DOI:10.19651/j.cnki.emt.2417438

双线性自注意力机制CAN总线入侵检测方法研究*

陈彦彬[1,2] 刘桂雄[2]

(1.揭阳职业技术学院实训与信息中心 揭阳 522051;2.华南理工大学机械与汽车工程学院 广州 510640)

摘 要:控制器局域网络(CAN)总线广泛应用于工业数据采集、车联网等领域,对其安全入侵检测非常重要。为全面提升检测方法性能,提出一种双线性自注意力机制CAN总线入侵检测方法,首先基于堆叠集成思想利用DNN、CNN和LSTM模型提取深度学习层特征;随后通过双线性层分别提取自注意力机制Transformer与FNet特征,再将其与深度学习层特征残差连接融合;最后通过全连接层入侵检测预测,体现高准确率、检测率和良好泛化性特点。在Car_Hacking公开数据集上实验表明,准确率、精确率、召回率、F1值和AUC值分别达0.951、0.996、0.997、0.960和0.984,且随着训练轮数增加其准确率、损失值误差分别保持在5%、10%以内,本文方法优于其他比较方法。应用于物联网实验装置评估结果显示,本文方法在异常攻击识别检测率达99.23%,对于提高测控系统安全性能具有重要推广价值。

关键词:入侵检测系统;控制区域网络CAN;自注意力机制;FNet

中图分类号:TN919 **文献标识码**:A **国家标准学科分类代码**:510.1010;510.4010

Study on bilinear self-attention mechanism for CAN bus intrusion detection method

Chen Yanbin[1,2] Liu Guixiong[2]

(1. Training and Information Center, Jieyang Polytechnic, Jieyang 522051, China;
2. School of Mechanical & Automotive Engineering, South China University of Technology, Guangzhou 510640, China)

Abstract: The controller area network (CAN) bus is widely used in industrial data acquisition, internet of vehicles and other fields, making its security intrusion detection very important. To comprehensively enhance the performance of the detection method, a bilinear self-attention mechanism for CAN bus intrusion detection is proposed. Firstly, based on the idea of stacked integration, DNN, CNN and LSTM models are used to extract and generate deep learning layer feature data; then, bilinear layers are used to generate self-attention mechanism and FNet feature data separately, which are then fused with deep learning layer feature data through a residual connection layer, and intrusion detection prediction is performed through a fully connected layer, demonstrating high accuracy, detection rate, and good generalization characteristics. Experiments on the Car_Hacking public dataset show that the accuracy, precision, recall, F1 score and AUC values are 0.951, 0.996, 0.997, 0.960 and 0.984, respectively, and as the number of training epochs increases, the accuracy and loss value error remain within 5% and 10%, respectively, indicating that this method outperforms other comparison methods. Application to IoT experimental devices evaluation shows that this method achieves a detection rate of 99.23% for abnormal attack identification, which has significant promotion value for enhancing the security performance of monitoring and control systems.

Keywords: intrusion detection system; controller area network; self-attention mechanism; FNet

0 引 言

控制区域网络(controller area network,CAN)总线是电子系统中应用广泛通信协议之一[1-3],但其面临着严峻安全挑战,主要表现为攻击者通过操纵CAN总线通信来干扰电子系统,使其遭受洪水攻击、欺骗攻击等各种恶意攻击,这可能导致电子系统功能异常、数据隐私泄露,甚至引发安全事故,故CAN总线入侵检测成为保障工业互联网、

收稿日期:2024-11-25

*基金项目:广东省科技厅特派员重点派驻任务(KTP20210400)、广东省高等教育学会"十四五"规划高等教育研究课题(22GYB018)项目资助

电子系统安全的重要手段及措施[4]。近年来,国内外学者研究应用统计分析、传统机器学习和深度学习等多种 CAN 总线入侵检测方法[5-10]。基于统计分析方法是对数据流量等参数统计学规律分析进行入侵检测,适用小样本、假设明确场景,但对数据量偏大、新型攻击适应性较差,如利用信息熵偏差分析的 CAN 入侵检测算法[11]、多目标优化信息熵入侵检测算法[12]、应用流量伪周期性的异常检测算法[13]、融合报文稳定性特征的入侵检测算法[14],以及信息熵重叠滑动窗口优化快速响应入侵检测系统[15]等。传统机器学习方法是利用支持向量机、树模型和聚类等提取特征进行入侵检测[16-18],具有模型相对简单、计算量小等特点,适用样本数据不平衡场景,但对于数据上下文语义、报文之间依赖关系等特征提取能力较弱,如研究支持向量机(support vector machine,SVM)非线性变化入侵检测算法实现对周期性和非周期性的异常报文数据识别[19];Derhab 等人研究利用 SVM 直方图入侵检测算法,使用特定的直方图捕捉数据报文频率、ID 和长度等特征实现攻击预测[20]。深度学习方法主要利用神经网络提取深层次特征进行入侵检测,适合于复杂、大规模数据场景,其通过单一或多种深度学习模型以串行、并行或串并混合叠加方式搭建网络模型以增强检测效果,但其容易发生过拟合,实际应用须权衡准确性、泛化性问题,如提取数据字段特征多层串行长短期记忆网络(long short-term memory, LSTM)入侵检测算法[21]、混合攻击场景下结合深度信念网络(deep belief network, DBN)与门控循环单元(gated recurrent unit,GRU)入侵检测算法[22]、利用自动编码器及深度神经网络(deep neural network,DNN)解决灾难性遗忘问题入侵检测算法[23],及构建多路卷积神经网络(convolutional neural networks, CNN)+LSTM 串行自注意力机制入侵检测算法[24]等,它们提取 CAN 总线数据局部、上下文长距离依赖关系等深层次特征仍不够全面丰富。

