基于指数平滑动态图的CAN总线入侵检测方法

韦文杰[1]，王建萍[1]，陈彬[2]，林福宏[1]
（1.北京科技大学计算机与通信工程学院，北京 100083；2.新唐智创电子技术有限公司，北京 100020）

摘　要：控制器局域网络（CAN）总线的安全性正面临现代车辆中动态非平稳通信模式的严峻挑战，传统静态检测方法难以有效捕捉此类特征。为此，提出一种基于指数平滑动态图神经网络（ES-DyGNN）的CAN总线入侵检测模型，旨在精准刻画电子控制单元（ECU）间的动态关联关系。与启发式动态模型不同，该方法通过严格定义的指数平滑图算子实现拓扑变化的自适应捕捉，推导了动态邻接序列的闭式展开式，并建立了刻画模型稳定性的Frobenius范数收敛界。同时，从理论上证明了攻击扰动的持续存在性下界，确保即使在噪声环境中仍能检测到细微的注入攻击。模型利用正弦时间嵌入技术增强节点的时间感知能力，并结合边缘条件注意力机制，使消息传递同时考虑特征相似性与平滑转移频率。在两个基准数据集上的实验结果表明，ES-DyGNN检测准确率超过99%，且单窗口推理时延为0.14 ms。理论分析与实验验证证明了该方法的高效性和实用性。

关键词：CAN总线入侵检测；动态图神经网络；指数平滑；车载安全
中图分类号：TN929.5
文献标志码：A
DOI：10.11959/j.issn.1000–436x.2026078

CAN bus intrusion detection method based on exponentially smoothed dynamic graph

Wei Wenjie[1], Wang Jianping[1], Chen Bin[2], Lin Fuhong[1]
1. School of Computer & Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China
2. Beijing Xintang Zhichuang Electronics and Technology Co., Ltd., Beijing 100020, China

Abstract: The security of controller area network (CAN) bus is increasingly challenged by volatile and non-stationary communication patterns in modern vehicles, which traditional static detection methods have failed to capture. ES-DyGNN, an exponentially smoothed dynamic graph neural network, was proposed to capture the evolving relationships between electronic control unit (ECU). Unlike heuristic dynamic models, this method was underpinned by a rigorous exponential smoothing graph operator that adaptively captured topological shifts. Closed form expansions for the dynamic adjacency sequences were derived and Frobenius norm convergence bounds that characterized the stability of the model were established. Furthermore, a theoretical lower bound on attack persistence was proven, ensuring subtle injections were detectable despite noise. Additionally, the model employed sinusoidal time embeddings and edge-conditional attention to weigh both feature similarity and transition frequencies during message passing. Through extensive evaluations on benchmark datasets, it was demonstrated that an accuracy of over 99% was achieved by ES-DyGNN, while an inference latency of less than 0.14 ms for each window was sustained. Through both rigorous theoretical analysis and extensive experimental validation, the proposed method demonstrates the feasibility of topology adaptation for automotive security.

Keywords: CAN bus intrusion detection, dynamic graph neural network, exponential smoothing, vehicular security

收稿日期：2026–02–02；**修回日期：**2026–03–17
通信作者：林福宏，fhlin@ustb.edu.cn
基金项目：国家重点研发计划基金资助项目（No.2022YFB3104903）
Foundation Item：The National Key Research and Development Program of China (No.2022YFB3104903)

0　引言

电子控制单元（electronic control unit, ECU）的普及彻底革新了现代汽车的功能实现[1]。ECU在协调发动机控制、传动系统、高级驾驶辅助及信息娱乐等各类系统的实时决策中发挥关键作用。随着车辆智能化程度提升，单车ECU数量持续增长，高端车型已突破150个[2]，因此高效可靠的ECU间通信成为核心需求。在此背景下，控制器局域网络（controller area network, CAN）凭借低时延、容错性及成本优势，成为车载内部通信的事实标准[3]。

然而，CAN协议存在显著安全缺陷。由于设计时假设车载网络处于封闭环境，CAN缺乏加密、身份认证等基础安全机制[4]。攻击者一旦入侵网络，即可通过注入伪造消息实现车辆控制，此类攻击常表现为ECU间交互模式的异常改变。现有检测工具难以应对这类威胁，主要原因有两点：一是将网络视为静态系统，无法追踪攻击过程中ECU关系的动态变化；二是攻击者可将恶意消息隐藏在总线自然波动中。研究表明，CAN流量具有“伪周期性”特征，即消息时序存在类噪声的细微自然变化，多数系统无法区分这种自然噪声与隐蔽攻击，导致误报率高或漏检问题。

为缓解上述风险，研究者提出多种CAN入侵检测系统（intrusion detection system, IDS）。早期方法聚焦于基于时序的技术（如消息频率分析、时钟漂移检测）及熵值等统计指标识别异常模式[3]。近年来，机器学习与深度学习方法（包括一维卷积神经网络、长短期记忆网络及自编码器）被用于建模复杂的时间依赖关系。

尽管取得这些进展，仍存在多个未解决的基础挑战。首先，基于频率和时钟漂移的方法具有车辆特异性，不同厂商和车型的传输速率与时钟特性差异显著[5]，且无法检测不违反时序周期的新型自适应攻击。部分学者基于周期性进行检测[6]，但可靠性不足。图1为拒绝服务（denial of service，DoS）攻击和模糊攻击伪周期下CAN总线ID特征序列的时域分布情况，其中虚线代表基于理想周期模型的预测时刻，实线为实际采样数据。由图1可知，尽管CAN总线流量在宏观上呈现重复的波形结构，表现出一定的规律性，但在微观的时间尺度上，实际波峰与理想周期时刻存在显著的相位偏差和非线性漂移，这种特征即“伪周期性”。特别是在图1(a)的DoS攻击场景下，高频注入导致总线竞争加剧，使原本的周期信号发生了明显的时序畸变。首先，如果采用传统的固定周期检测窗方法，这些正常的时序偏移极易被标记为异常，从而导致高误报率。其次，基于熵值的检测器对内容保留型攻击无效，例如当载荷篡改未显著改变符号分布时，此类方法将失效[7-8]。第三，CAN标识符与ECU功能的映射既非标准化也不公开，同一CAN-ID在不同车型中可能代表不同语义[9]，导致基于规则或ID依赖的方法难以泛化。此外，许多深度学习模型将CAN流量视为扁平时间序列，忽略了ECU间的潜在图结构及通信模式的时空演化特性[5]。在车载场景中，有效的入侵检测系统需超越单一异常消息识别，还应适应攻击导致的动态通信模式与拓扑突变，同时捕捉ECU间的复杂空间关系及总线的时序行为演化。此外，该系统还需在不同车型间具备良好泛化能力，避免依赖厂商私有CAN-ID语义。

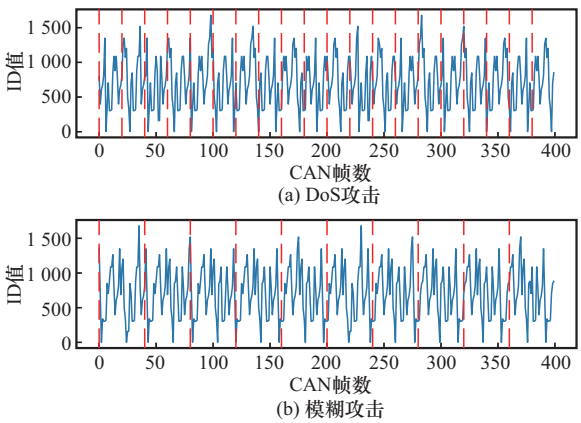


图1　DoS攻击和模糊攻击伪周期

为此，本文提出指数平滑动态图神经网络（exponentially smoothed dynamic graph neural network, ES-DyGNN）模型。该模型通过统一框架将原始CAN流量转化为演化图序列，其中节点表示ECU，边反映随时间变化的通信关系。如图2所示，ES-DyGNN在动态图基础上融合分层注意力与时间融合机制，实现对ECU交互模式及其攻击下演化特征的学习。本文主要贡献如下。

1) 利用带有限记忆的指数加权移动平均[10]（exponentially weighted moving average, EWMA）图算子，将近期邻接矩阵序列整合为时序演化的拓扑结构。理论推导动态邻接序列的闭式展开式，刻画其谱域行为特征，并证明模型稳定性的弗罗贝尼

