智能网联汽车网络安全入侵检测关键技术研究

一、研究背景及概述

当前智能网联汽车面临着越来越复杂的网络安全威胁，尤其是恶意的网络攻击。网络攻击利用车辆网络数据传输的脆弱性，通过恶意数据包注入对车辆控制系统进行干扰，可能导致安全隐患甚至交通事故。因此，如何实现对网络攻击的有效精准检测，保障智能网联汽车的安全，成为当前亟待解决的难题。

针对以上问题，课题聚焦智能网联汽车网络入侵检测，提出基于神经网络的高精度网络入侵检测方法。首先，分析了国内外在智能网联汽车入侵检测方面的研究现状。其次，研究了智能网联汽车网络攻击的动态检测方法，建立了基于特征交互的攻击检测模型，利用车载网络报文内的关联关系，提出了特征注意力交叉网络，实现报文特征的多阶交互及攻击数据的准确分类。最后，课题基于构建的数据集验证了所提出方法的有效性。课题基于以上研究成果，在国标《汽车网络安全入侵检测技术要求及试验方法》制定过程中提出了十余条修改建议，优化完善了国标标准技术要求制定。课题研究搭建的测试验证平台可以为国标后期验证试验提供支撑。

二、研究内容

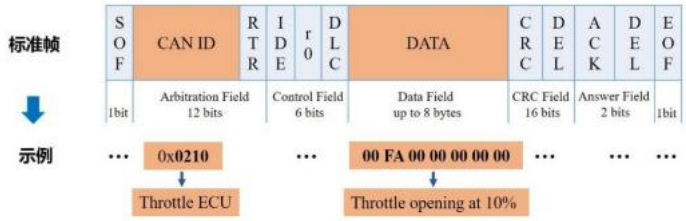
车载网络是车内车外沟通的媒介，是汽车判断自身状态、执行相关运动指令最为关键的途径。然而车载网络在设计之初便缺乏网络安全保护机制，非常容易受到黑客攻击威胁，影响车辆的正常行驶和人员的生命安全。网络注入攻击可以通过入侵车载网络篡改报文或者注入新报文来实现。针对CAN总线报文的攻击检测技术可以有效地保护汽车免受网络注入攻击。现有的基于汽车攻击检测方法仅利用了CAN总线报文中包含的信息，没有考虑不同特征之间的影响，导致检测精度不高、模型泛化能力弱。因此，本章提出了一种基于多特征交互的车载CAN攻击检测模型，分别利用因子分解机和交叉网络-注意力机制得到二阶交互特征与高阶交互特征，以此探索不同特征之间的关系，然后利用集成方法进行攻击检测，可在不对报文进行解析的前提下，实现对攻击的高精度检测。

（一）方法研究思路

常见的车载通信网络主要有局部互联网络（LIN），控制器局域网（CAN），FlexRay、车载以太网（Ethernet）和面向媒体的系统传输（MOST）。CAN凭借其较高的带宽、快速的传输速度和简单的接口设计，成为车载中最常用的网络协议。但CAN在设计之初没有考虑任何相应的网络安全措施，消息数据容易受到网络注入攻击的篡改或产生消息延迟。这些网络攻击不仅会带来隐私泄露和财产损失等潜在风险，而且会危及司机和其他交通参与者的生命财产安全。

CAN 是总线型拓扑结构，节点间采用广播的方式进行通信，节点在接收数据时会与发送方节点同步时间，并根据数据报文的 ID 来选择是否使用。CAN 采用差分信号传输，能有效抵抗电磁干扰。当多个节点试图同时传输数据时，CAN 通过带有冲突避免的载波侦听多路访问（CSMA/CA）和消息优先级仲裁（AMP）进行处理，保证了高优先级报文可以在总线上快速传输。随着车载系统的复杂化和智能化发展，CAN 也面临一些局限和挑战。一是数据传输速率受到限制，标准 CAN 总线的最大速率为 1Mbps，在复杂的车载网络中，无法满足部分高带宽应用的需求。例如，摄像头、雷达和激光雷达等高级驾驶辅助系统（ADAS）产生的数据量远超 CAN 的传输能力，因此通常需要借助以太网等高速通信协议。二是传输信息量少，标准 CAN 帧的数据字段最大只能传输 8 字节，对于需要大数据量的传感器通信来说不够高效。尽管 CANFD 已将数据段长度扩展到 64 字节，但与以太网相比，这一数据长度仍有很大局限。三是具有负载瓶颈，网络负载增加时，CAN 总线的仲裁延迟也会增加，导致实时性下降。特别是在多节点和高流量环境下，高优先级报文可能长期占用总线，影响低优先级任务的执行。CAN 的特点导致其自身的安全性较差，容易受到网络注入攻击的影响。CAN 协议是一种基于消息的广播协议，通过预先定义好的数据帧发送数据。一个数据帧由 7 种不同的位域组成，分别是帧起始（startofFrame，1 位）、仲裁域（ArbitrationField，12 位），CANID、控制域（ControlField，1 位）和用于有效载荷的数

