计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
2025,34(3):85−93 [doi: 10.15888/j.cnki.csa.009821] [CSTR: 32024.14.csa.009821]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

面向车联网 DoS 攻击的混合入侵检测系统①

郭健忠[1], 王　灿[1], 谢　斌[2], 闵　锐[2]

[1](武汉科技大学 汽车与交通工程学院, 武汉 430065)
[2](武汉保华显示科技有限公司, 武汉 430082)
通信作者: 王　灿, E-mail: 2424626449@qq.com

摘　要: 针对车联网中拒绝服务 (denial of service, DoS) 攻击难以防范且现有监督学习方法无法有效检测零日攻击的问题, 提出了一种混合 DoS 攻击入侵检测系统. 首先, 对数据集进行预处理, 提高数据的质量; 其次, 利用特征选择滤除冗余特征, 旨在获得代表性更强的特征; 再次, 采用集成学习方法将 5 种基于树结构的监督分类器堆叠集成用于检测已知 DoS 攻击; 最后, 提出了一种无监督异常检测方法, 将卷积去噪自动编码器与注意力机制相结合来建立正常行为模型, 用于检测堆叠集成模型漏报的未知 DoS 攻击. 实验结果表明, 对于已知 DoS 攻击检测, 所提系统在 Car-Hacking 数据集和 CICIDS2017 数据集上的检测准确率分别为 100% 和 99.967%; 对于未知 DoS 攻击检测, 所提系统在上述两个数据集上的检测准确率分别为 100% 和 83.953%, 并且在两个数据集上的平均测试时间分别为 0.072 ms 和 0.157 ms, 验证了所提系统的有效性和可行性.

关键词: 车联网; 入侵检测; DoS 攻击; 堆叠集成; 自动编码器

引用格式: 郭健忠,王灿,谢斌,闵锐.面向车联网 DoS 攻击的混合入侵检测系统.计算机系统应用,2025,34(3):85–93. http://www.c-s-a.org.cn/1003-3254/9821.html

Hybrid Intrusion Detection System for DoS Attacks in Internet of Vehicles

GUO Jian-Zhong[1], WANG Can[1], XIE Bin[2], MIN Rui[2]

[1](School of Automotive and Traffic Engineering, Wuhan University of Science and Technology, Wuhan 430065, China)
[2](Wuhan Baohua LCD Display Technology Co. Ltd., Wuhan 430082, China)

Abstract: To solve the problems that denial of service (DoS) attacks in the Internet of Vehicles are difficult to prevent and the existing supervised learning methods cannot effectively detect zero-day attacks, this study proposes a hybrid DoS attack intrusion detection system. Firstly, the dataset is preprocessed to improve data quality. Secondly, feature selection is used to filter out redundant features, which aims to obtain more representative features. Thirdly, the ensemble learning method is used to integrate five tree-based supervised classifiers through stacking to detect known DoS attacks. Finally, an unsupervised anomaly detection method is proposed, which combines the convolutional denoising autoencoder with the attention mechanism to establish a normal behavior model. It is used to detect unknown DoS attacks that are missed by stacking ensemble models. Experimental results show that for the detection of known DoS attacks, the detection accuracy of the proposed system on the Car-Hacking dataset and the CICIDS2017 dataset is 100% and 99.967%, respectively. For the detection of unknown DoS attacks, the detection accuracy of the proposed system on the above two datasets is 100% and 83.953%, respectively, and the average test time on the two datasets is 0.072 ms and 0.157 ms, respectively, which verifies the effectiveness and feasibility of the proposed system.

Key words: Internet of Vehicles (IoV); intrusion detection; DoS attack; stacking ensemble; autoencoder

① 收稿时间: 2024-09-06; 修改时间: 2024-10-10; 采用时间: 2024-11-12; csa 在线出版时间: 2025-01-17
CNKI 网络首发时间: 2025-01-17

智能网联技术的快速发展推动着以智能网联汽车为中心的车联网日趋完善, 车联网实现了人、车、路、云之间的信息交互, 构建了智慧交通新形态. 车联网主要包括车内网和车外网, 其中车内网实现车内数据的传输、通信及控制功能, 以总线通信作为主要通信方式, 其中控制器局域网络 (controller area network, CAN) 应用最为广泛, 而车外网则依托无线通信技术, 构建车辆与外部环境之间通信和互联的平台, 通过车辆和外部设备的实时通信, 实现车辆信息共享、安全升级等功能[1]. 在车联网蓬勃发展的同时, 海量的实时通信数据和对外通信接口的增加使得车辆更容易遭受到网络入侵. 相较于一般的网络而言, 车联网具有更加庞大且复杂的网络架构, 承载了的海量数据, 因而也增加了被攻击的风险和防范的难度. 并且车联网处于一个相对开放的网络环境中, 车内尤其是车外设备本身安全性的不足会暴露大量攻击面, 因而车联网更容易遭受到各种模式的网络攻击, 如果不能有效防范网络攻击, 将会给用户带来巨大的安全威胁[2,3]. 作为网络的保护屏障, 入侵检测系统 (intrusion detection system, IDS) 可以有效检测网络攻击, 然而区别于一般的 IDS, 车联网 IDS 不仅需要具备高准确率和低误报率, 还应满足车辆实时性要求, 并且车载控制器的计算能力和存储资源有限, IDS 需要在有限的资源下发挥作用[4]. 在车联网环境下的各种网络攻击类型中, 拒绝服务 (denial of service, DoS) 攻击危害性最大、影响范围最广. 由于车联网自身的复杂性和互联性, 车联网中的 DoS 攻击具有广泛性、隐蔽性和多样性等特点, DoS 攻击往往会伪装成正常网络流量或者利用车联网系统中的漏洞进行隐蔽攻击, 使得防御系统难以区分正常流量和恶意攻击, 因而 DoS 攻击往往难以被及时发现. 复杂多变的 DoS 的攻击对于车联网有着致命的威胁, 其不仅会致使相关功能服务失效, 还可能对车辆行驶安全构成严重威胁, 因此, 如何高效地检测 DoS 攻击成为当前领域的迫切需求.