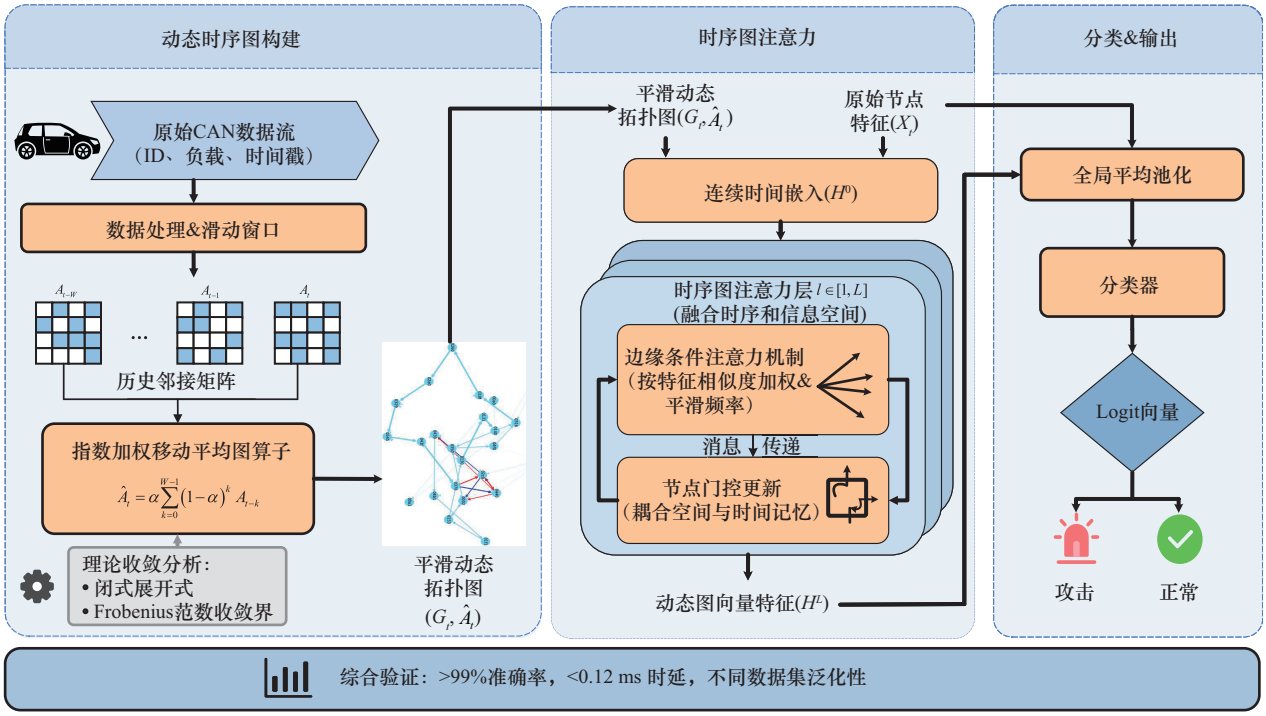


图2　系统架构

乌斯（Frobenius）范数收敛界。

2) 设计融合正弦时间嵌入与边缘条件注意力的模块，结合节点门控更新机制，在每一层实现空间消息传递与时间记忆的交织融合。该架构能即时响应通信模式演化，避免传统解耦递归结构导致的延迟问题。

3) 在两类基准CAN数据集上的评估表明，ES-DyGNN检测准确率超过99%，单窗口推理时延低于0.12 ms。消融实验验证了平滑算子与架构设计的必要性，跨数据集测试进一步证实了模型的泛化能力。

1　相关工作

CAN总线入侵检测研究已形成多技术路径，涵盖物理层指纹识别、时序分析、统计熵值及近年来的数据驱动深度学习[11]与图模型方法。本节系统梳理各领域代表性成果，分析现有技术瓶颈，为ES-DyGNN的设计提供理论与实践依据。

1.1　基于物理特征的检测方法

早期CAN总线入侵检测依赖物理层电压信号的细微差异实现ECU指纹识别[12]。Levy等[13]通过电压信号定位物理入侵，虽然检测率较高，但应用场景受限，其在ECU低功耗模式或信号波动时的准确性未经验证。Deng等[14]提出基于CAN-ID电压指纹的非周期恶意帧检测方法，但电压信号易受环境温度、供电电压等外部因素干扰。此类方法虽然在受控环境中精度较高，但需专用模拟前端，对温度和器件老化敏感，且难以跨车型或总线拓扑扩展。

1.2　侧信道分析方法

另一类方法是通过监控帧间时序统计特征（如消息频率、信息熵[15]、时钟漂移）检测异常[16-17]。Zhao等[18]基于时钟偏移为ECU建立唯一指纹，Lee等[19]通过分析相同CAN-ID连续消息的平均时间间隔与实际值残差实现异常检测，但需为不同ECU手动选择参数。

为捕捉更广泛的统计异常，熵基检测器计算CAN-ID、载荷字节或帧序列的香农熵或雷尼熵。Yu等[7]利用相邻消息时间间隔计算条件熵，Liu等[8]提出熵驱动时频分析方法，在特定攻击场景下实现高精度检测，但该类方法对动态环境中的高级持续性威胁适应性不足。

1.3　机器学习、深度学习与图神经网络

近年来，传统机器学习模型（支持向量机[20]、K近邻[21]、随机森林[22]）被应用于人工设计的时序与载荷特征；深度学习架构（卷积神经网络[1]、自编码器[23]）则用于学习更丰富的时序表示。尽管这些方法提升了检测率，但均将CAN流量视为

扁平时间序列，忽略了ECU间的依赖关系及车载通信的拓扑演化特性。

为此，图神经网络（GNN）被引入建模CAN消息共现或信号相关性诱导的静态ECU图结构。Zhang等[24]提出基于GNN的CAN总线入侵检测系统，将CAN消息流转化为有向属性图并训练GNN进行预测。King等[25]结合优先图分析与字节阈值技术实现细粒度无监督检测。Xiao等[26]提出CAN-GAT模型捕捉CAN总线消息间的相关性。然而，这些方法或假设固定邻接关系，或缺乏对图内特定恶意消息的定位能力。

1.4　本文方法

基于现有电压、时序、熵值及扁平序列模型的局限性，以及GNN方法在动态拓扑建模中的不足，本文提出ES-DyGNN模型。该模型通过有限记忆EWMA算子动态平滑CAN总线拓扑，将空间注意力与节点门控递归交织融合，实现结构与时间特征的联合学习，满足车载入侵检测对实时性与泛化性的要求。

2　CAN总线图的时间演化建模

本节提出一种基于指数加权移动平均算子的CAN总线图时间演化数学框架。该框架将瞬时邻接观测与衰减记忆核融合，通过推导平滑邻接矩阵的精细闭式解，证明其在正常通信条件下的渐近收敛性，并为突发注入攻击建立严格的敏感性边界。

2.1　指数平滑更新与闭式展开

为了将EWMA算子与CAN总线图充分融合，本文假设离散时间实例$t = 1,2,\cdots,N$，其中CAN总线消息被分割成窗口，每个窗口包含W条消息，建立以下定义。

1) $\boldsymbol{B}_t \in \mathbb{R}^{N\times N}$：在窗口$t$内构建的“瞬时”邻接矩阵，其元素定义为

$$[\boldsymbol{B}_t]_{ij} = \frac{n_{ij}^{(t)}}{W} \tag{1}$$

其中，$n_{ij}^{(t)}$表示在时间窗口t内节点$i \to j$发送的消息数量。该矩阵量化了特定时间窗口内节点间的瞬时流量模式。

2) $\boldsymbol{A}_t \in \mathbb{R}^{N\times N}$：在窗口$t$内构建的“瞬时”邻接矩阵在时间$t$时的“平滑”邻接矩阵，旨在结合历史信息与当前消息的关系。

假设$\{\boldsymbol{B}_t\}_{t=1}^{T} \in \mathbb{R}^{N\times N}$为从$W$个CAN消息的非重叠窗口中获得的瞬时邻接矩阵序列，通过EWMA核定义平滑邻接矩阵$\{\boldsymbol{A}_t\}$。

$$\begin{aligned} \boldsymbol{A}_t &= \alpha\boldsymbol{A}_{t-1} + (1-\alpha)\boldsymbol{B}_t \\ \boldsymbol{A}_1 &= \boldsymbol{B}_1, \quad 0 \leqslant \alpha < 1 \end{aligned} \tag{2}$$

对式(2)进行递归展开（当$t \leqslant H$时，尚未出现下降趋势），可得到闭合形式。

$$\begin{aligned} \boldsymbol{A}_t &= \alpha^{t-1}\boldsymbol{B}_1 + (1-\alpha)\sum_{t}^{k=2}\alpha^{t-k}\boldsymbol{B}_k \\ \Leftrightarrow \boldsymbol{A}_t &= \sum_{t}^{k=1}\alpha^{t-k}(1-\alpha)^{\mathbb{I}[k>1]}\boldsymbol{B}_k \end{aligned} \tag{3}$$

其中，$\mathbb{I}[k>1]$表示指示函数。当$t > H$时，式(3)中求和的有效起点为$k = t - H + 1$。对于每个滑动窗口W_t，根据Flag字段对该图进行标签的标注，标注规则为

$$y = \begin{cases} c_{\text{attack}}, & \exists r \in W_t : r.\text{Flag} = 'T' \\ 0, & \text{其他} \end{cases} \tag{4}$$

其中，c_{attack}表示特定攻击类别的整数索引。与传统的帧级或流级标注方案不同，本文的窗口级标注策略能够提供更精细的表征。每个固定长度的CAN总线窗口若包含任何带有注入标志$'T'$的帧，则标记为“攻击”，否则标记为“正常”。

该标注方法能显著提升抗噪能力，因为单个异常帧仅影响其自身窗口，而非后续所有窗口。对于持续性攻击（如多秒级拒绝服务攻击或多时长欺骗攻击）完全被连续标记为攻击的窗口所捕获，使网络能够学习持续异常的累积影响，而非孤立帧模式。除此之外，通过仅依赖注入异常帧而非车辆特定时间阈值或专有CAN-ID映射，本文方法提升了跨模型泛化能力，不需要对不同品牌的车辆进行单独定制，使其非常适合部署于异构汽车平台。

2.2　EWMA算子收敛性分析

2.1节推导了EWMA算子构建CAN总线图的过程，除了在节点基中的闭式表示外，EWMA算子可在频域中解释其滤波器的作用。假设在每个时间步k，瞬时邻接$\boldsymbol{B}_k$共享一个共同的正交特征基$\boldsymbol{U} \in R^{N\times N}$，使

$$\boldsymbol{B}_k = \boldsymbol{U}\boldsymbol{\Lambda}_k\boldsymbol{U}^{\mathrm{T}} \tag{5}$$

将式(5)代入闭式展开式(3)可得

$$\boldsymbol{A}_t = \boldsymbol{U}\left[\alpha^{t-1}\boldsymbol{\Lambda}_1 + (1-\alpha)\sum_{t}^{k=2}\alpha^{t-k}\boldsymbol{\Lambda}_k\right]\boldsymbol{U}^{\mathrm{T}} \tag{6}$$

