基于混合深度学习的物联网入侵检测模型研究

Study on IoT Intrusion Detection Models Using Hybrid Deep Learning

吴志祥，陆文红，曲 谱（中国联通黑龙江分公司，黑龙江 哈尔滨 150001）
Wu Zhixiang，Lu Wenhong，Qu Pu（China Unicom Heilongjiang Branch，Harbin 150001，China）

摘 要：
近年来，深度学习技术在提升物联网入侵侦测能力方面成效显著。然而，物联网设备运算能力有限、储存空间不足，这给部署资源密集型的入侵检测系统带来了挑战。提出了一款轻量级模型DL-BiLSTM，该模型融合了深度神经网络与双向长短期记忆网络，能够从复杂的网络数据中提取非线性且具备双向长距离依赖的特征。为解决物联网设备资源有限的问题，DL-BiLSTM采用增量主成分分析（IPCA）算法降低特征维度，为资源受限设备提供高效入侵侦测方案。

关键词：
物联网入侵侦测；深度学习；深度神经网络；双向长短期记忆网络
doi：10.12045/j.issn.1007-3043.2026.05.016
文章编号：1007-3043（2026）05-0086-07
中图分类号：TN915
文献标识码：A
开放科学（资源服务）标识码（OSID）：

Abstract：
In recent years, deep learning technology has demonstrated significant effectiveness in enhancing the intrusion detection capabilities of the Internet of Things（IoT）. However, the limited computational power and storage space of IoT devices pose challenges for deploying resource-intensive intrusion detection systems. To address this issue, researchers have proposed a lightweight model called DL-BiLSTM, which combines deep neural networks（DNN）with bidirectional long short-term memory networks（BiLSTM）to extract nonlinear features with bidirectional long-range dependencies from complex network data. To address the resource constraints of IoT devices, DL-BiLSTM employs the incremental principal component analysis（IPCA）algorithm to reduce feature dimensions, providing an efficient intrusion detection solution for resource-constrained IoT devices.

Keywords：
IoT intrusion detection；Deep learning；DNN；Bidirectional long short-term memory networks（BiLSTM）

引用格式：吴志祥，陆文红，曲谱. 基于混合深度学习的物联网入侵检测模型研究[J]. 邮电设计技术，2026（5）：86-92.

1 概述

1.1 研究背景与动机

随着科技的飞速发展，物联网（IoT）技术以前所未有的规模实现了各类设备的互联互通，其应用已渗透到健康照护、工业自动化、智慧城市、智慧物流等众多领域，深刻改变了人类的生活与生产方式。据统计，2020年联网设备数量为117亿，2025年增至310亿，预计2027年将突破410亿。然而，物联网的开放性与设备资源受限特性，使其面临严峻的网络安全挑战。多数物联网设备因设计初期缺乏安全考量，存在运算能力有限、内存不足、安全漏洞频发等问题，易成为黑客攻击目标，进而导致僵尸网络、DDoS攻击、数据窃取等安全事件频发[1-2]。有报告显示，约半数使用物联网设备的企业曾受安全漏洞的影响。因此，构建适应物联网环境的稳定、高效入侵侦测系统（IDS），已成为当前亟待解决的关键课题。

1.2 物联网发展趋势

收稿日期：2026-04-09

当前，物联网技术已广泛应用于智慧家居、工业物联网（IIoT）、车联网等领域，推动了各行业的数字化转型。在技术层面上，传感器精度、通信技术（如5G）、云计算与大数据处理能力的提升，为物联网的大规模应用提供了支撑[3]。未来，物联网的发展呈现三大趋势：一是与人工智能（AI）深度融合，实现数据的智能分析与自主决策，例如智慧安防中的异常行为识别；二是边缘计算技术的普及，减少数据传输延迟，提升系统响应速度；三是安全与隐私保护将成为核心研究方向。如何在保障设备与数据安全的同时推动技术应用，是行业发展的重要命题。