目前, 对于网络入侵检测的研究主要集中在基于签名的入侵检测方法和基于异常的入侵检测方法两方面, 其中基于签名的入侵检测方法主要利用监督学习方法对标签数据进行训练, 从而区分正常数据和恶意攻击. 在已知攻击检测方面表现优异, 误报率极低, 能够准确识别正常数据, 但是很难检测到零日攻击, 极易漏报, 将零日攻击误识别为正常数据. 而基于异常的入侵检测方法主要利用无监督或半监督方法, 能够有效地检测零日攻击[5,6]. 因此, 为保护车联网安全, 开发能够检测已知和未知攻击的 IDS 至关重要. 混合网络入侵检测方法结合了签名检测方法和异常检测方法, 融合两者的优点, 能够有效检测已知攻击和零日攻击. Yang 等人[7] 提出一种多层混合入侵检测系统 (multi-tiered hybrid intrusion detection system, MTH-IDS), 该系统主要利用多种机器学习模型来检测车联网中的已知攻击和零日攻击, 但是在车外网数据集上对于零日攻击的检测效果较差. Li 等人[8]针对物联网中 DoS 攻击难以预防的问题, 提出一种基于半监督学习的混合 DoS 攻击 IDS, 实现了较好的检测效果, 但是对于复杂多变的零日攻击检测仍然存在挑战.

为应对车联网中的已知和未知 DoS 攻击的威胁, 本文提出一种混合 DoS 攻击入侵检测系统, 采用集成学习方法堆叠集成了 5 种基于树结构的机器学习模型用于检测已知 DoS 攻击, 充分利用不同算法的优势以获得更强大的整体性能, 并且采用基于树结构 Parzen 估计器的贝叶斯优化方法 (Bayesian optimization-tree-structured Parzen estimator, BO-TPE) 对模型进行超参数优化, 从而进一步地优化模型检测效果. 同时提出了一种无监督异常检测方法, 该方法在卷积去噪自动编码器 (convolutional denoising autoencoder, CDAE) 的基础上融合注意力机制 (attention mechanism, AM), 用于检测堆叠集成模型漏报的未知 DoS 攻击.

1 入侵检测系统框架

1.1 系统整体架构

本文提出一种混合 IDS, 用于检测车内网和车外网中出现的已知和未知 DoS 攻击. 系统整体架构如图 1 所示, 主要包括 4 个部分: 数据预处理、特征选择、基于签名的 IDS 以及基于异常的 IDS. 由图 1 可知, 本文首先对收集的车内和车外网络流量原始数据集进行预处理来降低数据维度和滤除噪声, 然后通过特征选择对数据集进行特征筛选, 去除冗余特征和干扰噪声, 提高网络流量数据的质量, 并将处理完成后的数据输入到堆叠集成模型中对已知攻击进行检测; 最后利用基于 CDAE-AM 的无监督异常检测方法对堆叠集成模型标记为“正常”的数据进行未知 DoS 攻击检测.

1.2 数据预处理

原始的网络流量数据通常包含数字、字符等多种

数据类型, 会存在诸多噪声, 这些噪声很容易影响模型准确性和可靠性. 因此为提高数据集的数据质量, 加快模型收敛速度, 在数据集输入到模型之前需要进行预处理. 在所提出的 IDS 中, 数据预处理主要包括数据清理、Z-score 归一化、K-means 聚类采样以及 SMOTE 过采样.