由于$\boldsymbol{U}$对所有$\boldsymbol{B}_k$进行对角化处理，每个谱分

量（或称“模态”）均独立演化。式(6)中括号内矩阵的第i个对角元素为

$$[\boldsymbol{A}_t]_{ii}=\alpha^{t-1}\lambda_{1,i}+(1-\alpha)\sum_{t}^{k=2}\alpha^{t-k}\lambda_{k,i} \tag{7}$$

该值表示过去瞬时特征值$\{\lambda_{k,i}\}$的加权叠加，其系数呈指数衰减。

由此可以看出，EWMA算子作为模式选择性滤波器发挥作用，适合本文的场景，其中特征值$\lambda_{k,i}<1$通过α^{t-k}几何抑制，当$\lambda_{k,i}\approx 1$时，谱分量得以保留并主导$\boldsymbol{A}_t$的演化。因此，重复模式（如周期性诊断）保持为低频模式，孤立异常（如短暂注入）则被衰减。EWMA带窗口级标记的平滑图构建如算法1所示。

算法1 EWMA带窗口级标记的平滑图构建

输入 数据包日志D，其中字段包括{ Timestamp, CAN ID,DLC,DATA [0..7],Flag }，窗口大小W，步长S，衰减因子α，缓冲区历史长度H，其中$W=S$

输出 $\{G_t=(x,E,W,y,t,\text{batch})\}$

1) 初始化CAN-ID以索引映射$I\leftarrow\{\}$，并创建容量为H的队列Q

2) for $t=0\rightarrow|D|-W$，步长S，$|D|$表示日志中消息的个数，do

3) 提取滑动窗口$\boldsymbol{W}_t\leftarrow\boldsymbol{D}[t{:}t+W]$

4) 更新I中出现的任何新CAN-ID至$\boldsymbol{W}_t$

5) 构建瞬时邻接关系矩阵$\boldsymbol{B}\in\mathbb{R}^{n\times n}$:

6) $B[u,v]+=1$

7) 归一化$\boldsymbol{B}\leftarrow\dfrac{\boldsymbol{B}}{W}$并将$\boldsymbol{B}$放入$Q$

8) 计算平滑邻接矩阵

$$\boldsymbol{A}\leftarrow\sum_{k=t-|Q|+1}^{t}\alpha^{t-k}(1-\alpha)^{\mathbb{I}_{\|k>1\|}}\boldsymbol{B}_k$$

9) if max ($\boldsymbol{A}$) > 0:

10) 提取节点特征$x\in\mathbb{R}^{n\times f}$

11) 确定窗口级标签$y\in\{0,1,\cdots\}$:

$$y=\begin{cases}c_{\text{attack}}, & \exists r\in W_t{:}r.\text{Flag}='T'\\ 0, & \text{其他}\end{cases}$$

12) 提取边列表$E=\{(u,v)\,|\,\boldsymbol{A}_{\text{uv}}>0\}$

13) 设定边权重$W=\{\boldsymbol{A}_{\text{uv}}|(u,v)\in E\}$

14) 记录时间戳索引t和批量分配向量

15) end if

16) end for

17) 返回(x,E,W,y,t,batch)

接下来证明本文提出CAN总线图构建方法的收敛性。

定理1 假设$\lim\limits_{t\rightarrow\infty}\boldsymbol{B}_t=\boldsymbol{B}^*$，且对所有$t$满足$\|\boldsymbol{B}_t-\boldsymbol{B}^*\|_{\text{F}}\leqslant\delta$，则由EWMA定义的平滑序列$\{A_t\}$满足

$$\|\boldsymbol{A}_t-\boldsymbol{B}^*\|_{\text{F}}\leqslant\alpha^{t-1}\|\boldsymbol{B}_1-\boldsymbol{B}^*\|_{\text{F}}+\delta\left(1-\alpha^{t-1}\right) \tag{8}$$

因此有

$$\limsup_{t\rightarrow\infty}\|\boldsymbol{A}_t-\boldsymbol{B}^*\|_{\text{F}}\leqslant\delta \tag{9}$$

证明 根据递推公式$\boldsymbol{A}_t-\boldsymbol{B}^*=\alpha\left(\boldsymbol{A}_{t-1}-\boldsymbol{B}^*\right)+(1-\alpha)\left(\boldsymbol{B}_t-\boldsymbol{B}^*\right)$，对等式两边取Frobenius范数，并应用三角不等式，可得

$$\left\|\boldsymbol{A}_t-\boldsymbol{B}^*\right\|_{\text{F}}\leqslant\alpha\left\|\boldsymbol{A}_{t-1}-\boldsymbol{B}^*\right\|_{\text{F}}+(1-\alpha)\left\|\boldsymbol{B}_t-\boldsymbol{B}^*\right\|_{\text{F}} \tag{10}$$

令$e_t=\|\boldsymbol{A}_t-\boldsymbol{B}^*\|_{\text{F}}$，$b_t=\|\boldsymbol{B}_t-\boldsymbol{B}^*\|_{\text{F}}\leqslant\delta$，则有

$$e_t\leqslant\alpha e_{t-1}+(1-\alpha)\delta \tag{11}$$

展开线性离散不等式可得

$$e_t\leqslant\alpha^{t-1}e_1+(1-\alpha)\delta\sum_{m=0}^{}\alpha^m=$$
$$\alpha^{t-1}\left\|\boldsymbol{B}_1-\boldsymbol{B}^*\right\|_{\text{F}}+\delta(1-\alpha)\frac{1-\alpha^{t-1}}{1-\alpha}=$$
$$\alpha^{t-1}\left\|\boldsymbol{B}_1-\boldsymbol{B}^*\right\|_{\text{F}}+\delta\left(1-\alpha^{t-1}\right) \tag{12}$$

由于$0\leqslant\alpha<1$，当$t\rightarrow\infty$时，$\alpha^{t-1}\rightarrow 0$，因此$\limsup\limits_{t\rightarrow\infty}e_t\leqslant\delta$，证毕。

定理2 若在时刻t_0存在攻击注入，使$\|\boldsymbol{B}_{t_0}-\boldsymbol{B}^*\|_{\text{F}}\geqslant\epsilon$且$\epsilon\gg\delta$，则对EWMA序列$\{A_t\}$有

$$\|\boldsymbol{A}_{t_0}-\boldsymbol{B}^*\|_{\text{F}}\geqslant(1-\alpha)\epsilon \tag{13}$$

$$\left\|\boldsymbol{A}_{t_0+k}-\boldsymbol{B}^*\right\|_{\text{F}}\geqslant(1-\alpha)\alpha^k\epsilon-\delta,\quad k\geqslant 1 \tag{14}$$

证明 在时刻t_0，根据递推公式$\boldsymbol{A}_{t_0}-\boldsymbol{B}^*=\alpha(\boldsymbol{A}_{t_0-1}-\boldsymbol{B}^*)+(1-\alpha)(\boldsymbol{B}_{t_0}-\boldsymbol{B}^*)$，对等式两边取Frobenius范数并利用$\|\boldsymbol{A}_{t_0-1}-\boldsymbol{B}^*\|_{\text{F}}\leqslant\delta$（由定理1的稳态界）和$\|\boldsymbol{B}_{t_0}-\boldsymbol{B}^*\|_{\text{F}}\geqslant\epsilon k\geqslant 1$，可得

$$\|\boldsymbol{A}_{t_0}-\boldsymbol{B}^*\|_{\text{F}}\geqslant(1-\alpha)\|\boldsymbol{B}_{t_0}-\boldsymbol{B}^*\|_{F}-$$
$$\alpha\|\boldsymbol{A}_{n-1}-\boldsymbol{B}^*\|_{\text{F}}\geqslant(1-\alpha)\epsilon-\alpha\delta \tag{15}$$

由于$\epsilon\gg\delta$，可忽略$-\alpha\delta$，即证得$\|\boldsymbol{A}_{t_0}-\boldsymbol{B}^*\|_{\text{F}}\geqslant(1-\alpha)\epsilon$。

对于$k\geqslant 1$，递归应用一步界

$$\boldsymbol{A}_{t_0+k}-\boldsymbol{B}^{*}=\alpha(\boldsymbol{A}_{t_0+k-1}-\boldsymbol{B}^{*})+(1-\alpha)(\boldsymbol{B}_{t_0+k}-\boldsymbol{B}^{*}) \tag{16}$$

取范数并利用$\|\boldsymbol{B}_{t_0+k}-\boldsymbol{B}^{*}\|_{\mathrm{F}}\leqslant\delta$，可得

$$\|\boldsymbol{A}_{t_0+k}-\boldsymbol{B}^{*}\|_{\mathrm{F}}\geqslant\alpha\|\boldsymbol{A}_{t_0+k-1}-\boldsymbol{B}^{*}\|_{\mathrm{F}}-(1-\alpha)\delta \tag{17}$$

重复迭代k次后得到

$$\|\boldsymbol{A}_{t_0+k}-\boldsymbol{B}^{*}\|_{\mathrm{F}}\geqslant(1-\alpha)\alpha^{k}\epsilon-\delta \tag{18}$$

证毕。

上述定理揭示了EWMA算子在物理层面的关键特性，即攻击的“记忆持久性”。式(13)和式(14)表明，当CAN总线上发生突发注入（如DoS或Fuzzy攻击）时，大规模的流量扰动会导致邻接矩阵$\boldsymbol{A}_{t_0}$范数瞬间增大。即使攻击者停止注入，由于衰减因子α的存在，拓扑结构的异常并不会立即消失，而是以α^{k}的速率缓慢衰减，从而保证在信号低于噪声下限之前可以实现多窗口检测，确保即使在攻击信号微弱或间歇性出现（如低频隐蔽攻击）的情况下，累积的图结构差异仍能显著高于背景噪声界限δ。这种机制有效克服了传统无记忆检测方法容易漏检短时脉冲攻击的缺陷，解释了为何EWMA图平滑算子既能抑制随机波动，又能凸显真实的拓扑异常。