1.3 研究目的

本研究旨在提出一种高效能、低复杂度的混合深度学习轻量化神经网络模型，并将其应用于物联网入侵侦测，以解决物联网设备资源受限与安全漏洞并存问题。通过优化模型结构、数据处理技术及参数策略，提升该模型对复杂恶意活动的识别能力，降低安全风险。入侵侦测系统（IDS）是物联网安全的核心防线，由数据搜集、数据分析与响应元件构成[4]。传统IDS存在局限性：误用侦测技术难以应对未知攻击，异常侦测误报率较高。混合式IDS虽融合了两者优势，但深度学习模型的高复杂度使其难以适配资源受限的物联网设备[5]。为此，本研究以BiLSTM为基础，整合DNN以强化非线性特征提取能力，采用动态量化技术降低模型复杂度，结合IPCA算法进行特征降维，并通过Optuna框架优化超参数。

本研究的模型和算法体现为以下几个方面。

a）新型入侵侦测模型。提出一种DNN-BiLSTM混合模型，该模型融合了DNN的非线性特征提取能力与BiLSTM的长距离依赖处理优势。

b）轻量化方案。通过动态量化技术压缩模型，在保持模型性能的同时降低复杂度。

c）高效特征降维。采用IPCA算法适配物联网实时监控场景，提升系统适应性。

d）超参数优化。引入Optuna框架自动寻优超参数，确保模型性能最优。

2 技术与挑战

物联网设备安全挑战主要体现在4个方面。一是设备资源有限，计算、存储和能源供应不足，使传统安全机制难以适用，复杂加密算法可能导致设备性能下降。二是设备具有多样性，不同厂商设备在硬件、系统和通信协议等方面存在差异，且缺乏统一的安全标准，攻击者可利用兼容性问题和漏洞发起攻击。三是存在通信安全问题，Wi-Fi、蓝牙等协议存在缺陷，数据在传输过程中易被窃取或篡改。四是生命周期管理存在风险，部分设备因厂商停止安全更新，长期暴露于已知漏洞下。解决这些问题需多方协作，制定标准并研发检测技术。

入侵侦测系统核心元件包括数据搜集、数据分析和响应元件。数据搜集元件负责从网络流量、系统日志等多来源收集数据，其数据的全面性和精准性是系统有效运作的基础。数据分析元件运用特征侦测、异常侦测和机器学习等方法进行数据分析，其中特征侦测能识别已知入侵但对未知入侵的识别效果差；异常侦测可发现未知入侵，但误报率高；机器学习方法的适应性强，能提升侦测的准确度。响应元件在侦测到入侵后采取主动或被动措施，以减少入侵行为可能造成的损害。各元件协同工作，但它们的性能需不断优化以应对复杂的网络环境[6]。传统IDS技术分为基于特征和基于异常2类。基于特征的IDS依赖已知攻击特征库，其准确性高，但无法识别未知攻击；基于异常的IDS通过建立正常行为模型检测异常行为，能够发现未知攻击，却存在建模型难、误报率高的问题[7]。此外，传统IDS在处理海量流量和复杂网络时存在性能瓶颈。

深度学习在网络入侵检测中应用广泛。多层感知机、循环神经网络及其变体、卷积神经网络、深度信念网络等模型各有优势，采用集成多种模型的方法也能提升性能。但深度学习面临数据需求大、可解释性差、运算成本高等挑战[8]。

特征降维算法可降低高维数据的计算复杂性和过拟合风险，常见的特征降维算法有PCA、LDA、t-SNE等[9]。增量主成分分析（IPCA）适用于物联网海量数据降维，通过逐批处理数据来更新主成分分析预估值，能够应对动态数据环境，在不显著牺牲准确性的前提下解决传统PCA面临的内存和计算问题。

IPCA具有无需一次性加载全部数据，而是通过增量更新主成分估计的特点，能有效处理大规模或串流数据，尤其适合物联网环境。它在降低内存需求的同时，可达到近似传统PCA的降维效果，且在数据分布随时间缓慢变化时，动态适应性更强。在物联网入侵检测中，IPCA可提取高维复杂数据的关键特征，并通过监测独立成分变化来检测异常，且计算复杂度低，

能适应物联网设备的资源限制[9]。将IPCA与深度学习结合可提升物联网入侵检测性能。将IPCA提取的特征输入深度学习模型，能发挥前者特征降维的优势与后者非线性建模的能力，如结合CNN或RNN可更准确地识别入侵行为。传统PCA需批次处理所有数据，效率低，难以适应物联网即时监控的需求，而IPCA可弥补此不足[10]。