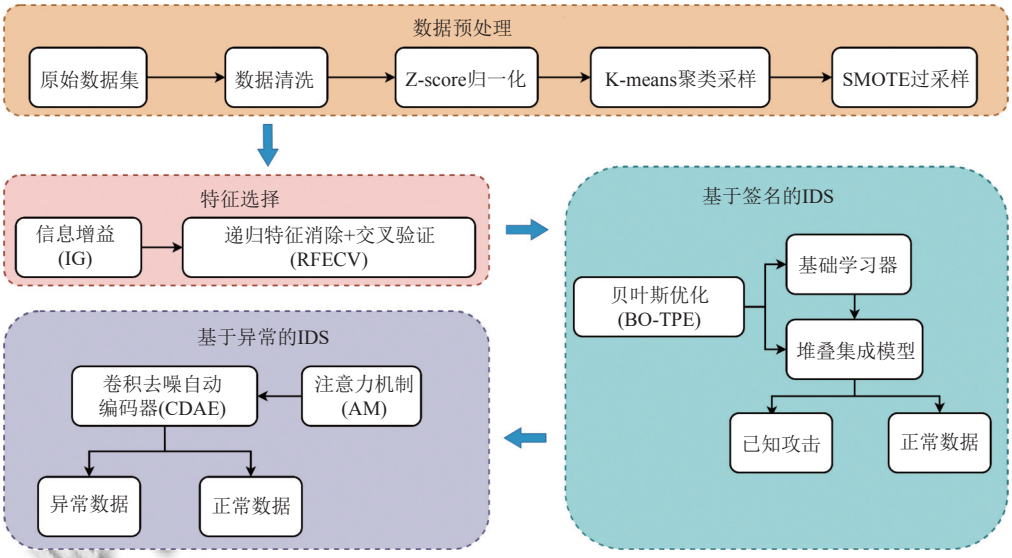

图 1 入侵检测系统框架

1.2.1 数据清理

数据清理的主要作用是清理数据集中不准确或缺失的数据, 删除重复的数据, 并且将缺省值填充, 一般填充为 0. 此外, 本文使用标签编码器对原始网络流量数据集中的标签进行编码, 将字符型标签转换为数字型标签, 并将含字母的十六进制数转换为十进制数.

1.2.2 Z-score 归一化

在进行数据清理之后, 通过 Z-score 算法对数据集进行归一化处理, 因为网络流量数据集中不同数据特征之间的数据尺度和维度不同, Z-score 归一化可将数据缩放到统一的数据间隔和范围, 以限制缩放差异对模型的影响. 经过该方法处理后的数据符合标准正态分布, 每个归一化后的数据 z 可以表示为:

$$z = \frac{x-u}{\sigma} \tag{1}$$

其中, x是原始数据, u和σ分别代表数据的平均值和标准差.

1.2.3 K-means 聚类采样

为减少训练数据量和降低模型的训练复杂性, 提高模型的运行效率, 可以在数据量较多的网络流量类型中运用数据采样技术来获得高代表性子数据集. K-means 聚类采样将原始数据分为k组聚类, 并选取k个聚类中心, 然后从每个聚类中采样一定比例的数据以形成代表性的子集, 以便在不丢失重要信息的基础上舍弃大量冗余数据[9]. K-means 算法的核心任务是找出最优聚类中心, 并最小化所有数据点与相应聚类中心之间的距离平方和, 其原理可以表示为:

$$\min \sum_{i=1}^{k} \sum_{B \in CL_i} (CL_i - B) \tag{2}$$

其中, CL_i为第i组聚类的中心, B为聚类数据点.

1.2.4 SMOTE 过采样

在网络流量数据集中, 正常样本所占的比例要远大于攻击样本且攻击样本种类繁多, 致使数据集的类不平衡问题严重, 如果数据集存在严重的不平衡, 预测结论往往偏向于数量较多的类样本, 容易影响模型的检测精度. SMOTE 过采样可以有效解决数据集类不平衡的问题, 该方法通过随机创建新的少数类样本来平衡数据集, 从而进一步提高数据集的质量[10]. 利用 SMOTE 过采样创建的样本x_n可以表示为:

$$x_n = x + rand(0,1) \times (x_i - x) \tag{3}$$

其中, x为少数类样本, x_i是从x的 K 近邻中随机抽取的样本.

1.3 特征选择

特征选择作为 IDS 的重要组成部分, 可以筛选出与结果高度相关的特征, 寻找最优特征子集, 在提高模

型准确性的同时减少模型训练所需的时间[11]. 本文利用信息增益 (information gain, IG) 和递归特征消除与交叉验证 (recursive feature elimination and cross validation, RFECV) 算法组成特征选择模块.

1.3.1 信息增益

IG 根据数据集各特征的信息熵选择特征, 用于表示数据集中某个特征信息使类信息的不确定性减少的程度. IG 可以快速地计算每个特征的重要性分数, 并根据每个特征的重要性分数进行排序以此选择出相关性最强的特征[12]. 在特征选择过程中, Y 作为目标变量, X 作为特征变量, 特征变量 X 相对于目标变量 Y 的 IG 可以表示为:

$$IG(Y,X) = H(Y) - H(Y|X) \tag{4}$$

其中, $H(Y)$ 是目标变量 Y 的熵, $H(Y|X)$ 是 Y 在 X 上的条件熵.

1.3.2 递归特征消除与交叉验证

在 IG 的基础上, 采用 RFECV 进一步地筛选出最佳特征组合. 递归特征消除 (recursive feature elimination, RFE) 主要通过反复训练模型来剔除不重要的特征, 逐步降低特征子集的维度, 直到达到预定的目标特征数量, 从而实现选择最优的特征子集的目的. 该方法在有效减少噪声干扰的同时, 最大限度地保留重要特征[13]. 但是 RFE 只是单纯基于特征权重来进行特征选择, 存在过拟合的风险. 而 RFECV 使用交叉验证的方法在每个子集上分别进行训练和验证来保留最佳特征, 使得特征选择结果更加稳定可靠, 从而提高模型的泛化能力.

1.4 混合入侵检测系统

为解决单一的基于签名的 IDS 和基于异常的 IDS 无法有效地同时检测已知和未知 DoS 攻击的问题, 本文提出一种混合 IDS, 用于检测车联网中的已知和未知 DoS 攻击. 首先, 通过基于树结构的堆叠集成模型检测已知 DoS 攻击, 其次, 构建一个基于 CDAE-AM 的无监督异常 IDS 来检测未知 DoS 攻击, 当堆叠集成模型检测已知攻击时, 将可能被识别为“正常”的未知攻击数据输入到 CDAE-AM 模型中, 从而实现对未知 DoS 攻击的检测.