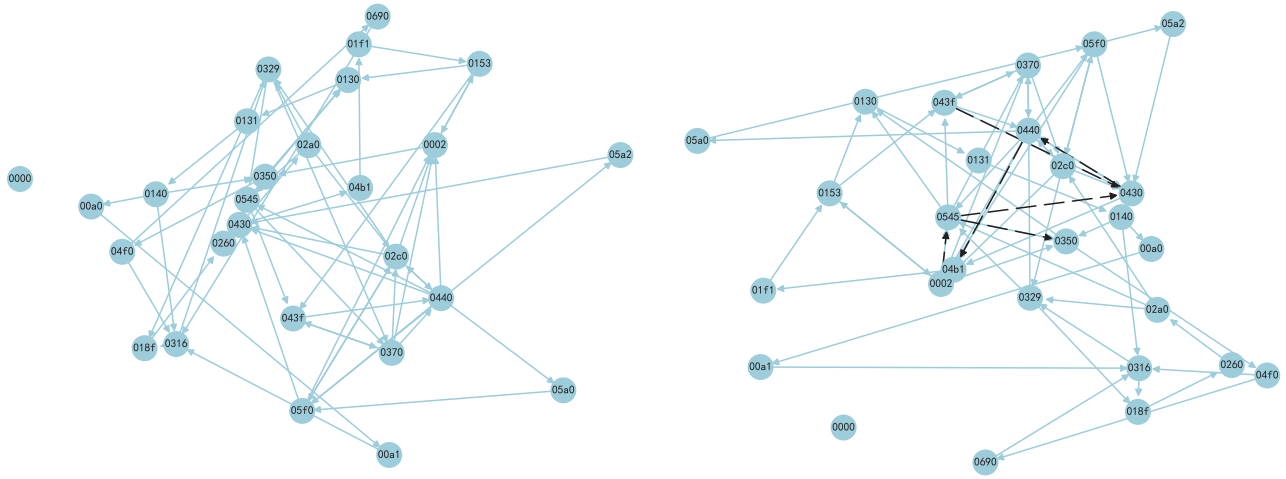
图3和图4为EWMA平滑处理的CAN总线图在DoS攻击下的变化。由图3可知，攻击注入引发了通信拓扑的剧烈重构。正常情况下，CAN总线表现为稀疏的周期性通信，而在攻击窗口中，以CAN-ID 0x0430和0x0545为中心的连接密度急剧上升。这是DoS攻击通过极短间隔持续发送高优先级报文，强行占据总线仲裁，导致这些恶意节点与其他节点间的通信频率在EWMA算子作用下被快速放大。进一步观察图4，点线加粗的边揭示了权重的显著正向偏移。这种权重峰值并非随机噪声，而是攻击者使特定路径的流量强度增加。EWMA算子通过平滑机制有效抑制了背景噪声引起的微小振荡（虚线细边），清晰地突出了由攻击行为主导的结构性异常，验证了模型在动态非平稳环境下捕捉攻击拓扑特征的能力。

3　模型架构

在智能汽车入侵检测领域，CAN总线通信具有动态突发特性，本文构建了既能编码精确时序信息又可实时调整图结构的模型，通过融合连续时间嵌入、边条件注意力机制和全局池化分类器来应对上述挑战。接下来对连续时间编码机制、图注意力层，以及池化分类头模块进行详细阐述，系统阐释各模块如何整合CAN总线的内在结构信息。

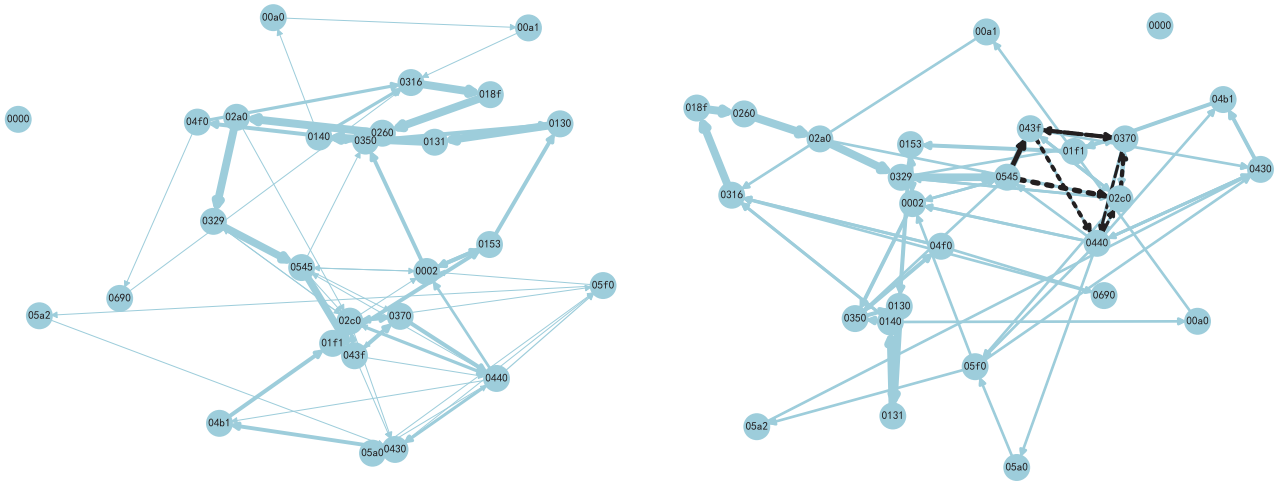
3.1　连续时间编码机制

现有的基于循环神经网络（recurrent neural network, RNN）或长短期记忆（long short term memory, LSTM）网络的方法虽然能处理序列信息，但在长序列中容易遗忘精细的相位特征，且难以捕捉非均匀采样下的绝对时间位置。为此，本节借鉴Transformer的位置编码思想[27]，针对CAN总线的“伪周期性”特性，设计了连续正弦时间嵌入机制。该机制通过将离散窗口索引直接映射到高维流形，



(a) 攻击注入前　　(b) 攻击注入后

图3　EWMA平滑处理的CAN总线图在DoS攻击下的变化（边切换）



(a) 攻击注入前　　(b) 攻击注入后

图4　EWMA 平滑处理的CAN总线图在DoS攻击下的变化（权重偏移）

能够保持时间位置的绝对真实性。这意味着无论异常流量出现在长序列的何处，模型都能通过多尺度正弦波的相位差，精确锚定其在全局时序位置（即某个窗口内），从而有效捕捉被传统模型忽略的长期相位漂移与非线性畸变线索。

对于包含 W 个连续CAN帧的每个滑动窗口 t，同一窗口内部的所有报文共享同一个时间嵌入。首先枚举该区块中观测到的 N_t 个不同CAN-ID，随后创建一个 N_t 维向量。

$$\boldsymbol{t} = \left[t,t,\cdots,t\right]^{\mathrm{T}} \in \mathbb{R}^{N_t} \tag{19}$$

为使网络能够区分粗略与精细的时间偏移，本节选择一个时间嵌入维度 L（偶数整数 $L = 16$）并构建一个“逆频率”向量 $\boldsymbol{\omega}$。

$$\boldsymbol{\omega}_k = \frac{1}{10\,000^{\frac{2k}{L}}},\quad k = 0,1,\cdots,\frac{L}{2} - 1 \tag{20}$$

其中，$\boldsymbol{\omega}$ 的前几个分量对应慢速振荡（捕捉多秒周期性信号，如发动机循环），后续分量则编码快速波动（低至亚毫秒级抖动），计算外积

$$\boldsymbol{T} = \boldsymbol{t} \times \boldsymbol{\omega}^{\mathrm{T}} \in \mathbb{R}^{N_t \times \frac{L}{2}} \tag{21}$$

使矩阵 $\boldsymbol{T}$ 的第 i 行包含CAN - ID$_i$ 的缩放时间向量。其中，×表示向量的外积。通过逐元素应用正弦和余弦函数，可生成一个完整的 L 维嵌入向量。

$$\mathrm{TimeEmb}(t) = \left[\sin \boldsymbol{T} \| \cos \boldsymbol{T}\right] \in \mathbb{R}^{N_t \times L} \tag{22}$$

通过将这两个部分拼接，确保时间嵌入的每个维度都具有唯一性和可逆性，且生成的嵌入能保留注意力机制所需的欧氏距离特性。最后，将TimeEmb(t) 与静态节点特征拼接，实现时间信息与有效载荷信息的融合。

$$\boldsymbol{X} = \left[x_1^{(t)},x_2^{(t)},\cdots,x_N^{(t)}\right]^{\mathrm{T}} \in \mathbb{R}^{N_t \times d_{\mathrm{in}}} \tag{23}$$

其中，每个 $x_i^{(t)}$ 编码了CAN-ID$_i$ 的归一化消息频率、平均DLC及有效载荷统计信息，因此 $d_{\mathrm{in}} = 3$。组合特征矩阵为

$$\boldsymbol{H}^{(0)} = \left[\boldsymbol{X} \| \mathrm{TimeEmb}(t)\right] \in \mathbb{R}^{N_t \times (d_{\mathrm{in}} + L)} \tag{24}$$

通过这种方式显式嵌入窗口时间戳，模型能够学习特定时间模式的相关性。这些模式（如周期性诊断消息或异常突发）与后续注意力层中图结构的变化相关。此外，即使两个CAN-ID有效载荷统计量看起来完全相同，模型仍能区分在时间 $t-1$ 观察到的特定CAN标识符的嵌入与时间 t 的另一个标识符的嵌入。