本文针对文献[24]所提方法在提取深层次特征时随着模型深度增加在一定程度上存在特征表示弱化问题,结合应用 DNN、CNN、LSTM 提取特征以整合深度学习模型优势、引入残差连接对经自注意力机制前后特征向量进行残差连接以防止特征弱化、引入 FNet+Transformer 双线性自注意力机制以丰富特征表示等方面对深度学习入侵检测方法加以改进提升[25],作者相关方法《双线性注意力机制物联网攻防方法及系统》(ZL2024109699778)获授权国家发明专利[26]。

1 CAN 总线原理与攻击类型

为了便于更好论述 CAN 总线入侵检测方法检测原理,下面先简要叙述 CAN 总线基本原理与主要攻击类型。

CAN 总线是一种多主机、多从机系统的串行通信协议,通过差分信号线、冲突检测和 CRC 校验等来确保数据传输可靠性及通信稳定性能[27]。CAN 总线上每个节点均可充当主机(或从机),多个节点能同时在总线上进行通信,节点设备以广播形式、没有加密与认证在 CAN 总线上传输数据帧。CAN 总线通过 CAN_H、CAN_L 高低电平两根差分信号线传输,含隐性、显性电平两种逻辑状态(逻辑 1、0),逻辑状态通过总线电平 U_{diff} 确定,令信号线 CAN_H、CAN_L 上电压分别为 U_{CAN_H}、U_{CAN_L},则 $U_{diff}=U_{CAN\_H}-U_{CAN\_L}$,且 $U_{diff}\approx 2$ V,显性电平(逻辑 0);$U_{diff}\approx 0$ V,隐性电平(逻辑 1)。

CAN 总线主要攻击类型有洪水攻击(flooding)、模糊攻击(fuzzing)、重放攻击(replay)和欺骗攻击(spoofing)等[28]。其中,洪水攻击 flooding 表现为攻击者通过向 CAN 总线发送大量无效数据帧,使正常通信受阻以干扰目标系统,如攻击者向电子系统发送大量虚假 CAN 消息,占用总线带宽,导致正常控制消息难以传递;模糊攻击 fuzzing 表现为攻击者通过向系统输入异常、随机的数据以发现潜在漏洞,如攻击者向电子系统发送异常、随机的 CAN 消息,导致系统错误、漏洞暴露;重放攻击 replay 表现为攻击者截获 CAN 总线上数据帧,并重新发送这些数据帧以模拟合法用户行为,如攻击者向电子系统发送重复指令或数据,致系统混乱、产生安全漏洞;欺骗攻击 spoofing 表现为攻击者伪装成合法节点向 CAN 总线发送虚假数据帧,欺骗系统以执行恶意操作,如攻击者向电子系统发送虚假的 CAN 消息,导致系统决策错误。

2 双线性自注意力机制 CAN 总线入侵检测方法机理

双线性自注意力机制 CAN 总线入侵检测方法机理如图 1 所示,攻击者向 CAN 总线发起攻击,入侵检测系统通过采集到攻击数据帧、特征数据标准化、双线性自注意力机制完成入侵检测预测并向总线上设备发出攻击检测结果,通知节点设备 CAN 总线上存在攻击以便做好防护。

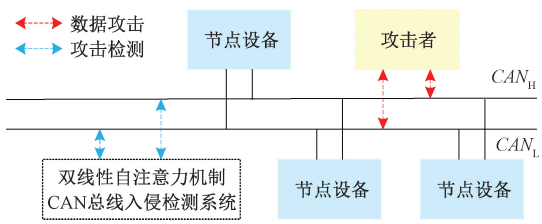

图 1 CAN 总线入侵检测方法机理框图

Fig. 1 Mechanism diagram of CAN bus intrusion detection method

本文提出的双线性自注意力机制 CAN 总线入侵检测方法网络架构如图 2 所示,分为输入层、深度学习层、双线性层、残差连接层、输出层等,这里深度学习层主要含 DNN[29]、CNN[30]、LSTM[31]等 3 种模型。首先,输入层输入标准化特征向量 $\boldsymbol{x}$ 到深度学习层提取特征;然后通过双线性层对深度学习特征向量拼接以生成更丰富特征表示,并利用 FNet+自注意力机制 Transformer 提取特征;再与