据域(datafield，64 位)、CRC 域(CRCField)、应答域(ACKField)和帧结尾(EndofFrame，1 位)组成。图中展示了 CAN 帧形式和一个实例。

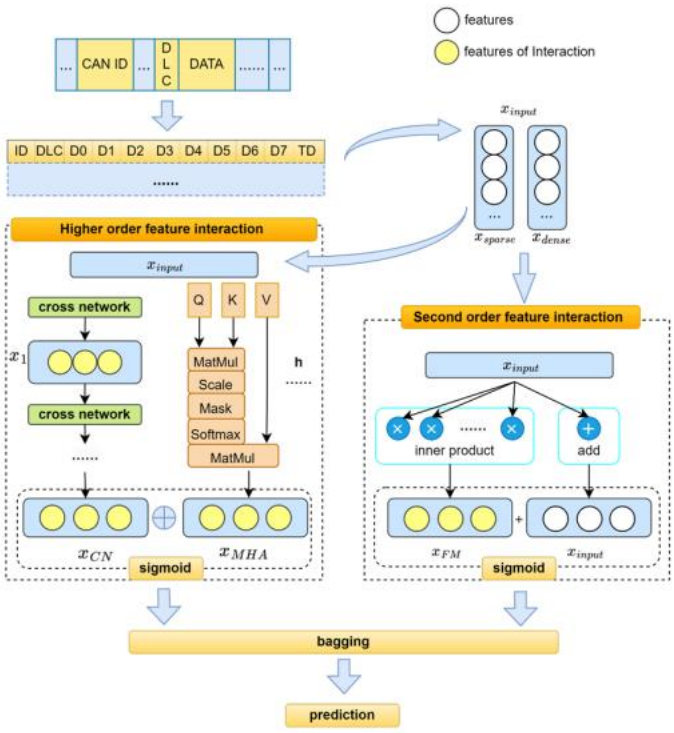


在 CAN 帧中 CANID 和数据域是至关重要的，ECU 接收所有数据帧，通过 CANID 执行命令，同时过滤不感兴趣的帧。CANID 也表示了传输的优先权。例如，如果攻击者伪造或注入高优先级，如 CANID 为 0x000 的数据帧，导致通信阻塞，使得正常的数据不能及时发送和传输，这在驾驶时是非常危险的。值得注意的是，每个 CANID 都有一个特定的时间间隔，该时间间隔将车辆状态信息广播到网络，以保持车辆状态一致。数据域中包含报文携带的信息。数据域分为 8 个字节，每个字节包含两个十六进制值，每个字节的取值范围为’00’到‘FF’,数据域中的每一字节内容都代表特定含义。比如在某款车型 CAN 协议中，CANID=’0210’表示油门控制 ECU 单元，其报文数据域代表了加速踏板开度信号，“00FA0000000000”代表其加速踏板油门开度为 10%。CAN 数据帧具备上下文关联性，因为消息 ID 和载荷数据都与车辆的运行状态密切相关。ECU 通过 CANID 来判断哪些数据帧是其所需的，同时 CANID 还决定了传输的优先级。若大量高优先级数据帧(如 ID 为 0x000 的帧)被注入 CAN 总线，则可能导致正常消息无法及时传输，这在车辆行驶过程中是

极其危险的。相同的数据值在不同车辆的 CAN 协议中可能代表不同的含义，这些差异由车辆制造商决定。尽管如此，数据字段与 CANID 之间的关系能够被推测出来，例如图示例中第二个字节’FA’与 CANID’0210’之间的关联。因此本章进一步探索这些数据帧之间的关联性，任何与预期关系的偏差或新关系的出现都可能指向网络注入攻击。

（二）模型搭建与验证

在分析了以 CAN 总线为例的车载网络协议特点的基础上，课题提出了一种基于多特征交互学习的 IDS 模型，模型架构如图所示。本工作的主要思想是将高维度的车载网络报文特征分成连续变量和类别变量进行处理，分别利用 FM 的方法和特征注意力交叉网络的方法实特征交互。车载网络报文特征对应的向量在特征空间里的关系，实现 IDS 模型的非线性特征建模。然后利用 bagging 方法对得到的特征信息进行判断，进行车载网络的入侵检测。



课题研究搭建的入侵检测数据集、测试环境、车载域控制器及智能网联汽车实车平台等测试验证平台可以为国标后期验证试验提供有力支撑

实车测试平台

本部分内容节选自该课题研究报告，非全部内容，仅供参考了解。