基于关联规则与离群点的新能源汽车动力域入侵检测

余辰熠[1]，魏洪乾[1,2]，张幽彤[1]

（1. 北京理工大学 机械与车辆学院，北京 100081；2. 汽车测控与安全四川省重点实验室，成都 610039）

摘 要：为提高新能源汽车动力域中针对篡改攻击的入侵检测系统效果，建立包括关联规则检测和离群点检测的动力域防护模型，通过实车采集固定工况下的动力域报文数据，基于关联规则算法建立规则库检测篡改攻击；在关联规则检测的基础上通过离群点检测，检测复杂类型的篡改攻击。仿真结果表明，该方法相比于传统的关联规则方法检测准确率提高5.83%，能有效检测针对新能源汽车动力域的篡改攻击。

关键词：动力域；篡改攻击；入侵检测系统；关联规则；离群点检测

中图分类号：U461.91 **文献标志码：**A **DOI：**10.3969/j.issn.2095-1469.2024.03.09

Intrusion Detection in New Energy Vehicle Power Domains Based on Association Rules and Outlier Detection

YU Chenyi[1]，WEI Hongqian[1,2]，ZHANG Youtong[1]

（1. School of Mechanical and Vehicular Engineering，Beijing Institute of Technology，Beijing 100081，China；
2. Vehicle Measurement，Control and Safety Key Laboratory of Sichuan Province，Chengdu 610039，China）

Abstract: To improve the effectiveness of intrusion detection systems against tampering attacks in the power domain of new energy vehicles, a power domain protection model is established, including both association rule detection and outlier detection. By collecting the power domain messages from the actual vehicles and establishing a rule base using the association rule algorithm, this model aims to detect tampering attacks. On the basis of association rule detection, complex types of tampering attacks are identified through outlier detection. The simulation results show that this method improves the detection accuracy by 5.83% compared to traditional association rule methods, effectively detecting tampering attacks in the power domain of new energy vehicles.

Keywords: automobile power domain; tampering attacks; intrusion detection systems; association rules; outlier detection

随着汽车的智能网联化发展，车载网络信息安全问题不容忽视。非法的攻击者能通过WIFI、蓝牙、OBD接口等途径入侵到汽车的内部网络，如汽车总线网络（汽车动力控制系统）等，影响汽车的

收稿日期：2023-03-21 改稿日期：2023-04-19 网络首发日期：2024-03-28

参考文献引用格式：

余辰熠，魏洪乾，张幽彤．基于关联规则与离群点的新能源汽车动力域入侵检测[J]．汽车工程学报，2024，14(3)：412-421.

YU Chenyi，WEI Hongqian，ZHANG Youtong．Intrusion Detection in New Energy Vehicle Power Domains Based on Association Rules and Outlier Detection[J]．Chinese Journal of Automotive Engineering，2024，14(3)：412-421.(in Chinese)

行驶安全。当前针对汽车内部网络的安全防护手段主要有通信数据加密，安全通信协议，异常入侵检测技术等。相比于加密技术、通讯协议的制定，入侵检测方法更容易在已有的汽车ECU上实现。目前主流的入侵检测方法主要有如下几个方向：基于特征提取的检测方法、基于信号的入侵检测方法、基于机器学习的身份识别方法等。基于特征的检测方法中，用于实现攻击类型研究的网络特征主要有车载ECU物理特征信号（通常被称为指纹特征）、时钟偏移、频率特征、远程帧等[1-4]。提取攻击数据特征[5]方法受攻击模型影响，不一定适用于实车情况；基于信号的入侵检测利用信息理论的方法，例如引入信息熵概念，应用于低成本车载网络入侵研究中[6]。MÜTER等[7]首次将信息熵这一信息论名词带入车载网络安全研究中。WU Wufei等[8]提出一种定量的滑动窗口策略。于赫等[9]基于理论和试验两方面表明了使用信息熵的车载CAN总线信息安全研究和入侵监听方法对重放、泛洪等不同入侵方式的检查有效性，但该方法容易受到汽车不同状态的异常熵值抖动影响。

基于机器学习、神经网络的新兴方法中，宋和春[10]用梯度提升决策树（GBDT）分类模型处理ECU电压数据进行身份识别，KANG等[11]提出一种基于深度神经网络（DNN）的新车载网络安全保护方法，KHAN等[12]开发了一种基于长短时记忆的神经网络模型，用于检测重放攻击和幅度变换攻击。但这些方法复杂度高，带宽消耗大。