1.4.1 基于签名的入侵检测系统

原始数据集在经过数据预处理和特征选择模块处理之后输入到基于签名的 IDS, 基于签名的 IDS 主要利用监督学习方法对正常数据和恶意攻击数据进行分类. 在机器学习中, 不同的算法具有不同的优缺点, 为避免单个算法在处理不同数据集时的偏好, 可以将不同的监督学习算法组合起来, 形成一个强监督学习算法[14]. 如图 2 所示, 本文所提出的基于签名的 IDS 将决策树 (decision tree, DT)、随机森林 (random forest, RF)、极端随机树 (extremely randomized trees, ET)、极端梯度提升 (extreme gradient boosting, XGBoost) 以及自适应增强 (adaptive boosting, AdaBoost) 这 5 种树结构分类器为基础模型, 通过集成学习的方法得到堆叠模型. 在基本模型中挑选综合性能最好的一个作为元模型, 将各基础模型的输出构造为训练集, 该训练集将被作为输入特征来训练元模型, 并通过元模型来进行最后的预测操作. 相比于单个的基础模型, 堆叠模型具有相对稳定的性能和更好的泛化能力[15].

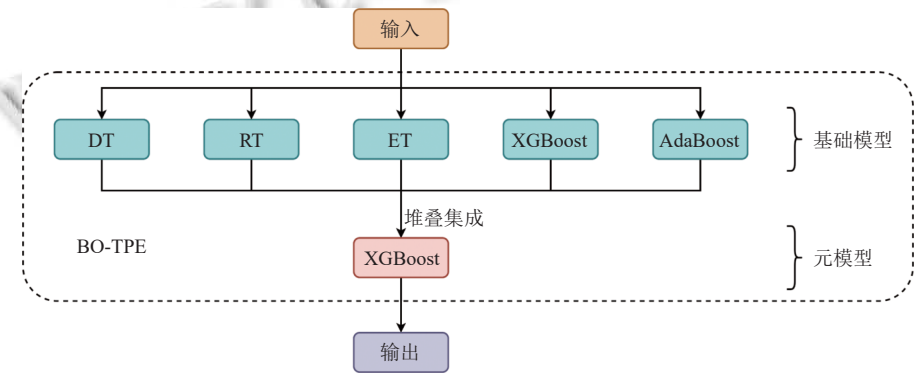

图 2 基于树结构的堆叠集成模型

为进一步提高模型的性能, 需要通过超参数调优的过程来寻找最佳超参数配置. 本文采用 BO-TPE 方法对基础模型和元模型进行超参数优化, BO-TPE 属于贝叶斯优化的一种方法, 可以在几次迭代中检测到接

近最优的超参数组合[16].

1.4.2 基于异常的入侵检测系统

基于签名的 IDS 检测完成后将标记为“正常”的数据输入到基于异常的 IDS 中, 基于异常的 IDS 用于检测“正常”数据当中是否存在零日攻击, 这些零日攻击可能是现有攻击的变体, 也可能是全新的攻击. 针对零日攻击的检测, 本文提出一种基于 CDAE-AM 的无监督异常检测方法, 该方法在卷积去噪自动编码器 (CDAE) 的基础上添加了注意力机制 (AM), 通过使用正常数据训练模型, 从而建立正常行为模型, 一旦检测到偏离正常行为的数据就会标记为异常.

CDAE-AM 的基础模型为自动编码器 (autoencoder, AE), AE 结构包括输入层、编码器、隐藏层、解码器和输出层, 首先将数据传递给输入层, 编码器通过压缩将数据编码为潜在维度, 然后解码器对压缩后的数据进行解码, 并在输出层重建原始表征, 从而获得重构误差[17]. AE 经过无监督训练后, 在测试过程中正常数据将会产生低重构误差, 而异常值或受到攻击的数据则会产生较高的重构误差, 因此可以通过设置重构误差阈值达到检测异常的目的.

如图 3 所示, CDAE-AM 模型在 AE 编码器的基础上首先引入卷积神经网络 (convolutional neural network, CNN), CNN 的优势在于它能够有效地处理数据并学习其内在结构和特征. CNN 主要包括卷积层 (Conv1D) 和池化层 (MaxPooling1D) 两部分, Conv1D 主要用于学习数据的空间特征, MaxPooling1D 可以减少特征映射的维数和后续层所需的参数, 同时为使模型训练过程更加稳定, 使用批处理归一化 (BatchNormalization) 对 CNN 输出的结果进行调整. 其次在 CNN 层后应用注意力机制 (AM), AM 具有较强的时间特征提取能力, 避免了高层次的空间特征提取造成的时间信息丢失, 从而保留更多的时空特征, 并且将结果输入到 Dropout 层以防止过拟合. 然后在 AE 解码器的基础上引入转置卷积层 (Conv1DTranspose), 通过特征重建和逆卷积操作, 帮助解码器从潜在维度中恢复出更高质量的原始数据, 最后将输入的正常数据和符合高斯分布的噪声结合起来, 提高网络流量数据的抗干扰性和泛化性.