3.2　图注意力层

在为每个节点嵌入精确时间信息后，接下来通过CAN总线拓扑结构传播并融合信息，同时兼顾语义相似性和智能汽车产生的实际流量强度。本节将时间窗口 t 的唯一CAN-ID集合 V 视为有向图 $G_t = (V_t,E_t)$ 的节点集，边列表为

$$\mathrm{edge\_index} = \left[\mathcal{I},\mathcal{J}\right] \in \mathbb{N}^{2 \times E_t} \tag{25}$$

其中，每一列 (i,j) 表示从节点 i 到节点 j 的有向转移。每条此类边均关联一个标量权重，具体为

$$w_{ij} = \boldsymbol{A}_t(i,j) \tag{26}$$

其中，$\boldsymbol{A}_t(i,j)$ 表示 $i \to j$ 通信通道的指数平滑频率，用于捕捉该通道的历史强度。设 $\boldsymbol{H}=$

$\boldsymbol{H}^{(0)} \in \mathbb{R}^{N_t \times (d_{\text{in}} + D)}$ 为时间增强特征矩阵。首先通过可学习的线性变换，将 $\boldsymbol{H}$ 投影到维度为 $d_h = 64$ 的查询、键和值空间中，有

$$\boldsymbol{Q} = \boldsymbol{H}\boldsymbol{W}_{\boldsymbol{Q}},\quad \boldsymbol{K} = \boldsymbol{H}\boldsymbol{W}_{\boldsymbol{K}},\quad \boldsymbol{V} = \boldsymbol{H}\boldsymbol{W}_{\boldsymbol{V}}$$
$$\boldsymbol{W}_{\boldsymbol{Q}},\boldsymbol{W}_{\boldsymbol{K}},\boldsymbol{W}_{\boldsymbol{V}} \in \mathbb{R}^{(d_{\text{in}} + D) \times d_h} \tag{27}$$

其中，$\boldsymbol{Q}_i \in \mathbb{R}^{d_h}$ 表示节点 i 的查询请求，$\boldsymbol{K}_j$ 表示节点 j 的键值，$\boldsymbol{V}_i$ 表示消息内容。对于每个有向边 $(i \to j) \in E_t$，未归一化的注意力分数为

$$e_{ij} = \frac{\left\langle \boldsymbol{Q}_i, \boldsymbol{K}_j \right\rangle}{\sqrt{d_h}} \tag{28}$$

其中，$\langle \bullet, \bullet \rangle$ 表示欧几里得内积。该标准化点积用于衡量源嵌入与目标嵌入之间的特征相似性。为整合CAN总线的实际流量数据，通过边属性 w_{ij} 对各评分进行加权，并对节点 j 的所有入边应用softmax归一化处理，具体为

$$\alpha_{ij} = \frac{\exp(e_{ij})}{\sum\limits_{i':i' \to j} \exp(e_{i'j})},\quad \tilde{\alpha}_{ij} = \alpha_{ij}\left(w_{ij}\right)^{\gamma} \tag{29}$$

其中，$\gamma \geqslant 1$ 用来进一步放大权重差异。本文的实验设置 $\gamma = 1$，可保持原始通信频率的相对比例，减少对噪声的敏感，如果 γ 太大，可能将正常通信中的瞬时流量峰值误判为异常。因此，从节点 i 传递到节点 j 的最终消息为

$$m_{ij} = \tilde{\alpha}_{ij}\boldsymbol{V}_i \in \mathbb{R}^{d_h} \tag{30}$$

节点 j 通过简单求和聚合其传入消息，从而生成更新后的嵌入向量，即

$$H_j' = \sum_{i:i \to j} m_{ij},\quad \boldsymbol{H}' \in \mathbb{R}^{N_t \times d_h} \tag{31}$$

聚合过程使节点能够整合邻居的信息，捕捉CAN总线上ECU之间的通信依赖关系。例如，若节点 i 是高频发送者（如发动机控制单元），则其传递的消息权重 α_{ij} 更高，对节点 j 的特征更新影响更大。为增强梯度传递和模型表达能力，可选择性地添加残差连接和层归一化，具体为

$$\hat{\boldsymbol{H}}^{(\ell+1)} = \text{LayerNorm}\left(\boldsymbol{H}^{(\ell)} + \boldsymbol{H}'\right) \tag{32}$$

3.3　池化分类头

经过 L 层时间图注意力机制处理后，每个节点 $j \in V_t$ 将获得一个信息丰富的嵌入向量 $\boldsymbol{H}_j' \in \mathbb{R}^{d_h}$，该向量整合了负载统计信息、精确的时间线索以及多跳拓扑交互数据。为获得适用于实时入侵决策的紧凑型CAN窗口描述符，采用置换不变池化算子，具体为

$$g^{(t)} = \frac{1}{N_t}\sum_{N_t}^{j=1} \boldsymbol{H}_j' \tag{33}$$

其中，$N_t = \left|V_t\right|$ 表示在时间窗口 t 内活跃的CAN-ID数量，将整个动态图压缩为一个固定维度的全局向量 $g^{(t)}$。均值池化确保模型平衡高频和低频ECU的贡献，避免单个节点（如高通信量的ECU）主导全局特征。例如，在DoS攻击中，异常节点的特征会通过均值池化被放大，从而被分类器捕捉。将全局图特征 $g^{(t)}$ 映射到 C 维logit向量，用于预测入侵类型（如DoS、模糊攻击等）。采用了一个双参数线性分类器，$\boldsymbol{W}_o$ 和 $\boldsymbol{b}_o$ 是可学习参数，通过训练优化以最小化分类损失。

$$\boldsymbol{l} = \boldsymbol{W}_o g^{(t)} + \boldsymbol{b}_o,\quad \boldsymbol{W}_o \in \mathbb{R}^{C \times d_h}, \boldsymbol{b}_o \in \mathbb{R}^{C} \tag{34}$$

通过log-softmax函数将得到的logit向量 $\boldsymbol{l} \in \mathbb{R}^{C}$ 转换为类别概率，具体为

$$\hat{y}_c^{(t)} = \log\left(\text{softmax}(\boldsymbol{l})\right)_c = \boldsymbol{l}_c - \log\left(\sum_{C}^{c'=1} e^{\boldsymbol{l}_{c'}}\right) \tag{35}$$

在训练过程中，使用最小化负对数似然损失

$$\mathcal{L} = -\frac{1}{M}\sum_{M}^{m=1} \hat{y}_{y^{(tm)}}^{(t_m)} \tag{36}$$

其中，$\{t_m\}_{m=1}^{M}$ 是批处理中的标记窗口，$y^{(t_m)} \in \{1,\cdots,C\}$ 是真实类别。

4　性能评估

4.1　数据集及指标介绍

1) 数据集介绍

Car-Hacking数据集[1]。该数据集包括拒绝服务攻击、模糊攻击、驱动齿轮欺骗和转速表欺骗。它是通过记录真实车辆通过OBD-Ⅱ端口进行消息注入攻击时的CAN流量构建的。

CAN-intrusion数据集[28]。该数据集中的攻击场景分为消息注入攻击和冒充攻击两类，具体类型包括拒绝服务攻击、模糊攻击、冒充攻击和无攻击状态，所有这些都是通过记录真实车辆通过OBD-Ⅱ端口的CAN流量构建的。

表1为Car-Hacking和CAN-intrusion数据集的标签和攻击类别。

所有实验均在配备NVIDIA GeForce RTX 3060 GPU的本地工作站上进行。RTX 3060的运算能力约为12.7 TFLOP（FP32），Orin和Pegasus这样的汽车系统则提供254~320 TOPS，满足典型的L3/L4需求。1 TFLOP（FP32）大致相当于4 TOPS

（INT8），因此本文测试平台的性能与智能车辆的硬件限制相当。

表 1　Car-Hacking 和 CAN-intrusion 数据集的标签和攻击类别

数据集	标签	攻击类别
Car-Hacking 数据集	0	拒绝服务攻击
	1	模糊攻击
	2	驱动齿轮欺骗
	3	转速表欺骗
	4	正常
CAN-intrusion 数据集	0	拒绝服务攻击
	1	模糊攻击
	2	冒充攻击
	3	正常

2) 指标

推理时间。通过禁用梯度追踪功能，在推理模式下测量处理单个窗口所需的端到端耗时。通过量化模型处理单窗口流量图所需的时间，为汽车控制器在分类突发网络数据包时可能遭遇的最坏情况处理延迟提供参考。

GPU 峰值内存。在开始推理之前，重置内存跟踪计数器，以确保仅记录模型执行期间的内存分配。在 GPU 平台上，记录最大分配的设备内存。对于车辆嵌入式场景，该指标尤为关键，因为 ECU 通常有严格的随机存取存储器（RAM）限制。

3) 对比实验模型

文献[26]模型通过可学习点积和 ReLU 扩展了图注意力网络（graph attention network, GAT），通过在时间相邻的 8 B 有效载荷节点上堆叠两层，并引入了 CAN 定制的注意力权重。

文献[29]模型依次耦合图卷积网络（graph convolutional network, GCN）用于空间拓扑和 LSTM 用于时间动态序列，构建了具有余弦相似性和增强循环熵特征的无人机控制区域网络（unmanned aerial vehicle controller area network, UAV-CAN）图。

文献[30]模型采用基于求和的多层感知机（multi-layer perceptron, MLP）进行单射多重集聚合，产生可证明的最大判别力，完整保留图的结构信息。

4.2　不同长度的窗口

为了展示不同长度的窗口对模型准确率的影响，设 $H=0$ 表示不使用窗口，$H=10$、20、40 表示使用相应长度的窗口。Car-Hacking 数据集上不同窗口长度下模型的准确率如图 5 所示。从图 5 可以看出，当没有历史信息（$H=0$）时，模型收敛速度缓慢；引入 $H=10$ 的短记忆窗口显著加速了收敛速度（到第 60 次迭代时超过 99.0%），并达到最高的最终准确率 99.2%；更长的缓冲区（$H=20$ 或 40）仅带来边际准确率提升，但收益递减。