动力域作为汽车动力和操控功能核心的域控系统之一，其通信安全值得重点关注[18]。一般而言，新能源汽车动力域集成部分整车控制器、车载充电机、电机控制器等组件的控制功能[19]，并和外部接口相连，其中的信息包含各动力单元的相关控制和状态信息，如驾驶控制指令、电机转速、车速等。与信息娱乐域等舒适系统不同，动力域通信需求不高，因此采用的异构芯片算力较低；动力域内部主要通过CAN总线通信，缺乏认证手段，很容易实现报文监听，可能的攻击包括DoS攻击、大流量注入攻击、重放攻击、篡改攻击，前三者可以通过检测报文ID、周期等基本特征实现防护，而篡改攻击通过更改某条报文的数据段信息实现异常入侵行为，它不会更改原始报文的收发频率和工作ID值。当前汽车防护系统很难通过基于频率或基于身份学习的方法识别极其隐秘的篡改攻击行为。因此，如何根据动力域内部的通信数据设计汽车安全防护策略成为汽车信息安全的核心工作。

通常，控制系统的核心数据之间存在一定的关联性。比如，离群点检测在数据分析领域中用于获取异常数据，能实现入侵检测、医学诊断[15]等，根据邻近数据的相似或者相异程度度量[16]评估数据关系。然而，篡改攻击发生时却会违反动力域相关信息的关联规则。因此，根据动力域内的报文信息设计合理的关联规则，探究不同报文的关联程度和合法程度，即可以评估当前接收报文的合法性，从而确定当前汽车的动力域系统是否遭受到非法的篡改攻击行为。

从以上角度出发，本文研究了基于关联规则和离群点检测的动力域篡改攻击入侵行为检测技术。首先采用关联规则算法获取离线数据的关联性，然后建立关联规则库，接着在规则库的基础上引入基于距离的检测算法，最后基于阈值[17]的离群点检测计算用于判断连续时间序列的数据是否存在偏移明显的离群点。该检测方法所需资源少，适用于动力域信息环境，能检测不违反关联规则的复杂类型篡改攻击。

本文从挖掘动力域信息之间关联规则和离群点检测的角度，提出基于动力域信息的入侵检测方法。

本方法的创新点如下：采用新的关联规则算法，减少计算循环次数，且能在扩充训练集时实现增量数据合并而不需要重新计算；在规则总结中细化规则分类；在规则检测的基础上进行离群点检测，能检测同时篡改关联数据的复杂攻击，提高入

侵检测的准确率。试验采用实车数据构建攻击场景，最终实现入侵检测，说明该方法在实车上具备执行条件，具有一定的应用性。

1 关联规则和离群点检测

1.1 关联规则相关概念

关联规则描述数据库中不同类别数据间的关系[13]，通常认为具有高频次相关性的项集之间存在内在关联性。

关联规则算法中的基本定义如下。

定义 1：设 I=｛i_1，i_2，…，i_m｝是一个全局项的集合，其中 i_j（1≤j≤m）是项（item）的唯一标识，j表示项的序号。

事务数据库（Transactional Databases）D=｛t_1，t_2，…，t_n｝是一个事务（Transaction）的集合，每个事务 t_i（1≤i≤n）都对应 I 上的一个子集，其中 t_i 是事务的唯一标识，i表示事务的序号。

定义 2：由 I 中部分或全部项构成的一个集合称为项集（itemset），任何非空项集中均不含有重复项。如 I_1=｛i_1，i_3，i_4｝是一个项集。I_1 中项的个数为 k 个，则称 I_1 为 k–项集。

项集在数据库中的支持度是包含该项集的事务在数据库中的出现概率，计算式为：

$$\text{Support}\{A \rightarrow B\} = P(A \cup B)。 \tag{1}$$

n 为总数。设定项目的最小支持度，称为最小支持度阈值，小于该阈值的项目类型将会在计算中被忽视。项集的支持度大于或等于 min_sup，则称其为频繁项集（Frequent Itemsets）。

Confidence（置信度）：表示当 A 项出现时 B 项同时出现的频率，记作｛A→B｝，计算式如下：

$$\text{Confidence}\{A \rightarrow B\} = \frac{P(A \cup B)}{P(A)}。 \tag{2}$$

两个关键指标，即支持度（Support）和置信度（Confidence），前者反映某个数据类型在总数据中出现的次数，后者反映两个不同类型的数据之间存在关联的可能性。

为实现合理的规则过滤，采用相关性系数（又叫提升度）这一指标判断二者的相关性。

Lift（提升度）：指 A 项和 B 项一同出现的频率，但同时要考虑这两项各自出现的频率。其计算式为：

$$\text{Lift}\{A \rightarrow B\} = \frac{P(B|A)}{P(B)} = \frac{P(A \cup B)}{P(A)*P(B)}。 \tag{3}$$

1.2 离群点检测算法相关概念

离群点指一个时间序列中显著偏离正常数据的异常值。经典算法 LOF 的思想是：通过某个数据在其邻域范围内的函数分析该点是否属于异常点，如果样本点附近的样本密度小于平均值，则该点有可能为异常离群点。离群点检测采用基于密度、距离等参数的检测方法，部分相关定义如下。