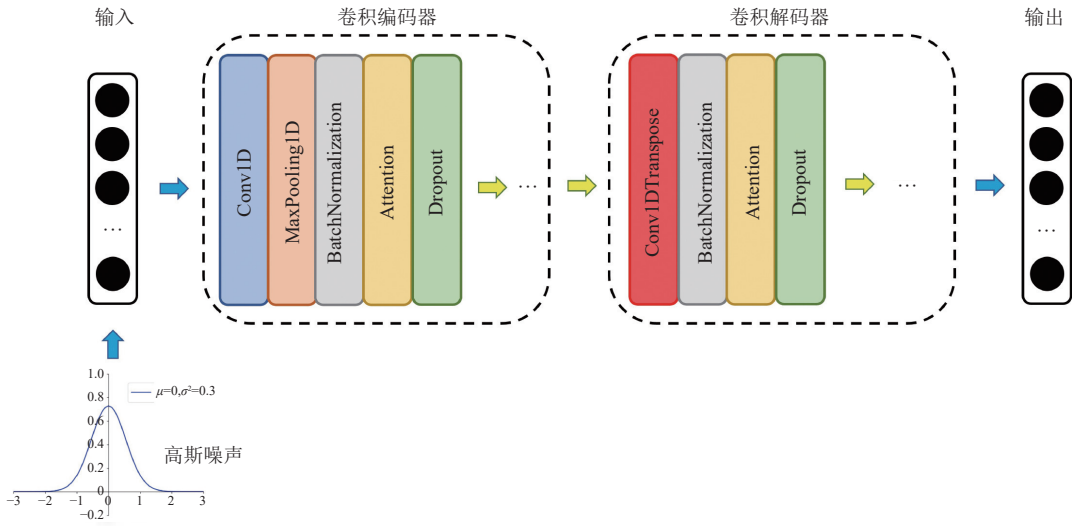

图 3 CDAE-AM 模型

2 实验与分析

2.1 实验设置

实验硬件环境为 Linux 64 位操作系统, 12 核的处理器以及 NVIDIA GeForce RTX3080 显卡, 软件环境为 Python 3.8.10, TensorFlow 2.9.0. 为更贴近现实情况, 分别对车内网和车外网数据集进行多次分组实验, 分别将每种 DoS 攻击作为未知 DoS 攻击, 不参与堆叠集成模型的训练, 并将测试结果中标记为“正常”的数据输入到 CDAE-AM 模型中, 输入内容包括正常数据和未被堆叠集成模型识别到的未知 DoS 攻击, 以此检测未知攻击.

2.2 数据集说明

针对 DoS 攻击检测, 本文选取了与 DoS 攻击相关的数据, 对于车内网 IDS 的性能评估, 采用 CAN 报文

数据集 Car-Hacking 数据集[18]中的 DoS 攻击数据集; 对于车外网 IDS 的性能评估, 采用网络流量数据集 CICIDS2017[19]中包含 DoS/DDoS 攻击数据的星期三和星期五数据集以及仅由正常数据组成的星期一数据集. 在实验过程中, 针对已知 DoS 攻击和正常数据, 70% 的数据集被分配为训练集, 30% 的已知 DoS 攻击、正常数据以及全部的未知 DoS 攻击作为测试集, 所采用的数据集的详细情况如表 1、表 2 所示.

表 1 Car-Hacking 数据集样本分布

类别	训练样本数	测试样本数
Normal	2 132 942	914 119
DoS	411 265	176 256

表 2 CICIDS2017 数据集样本分布

类别	原始训练样本数	平衡训练样本数	测试样本数
BENIGN	747 367	747 367	320 300
DDoS	89 619	89 619	38 408
DoS GoldenEye	7 205	7 205	3 088
DoS Hulk	161 751	161 751	69 322
DoS Slowhttptest	3 849	5 000	1 650
DoS slowloris	4 057	5 000	1 739
Heartbleed	8	100	3

2.3 评价指标

本实验的评价指标主要包括准确率 (accuracy, *Acc*)、精确率 (precision, *Pre*)、召回率 (recall, *Rec*)、*F*1 分数 (*F*1 score, *F*1) 和误报率 (false alarm rate, *FAR*), 表达式分别为:

$$Acc = \frac{TP+TN}{TP+TN+FP+FN} \tag{5}$$

$$Pre = \frac{TP}{TP+FP} \tag{6}$$

$$Rec = \frac{TP}{TP+FN} \tag{7}$$

$$F1 = \frac{2\times Pre\times Rec}{Pre+Rec} \tag{8}$$

$$FAR = \frac{FP}{FP+TN} \tag{9}$$

其中, TP为真阳性, 代表正确分类的攻击样本数量; TN为真阴性, 代表正确分类的正常样本数量; FP为假阳性, 代表错误分类为攻击的正常样本数量; FN为假阴性, 代表错误分类为正常的攻击样本数量.

2.4 已知 DoS 攻击检测结果分析

对于已知 DoS 攻击检测, 所提系统中的堆叠集成模型在 Car-Hacking 数据集和 CICIDS2017 数据集上的表现分别如表 3 和表 4 所示, 相比于其他监督机器学习和深度学习模型, 本文所提出的堆叠集成模型在准确率、精确率、召回率、*F*1 分数以及误报率方面具有明显的优势. 对于 Car-Hacking 数据集, 虽然其他方法也实现了较高精度的检测, 但本文方法可以达到 100% 的高准确率, 相比于其他方法更优; 对于 CICIDS2017 数据集, 对比其他文献中提出的方法, 本文方法在准确率上提升了 0.072%–3.777%, 在精确率上提升了 0.297%–3.777%, 在召回率上提升了 0.147%–4.737%, 在 *F*1 分数上提升了 0.072%–4.727%, 在误报率上降低了 0.031%–0.761%. 因此, 实验结果表明, 相比于其他传统机器学习、深度学习等基线模型, 本文所提出的基于签名的 IDS 可以更加有效地检测已知 DoS 攻击.