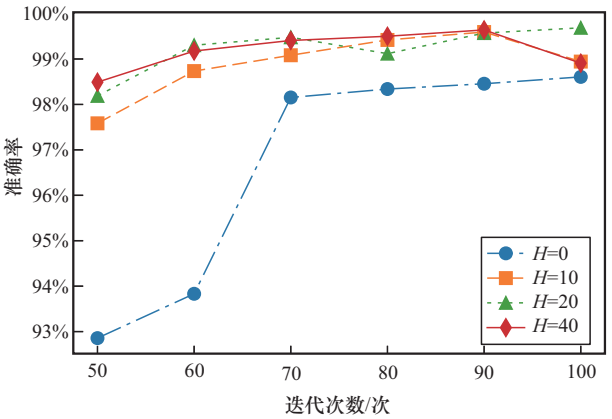


图 5　Car-Hacking 数据集上不同窗口长度下模型的准确率

图 6 为 Car-Hacking 数据集上不同长度的窗口模型的推理性能。从图 6 可以看出，$H=10$ 的模型仅产生 0.14 ms 的轻微时延并占用 5.4 KB 内存；$H=20$ 时延增加到 0.20 ms，内存使用量增加到 5.6 KB；$H=40$ 时延增加到 0.18 ms，内存使用量增加到 7.1 KB。$H=10$ 的配置实现了最佳平衡，显著提高了检测准确率和收敛速度，并保持最小的内存占用。因此，后续实验中采用 $H=10$ 作为默认值。

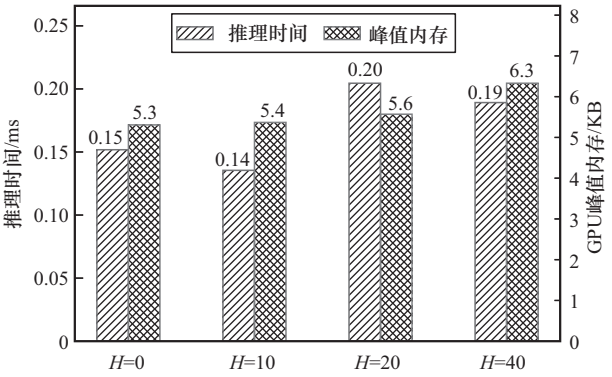


图 6　Car-Hacking 数据集上不同长度的窗口模型的推理性能

4.3　不同尺度的窗口

为阐明窗口内不同尺度信息对模型的影响，分别在 W=50、100、150、200 和 300 的条件下进行了实验。图 7 为不同窗口尺度下的模型准确率。当 W=50 和 100、迭代次数为 100 次时，最终准确率达到 99% 以上。图 8 为 CAN 报文窗口尺度对模型性能的影响，其展示了处理整个 CAN 数据包日志所需的推理时间，并不是单个图的推理时间。因为在实际部署中，车辆 1 s 可能产生数千条 CAN 报文日志，处理整个日志的总时间能够直观地反映不同窗口尺度在处理宏观连续数据流时的真实系统负载。

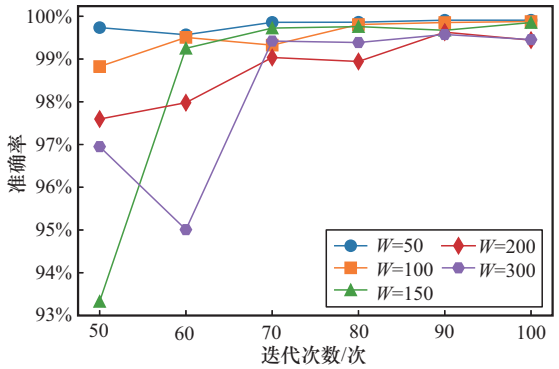


图 7　不同窗口尺度下的模型准确率

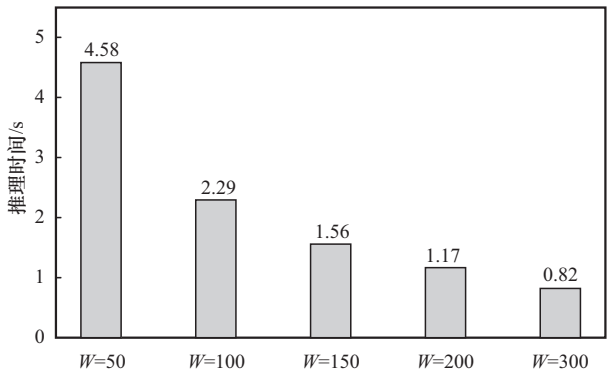


图 8　CAN 报文窗口尺度对模型性能的影响

由图 8 可以看出，最小窗口（W=50）因生成更多图导致最大开销（4.58 s），W=100 时总推理时间缩短超过一半（2.29 s）。随着窗口数量减少，更大窗口（W=150、200、300）的运行时间分别降至 1.56 s、1.17 s 和 0.82 s。当窗口尺度超过 100 时，运行时间的提升幅度相对于微小的准确率增长已不明显。结果表明，W=100 在高准确率、快速收敛和高效推理之间实现了最佳平衡。

4.4　消融实验

本节评估了模型各模块的有效性，包括本文模型、移除连续时间嵌入、移除图注意力机制和多层感知机（代表非图结构），并在两个数据集及不同窗口尺度上进行了验证。

图 9 和图 10 为消融模型在 Car-Hacking 数据集不同窗口尺度下准确率随迭代次数的变化。在所有模型中，本文模型始终保持最高准确率，当 W=100 时准确率快速攀升至 99%。移除连续时间嵌入或图注意力机制会导致准确率显著下降，在 W=100 时，移除连续时间嵌入准确率稳定在 96% 左右，移除图注意力机制准确率稳定在 98% 左右，本文模型准确率达 99.5%。非图结构多层感知机模型表现落后于其他模型，凸显了空间与时间建模的双重重要性。这些结果不仅验证了模型的有效性，而且表明模型能够捕捉 CAN 总线拓扑的演变。

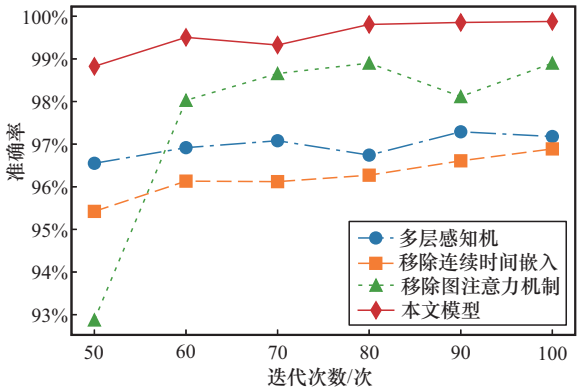


图 9　消融模型在 Car-Hacking 数据集上准确率随迭代次数的变化（W=100）

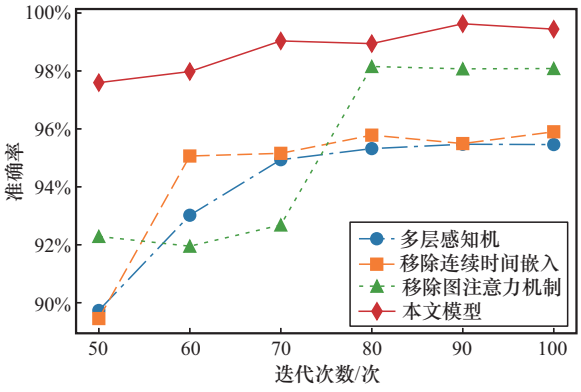


图 10　消融模型在 Car-Hacking 数据集上准确率随迭代次数的变化（W=200）

图 11 和图 12 为消融模型在 CAN-Intrusion 数据集不同窗口尺度下准确率随迭代次数的变化。从

图 11 和图 12 可以看出，本文模型在不同窗口尺度下的准确率均表现最佳，稳定在 96%。

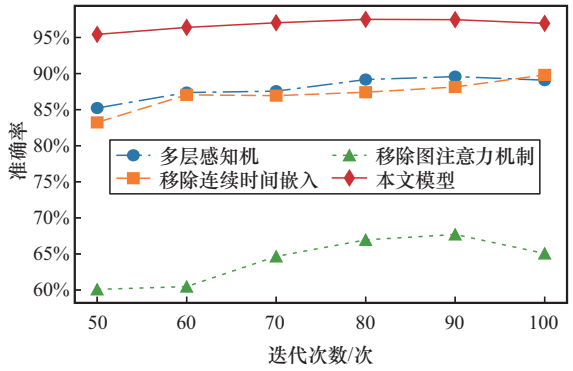


图 11　消融模型在 CAN-Intrusion 数据集上准确率随迭代次数的变化（W=100）

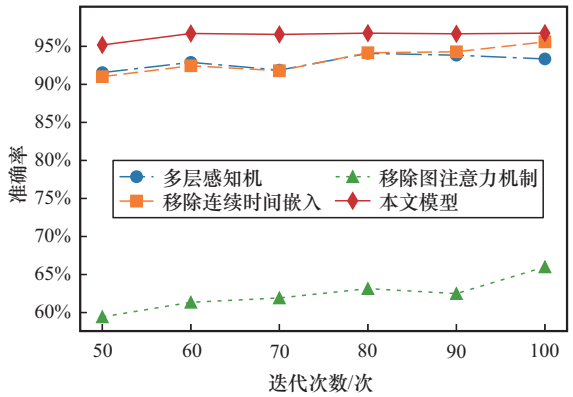


图 12　消融模型在 CAN-Intrusion 数据集上准确率随迭代次数的变化（W=200）

从图 11 和图 12 可以看出，当 W=100 时，本文模型的优势相较 W=200 时更突出。此外，移除图注意力机制后模型表现较差，准确率稳定在 65% 左右，说明在 CAN-Intrusion 数据集上采用均匀聚合的方法并不适用，这也证明了本文模型各模块的重要性。

