOU Xiaorong, TANG Jianliang, et al. Complete Solution Classification for the Perspective-three-point Problem[J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2003, 25(8): 930-943.

[12] 南方测绘. NTS-352R 技术参数[Z/OL]. [2024-03-25]. http://www.southsurvey.com/product-2929.html.