表 3 Car-Hacking 数据集上已知攻击检测结果对比 (%)

方法	*Acc*	*Pre*	*Rec*	*F*1	*FAR*
KNN[20]	99.78	99.98	99.29	99.64	—
ANN[20]	99.93	99.95	99.82	99.88	—
CNN[21]	99.77	99.77	98.4	99.41	0.23
LSTM[21]	99.77	99.77	99.97	99.97	0.23
CAAE[22]	—	99.99	98.65	99.31	—
MTH-IDS[7]	99.999	—	99.999	99.999	0.000 6
集成模型	**100**	**100**	**100**	**100**	**0**

注: 加粗字体表示最优值

表 4 CICIDS2017 数据集上已知攻击检测结果对比 (%)

方法	*Acc*	*Pre*	*Rec*	*F*1	*FAR*
KNN[23]	98.69	99.67	99.73	99.56	0.15
SVC[23]	96.19	96.19	95.23	95.24	0.42
CANET[24]	99.88	—	99.82	—	0.06
ANN[5]	99.58	99.56	99.58	99.54	0.63
LSTM[5]	99.57	99.55	99.57	99.54	0.79
MTH-IDS[7]	99.895	—	99.806	99.895	0.084
集成模型	**99.967**	**99.967**	**99.967**	**99.967**	**0.029**

注: 加粗字体表示最优值

2.5 未知 DoS 攻击检测结果分析

对于未知 DoS 攻击检测, 因 Car-Hacking 数据集中只有一种 DoS 攻击类型, 故将该类别的 DoS 攻击作为未知攻击. 由表 5 可知, 对于 Car-Hacking 数据集中未知 DoS 攻击的检测, 其检测准确率高达 100%, 与 MTH-IDS[7]持平, 但相比于其他无监督和半监督方法在准确率上提升了 2.1%–30.95%, 在精确率上提升了 0.08%–44.28%, 在召回率上提升了 0.12%–69.82%, 在 *F*1 分数上提升了 0.93%–54.42%. 对于 CICIDS2017 数

据集而言, 该数据集包含多种不同类别的 DoS 攻击数据, 分别将每种 DoS 攻击作为未知攻击进行多组实验, 并将堆叠集成模型识别为“正常”的数据输入到 CDAE-AM 模型中. 由表 6 可知, 堆叠集成模型在未知 DoS 攻击检测方面, 误报数低, 能够准确识别正常数据, 但是漏报数极高, 将大量未知 DoS 攻击都识别为“正常”数据, 因而采用无监督模型 CDAE-AM 弥补这一缺点. 由表 7 可知, 接收堆叠集成模型输出的“正常”数据, CDAE-AM 模型对各类未知 DoS 攻击的检测的平均召回率和平均 *F*1 分数分别为 83.953% 和 83.186%, 平均误报率为 2.383%. 虽然 MTH-IDS[7]在 Car-Hacking 数据集上对于未知 DoS 攻击检测的召回率、*F*1 分数以及误报率与本文所提出的方法相同, 但在 CICIDS2017 数据集中对各类未知 DoS 攻击检测的平均召回率和平均 *F*1 分数上, 本文方法分别提升了 4.853% 和 2.066%, 在平均误报率上降低了 12.474%, 而且经过多组实验分析表明, 相比于无监督模型 AE、CAE 和 CDAE, CDAE-AM 在各项评价指标上表现更优. 因此, 实验结果表明, 所提方法相比于其他的无监督方法具有一定的优势, 可以有效检测车内和车外网络数据集中的未知 DoS 攻击, 但是零日攻击检测仍然是一个极具挑战性的难题, 仍需要去不断地改进.

表 5 Car-Hacking 数据集上未知攻击检测结果对比 (%)

方法	*Acc*	*Pre*	*Rec*	*F*1	*FAR*
OCSVM[25]	69.05	55.72	99.31	71.39	—
SVM[25]	71.99	93.13	30.18	45.58	—
DAE[25]	96.24	91.27	99.88	95.38	—
CAAE[22]	—	99.92	98.23	99.07	—
MTH-IDS[7]	—	—	100	100	0
GIDS[18]	97.9	96.8	99.6	—	—
CDAE-AM	**100**	**100**	**100**	**100**	**0**

注: 加粗字体表示最优值

表 6 堆叠集成模型未知攻击检测结果

攻击类型	样本数	检测数	漏报数	误报数
DDoS	128 027	72 427	55 600	98
DoS GoldenEye	10 293	5 155	5 138	94
DoS Hulk	231 073	1 127	229 946	57
DoS Slowhttptest	5 499	1 791	3 708	62
DoS Slowloris	5 796	4 852	944	89
Heartbleed	11	0	11	90

2.6 系统可行性分析

不同于一般网络的 IDS, 车联网环境下的 IDS 在实现高精度检测的同时, 还需要满足车联网系统实时性的要求, 从而减小车辆系统的延迟, 并且考虑到车载控制器在计算和存储资源上的限制, 需要选择较小的入侵检测模型以确保整个车载系统的能够正常运行.为评估所提出的 IDS 在车辆系统中的可行性, 通过单线程模拟部署模型推理, 分别对 Car-Hacking 数据集和 CICIDS2017 数据集下的整个 IDS 的模型大小及单个报文的平均测试时间进行了分析. 如表 8 所示, 上述两个数据集中的每个数据包的平均测试时间分别为 0.072 ms 和 0.157 ms, 远小于车辆交通安全应用中 10 ms 的延时要求[7], 对车联网的实时性影响较低. 而且 IDS 模型的总大小分别为 2.488 MB 和 39.910 MB, 可以满足大多数车载控制器的资源限制. 因此, 实验分析结果表明, 所提系统在实时车载系统上具有一定的可行性.