定义 1：dist（d_i，d_j）：表示数据点 d_i 到 d_j 的欧式距离。

定义 2：k 距离，按大小排序后，数据点 i 到第 k 个数据的距离。

定义 3：可达距离，数据点 r 的 k 距离和数据点 d 到 dr 间距中的最大值。

其中数据点 d_i 和 d_j 的欧式距离为：

$$\text{dist}(d_i, d_j) = \sqrt{\sum_{k=1}^{n}(x_{ik} - x_{jk})^2}。 \tag{4}$$

式中：x_{ik} 和 x_{jk} 分别为两个数据点的距离。

2 入侵检测方法流程

2.1 建立入侵检测模型

根据动力域平台特征和报文信息特征，构建针对动力域报文信息的安全防护模型，该模型融合协议分析、频繁项集挖掘、规则评价等不同技术。图 1 为模型的整体结构。第 1 部分为基于报文特征的基本规则检测，特征包括报文 ID、周期、长度检测，这部分能实现对 DoS 攻击、大流量注入攻击和重放攻击的防护；第 2 部分为对关联性数据的规则检测，实现对篡改单一数据攻击的检测；第 3 部分为本文研究的重点，基于关联规则的离群点检测实现对篡改攻击的复杂规则检测。

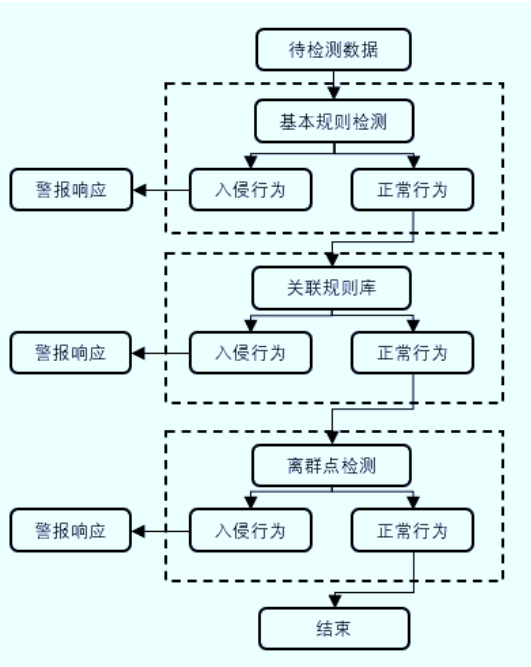


图 1　入侵检测模型

2.2　建立关联规则库

建立规则库需要生成强关联规则，有 3 个步骤：数据预处理、频繁项集挖掘、关联规则生成，图 2 为模型生成关联规则的流程。使用关联规则算法流程为：归一化处理报文数据，采用特征分箱的策略处理动力域的连续数据；根据支持度（Support），采用关联规则算法在数据库中发掘具有频繁特性的数据类型，如果需要扩展原有数据库则采集新数据，和原有数据合并，最后根据先验经验从频繁项集中生成关联规则；根据置信度（Confidence），从上述关联数据的集合中发掘具有高频次同步出现特点的相关数据集合，基于评价指标提升度（Lift）总结有效的强关联规则，并对规则分类。根据提升度（Lift）从上述规则中分析获取符合实际的有效关联规则。提升度>1 认为有关联，>3认为值得关注。

传统关联规则算法 Apriori 算法的核心规则在于：若 A 是一个频繁项集，则 A 的每一个子集都是一个频繁项集。通常的做法是统计各个项的数量，设定最小支持度，找出所有频繁 1-项集，然后在其中找出频繁 2-项集，以此类推。该算法适用小型数据库，在执行过程中产生大量冗余的中间频繁项集，本文采用 FP-growth 算法 [14] 构建 FP 树，将原有的表格数据映射到多分支的树状结构中，整个数据库的扫描次数由复杂的 k 次减少到 2 次，减少计算循环次数，且能在扩充训练集时实现增量数据合并而不需要重新计算；传统算法只能挖掘线性正相关规则，本文考虑负相关关联规则和非线性关联规则，提高规则检测的准确度。

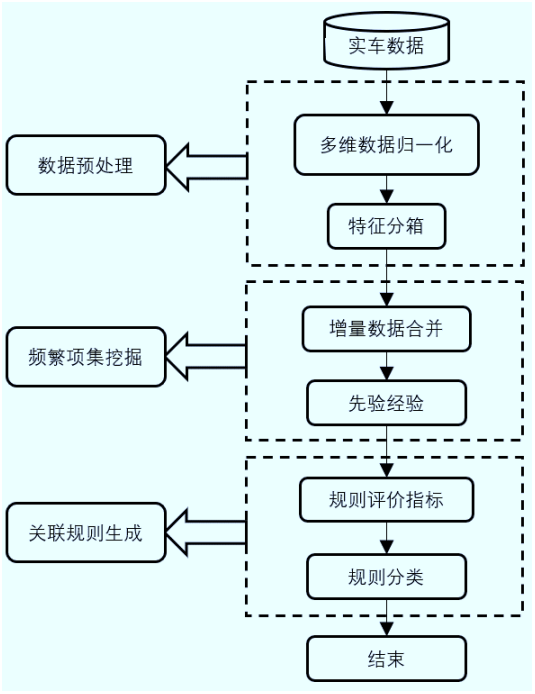


图 2　关联规则生成流程

传统关联规则算法只适用挖掘线性正相关的关联性，对其余类型的关联规则缺乏重视，频繁项集挖掘后，根据规则评价可以获得正相关关联规则、负相关关联规则、非线性相关规则。

对于存在负相关性的数据，其计算逻辑和正相关类似，数据处理中可以利用已有的先验相关性降低计算成本，其计算式为：

$$\text{Confidence}\{\text{A}\rightarrow\bar{\text{B}}\}=\frac{P(\text{A}\cup\bar{\text{B}})}{P(\text{A})}。\tag{5}$$