为了证明模型高质量的表征学习能力，表 2~表 4 分别展示了本文模型与消融模型在 Car-Hacking 数据集上不同窗口尺度 $W\in\{50,150,300\}$ 下的精确率（Pre）、召回率（Re）、F1 分数，其中 MACRO 表示宏平均，即对所有类的指标值求算术平均值。在所有窗口尺度中，完整模型的各项指标始终优于其消融模型，当窗口长度 $W\geqslant 50$ 时，F1 分数均超过 99%，上述实验验证了本文模型各模块的合理性和重要性。

4.5　对比实验

不同模型在 Car-Hacking 和 CAN-Intrusion 数据集上的性能如图 13 所示，其中 W=200，迭代次数为 50~100 次。从图 13(a)和图 13(b)可以看出，本文模型收敛速度最快，并达到最高的最终准确率；文献[26]的表现也很优越，但在整个训练过程中落后于本文模型；文献[30]实现了中等准确率；文献[29]未能超过 98.6%，这表明静态邻接卷积足以捕捉 CAN 总线入侵模式固有的时空动态。从图 13(c)和图 13(d)可以看出，本文模型仅需 0.14 ms 处理一个

表 2　　W=50 时模型在 Car-Hacking 数据集上的性能

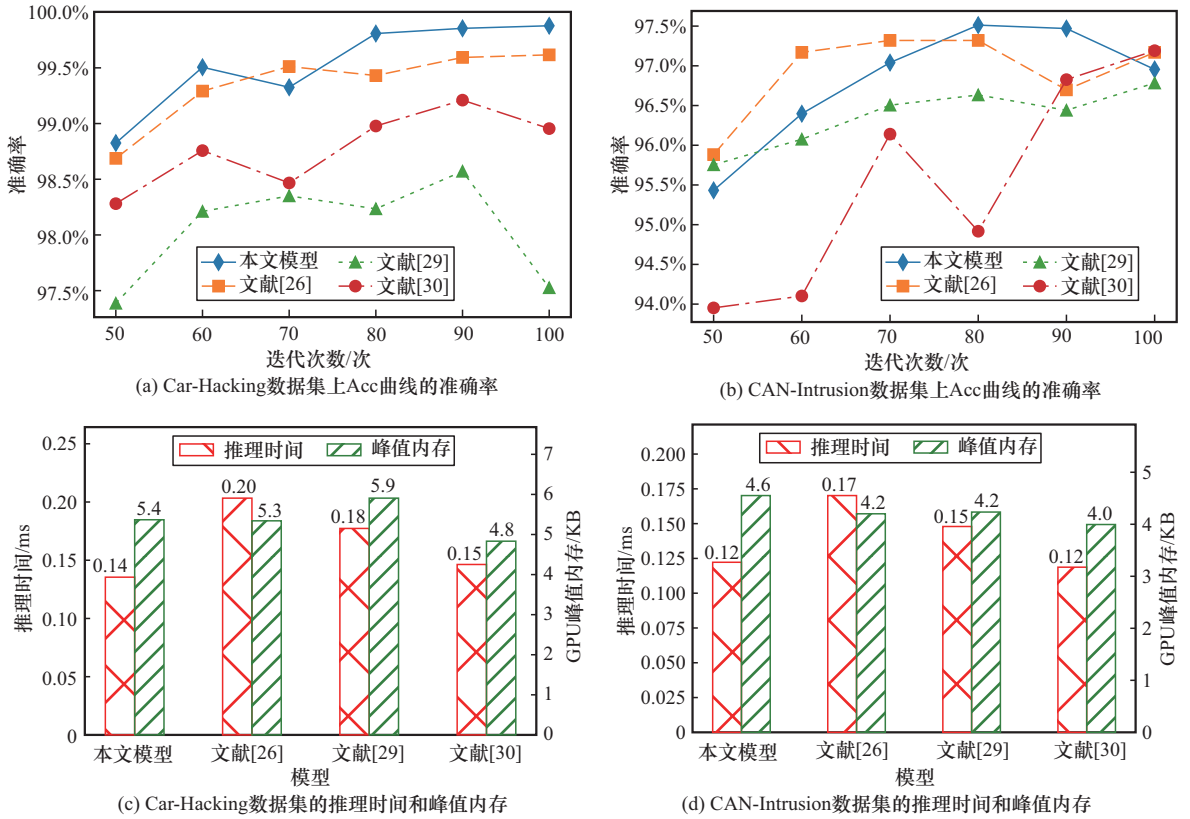
类别	多层感知机			移除连续时间嵌入			移除图注意力机制			本文模型		
	Pre	Re	F1 分数	Pre	Re	F1 分数	Pre	Re	F1 分数	Pre	Re	F1 分数
0	**100.00%**	98.87%	99.43%	99.43%	98.71%	99.07%	99.70%	99.01%	99.35%	99.86%	**99.95%**	**99.91%**
1	97.03%	97.39%	97.21%	96.44%	97.88%	97.16%	99.37%	98.15%	98.75%	**100.00%**	**99.62%**	**99.81%**
2	99.93%	99.47%	99.70%	98.78%	99.50%	99.14%	99.95%	99.71%	99.83%	**100.00%**	**100.00%**	**100.00%**
3	99.87%	99.11%	99.49%	99.56%	99.47%	99.51%	99.82%	99.53%	99.67%	**99.96%**	**99.99%**	**99.97%**
4	96.48%	97.94%	97.20%	97.08%	95.92%	96.50%	97.62%	99.23%	98.42%	**99.74%**	**99.90%**	**99.82%**
MACRO	98.66%	98.56%	98.61%	98.26%	98.30%	98.28%	99.29%	99.13%	99.21%	**99.91%**	**99.89%**	**99.90%**

表 3　　W=150 时模型在 Car-Hacking 数据集上的性能

类别	多层感知机			移除连续时间嵌入			移除图注意力机制			本文模型		
	Pre	Re	F1 分数	Pre	Re	F1 分数	Pre	Re	F1 分数	Pre	Re	F1 分数
0	98.79%	94.88%	96.80%	99.55%	90.99%	95.08%	99.51%	97.00%	98.24%	**100.00%**	**100.00%**	**100.00%**
1	87.43%	98.01%	92.42%	91.40%	98.19%	94.67%	98.94%	97.78%	98.35%	**100.00%**	**99.59%**	**99.80%**
2	98.90%	99.31%	99.10%	99.76%	98.86%	99.30%	100.00%	99.65%	99.83%	**100.00%**	**100.00%**	**100.00%**
3	98.38%	98.35%	98.36%	98.49%	97.89%	98.19%	99.47%	98.50%	98.98%	**100.00%**	**99.62%**	**99.81%**
4	93.77%	88.58%	91.10%	91.40%	92.70%	92.05%	98.65%	97.09%	99.67%	**99.42%**	**100.00%**	**99.71%**
MACRO	95.46%	95.83%	95.56%	96.12%	95.73%	95.86%	98.70%	98.32%	98.50%	**99.88%**	**99.84%**	**99.86%**

表4　W=300时模型在Car-Hacking数据集上的性能

类别	多层感知机			移除连续时间嵌入			移除图注意力机制			本文模型		
	Pre	Re	F1 分数	Pre	Re	F1 分数	Pre	Re	F1 分数	Pre	Re	F1 分数
0	91.17%	70.94%	79.79%	93.60%	84.94%	89.06%	**100.00%**	94.06%	96.94%	99.60%	**99.08%**	**99.34%**
1	84.93%	98.41%	91.18%	88.62%	95.56%	91.96%	95.98%	98.52%	97.23%	**100.00%**	**98.84%**	**99.41%**
2	99.86%	98.79%	99.32%	99.64%	97.72%	98.67%	99.93%	99.64%	99.79%	**100.00%**	**99.79%**	**99.89%**
3	97.47%	96.32%	96.89%	98.44%	97.28%	97.85%	98.02%	98.31%	98.16%	**100.00%**	**99.34%**	**99.67%**
4	79.50%	82.28%	80.87%	84.70%	87.05%	85.85%	93.89%	95.23%	94.56%	**97.97%**	**99.86%**	**98.91%**
MACRO	90.59%	89.35%	89.61%	93.00%	92.51%	92.68%	99.91%	97.15%	97.34%	**99.52%**	**99.38%**	**99.44%**



(a) Car-Hacking数据集上Acc曲线的准确率　(b) CAN-Intrusion数据集上Acc曲线的准确率

(c) Car-Hacking数据集的推理时间和峰值内存　(d) CAN-Intrusion数据集的推理时间和峰值内存

图13　不同模型在Car-Hacking和CAN-Intrusion数据集上的性能

窗口，峰值内存占用为5.4 KB；尽管文献[26]略慢且内存占用稍低，但它在准确率上牺牲了0.2%~0.3%；文献[29-30]处理更快且内存占用更低，但其较差的检测性能使其不适合安全关键部署。本文模型在检测准确率和计算效率之间取得了最佳平衡，满足车载入侵检测所需的亚毫秒延迟和最小内存要求。

表5为不同模型在Car-Hacking数据集（W=200）和CAN-Intrusion数据集（W=100）上评估模型的Pre、Re和F1分数。在Car-Hacking数据集上，本文模型在5个攻击类别（0~4）中均达到最高的F1分数。在CAN-Intrusion数据集上，本文模型达到了93.07%的F1分数，超过了所有基线。结果表明，本文模型对CAN攻击类型具有稳健检测。

5　结束语

本文主要提出基于指数平滑动态图的CAN总线入侵检测框架，将动态拓扑自适应与时空图学习相结合，通过有限记忆指数平滑算子构建时变邻接关系。该模型通过融合正弦时间嵌入与边条件注意力机制，并结合节点门控循环网络，能够即时响应结构异常和时间异常。结果表明，本文模型的检测