深度学习特征残差连接运算，以整合深度学习模型优势防止特征弱化；最后经两个全连接层进行入侵检测分类预测。

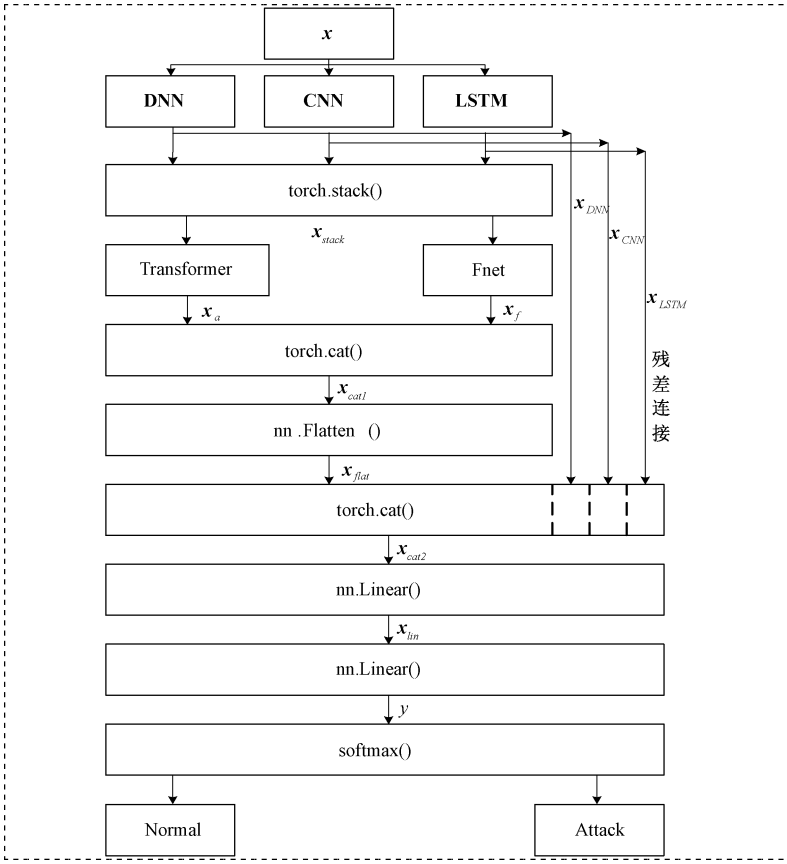

图 2　CAN 总线入侵检测方法网络架构框图

Fig. 2　Network architecture diagram of CAN bus intrusion detection method

下面讨论分析特征融合机制、FNet＋Transformer 双线性机制的实现方法。

2.1　特征融合机制实现

为更好地检测出 CAN 总线数据攻击，需进行特征数据标准化，特征数据标准化格式构成如图 3 所示。入侵检测系统通过采集到攻击数据帧，并进行如下操作：1）对 11 bit 的 *Arbitration_ID* 进行 one-hot 编码，形成 one-hot 编码向量 $ID\in R^{48}$；2）将 *Data* 以字节为单位分别转化为整数序列，并形成数据域向量 $DATA\in R^{8}$；3）对标签 *Label* 进行向量化处理，形成标签向量 $\boldsymbol{L}\in R$。原始 CAN 总线数据帧经向量化并分组（$time\_step=64$）后形成输入特征向量 $\boldsymbol{x}\in R^{64\times 57}$，即可输入双线性自注意力机制 CAN 总线入侵检测方法进行入侵检测预测输出。

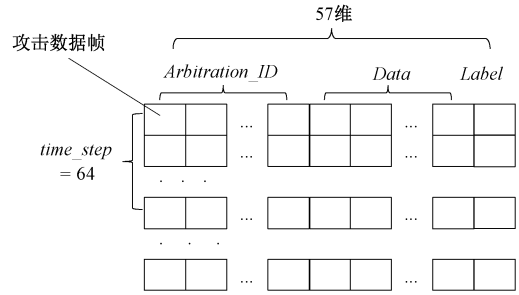

图 3　特征数据标准化格式构成

Fig. 3　Composition of feature data standardization format

1）特征拼接融合

为充分发挥多种神经网络模型优势，图 2 标准化后的特征向量 $\boldsymbol{x}$ 经过 DNN、CNN 和 LSTM 深度学习模型提取特征，分别形成特征向量 $\boldsymbol{x}_{DNN}\in R^{100}$、$\boldsymbol{x}_{CNN}\in R^{100}$、$\boldsymbol{x}_{LSTM}\in R^{100}$。

若向量水平、垂直拼接操作分别用⊕、⊙表示，则第 I 次融合将深度学习模型特征向量 $\boldsymbol{x}_{DNN}$、$\boldsymbol{x}_{CNN}$、$\boldsymbol{x}_{LSTM}$ 通过 $\boldsymbol{x}_{stack}=\boldsymbol{x}_{DNN}\odot\boldsymbol{x}_{CNN}\odot\boldsymbol{x}_{LSTM}$ 运算为特征向量 $\boldsymbol{x}_{stack}\in R^{3\times 100}$；第 II 次融合将自注意力 Transformer 特征向量 $\boldsymbol{x}_{a}\in R^{3\times 100}$ 与 FNet 特征向量 $\boldsymbol{x}_{f}\in R^{3\times 100}$ 通过 $\boldsymbol{x}_{cat1}=\boldsymbol{x}_{a}\oplus\boldsymbol{x}_{f}$ 运算为特征向量 $\boldsymbol{x}_{cat1}\in R^{6\times 100}$。

输出层通过两个全连接层，先将特征向量 $\boldsymbol{x}_{cat2}\in R^{900}$ 转换为特征向量 $\boldsymbol{x}_{lin}\in R^{100}$，再将特征向量 $\boldsymbol{x}_{lin}$ 转换为输出 $\boldsymbol{y}\in R^{2}$，并经 $softmax(\cdot)$ 激活函数输出入侵检测二分类预测结果。

2）残差融合

引入残差连接目的是防止神经网络模型特征弱化，残差连接结构如图 4 所示，主要由展平操作、拼接操作和残

差连接组成。

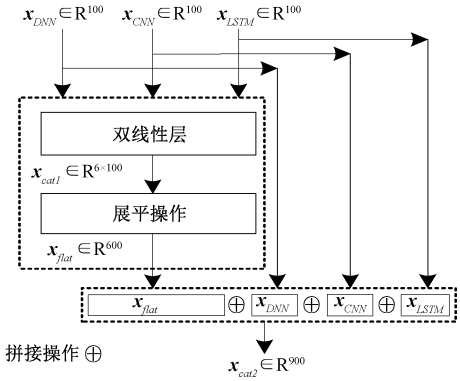

图 4 残差连接结构图

Fig. 4 Residual connection structure diagram

首先,由特征向量 $\boldsymbol{x}_{DNN}$、$\boldsymbol{x}_{CNN}$、$\boldsymbol{x}_{LSTM}$ 经双线性层输出特征向量 $\boldsymbol{x}_{cat1}\in R^{6\times100}$,经展平操作得特征向量 $\boldsymbol{x}_{flat}\in R^{600}$;最后,再利用 $\boldsymbol{x}_{cat2}=x_{flat}\oplus\boldsymbol{x}_{DNN}\oplus\boldsymbol{x}_{CNN}\oplus\boldsymbol{x}_{LSTM}$ 拼接运算,得到残差连接特征向量 $\boldsymbol{x}_{cat2}\in R^{900}$。