3 主要做法

本研究提出的DNN-BiLSTM模型，融合了深度神经网络（DNN）抽取复杂非线性特征的能力与双向长短期记忆网络（BiLSTM）精准捕捉序列长距依赖的优势，能够从物联网流量数据中同步学习时序与深度信息（见图1）。

3.1 DNN层

DNN层是模型中非线性特征提取的关键部分，位于模型开端，用于对预处理后的IoT数据进行深度抽象，挖掘隐藏模式。它由多个全连接层构成，本模型采用3层（Layer1、Layer2、Layer3），各层含有一定数量的神经元，神经元间通过权重连接，基于权重实现数据处理，其计算方式为：

$$y = \varphi(W^{\mathrm{T}}x + b) \tag{1}$$

其中，x是输入向量，W是权重矩阵，b是偏差向量，φ是非线性启动函数。在本研究中，采用ReLU（Rectified LinearUnit）作为启动函数，其定义为：

$$\varphi(Z)=\max(0,Z) \tag{2}$$

ReLU函数相较于Sigmoid和Tanh，具有收敛快、不易梯度消失的优势，能够加速模型训练。为防止过拟合，在每个全连接层后加入Dropout技术，随机丢弃部分神经元，使模型学习到更具泛化性的特征。

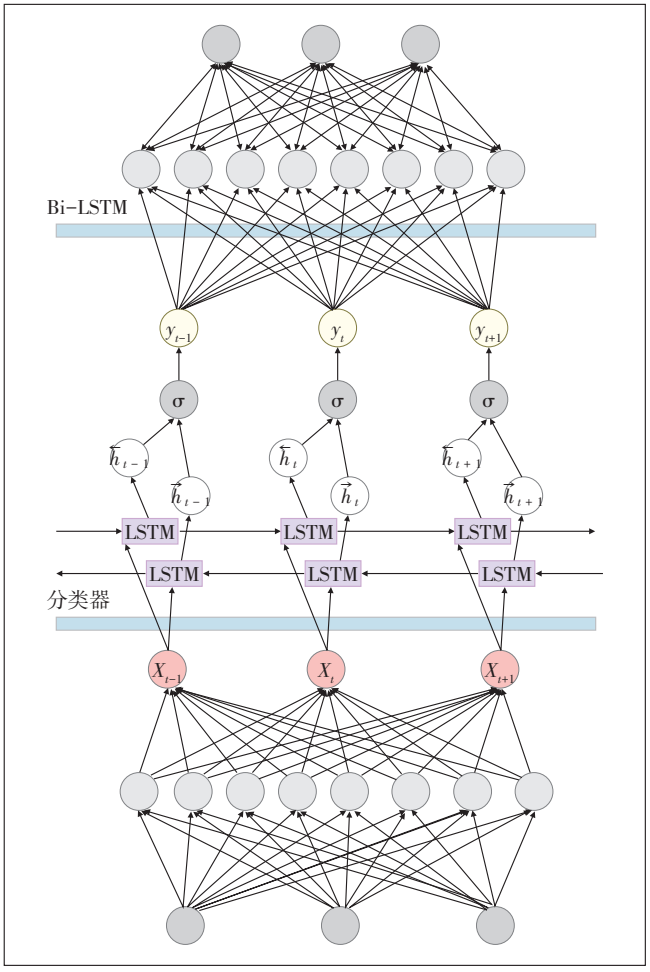

图1 DNN-BiLSTM

3.2 BiLSTM层

DNN提取初级特征后的数据被输入BiLSTM层。因IoT数据具时间序列特性，且入侵行为含时间依赖模式，BiLSTM能双向处理序列信息，捕捉上下文时间特征，在识别此类入侵时表现佳。其单元由正反向LSTM并联而成，LSTM借助记忆单元和输入、遗忘、输出三门控机制，解决了传统RNN梯度消失问题，图2所示为典型LSTM单元的架构。