$$\text{Lift}\{\text{A}\rightarrow\bar{\text{B}}\}=\frac{P(\bar{\text{B}}|\text{A})}{P(\bar{\text{B}})}=\frac{P(\text{A}\cup\bar{\text{B}})}{P(\text{A})*P(\bar{\text{B}})}。\tag{6}$$

2.3　离群点检测阈值计算

复杂篡改攻击同时改变具有关联性的数据，在不违反关联规则的前提下实现入侵，同时篡改多组数据，使动力域信息在篡改处产生明显变化形成明显的离群点。动力域信息有明确的时间戳，通过计

算局部离群点和邻域数据的欧氏距离，根据数据点 d_i 的欧式距离的变化设置用于检测离群点的阈值，大于阈值的视为异常信号。

图 3 为模型离群点检测流程，基于强关联规则的相关数据对测试集的数据进行基于距离的离群点检测计算，根据各关联规则的邻近数据相异度量值获得阈值，高于阈值的视为异常入侵信号。

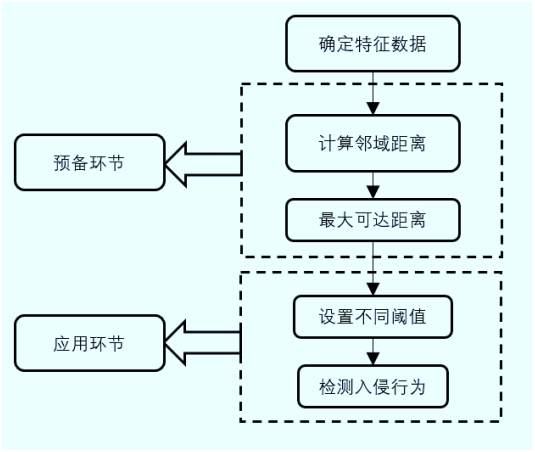


图 3 离群点检测流程

3 动力域信息分析

3.1 测试数据介绍和预处理

报文采集自图 4 车型，其中动力域的有效信号约 56 万条，根据协议解析，部分相关数据如图 5 所示。因为实际报文的周期不同，因此不同信号需要归一化处理，变成单一时间窗口内的一组事务，事务中的每项对应实车信号，包括挡位、踏板、电机转矩、车速等。

在不考虑 CAN 协议中的保留位、功能开关的状态位、警示位的前提下，选取动力域相关信息，见表 1～5，每个信号按照顺序编号 A 到 N。

3.2 关联规则挖掘

对数据执行频繁项集挖掘获得关联规则，并通过规则评价筛选有效的强关联规则。挖掘的规则可以分为以下 3 类：正相关关联规则、负相关关联规

表 1 驾驶状态信息（A、B、C、D、E）

信号名	总线数据	定义解释	信号解释
VCU_Ang_Stat_ PhysicsAccPedal（编号 A）	0～255	加速踏板物理位置 范围：0～100	单位：%
VCU_Ang_Stat_ RealAccPedal（编号 B）	0～200	实际表现加速踏板开度 范围：0～100	单位：%
VCU_Flg_Stat_ BrakePedal（编号 C）	0～3	制动踏板开关信号	0：释放 1：踩下 2：保留 3：异常
VCU_Dig_Stat_ PhysicsGear（编号 D）	0～15	挡位物理位置	0：D 挡，1：R 挡，2：N 挡，3：P 挡，4～15：无效。
VCU_Dig_Stat_ RealGear（编号 E）	0～15	实际表现挡位位置	0：D 挡，1：R 挡，2：N 挡，3：P 挡，4～15：无效。

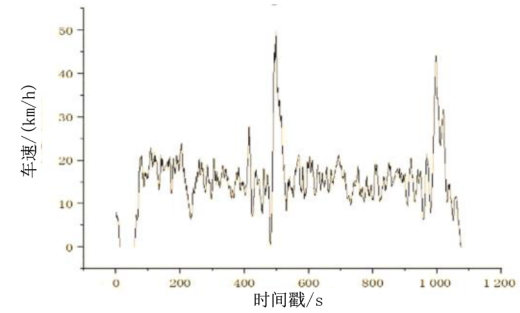
表 2 电机控制信息（F、G、H）

信号名	总线数据	定义解释	信号解释
can_num_MotorTq_req（编号 F）	0～10 000	电机转矩请求 单位：Nm 精度：0.1 范围：−500～500	电机转矩请求
can_num_MotTorque （编号 G）	0～10 000	电机当前转矩 单位：Nm 精度：0.1 范围：−500～500	电机当前转矩
can_num_MotSpeed（编号 H）	0～40 000	电机当前转速 单位：r/min 精度：1 范围：−20 000～20 000	电机当前转速