2.2 FNet+Transformer 双线性自注意力机制

在 Transformer 上融合 FNet 形成双线性自注意力机制以丰富模型特征表示。

Transformer 通过对特征向量 $\boldsymbol{x}_{stack}$ 进行自注意力计算以捕捉关联信息。设特征向量 $\boldsymbol{x}_{stack}$ 矩阵、查询向量 $\boldsymbol{Q}$、键向量 $\boldsymbol{K}$、数值向量 $\boldsymbol{V}$ 对应参数矩阵和键向量维度分别为 $\boldsymbol{X}_S$、$\boldsymbol{W}_Q$、$\boldsymbol{W}_K$、$\boldsymbol{W}_V$ 和 d_k,则 Transformer 自注意力分数 Attention 计算公式[23]:

$$\text{Attention}=softmax\left[\frac{\mathbf{X}_S\mathbf{W}_Q(\mathbf{X}_S\mathbf{W}_K)^{\mathrm{T}}}{\sqrt{d_k}}\right]\mathbf{X}_S\mathbf{W}_V \tag{1}$$

令 Transformer 维度 d_model、注意力头数 $nhead$ 分别为 100、2,则经过 Transformer 后输出得特征向量 $\boldsymbol{x}_a\in R^{3\times100}$。

傅里叶变换广泛应用于信号检测与处理领域[25,32-35]。FNet[25]使用 FNetBlock 变换、FeedForward 神经网络迭代循环对特征向量 $\boldsymbol{x}_{stack}$ 变换,FNet 特征提取流程如图 5 所示,其中 FNetBlock 变换含 2 次一维快速傅里叶变换 f_t 再取实部计算 Re 记 $Re\{f_t[f_t(\cdot)]\}$;FeedForward 神经网络含线性变换 Linear、激活函数 GELU、丢弃 Dropout 等处理;步骤 Step2、4 的 PreNorm 层进行层归一化、残差连接运算。设线性变换输出为 $\boldsymbol{x}_{fn\_lin}\in R^{100}$,则 GELU 计算公式[24]:

$$\text{GELU}(\boldsymbol{x}_{fn\_lin})\approx 0.5\boldsymbol{x}_{fn\_lin}\left\{1+\tanh\left[\sqrt{\frac{2}{\pi}}(\boldsymbol{x}_{fn\_lin}+0.044\,715\boldsymbol{x}_{fn\_lin}{}^3)\right]\right\} \tag{2}$$

若模型深度 $D_{epth}=2$、线性变换隐藏维度 $Dim_{hid}=100$ 和丢弃率 $D_{ropout}=0.01$,则经迭代递归计算得特征向量 $\boldsymbol{x}_f\in R^{3\times100}$。

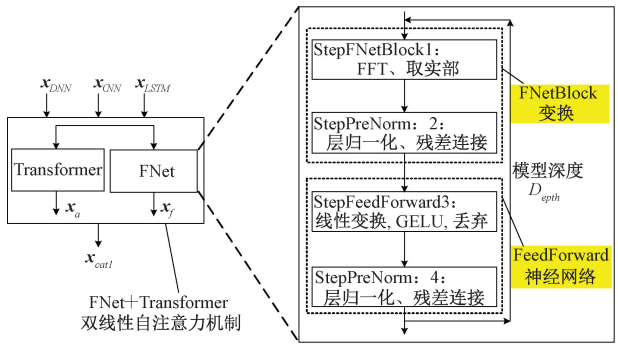

图 5 FNet 特征提取流程图

Fig. 5 FNet feature extraction flowchart

3 实验验证及对比分析

3.1 实验准备

选择具有各类总线攻击的公开数据集 Car_ Hacking_Challenge_Dataset_rev20Mar2021[36](Car_Hacking)作为实验数据集(含 806 390 条记录,具有 *Timestamp*、*Arbitration_ID*、*DLC*、*Data*、*Class*、*SubClass* 等 6 个方面特征属性),对原始数据集标准化并分组($time\_step=64$),形成输入数据集 $\boldsymbol{X}\in R^{12\,600\times64\times57}$。表 1 为 Car_Hacking 输入数据集,特征数据标准化按 2.1 节图 3 格式进行。训练集、验证集划分比例为 90%、10%。双线性自注意力机制 CAN 总线入侵检测方法算法采用 Python 3 编写,深度学习框架选择 PyTorch,计算环境选用谷歌提供 google colab 云平台,并配置 T4 GPU 硬件加速器。

表 1 Car_Hacking 输入数据集

Table 1 Car_Hacking input dataset

标签	原始数量/条	数据标准化后数量/条
Normal	733 752	7 393
Attack	72 638	5 207
总数	806 390	12 600

选用精确率(Precision)、召回率(Recall)、准确率(Accuracy)、F1 值(F1 Score)和 AUC 值(area under the ROC curve)等 4 个评价指标。令正确检到正常、攻击数据帧数量分别为 TP、TN;误检、漏检中正常数据帧数量分别为 FP、FN;正常、攻击数据中帧数量分别为 m、n;正常、攻击数据中帧预测得分分别为 S_p、S_n;若 $S_{pi}>S_{nj}$、$S_{pi}=S_{nj}$,指示函数 $I(S_{pi},S_{nj})$分别取值 1、0.5,否则其值为 0。评价指标公式如下:

$$\begin{cases}\text{Precision}=\dfrac{TP}{TP+FP};\ \text{Recall}=\dfrac{TP}{TP+FN}\\ \text{Accuracy}=\dfrac{TP+TN}{TP+TN+FP+FN}\\ \text{F1}=\dfrac{2TP}{2TP+FP+FN}\\ \text{AUC}=\dfrac{1}{m+n}\displaystyle\sum_{i=1}^{m}\sum_{j=1}^{n}I(S_{p_i},S_{n_j})\end{cases} \tag{3}$$

表 2 为实验模型参数表。双线性自注意力机制 CAN 总线入侵检测方法算法中训练数据批次大小、次数、分组时间步及检测分类数分别设置 20、3、64、2，学习率、丢弃率分别设置为 0.001、0.01，选用 Adam 优化器、CrossEntropy 损失函数。