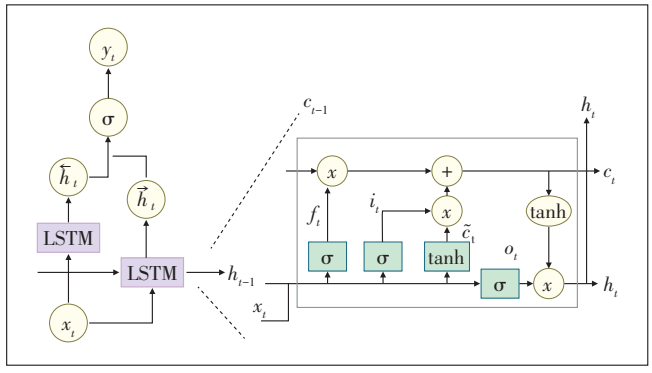

图2 LSTM单元架构

以正向LSTM单元为例，各门控机制的计算公式如下：

$$i_t = \sigma(w_{xi}x_t + w_{hi}h_{t-1} + b_i) \tag{3}$$

$$f_t = \sigma(w_{xf}x_t + w_{hf}w_{t-1} + b_f) \tag{4}$$

$$O_t = \sigma(w_{xo}x_t + w_{ho}h_{t-1} + b_o) \tag{5}$$

$$\tilde{c}_t = \tanh(w_{xc}x_t + W_{hc}h_{t-1} + b_c) \tag{6}$$

$$C_t = f_tC_{t-1} + i_t\tilde{c}_t \tag{7}$$

$$h_t = O_t\tanh(C_t) \tag{8}$$

其中，i_t、f_t、O_t分别是t时刻的输入门、遗忘门与输

出门；w与U是权重矩阵；b是偏置向量；σ是sigmoid激活函数；C是候选记忆单元；C_t是t时刻的记忆单元；h_t是输出向量。反向LSTM单元的计算方式与正向LSTM单元相同，但处理顺序相反，它是从序列的尾部向前进行处理的。

3.3 双向长短期记忆网络（BiLSTM）

双向长短期记忆网络（BiLSTM）在处理物联网时间序列流量等序列数据时性能卓越，它能够捕捉时间依赖关系与上下文信息，这对于精准入侵检测至关重要[11]。BiLSTM基于LSTM发展而来，LSTM是为了解决传统RNN的梯度消失问题而提出的，它在处理长序列时更加稳健，典型的BiLSTM单元架构如图3所示。

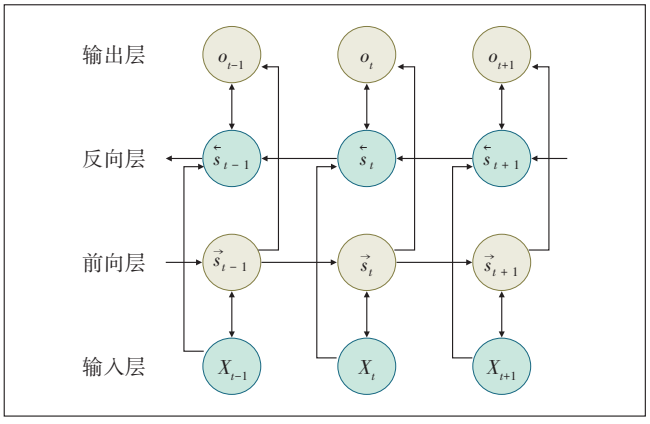

图3　BiLSTM单元架构

假设给定一个序列，正向LSTM单元按时间顺序依次计算各时刻的隐态；反向LSTM单元按相反时间顺序计算隐态。最终的输出是在每个时刻t，将正向与反向的隐态进行拼接，$h_t=[\vec{h}_t:\hat{h}_t]$，其中$[\cdots]$表示的是向量拼接操作，公式如下：

$$\vec{h}_t = \tanh(w_h x_t + w_h \vec{h} h_{t-1} + b_{\sqrt{h}}) \tag{9}$$

$$\hat{h}_t = \tanh(w_{n_t} x_t + w_h \overline{h}_{t-1}) + b_{\sqrt{h}} \tag{10}$$

$$h_t = \vec{h}_t + \hat{h}_t \tag{11}$$

BiLSTM能同时捕捉序列中某个时间点的前后信息，完整把握上下文关系。物联网入侵大多呈现连续异常模式，这一特质使BiLSTM在识别复杂入侵时表现出色、应用广泛[12]。BiLSTM层拼接正反向LSTM输出，以此作为特征表示，从而整合双向特征，全面捕获时间依赖关系与上下文信息，提升入侵检测能力。