表5 不同模型在Car-Hacking与CAN-Intrusion数据集的指标情况

数据集	类别	本文模型			文献[26]			文献[29]			文献[30]		
		Pre	Re	F1分数	Pre	Re	F1分数	Pre	Re	F1分数	Pre	Re	F1分数
Car-Hacking	0	99.82%	99.91%	99.86%	100.00%	99.63%	99.82%	87.48%	99.72%	93.20%	99.90%	95.95%	97.89%
	1	100.00%	99.58%	99.79%	99.93%	99.41%	99.67%	100.00%	99.26%	99.63%	99.85%	99.63%	99.74%
	2	100.00%	99.95%	99.98%	100.00%	99.81%	99.90%	99.95%	99.62%	99.78%	99.95%	99.47%	99.71%
	3	99.92%	99.95%	99.94%	99.55%	99.65%	99.60%	99.19%	98.80%	99.00%	99.65%	99.00%	99.32%
	4	99.67%	99.91%	99.79%	98.91%	99.52%	99.21%	97.91%	91.95%	94.84%	96.34%	99.52%	97.90%
	MACRO	99.88%	99.86%	99.87%	99.68%	99.60%	99.64%	96.91%	97.87%	97.29%	99.14%	98.71%	98.91%
CAN-Intrusion	0	99.87%	100.00%	99.94%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%	100.00%
	1	84.43%	71.03%	77.16%	81.00%	64.29%	71.68%	69.62%	71.83%	70.70%	72.63%	78.97%	75.67%
	2	100.00%	98.02%	99.00%	99.78%	100.00%	99.89%	100.00%	100.00%	100.00%	99.94%	99.83%	99.89%
	3	94.29%	98.18%	96.19%	95.17%	97.69%	96.41%	96.07%	95.65%	95.86%	96.94%	95.87%	96.40%
	MACRO	94.65%	91.81%	93.07%	93.99%	90.49%	92.00%	91.42%	91.87%	91.64%	92.38%	93.67%	92.99%

准确率高达99.8%，单窗口推理时延为0.14 ms，这证明了本文模型的高效性。

参考文献：

[1] Song H M, Woo J, Kim H K. In-vehicle network intrusion detection using deep convolutional neural network[J]. Vehicular Communications, 2020, 21: 100198.

[2] Martínez-Cruz A, Ramírez-Gutiérrez K A, Feregrino-Uribe C, et al. Security on in-vehicle communication protocols: Issues, challenges, and future research directions[J]. Computer Communications, 2021, 180: 1-20.

[3] Rajapaksha S, Kalutarage H, Al-Kadri M O, et al. AI-based intrusion detection systems for in-vehicle networks: a survey[J]. ACM Computing Surveys, 2023, 55(11): 1-40.

[4] Khan M H, Javed A R, Iqbal Z, et al. DivaCAN: detecting in-vehicle intrusion attacks on a controller area network using ensemble learning[J]. Computers & Security, 2024, 139: 103712.

[5] Song J R, Qin G H, Liang Y H, et al. DGIDS: dynamic graph-based intrusion detection system for CAN[J]. Computers & Security, 2024, 147: 104076.

[6] Wei Y H, Cheng C, Xie G Q. OFIDS: online learning-enabled and fingerprint-based intrusion detection system in controller area networks[J]. IEEE Transactions on Dependable and Secure Computing, 2023, 20(6): 4607-4620.

[7] Yu Z W, Liu Y, Xie G Q, et al. TCE-IDS: time interval conditional entropy- based intrusion detection system for automotive controller area networks[J]. IEEE Transactions on Industrial Informatics, 2023, 19(2): 1185-1195.

[8] Liu W N, Qin G H, Liang Y H, et al. ETFIDS: an entropy-driven, time-frequency analysis framework for in-vehicle CAN signal intrusion detection[J]. IEEE Internet of Things Journal, 2025, 12(12): 21507-21522.

[9] Kulandaivel S, Goyal T, Agrawal A K, et al. CANvas: fast and inexpensive automotive network mapping[C]//28th USENIX Security Symposium (USENIX Security 19). Berkeley: USENIX Association, 2019: 389-405.

[10] Lucas J M, Saccucci M S. Exponentially weighted moving average control schemes: properties and enhancements[J]. Technometrics, 1990, 32(1): 1-12.

[11] 熊炫睿, 郭星佑, 宁兆龙, 等. 基于数据增强和多解释方法融合的入侵检测方法[J]. 通信学报, 2025, 46(10): 191-206.
Xiong X R, Guo X Y, Ning Z L, et al. Intrusion detection method based on data augmentation and multi-explanation method fusion[J]. Journal on Communications, 2025, 46(10): 191-206.

[12] Xun Y J, Deng Z Y, Liu J J, et al. Side channel analysis: a novel intrusion detection system based on vehicle voltage signals[J]. IEEE Transactions on Vehicular Technology, 2023, 72(6): 7240-7250.

[13] Levy E, Shabtai A, Groza B, et al. CAN-LOC: spoofing detection and physical intrusion localization on an in-vehicle CAN bus based on deep features of voltage signals[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 4800-4814.

[14] Deng Z Y, Liu J J, Xun Y J, et al. IdentifierIDS: a practical voltage-based intrusion detection system for real in-vehicle networks[J]. IEEE Transactions on Information Forensics and Security, 2024, 19: 661-676.

[15] Aljabri W, Hamid M A, Mosli R. Enhancing real-time intrusion detection system for in-vehicle networks by employing novel feature engineering techniques and lightweight modeling[J]. Ad Hoc Networks, 2025, 169: 103737.

[16] Han M L, Kwak B I, Kim H K. Event-triggered interval-based anomaly detection and attack identification methods for an in-vehicle network[J]. IEEE Transactions on Information Forensics and Security, 2021, 16: 2941-2956.

[17] Halder S, Conti M, Das S K. COIDS: a clock offset based intrusion detection system for controller area networks[C]//Proceedings of the 21st International Conference on Distributed Computing and Networking. New York: ACM Press, 2020: 1-10.

[18] Zhao Y L, Xun Y J, Liu J J. ClockIDS: a real-time vehicle intrusion detection system based on clock skew[J]. IEEE Internet of Things Journal, 2022, 9(17): 15593-15606.

[19] Lee S, Choi W, Jo H J, et al. ErrIDS: an enhanced cumulative timing error-based automotive intrusion detection system[J]. IEEE Transactions on Intelligent Transportation Systems, 2023, 24(11): 12406-12421.

[20] 刘奇旭, 肖聚鑫, 谭耀康, 等. 工业互联网流量分析技术综述[J]. 通信学报, 2024, 45(8): 221-237.
Liu Q X, Xiao J X, Tan Y K, et al. Survey of industrial Internet traffic analysis technology[J]. Journal on Communications, 2024, 45(8): 221-237.
[21] Refat R U D, Elkhail A A, Hafeez A, et al. Detecting CAN bus intrusion by applying machine learning method to graph based features[C]// Proceedings Of SAI intelligent systems conference. Cham: Springer International Publishing. Berlin: Springer, 2021: 730-748.
[22] Korium M S, Saber M, Beattie A, et al. Intrusion detection system for cyberattacks in the Internet of Vehicles environment[J]. Ad Hoc Networks, 2024, 153: 103330.
[23] 刘涛涛, 付钰, 王坤, 等. 基于VAE-CWGAN和特征统计重要性融合的网络入侵检测方法[J]. 通信学报, 2024, 45(2): 54-67.
Liu T T, Fu Y, Wang K, et al. Network intrusion detection method based on VAE-CWGAN and fusion of statistical importance of feature[J]. Journal on Communications, 2024, 45(2): 54-67.
[24] Zhang H R, Zeng K, Lin S. Federated graph neural network for fast anomaly detection in controller area networks[J]. IEEE Transactions on Information Forensics and Security, 2023, 18: 1566-1579.
[25] King I J, Bowman B, Huang H H. Fine-grained graph-based anomaly detection on vehicle controller area networks[C]//Proceedings of the 2024 IEEE International Conference on Big Data (BigData). Piscataway: IEEE Press, 2024: 1346-1351.
[26] Xiao J C, Yang L, Zhong F L, et al. Robust anomaly-based intrusion detection system for in-vehicle network by graph neural network framework[J]. Applied Intelligence, 2023, 53(3): 3183-3206.
[27] Vaswani A, Shazeer N, Parmar N, et al. Attention is all you need[C]// Proceedings of the 31st International Conference on Neural Information Processing Systems (NeurIPS). New York: ACM Press, 2017: 6000-6010.
[28] Lee H, Jeong S H, Kim H K. OTIDS: a novel intrusion detection system for in-vehicle network by using remote frame[C]//Proceedings of the 2017 15th Annual Conference on Privacy, Security and Trust (PST). Piscataway: IEEE Press, 2017: 57-5709.
[29] Du Y, Li Y L, Cheng P, et al. UGL: a comprehensive hybrid model integrating GCN and LSTM for enhanced intrusion detection in UAV controller area networks[J]. Computer Networks, 2025, 262: 111157.
[30] Stocker S N, Gasteiger J, Becker F, et al. How robust are modern graph neural network potentials in long and hot molecular dynamics simulations?[J]. Machine Learning (Science and Technology), 2022, 3(4): 8.

[作者简介]

韦文杰（1993– ），男，山西朔州人，北京科技大学博士生，主要研究方向为深度学习、网络安全和异常检测。

王建萍（1974– ），女，河北保定人，博士，北京科技大学教授，主要研究方向为可见光通信、人工智能。

陈彬（1995– ），男，北京人，新唐智创电子技术有限公司网络维护工程师，主要研究方向为计算机网络运维。

林福宏（1981– ），男，北京人，博士，北京科技大学教授，主要研究方向为网络安全、人工智能和边缘计算。