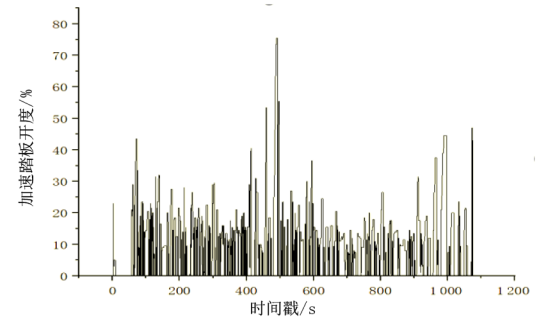
表 3 EPS 状态信息（I、J、K）

信号名	总线数据	定义解释	信号解释
EPS_Ang_Stat_SteeringTorque（编号 I）	0～255	方向盘力矩	单位：Nm
EPS_Ang_Stat_SteeringAngle （编号 J）	−7 799～7 799	转向角信号	有符号数 单位：(°)
EPS_Ang_Stat_SAS_SteeringRotSpd（编号 K）	0～254	转向角速度信号	单位：(°)/s

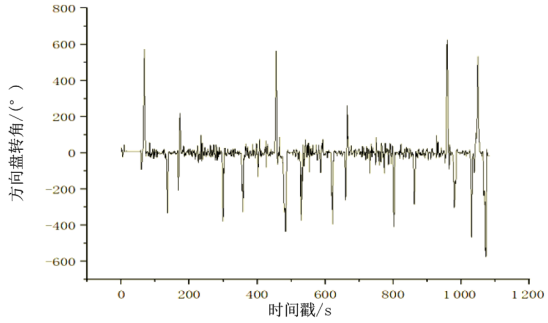
图4　测试所用的实车



（a）



（b）



（c）

图5　部分相关信号

则、非线性相关关联规则。其中正相关的关联规则按照信号特征又被分为物理信号和实际信号关系、因果关系两种。

3.2.1　物理信号和实际信号关系的正相关关联规则

物理信号和实际信号的关系是驾驶行为请求信号和动力域组件响应信号的表现。以加速踏板物理位置和实际表现开度为例，基于特征分箱的思想，信号 A 分为等距的 A1、A2、A3。在该处理策略下，计算各子项之间的频繁项集以及相关置信度、提升度。计算结果见表6。数据涉及物理信号和实际信号的关联性。

3.2.2　因果关系的正相关关联规则

在实际驾驶行为中，部分信息存在因果关系。设置前项为在时序上具有相对高优先级的信号。

以待处理数据F和G为例，对应电机转矩请求信号和响应信号均为连续数据，根据数据范围区间处理为｛<0，0，>0｝类型的项集集合，计算结果见表7。

从上述类型的数据可以得知，利用置信度和提升度这两个指标能实现满足线性相关关联规则筛选。筛选满足高置信度阈值的关联规则并整合，能快速挖掘这类型关联规则的因果性。

3.2.3　负相关关联规则

驾驶行为中部分数据存在明显负相关关系，前项和后项的置信度和提升度用负相关的公式获得。以加速踏板开度和制动踏板的关系为例，制动踏板踩下为C1，保留为C2，释放为C0，B 表示踏板开度，划分为3个等距区间B1、B2、B3。

如表8所示，实际驾驶行为中加速踏板和制动踏板互相制约，反映在表格中的是对应加速踏板存在开度的3个数据区间B1、B2、B3和反映制动踏板踩下的两个数据区间C1、C2之间不存在正相关性。

表4　ESC状态信息（L、M）

信号名	总线数据	定义解释	信号解释
ESC_Ang_Stat_YawRate （编号L）	0～16 382	横摆角速度	单位：(°)/s
ESC_Ang_Stat_LateralAccelaration （编号M）	0～2 490	横向加速度信号	单位：m/s²

表 5 ABS 状态信息（N）

信号名	总线数据	定义解释	信号解释
Wheel_Speed_ABS （编号 N）	0～65 535	精度：0.01 单位：km/h	车速信号

表 6 物理信号和实际信号的关联规则计算

	关联度	支持度	置信度	提升度
A∫B	A1=>B1	0.323 7	0.971 0	2.999 6
	A2=>B2	0.333 3	1	3.000 0
	A3=>B3	0.338 2	1	2.956 8
D∫E	D1=>E1	0.923 6	1	1.082 7
	D2=>E2	0.046 1	1	21.690 0
	D3=>E3	0.024 4	1	40.980 0
	D4=>E4	0.000 6	1	167.000 0