3.4 深度神经网络（DNN）整合策略

在本研究中，深度神经网络（DNN）的有效整合是提升入侵检测能力的关键。为了在资源受限的物联网环境中实现高效准确的检测，本文采用了精细整合策略。DNN因具有强非线性特征提取能力，被用于前期特征提取。物联网原始流量包含连接与统计等特征，若直接使用，难发挥其能力，因此需融合物联网特定先验知识与预处理特征。通过分析MQTT、CoAP等协议，提取潜在的通信模式特征，将这些特征与原始流量特征共同作为DNN的初始输入，可助其更快、更准确地发现入侵模式，缩短训练时间。

图4所示的前期特征融合示意图表明，不同来源的特征在输入DNN之前进行了汇总整合。融入物联网专业知识的初始输入，增强了模型的针对性与泛化能力。DNN中间层需设计层间有效交互，以传递和强化入侵检测相关的特征。传统的依次传递模式需要平衡物联网场景下的资源限制与检测精准度。

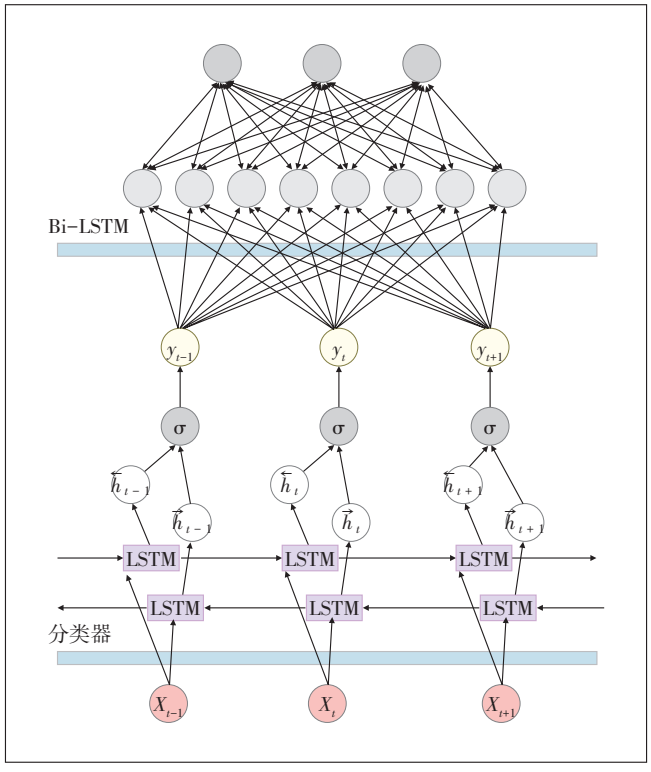

图4　DNN整合BiLSTM方式

如图5所示，DNN输出层结果需与动态量化模块及其他模块匹配，以实现轻量级且准确的入侵判定。其输出为高维特征向量，本研究通过特定的映像函数将其转换为兼容动态量化算法的格式，既能保留入侵相关的特征，又能满足降低储存与计算成本的需求，例如，如果动态量化算法要求输入为固定精度的特征