表 7 CICIDS2017 数据集上未知攻击检测结果对比 (%)

攻击类型	方法	*Acc*	*Pre*	*Rec*	*F*1	*FAR*
DDoS	MTH-IDS[7]	—	—	62.697	71.902	11.698
	AE	78.957	81.991	78.957	78.446	5.646
	CAE	79.312	83.109	79.312	78.702	3.755
	CDAE	79.486	83.186	79.486	78.898	3.819
	CDAE-AM	**79.712**	**83.759**	**79.712**	**79.085**	**2.977**
DoS GoldenEye	MTH-IDS[7]	—	—	83.931	82.127	20.461
	AE	83.299	85.920	83.299	82.989	3.196
	CAE	84.601	86.726	84.601	84.375	3.371
	CDAE	84.752	87.091	84.752	84.507	**2.691**
	CDAE-AM	**84.786**	**87.099**	**84.786**	**84.545**	2.730
DoS Hulk	MTH-IDS[7]	—	—	67.440	75.248	11.806
	AE	80.872	83.299	80.872	80.517	5.629
	CAE	81.786	84.690	81.786	81.397	3.746
	CDAE	81.749	84.660	81.749	81.357	3.760
	CDAE-AM	**82.078**	**85.240**	**82.078**	**81.666**	**2.943**
DoS Slowhttptest	MTH-IDS[7]	—	—	76.687	78.339	19.094
	AE	63.202	74.027	63.202	58.532	3.237
	CAE	87.298	88.608	87.298	87.189	3.492
	CDAE	89.716	90.253	89.716	89.682	4.510
	CDAE-AM	**90.071**	**90.907**	**90.071**	**90.020**	**2.782**
DoS Slowloris	MTH-IDS[7]	—	—	**83.834**	**87.447**	7.902
	AE	66.546	74.026	66.546	63.722	5.556
	CAE	66.831	75.926	66.831	63.642	3.554
	CDAE	67.055	75.995	67.055	63.956	3.623
	CDAE-AM	**67.072**	**76.739**	67.072	63.800	**2.864**
Heartbleed	MTH-IDS[7]	—	—	100	91.667	18.182
	AE	100	100	100	100	0
	CAE	100	100	100	100	0
	CDAE	100	100	100	100	0
	CDAE-AM	**100**	**100**	**100**	**100**	**0**
Average	MTH-IDS[7]	—	—	79.10	81.12	14.857
	AE	78.813	83.211	78.813	77.368	3.877
	CAE	83.305	86.510	83.305	82.551	2.986
	CDAE	83.793	86.864	83.793	83.067	3.067
	CDAE-AM	**83.953**	**87.291**	**83.953**	**83.186**	**2.383**

注: 加粗字体表示最优值

表 8 系统可行性分析

数据集	系统组件	平均测试时间 (ms)	大小 (MB)
Car-Hacking	签名检测	0.002	0.300
	异常检测	0.070	2.188
	总计	**0.072**	**2.488**
CICIDS2017	签名检测	0.074	37.195
	异常检测	0.083	2.715
	总计	**0.157**	**39.910**

3 结论

针对 DoS 攻击下车联网网络入侵检测问题, 本文提出一种结合签名检测方法和异常检测方法的混合入侵检测系统, 用于检测车联网中可能出现的已知和未知 DoS 攻击. 对于混合 IDS 中的签名检测, 通过树结构堆叠集成模型来检测已知 DoS 攻击; 对于异常检测, 通过无监督模型 CDAE-AM 来检测堆叠集成模型漏报的未知 DoS 攻击. 采用分别代表车内网和车外网的 Car-Hacking 数据集和 CICIDS2017 数据集对所提系统进行性能评估, 并基于准确率 (*Acc*)、精确率 (*Pre*)、召回率 (*Rec*)、*F*1 分数以及误报率 (*FAR*) 这 5 个指标验证了所提系统的优势. 对于已知 DoS 攻击的检测, 在两个数据集上的准确率分别为 100% 和 99.967%; 对于未知 DoS 攻击的检测, 准确率分别为 100% 和 83.953%, 与其他方法比较的结果表明所提系统的综合性能表现更优. 同时, 所提系统在两个数据集上的平均测试时间较短且占用内存资源较少, 具有一定的可行性. 在未来的工作中, 可以考虑研究如何有效检测车联网中可能出现的所有攻击, 而不仅是 DoS 攻击, 从而进一步提升模型整体检测性能.