表 7 因果关系的信号关联规则计算

	关联度	支持度	置信度	提升度
F∫G	F1=>G1	0.224 3	0.983 6	4.385 2
	F2=>G2	0.152 9	0.969 9	6.343 4
	F3=>G3	0.622 8	0.996 3	1.599 7

表 8 负相关关联规则计算

	关联度	支持度	置信度	提升度
B∫C	B1=>C1	0	0	0
	B2=>C1	0	0	0
	B3=>C1	0	0	0
	B1=>C2	0	0	0
	B2=>C2	0	0	0
	B3=>C2	0	0	0
	B1=>C0	0.323 7	1.000 0	3.089 3
	B2=>C0	0.333 3	1.000 0	3.000 0
	B3=>C0	0.338 2	1.000 0	2.956 8

3.2.4 非线性关系的关联规则

驾驶行为中有些数据不存在明显的线性关系，但基于驾驶安全，二者之间存在一定的制约关系。以车速和方向盘转角为例，从信息来源看，二者无明显相关性，实际工况中高车速情况下方向盘转角和角速度必然受限，以确保行车安全。

图 6 为方向盘转角和车速的关系分布图，基于特征分箱分配区间 J1、J2、J3。转向角度在±30°之间对应｛方向盘转角小｝，±260°之间对应｛方向盘转角中等｝（这个范围内数据量大于正态分布的 2σ 区间），角度绝对值大于 260° 对应｛方向盘转角大｝。车速信号 N 以 21 为区间分界点。

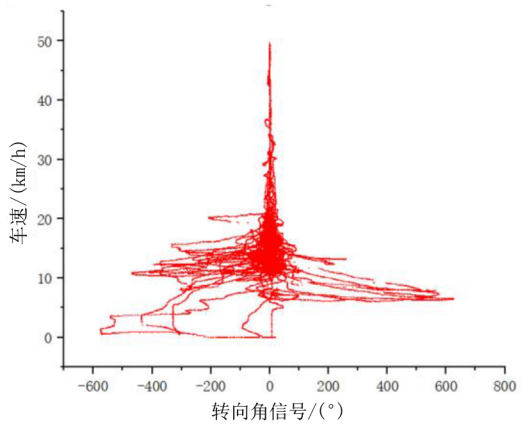


图 6 方向盘转角和车速分布图

表 9 方向盘转角车速的非线性关联规则计算

	关联度	支持度	置信度	提升度
J1	J1=>N1	0.771 3	0.885 0	1.147 4
	J1=>N2		0.115 0	0.149 1
J2	J2=>N1	0.183 4	1.000 0	5.452 6
	J2=>N2		0	0
J3	J3=>N1	0.045 3	1.000 0	22.075 1
	J3=>N2		0	0

由表 9 可知，由于 N 的分布涉及 J 的 3 个子项区间，因此置信度和提升度较低，J1 在各个车速区间内都能正常匹配；J2 对应的车速区间在 N1 范围；J3 对应车速区间在 N1 范围内，因此，二者的关联规则计算置信度和提升度在表中表现显著。

3.3 基于关联规则的离群点计算

获得关联规则后，对具有关联性的相关数据执行离群点检测，用于筛选偏离标准的异常离群值，原有的检测无法排除同时篡改具有关联性报文数据攻击，而这一方法能补充基于关联规则的检测。计算局部离群点和邻域数据的欧氏距离，根据数据点 d_i 的欧式距离的变化设置异常信号阈值，大于阈值的视为异常信号。以车速信号为例，选取车速信号数量约为 5 万个，计算获得的离群值如图 7 所示。

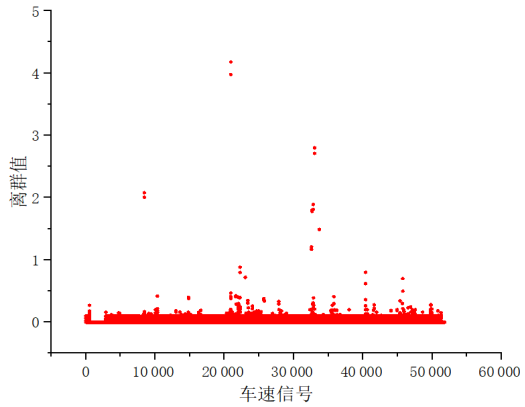


图 7　车速信号离群值

由图 7 可知，大部分数据点的离群值都在 1 以下。如果设定 1 为离群点阈值，则在后续的检测中对大于这一阈值的视为异常信号；图中大于 1 的离群点视为系统误差，调整离群点阈值能同时改变最终检测的准确率和误报率，阈值如果升高，则最终的误报率下降，准确率上升。所以合理设置阈值能提高检测效果。