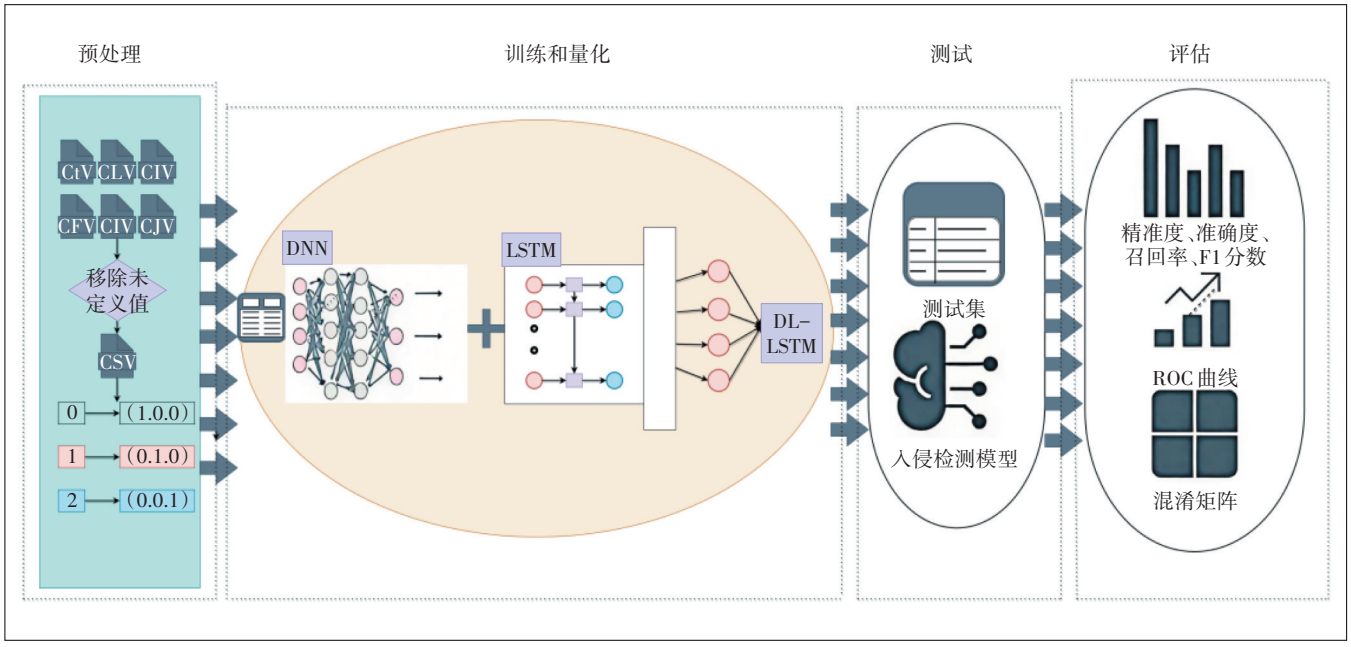

图5 混合深度学习流程

向量，映像函数会对DNN的浮点值输出进行量化与编码操作，将其转换为符合要求的格式。这样，整合后的结果可以直接输入到动态量化模块中，进一步优化模型的性能，以适配物联网轻量化的需求。

本研究的DNN-BiLSTM模型融合了DNN非线性特征提取和BiLSTM捕捉时间依赖的优势，以应对物联网入侵检测中复杂特征识别与时序分析的挑战。预处理是基础，DNN初步提取特征，BiLSTM双向处理时序数据，以捕捉入侵征兆，进而提升检查的准确性，输出层与训练策略则保障了结果的可解释性及模型的高效性。

3.5 轻量级物联网入侵检测方法

本研究探索了创新混合深度学习的轻量级物联网入侵检测方法，以提升系统安全性。研究采用的动态量化与融合的DNN搭配BiLSTM模型，通过特征降维预处理实现模型轻量化，从而减少设备资源消耗。动态量化机制能够使模型在变化的物联网环境中保持稳定性能，增强量化模型在轻量级入侵检测中的稳健性。量化后需校准以减少精度损失，具体方法是在大量校准数据集上运行模型，利用交叉熵等损失函数和反向传播微调参数与权重，在减少储存和计算量的同时，尽量维持原始检测性能，使准确率等指标接近未量化模型。

3.6 动态量化在模型中的应用

动态量化技术在模型构架的多个关键环节发挥核心作用，助力模型在资源受限的物联网环境下高效准确运行[13]。它采用跨层动态协同量化机制，某层参数调整信息会传递给相关层，使各层微调参数，避免信息流传输中量化过度或不足，进而整体优化性能。通过动态量化压缩融合的DNN-BiLSTM模型，在保证特征提取与检测性能的同时，降低模型大小和复杂度，便于物联网部署[14]。因Linear结构量化效果差且容易导致精度损失，主要对BiLSTM中的LSTM单元进行量化，测试前加载量化模型及参数用于评价。