表 2　实验模型参数表

Table 2　Experimental model parameters

参数名称	指标值	参数名称	指标值
批次大小 *batch_size*	20	损失函数 *Loss*	CrossEntropy
训练次数 *epochs*	3	优化器 *Optimizer*	Adam
分组时间步 *time_step*	64	学习率 *Learning*	0.001
检测分类数 *nb_class*	2	丢弃率 *dropout*	0.01

3.2　模型评价指标对比

在实验中，选取以下经典机器学习算法及深度学习模型作为对比算法模型以对比评估检测性能，包含决策树（模型 I）、随机森林（模型 II）、逻辑回归（模型 III）、xgboost（模型 IV）、DNN（模型 V）、LSTM（模型 VI）、CNN（模型 VII）、Tansformer（模型 VIII）、文献[24]模型（模型 IX）以及本文方法（模型 X）。

表 3 为不同模型在文献[36]数据集上进行实验评估对比结果，显示本文模型 X 的 Accuracy、Precision、Recall、F1、AUC 均高于所有对比方法，分别达到 0.951、0.996、0.997、0.960 和 0.984，显示出模型 X 在 CAN 总线入侵检测方面具有明显性能优势。

表 3　不同模型在 Car_Hacking 数据集上实验评估对比

Table 3　Comparison of experimental evaluations of different models on the Car_Hacking dataset

模型编号	模型名称	Accuracy	Precision	Recall	F1	AUC
I	决策树	0.699	0.746	0.749	0.747	0.688
II	随机森林	0.741	0.749	0.848	0.796	0.778
III	逻辑回归	0.699	0.702	0.858	0.772	0.712
IV	xgboost	0.872	0.836	0.976	0.901	0.927
V	DNN	0.848	0.871	0.874	0.873	0.915
VI	LSTM	0.852	0.963	0.983	0.888	0.902
VII	CNN	0.890	0.925	0.956	0.912	0.938
VIII	Transformer	0.852	0.963	0.983	0.888	0.902
IX	文献[24]模型	0.860	0.856	0.860	0.858	0.927
X	本文方法	**0.951**	**0.996**	**0.997**	**0.960**	**0.984**

表 4 为本文方法消融实验评估对比结果，分别比较仅 FNet、仅 Transformer、FNet＋Transformer 与本文方法性能。实验结果显示本文方法在 Accuracy、Precision、Recall、F1、AUC 等性能指标均高于对比方法，表明 FNet、Transformer、残差连接有利于提升本文方法检测性能。

表 4　本文方法消融实验评估对比

Table 4　Ablation experiment evaluation comparison of the method in this paper

模型名称	Accuracy	Precision	Recall	F1	AUC
仅 FNet	0.929	0.940	0.920	0.930	0.932
仅 Transformer	0.935	0.930	0.895	0.918	0.965
FNet＋Transformer	0.944	0.988	0.993	0.943	0.977
本文方法	**0.951**	**0.996**	**0.997**	**0.960**	**0.984**

不同模型 ROC 曲线（即接受者操作特性曲线）对比如图 6 所示，横坐标、纵坐标分别为假阳性率 FPR＝$FP/(FP+TN)$、真阳性率 TPR ＝$TP/(TP+FN)$，曲线下面积即为 AUC。模型 X 曲线接近左上角，AUC＝0.984

(接近 1),表明其具有最优检测性能。

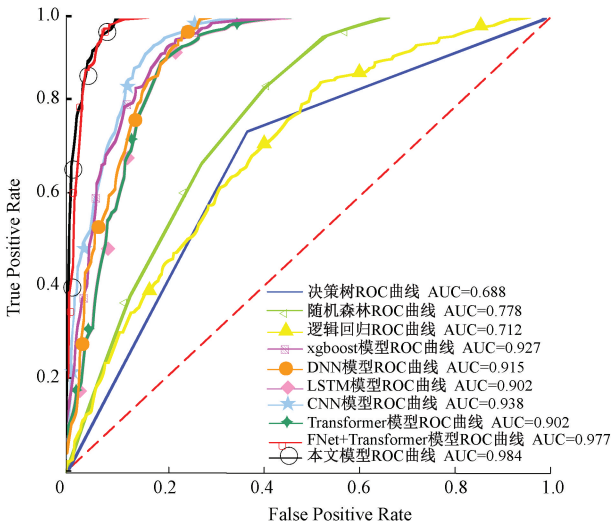

图 6　不同模型 ROC 曲线对比图

Fig. 6　Comparison of ROC curves for different models

3.3　泛化能力分析

本文模型 X 可视化训练过程(*epochs*=5)如图 7 所示,图 7(a)、(b)横坐标均为训练周期(*epochs*),纵坐标为准确率 Accuracy、损失值 LOSS,带空心圈曲线、曲线分别训练集、验证集的可视化训练过程曲线。

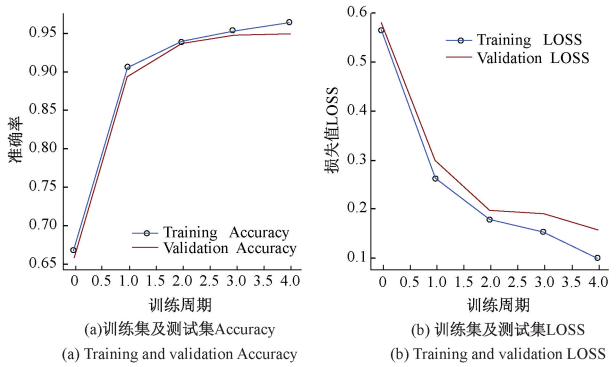

图 7　本文模型 X 可视化训练过程图

Fig. 7　Visualization of the training process for the model X

由图 7(a)、(b)看出,随着 *epochs* 增加,Accuracy 提升,LOSS 下降,且训练集、验证集之间 Accuracy 误差在 5%以内、LOSS 误差在 10%以内,本文模型 X 体现出较好的泛化能力。