3.4　关联规则和离群点阈值制定

按照上节多种类型的关联规则分析，在筛选去除冗余规则后，本节制定关联规则内容见表 10。

表 10　关联规则描述

序号	规则
1	PhysicsAccPedal=RealAccPedal
2	PhysicsGear=RealGear
3	BrakePedal∩PhysicsAccPedal=0
4	|MotorTq_req-MotTorque|≤4
5	MotorSpeed_req=0
6	SteeringRotS=d（SteeringAngles）
7	HighSpeed-LowSteeringAngles
8	RealAccPedal-MotSpeed-Speed

基于上述动力域信息，获得需要计算离群点判断阈值的信号，见表 11。

4　试验结果

本节负责构建具体的篡改攻击，攻击和数据内容与具体的控车信号相关。具体执行方式是在测试集中随机插入篡改攻击，采用本文提出的方法对带有异常信号的数据集进行入侵检测，并统计检测的攻击数量。

表 11　离群点判断阈值

信号编号	离群点判断阈值	测试集准确度%
A、B	20	99.93
F	25	99.96
G	25	99.95
J	J	99.94
N	1	99.97

本文设置的不违反关联规则的复杂篡改攻击和仅篡改单一数据的篡改攻击比例约为 1∶10，据此设置不同数量的攻击用例，具体的篡改攻击方式见表 12。

表 12　攻击用例

信号篡改	攻击方式	次数
违反规则 1	PhysicsAccPedal 或 RealAccPedal 修改为随机值	200
违反规则 2	PhysicsGear 或 RealGear 修改为随机值	200
违反规则 3	BrakePedal 或 PhysicsAccPedal 修改为随机值	200
违反规则 4	MotorTq_req 或 MotTorque 修改为随机值	200
违反规则 5	MotorSpeed_req 修改为随机值	200
违反规则 6	SteeringRotS 或 SteeringAngles 修改为随机值	200
违反规则 7	SteeringAngles 修改为随机值	200
违反规则 8	MotSpeed 或 Speed 修改为随机值	200
规则 1 篡改	同时篡改 PhysicsAccPedal 和 RealAccPedal	20
规则 3 篡改	同时篡改 BrakePedal 和 PhysicsAccPedal	20
规则 4 篡改	同时篡改 MotorTq_req 和 MotTorque	20
规则 6 篡改	同时篡改 SteeringRotS 和 SteeringAngles	20
规则 8 篡改	同时篡改 RealAccPedal、MotSpeed 和 Speed	20

本次测试用的正常数据数量为 157 495 个。本文提出的方法和基于关键特征和关联规则的入侵检测方法对比，最终针对篡改攻击的检测结果见表 13。

表 13　测试结果

检测方式	准确率%	误报率%
关键特征和关联规则检测	87.76	1.43
关联规则和离群点检测	92.88	1.25

已有的基于关键特征和规则的入侵检测方法中，基于关键特征的入侵检测方法无法检测篡改攻击。基于规则的入侵检测方法能检测篡改单一数据的攻击，但如果攻击同时篡改关联数据，使关联规则并没有被违反，则上述方法无效，因此，在本文采用的攻击用例中，综合检测准确率仅为87.76%；本文采用的检测方法在生成强关联规则的基础上引入离群点检测，最终在不增大入侵检测误报率的前提下准确率提升5.83%。

5 结论

本文针对新能源汽车动力域篡改攻击的入侵检测，提出了基于关联规则和离群点检测的模型及实现方法。结合实车测试数据，采用FP-growth算法进行频繁项集挖掘，基于规则评价建立关联规则库，在规则检测的基础上，通过检测关联数据的离群点，实现对复杂类型篡改攻击的检测。仿真研究和传统方法对比结果表明，这种策略能筛选出有价值的关联规则，并获得合适的离群点检测阈值，用于实现篡改类型的异常入侵检测，并取得较好的检测效果。

虽然本方法仅在汽车动力域上面进行了实车验证，但是相关的理论和思路可以拓展到汽车的其他系统中。

参考文献（References）

[1] CHO K, SHIN K G S. Fingerprinting Electronic Control Units for Vehicle Intrusion Detection[C]//SEC'16: Proceedings of the 25th USENIX Conference on Security Symposium, Aug. 10-12, 2016, Austin TX USA. Berkely: USENIX Association, c2016: 911-927.

[2] HALDER S, CONTI M, DAS S K, et al. COIDS: A Clock Offset Based Intrusion Detection System for Controller Area Networks[C]//ICDCN'20: Proceedings of the 21st International Conference on Distributed Computing and Networking, Jan. 4-7, 2020, Kolkata India. New York: Association for Computing Machinery, c2020: 1-10.

[3] 王超，李飞. 基于关联规则挖掘的车载网络入侵检测技术研究[J]. 数据挖掘，2017，7(3)：65-69.
WANG Chao, LI Fei. Research on Intrusion Detection Technology Based on Association Rules Mining in Vehicular Networks [J]. Data Mining, 2017, 7 (3): 65-69. (in Chinese)

[4] LEE H, JEONG S, KIM H K, et al. OTIDS: A Novel Intrusion Detection System for In-Vehicle Network by Using Remote Frame[C]//Proceedings of 2017 15th Annual Conference on Privacy, Security and Trust (PST), Aug. 28-30, 2017, Calgary, AB, Canada. Piscataway NJ: IEEE, c2017: 57-5709.