参考文献

1 况博裕, 李雨泽, 顾芳铭, 等. 车联网安全研究综述: 威胁、对策与未来展望. 计算机研究与发展, 2023, 60(10): 2304–2321. [doi: 10.7544/issn1000-1239.202330464]

2 吴武飞, 李仁发, 曾刚, 等. 智能网联车网络安全研究综述. 通信学报, 2020, 41(6): 161–174. [doi: 10.11959/j.issn.1000-436x.2020130]

3 李兴华, 钟成, 陈颖, 等. 车联网安全综述. 信息安全学报, 2019, 4(3): 17–33. [doi: 10.19363/J.cnki.cn10-1380/tn.2019.05.02]

4 关宇昕, 冀浩杰, 崔哲, 等. 智能网联汽车车载 CAN 网络入侵检测方法综述. 汽车工程, 2023, 45(6): 922–935. [doi: 10.19562/j.chinasae.qcgc.2023.ep.002]

5 Gamage S, Samarabandu J. Deep learning methods in network intrusion detection: A survey and an objective comparison. Journal of Network and Computer Applications, 2020, 169: 102767. [doi: 10.1016/j.jnca.2020.102767]

6 Madhu B, Chari MVG, Vankdothu R, *et al*. Intrusion detection models for IoT networks via deep learning approaches. Measurement: Sensors, 2023, 25: 100641. [doi: 10.1016/j.measen.2022.100641]

7 Yang L, Moubayed A, Shami A. MTH-IDS: a multitiered hybrid intrusion detection system for Internet of Vehicles. IEEE Internet of Things Journal, 2022, 9(1): 616–632. [doi: 10.1109/JIOT.2021.3084796]

8 Li SF, Cao Y, Liu SH, *et al*. HDA-IDS: A hybrid DoS attacks intrusion detection system for IoT by using semi-supervised CL-GAN. Expert Systems with Applications, 2024, 238: 122198. [doi: 10.1016/j.eswa.2023.122198]

9 Ikotun AM, Ezugwu AE, Abualigah L, *et al*. K-means clustering algorithms: A comprehensive review, variants analysis, and advances in the era of big data. Information Sciences, 2023, 622: 178–210. [doi: 10.1016/j.ins.2022.11.139]

10 Chen ZX, Yan QB, Han HB, *et al*. Machine learning based mobile malware detection using highly imbalanced network traffic. Information Sciences, 2018, 433–434: 346–364. [doi: 10.1016/j.ins.2017.04.044]

11 Salo F, Nassif AB, Essex A. Dimensionality reduction with IG-PCA and ensemble classifier for network intrusion detection. Computer Networks, 2019, 148: 164–175. [doi: 10.1016/j.comnet.2018.11.010]

12 Thakkar A, Lohiya R. Attack classification using feature selection techniques: A comparative study. Journal of Ambient Intelligence and Humanized Computing, 2021, 12(1): 1249–1266. [doi: 10.1007/s12652-020-02167-9]

13 Kannari PR, Chowdary NS, Biradar RL. An anomaly-based intrusion detection system using recursive feature elimination technique for improved attack detection. Theoretical Computer Science, 2022, 931: 56–64. [doi: 10.1016/j.tcs.2022.07.030]

14 Zhang CY, Jia DH, Wang LY, *et al*. Comparative research on network intrusion detection methods based on machine learning. Computers & Security, 2022, 121: 102861. [doi: 10.1016/j.cose.2022.102861]

15 Cao YZ, Wang ZH, Ding HW, *et al*. An intrusion detection system based on stacked ensemble learning for IoT network. Computers and Electrical Engineering, 2023, 110: 108836. [doi: 10.1016/j.compeleceng.2023.108836]

16 Yang L, Shami A. On hyperparameter optimization of

machine learning algorithms: Theory and practice. Neurocomputing, 2020, 415: 295–316. [doi: 10.1016/j.neucom.2020.07.061]

17 Mushtaq E, Zameer A, Umer M, *et al*. A two-stage intrusion detection system with auto-encoder and LSTMs. Applied Soft Computing, 2022, 121: 108768. [doi: 10.1016/j.asoc.2022.108768]

18 Seo E, Song HM, Kim HK. GIDS: GAN based intrusion detection system for in-vehicle network. Proceedings of the 16th Annual Conference on Privacy, Security and Trust. Belfast: IEEE, 2018. 1–6. [doi: 10.1109/PST.2018.8514157]

19 Sharafaldin I, Lashkari AH, Ghorbani AA. Toward generating a new intrusion detection dataset and intrusion traffic characterization. Proceedings of the 4th International Conference on Information Systems Security and Privacy. Funchal: SciTePress, 2018. 108–116. [doi: 10.5220/0006639801080116]

20 Song HM, Woo JY, Kim HK. In-vehicle network intrusion detection using deep convolutional neural network. Vehicular Communications, 2020, 21: 100198. [doi: 10.1016/j.vehcom.2019.100198]

21 Khatri N, Lee S, Nam SY. Transfer learning-based intrusion detection system for a controller area network. IEEE Access, 2023, 11: 120963–120982. [doi: 10.1109/ACCESS.2023.3328182]

22 Hoang TN, Kim D. Detecting in-vehicle intrusion via semi-supervised learning-based convolutional adversarial autoencoders. Vehicular Communications, 2022, 38: 100520. [doi: 10.1016/j.vehcom.2022.100520]

23 Danso PK, Neto ECP, Dadkhah S, *et al*. Ensemble-based intrusion detection for Internet of Things devices. Proceedings of the 19th IEEE International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI. Marietta: IEEE, 2022. 34–39. [doi: 10.1109/HONET56683.2022.10019140]

24 Ren KY, Yuan S, Zhang C, *et al*. CANET: A hierarchical CNN-attention model for network intrusion detection. Computer Communications, 2023, 205: 170–181. [doi: 10.1016/j.comcom.2023.04.018]

25 Song HM, Kim HK. Self-supervised anomaly detection for in-vehicle network using noised pseudo normal data. IEEE Transactions on Vehicular Technology, 2021, 70(2): 1098–1108. [doi: 10.1109/TVT.2021.3051026]

(校对责编: 王欣欣)