4　实验装置设计与应用结果

本文搭建实验装置系统拓扑如图 8 所示,包括 CAN 总线节点设备、嵌入式网关、PC 攻击端和 Gradio 服务器等,目的是用于验证 CAN 总线入侵检测方法有效性。

CAN 总线节点设备采用 STM32 系列处理器自带基本扩展 CAN 外设(即 bxCAN),支持 CAN 协议 2.0A、2.0B 主动模式,最高波特率 1 Mbps,具有 2 个 3 级深度接收 FIFO[37]。通过 STM32F103VET6 主控芯片自带 CAN 控制器,搭建 CAN 总线节点设备,建立 CAN 总线网络。

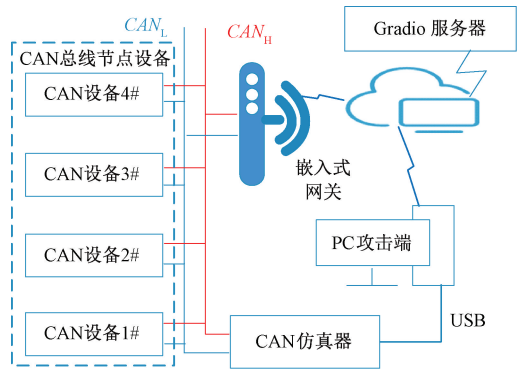

图 8　实验装置系统拓扑图

Fig. 8　System topology diagram of the experimental setup

嵌入式网关作为实验装置数据格式转换设备,起到实时监测、处理 CAN 总线数据流作用,它以 JSON 格式将检测数据推送至 Gradio 服务器并接收处理结果。选取搭载 Broadcom BCM2711 处理器树莓派 4B 作为嵌入式网关,具有 CAN 总线接口、wifi 网络接口,运行 linux 操作系统,支持 Python 编程语言,以满足 Gradio 客户端调用需求。

PC 攻击端由计算机、CAN 总线仿真器等组成,使用 CAN 总线仿真器生成各种正常行为、入侵攻击行为数据;可以登录 Gradio 服务器,进行入侵检测服务部署,同时在该电脑上还运行应用程序界面监测检测效果。

Gradio 服务器是整个实验装置核心设备,部署 CAN 总线入侵检测算法并将检测结果推送回嵌入式网关,实现算法部署、用户交互、结果展示与传递。

在搭建完实验装置后,分别将本文模型 X、FNet+Transformer 模型部署到 Gradio 服务器,并运行应用程序得到实验装置用户界面,实验装置应用程序界面如图 9 所示,可选择启用 CAN 设备、查看收到 CAN 数据包及检测到入侵数据包数量、显示模型评价指标等。

图 9　实验装置应用程序界面

Fig. 9　Application interface of the experimental setup

实验装置通过嵌入式网关采集监测 CAN 总线数据,

然后调用 Gradio 服务器上入侵检测算法进行检测。以连续方式发送分别含有洪水攻击、模糊攻击、重放攻击和欺骗攻击等攻击的 CAN 总线数据帧，测试单一工况下模型 X 入侵检测效果。表 5 为本文模型 X 在 4 种工况下入侵检测统计，结果表明本文方法对洪水攻击、模糊攻击、重放攻击和欺骗攻击等不同工况下入侵检测效果较好，识别率分别为 99.00%、99.60%、99.20%、99.80%。

表 5　本文模型 X 在 4 种工况下入侵检测统计

Table 5　Intrusion detection statistics of model X under four operating conditions in this paper

工况	发送攻击数据帧	识别攻击数据帧	识别率/%
洪水攻击	500	495	99.00
模糊攻击	500	498	99.60
重放攻击	500	496	99.20
欺骗攻击	500	499	99.80
平均	500	497	99.40

表 6 为不同模型综合工况下入侵检测对比，以连续方式发送含有多种攻击类型的 CAN 总线数据帧，测试综合工况下本文模型 X、FNet＋Transformer 模型入侵检测效果，表明本文方法对 CAN 总线入侵数据帧攻击检测效果最好，识别率达 99.23%，与表 3 结论相同。

表 6　不同模型综合工况下入侵检测对比

Table 6　Comparison of intrusion detection for different models under combined operating conditions

模型名称	发送 CAN 数据帧	发送攻击数据帧	识别攻击数据帧	识别率/%
FNet＋Transformer	3 688	130	118	90.77
模型 X	3 688	130	129	99.23

5　结　　论

本文创新性提出由输入层、深度学习层、双线性层、残差连接层、输出层组成的双线性自注意力机制 CAN 总线入侵检测方法，通过双线性层对深度学习层特征融合并提取注意力机制 Transformer 与 FNet 特征，再残差连接深度学习特征后经输出层完成入侵检测预测输出。在公开数据集实验对比评估其性能并搭建 CAN 总线物联网实验装置验证本文方法有效性，结果表明本文方法比其他对比方法有明显优势，准确率、精确率、召回率、F1 值和 AUC 值分别为 0.951、0.996、0.997、0.960 和 0.984；综合工况下入侵检测识别率达 99.23%；随着训练轮数增加，准确率、损失值误差分别在 5%、10%以内。本文方法具有较高准确率、检测率和良好泛化性特点，可在测控系统 CAN 总线数据入侵检测推广应用。

参考文献

[1] DUPONT G, HARTOG J D, ETALLE S, et al. A survey of network intrusion detection systems for controller area network[C]. 2019 IEEE International Conference on Vehicular Electronics and Safety(ICVES), 2019: 1-6.