[5] TAYLOR A, LENLANC S, JAPKOWICZ N. Anomaly Detection in Automobile Control Network Data with Long Short-Term Memory Networks[C]//Proceedings of IEEE International Conference on Data Science & Advanced Analytics, Oct. 17-19, 2016, Montreal, QC, Canada. Piscataway NJ: IEEE, c2016: 130-139.

[6] WYK F V, WANG Yiyang, KHOJANDI A, et al. Real-Time Sensor Anomaly Detection and Identification in Automated Vehicles[J]. IEEE Transactions on Intelligent Transportation Systems, 2020, 21(3): 1264-1276.

[7] MÜTER M, ASAJ N. Entropy-Based Anomaly Detection for In-Vehicle Networks [C]//Proceedings of Intelligent Vehicles Symposium, June 5-9, 2011, Baden-Baden, Germany. Piscataway NJ: IEEE, c2011: 1110-1115.

[8] WU Wufei, HUANG Yizhi, KURACHI R, et al. Sliding Window Optimized Information Entropy Analysis Method for Intrusion Detection on In-Vehicle Networks[J]. IEEE Access, 2018, 6: 45233-45245.

[9] 于赫，秦贵和，孙铭会，等. 车载CAN总线网络安全问题及异常检测方法[J]. 吉林大学学报(工学版)，2016，46(4)：1246-1253.
YU He, QIN Guihe, SUN Minghui, et al. Cyber Security and Anomaly Detection Method for In-Vehicle CAN[J]. Journal of Jilin University (Engineering and Technology Edition), 2016, 46(4): 1246-1253. (in Chinese)

[10] 宋和春. 面向车载网络的入侵检测系统研究[D]. 西安：西安电子科技大学，2020.

SONG Hechun. Research on Intrusion Detection System for In-Vehicle Networks[D]. Xi'an: Xi'an University of Electronic Science and Technology, 2020.(in Chinese)

[11] KANG M J, KANG J W. A Novel Intrusion Detection Method Using Deep Neural Network for In-Vehicle Network Security[C]//2016 IEEE 83rd Vehicular Technology Conference (VTC Spring), May 15-18, 2016, Nanjing, China. Piscataway NJ: IEEE, c2016: 1-5.

[12] KHAN Z, CHOWDHURY M, ISLAM M, et al. Long Short-Term Memory Neural Network-Based Attack Detection Model for In-Vehicle Network Security[J]. IEEE Sensors Letters, 2020, 4(6): 1-4.

[13] SU Tong, XU Haitao, ZHOU Xianwei. Particle Swarm Optimization Based Association Rule Mining in Big Data Environment[J]. IEEE Access, 2019, 7: 16108-161016.

[14] HAN Jiawei, PEI Jian, YIN Yiwen. Mining Frequent Patterns Without Candidate Generation[J]. ACM SIGMOD Record, 2000, 29(2): 1-12.

[15] 刘财辉, 刘地金. 离群点检测的邻近性方法综述[J]. 计算机工程与应用, 2022, 58(21): 1-12.
LIU Caihui, LIU Dijin. Survey of Proximity Methods for Outlier Detection[J]. Computer Engineering and Applications, 2022, 58(21): 1-12.(in Chinese)

[16] 黄彧. 相似性度量的研究及其在数据挖掘中的应用[D]. 福州: 福建师范大学, 2009.
HUANG Yu. A Study on Similarity Method and Its Application in Data Mining[D]. Fuzhou: Fujian Normal University, 2009.(in Chinese)

[17] TRAN L, FAN Liyue, SHAHABI C. Distance-Based Outlier Detection in Data Streams[J]. Proceedings of the VLDB Endowment, 2016, 9(12): 1089-1100.

[18] 马小超. 电动汽车动力域控制器设计研究[J]. 汽车电器, 2022(7): 7-10.
MA Xiaochao. Design and Research of Power Domain Control Unit for an Electric Vehicle[J]. Auto Electric Parts, 2022(7): 7-10.(in Chinese)

[19] 闫磊, 王刚, 宋金梦, 等. 动力域控制器功能安全概念阶段开发[J]. 中国汽车, 2022(5): 19-25.
YAN Lei, WANG Gang, SONG Jinmeng, et al. Development of Functional Safety Concept of Dynamic Domain Controllers[J]. China Auto, 2022(5): 19-25.(in Chinese)

作者简介

余辰熠（1998-），男，福建福州人，硕士研究生，主要研究方向为智能车辆网络安全。
Tel：15910520326
E-mail：wuwetianke@163.com

通信作者

魏洪乾（1992-），男，山东滨州人，博士，助理研究员，主要研究方向为智能车辆控制和汽车网络安全。
E-mail：bit_hongqian@126.com