[2] 刘云平，范嘉宇，苏东彦，等. 基于平滑滤波的多传感器异步融合方法研究[J]. 电子测量技术，2023，46(16)：38-45.
LIU Y P, FAN J Y, SU D Y, et al. Research on asynchronous multi-sensor fusion location method based on smoothing filtering [J]. Electronic Measurement Technology, 2023, 46(16): 38-45.

[3] 苏锦强，范伟军，胡晓峰，等. IBooster 总成三工位耐久测试系统设计[J]. 中国测试，2022，48(9)：152-157.
SU J Q, FAN W J, HU X F, et al. Design of three position durability test system for IBooster assembly[J]. China Measurement & Test, 2022, 48(9): 152-157.

[4] 孙元皓. 基于深度学习的工业控制网络入侵检测技术研究[D]. 西安：西安理工大学，2023.
SUN Y H. Research on intrusion detection technology of industrial control networks based on deep learning[D]. Xi′an: Xi′an University of Technology, 2023.

[5] LUO F, WANG J, ZHANG X, et al. In-vehicle network intrusion detection systems: A systematic survey of deep learning-based approaches[J]. PeerJ Computer Science, 2023, 9: 1648.

[6] 邓淼磊，阚雨培，孙川川，等. 基于深度学习的网络入侵检测系统综述[J/OL]. 计算机应用，1-13[2024-07-26]. http://kns.cnki.net/kcms/detail/51.1307.TP.20240723.1515.004.html.
DENG M L, KAN Y P, SUN CH CH, et al. Summary of network intrusion detection systems based on deep learning[J/OL]. Journal of Computer Applications, 1-13[2024-07-26]. http://kns.cnki.net/kcms/detail/51.1307.TP.20240723.1515.004.html.

[7] ZHANG J, WU ZH CH, LI F, et al. A deep learning framework for driving behavior identification on in-vehicle CAN-BUS sensor data[J]. Sensors, 2019, 19(6): 1356.

[8] LIN H C, WANG P, CHAO K M, et al. Using deep learning networks to identify cyber attacks on intrusion detection for in-vehicle networks[J]. Electronics, 2022, 11(14): 2180.

[9] WYK F V, WANG Y Y, 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.

[10] 曹举阳,王思山,司华超,等. 基于 Transformer 编码器的 CAN/CAN-FD 协议入侵检测研究[J/OL]. 计算机工程与应用,1-12[2024-12-07]. http://kns.cnki.net/kcms/detail/11.2127.TP.20240913.1550.006.html.
CAO J Y, WANG S SH, SI H CH, et al. Research on intrusion detection for CAN/CAN-FD protocols based on Transformer encoder [J/OL]. Computer Engineering and Applications, 1-12 [2024-12-07]. http://kns.cnki.net/kcms/detail/11.2127.TP.20240913.1550.006.html.

[11] VIRMANI D, TANEJA S, CHAWLA T, et al. Entropy deviation method for analyzing network intrusion [C]. 2016 International Conference on Computing, Communication and Automation, 2016: 515-519.

[12] 张金锋,张震,刘少勋,等. 车载资源约束下的控制器域网络异常检测自适应优化方法[J]. 电子与信息学报,2023,45(7):2432-2442.
ZHANG J F, ZHANG ZH, LIU SH X, et al. Adaptive optimization method for controller area network anomaly detection under vehicular resource constraints[J]. Journal of Electronics & Information Technology, 2023, 45(7): 2432-2442.

[13] 徐雪峤. 汽车总线异常流量检测方法研究[D]. 北京:北方工业大学,2024.
XU X Q. Research on the method of detecting abnormal traffic in automotive buses [D]. Beijing: North China University of Technology, 2024.

[14] 季一木,焦志鹏,刘尚东,等. 基于通信特征的 CAN 总线泛洪攻击检测方法[J]. 网络与信息安全学报,2020,6(1):27-37.
JI Y M, JIAO ZH P, LIU SH D, et al. CAN bus flooding attack detection based on communication characteristics[J]. Chinese Journal of Network and Information Security, 2020, 6(1): 27-37.

[15] 尹志华,魏洪乾,张幽彤. 面向总线网络攻击的快速响应熵分析与入侵检测系统[J]. 北京理工大学学报,2024,44(9):947-959.
YIN ZH H, WEI H Q, ZHANG Y T. Quick response entropy analysis and intrusion detection system for bus network attacks[J]. Transactions of Beijing Institute of Technology, 2024, 44(9): 947-959.

[16] ZHANG W B. LAZARO J P. A survey on network security traffic analysis and anomaly detection techniques [J]. International Journal of Emerging Technologies and Advanced Applications,2024, 1(4): 8-16.

[17] 彭海德. 汽车 CAN 网络的入侵检测方法研究[D]. 大连:大连理工大学,2021.
PENG H D. Research on intrusion detection method of automobile CAN networks [D]. Dalian: Dalian University of Technology, 2021.

[18] 赵嘉,谷良,吴瑶. 基于互信息和 GWB-LSSVM 的网络攻击检测模型[J]. 电子测量技术,2022, 45(24): 98-104.
ZHAO J, GU L, WU Y. Network attack detection model based on MI-GWB-LSSVM [J]. Electronic Measurement Technology, 2022, 45(24): 98-104.

[19] 罗峰,胡强,侯硕,等. 基于支持向量机的 CAN-FD 网络异常入侵检测[J]. 同济大学学报(自然科学版),2020, 48(12):1790-1796.
LUO F, HU Q, HOU SH, et al. Anomaly intrusion detection for CAN-FD bus by support vector machine[J]. Journal of Tongji University(Natural Science), 2020, 48(12): 1790-1796.

[20] DERHAB A, BELAOUED M, MOHIUDDIN I, et al. Histogram-based intrusion detection and filtering framework for secure and safe in-vehicle networks [J]. IEEE Transactions on Intelligent Transportation Systems,2022,23(3):2366-2379.

[21] 银鹰,周志洪,姚立红. 基于 LSTM 的 CAN 入侵检测模型研究[J]. 信息网络安全,2022,22(12):57-66.
YIN Y, ZHOU ZH H, YAO L H. Research on LSTM-Based CAN intrusion detection model [J]. Netinfo Security, 2022, 22(12): 57-66.

[22] 毛智超,吴黎兵,马亚军,等. 基于 DBN 与带注意力机制 GRU 的 CAN 总线入侵检测模型[J]. 武汉大学学报(理学版),2023,69(5):598-608.
MAO ZH CH, WU L B, MA Y J, et al. Intrusion detection model for CAN bus using DBN and attention-based GRU[J]. Journal of Wuhan University (Natural Science Edition), 2023, 69(5): 598-608.

[23] 张碧洪. 基于改进型自动编码器的车载网入侵检测算法[D]. 杭州:浙江理工大学,2023.
ZHANG B H. Intrusion detection algorithm for in-vehicle network based on improved autoencoders[D]. Hangzhou: Zhejiang University of Science and Technology, 2023.

[24] 李思涌,吴书汉,孙伟. 基于注意力机制的 CNN-LSTM 网络车内 CAN 总线入侵检测技术[J]. 信息安全研究,2023,9(10):961-967.
LI S Y, WU SH H, SUN W. A CNN-LSTM method based on attention mechanism for in-vehicle CAN bus

intrusion detection[J]. Journal of Information Security Research, 2023, 9(10): 961-967.

[25] LEE-THORP J, AINSLIE J, ECKSTEIN I, et al. FNet: mixing tokens with fourier Transforms[J]. ArXiv preprint arXiv:2105.03824,2022.

[26] 陈彦彬,林燕雄,黄佳旭,等.双线性注意力机制物联网攻防方法及系统:ZL2024109699778[P]. 2024-10-31.
CHEN Y B, LIN Y X, HUANG J X, et al. Bilinear attention mechanism for IoT attack-defense methods and systems:ZL2024109699778[P]. 2024-10-31.

[27] 李超超,武恪,方菱.基于 AUTOSAR 的 CAN 通信栈设计[J].电子测量技术,2021,44(23):139-145.
LI CH CH, WU K, FANG L. Design of CAN communication stack based on AUTOSAR [J]. Electronic Measurement Technology, 2021, 44(23): 139-145.

[28] MEE L H, BYUNG I K, HUY K K. Anomaly intrusion detection method for vehicular networks based on survival analysis[J]. Vehicular Communications, 2018,14:52-63.

[29] 张子迎,陈玉炜,王宇华.基于 XGBoost-DNN 的工业控制系统入侵检测架构[J].哈尔滨工程大学学报,2024,45(11): 2243-2249.
ZHANG Z Y, CHEN Y W, WANG Y H. An intrusion detection architecture for ICS based on XGBoost-DNN[J]. Journal of Harbin Engineering University, 2024,45(11):2243-2249.

[30] 倪志伟,行鸿彦,侯天浩,等.基于生成对抗网络和混合时空神经网络的入侵检测[J].电子测量技术,2024,47(2):17-24.
NI ZH W, XING H Y, HOU T H, et al. Intrusion detection based on generative adversarial networks and hybrid spatio-temporal neural networks[J]. Electronic Measurement Technology, 2024, 47(2): 17-24.

[31] 潘洁.工业控制系统数据驱动的入侵检测研究[D].杭州:浙江大学,2023.
PAN J. Research on data-driven intrusion detection in industrial control systems[D]. Hangzhou: Zhejiang University, 2023.

[32] 姚贺龙,吕东澔,张勇,等.基于傅里叶分解方法的肌肉疲劳状态分类研究[J].电子测量与仪器学报,2023,37(6):48-58.
YAO H L, LYU D H, ZHANG Y, et al. Study of muscle fatigue state classification based on Fourier decomposition method [J]. Journal of Electronic Measurement and Instrumentation, 2023, 37(6): 48-58.

[33] 刘庭凤,张荣芬,刘宇红.基于 FRFT-TFDR 的语音通信双绞线故障检测研究[J].电子测量与仪器学报,2023,37(4):204-212.
LIU T F, ZHANG R F, LIU Y H. Research on fault detection of voice communication twisted pair based on FRFT-TFDR[J]. Journal of Electronic Measurement and Instrumentation, 2023, 37(4): 204-212.

[34] 郭钰荣,姚金杰,白建胜,等.基于 FEEMD 算法对小样本电磁信号的识别与分类[J].国外电子测量技术,2023,42(4):166-172.
GUO Y R, YAO J J, BAI J SH, et al. Recognition and classification of small sample electromagnetic signals based on FEEMD algorithm[J]. Foreign Electronic Measurement Technology, 2023, 42(4):166-172.

[35] 冯治国,金日,罗冲,等.基于 Transformer 神经网络的变压器状态监测[J].国外电子测量技术,2023,42(2):145-150.
FENG ZH G, JIN R, LUO CH, et al. Power transformer state monitoring based on Transformer deep neural network [J]. Foreign Electronic Measurement Technology, 2023, 42(2): 145-150.

[36] Car-hacking dataset for the intrusion detection[Z/OL]. https://ieee-dataport. org/open-acc-ess/car-hacking-attack-defense-challenge-2020-dataset.

[37] 郭丽萍,张艳荣,林思苗.嵌入式设备电源控制系统的 CAN 通信软硬件设计[J].中国测试,2017,43(10):109-113.
GUO L P, ZHANG Y R, LIN S M. Software and hardware design based on CAN communication for control system of embedded device power supply[J]. China Measurement & Test, 2017, 43(10): 109-113.

作者简介

陈彦彬(通信作者),本科,高级实验师、高级工程师,主要研究方向为电子技术教学与科研。
E-mail:chenyanbin01@126.com

刘桂雄,博士,教授,博士生导师,主要研究方向为精密检测与智能仪器仪表、现代传感与智慧物联。