本研究提出基于双隐层DNN与BiLSTM融合的轻量级系统。DNN能学习潜在信息且结构简洁，可优化BiLSTM的非线性特征提取能力，同时兼顾模型的规模与即时性。此外，使用Optuna超参数优化框架，优化学习率、隐藏层神经元数量、层数、批量大小等超参数，以平衡检测准确率、召回率及资源消耗。这些超参数分别影响权重更新步长、模型复杂度、训练稳定性与收敛速度。

3.7 Optuna模型超参数优化框架

在深度学习中，超参数调校可提升模型的分类性能[15]。本研究采用Optuna框架寻找最优超参数，平衡检测准确率、召回率及资源消耗。需优化的超参数包括学习率（影响权重更新步长与收敛）、隐藏层神经元数量与层数（影响模型复杂度及过拟合风险）、批量大

小（影响训练稳定性与速度）。Optuna超参数优化框架流程如图6所示。

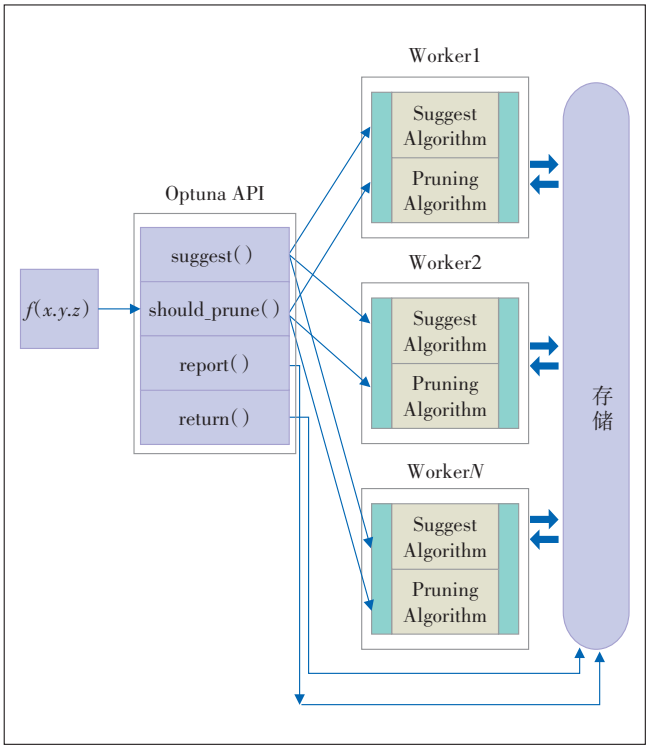

图6　Optuna超参数优化框架流程

通过超参数优化框架，能够在复杂空间中高效地找到最优超参数，进而提升物联网轻量级入侵侦测模型性能，使其更准确快速的检测入侵。

Optuna相较于传统调参技术有三大改进：动态构建超参数搜寻空间，依据历史结果确定下一组参数，提升调参效率与准确性；整合先进的采样与剪枝算法，快速确定最优空间并筛除无效路径；具有通用构架与简易设定，适用于多种目标，可扩展至大规模分布式环境[16-17]。

4 验证与总结

本研究模型建立后，在实际环境中对其进行了测试。对模型的几项主要指标进行了实际验证，包括准确率（Accuracy）、召回率（Recall）、F1值（F1-Score），以及模型的训练时间（Training Time）和模型大小（Model Size）。为全面评价所提模型，实验设计采用多元严谨的策略：按比例将数据集划分为训练集与测试集，检验模型的学习及泛化能力；采用交叉验证方法来提升结果的稳定性，避免偶然误差；将所提模型与多种方法进行对比，从多个指标进行评估，凸显本研究在准确性与效率上的优势，验证其实际可行性与优越性。将本研究效果与多种经典入侵侦测方法进行了对比实验，包括传统机器学习方法如DNN、BiLSTM，及基于深度学习的CNN、RNN等现有方法。在相同数据集上进行实验，比较各方法在检测指标上的表现，可直观评价所提方法的性能。通过上述检测指标与评价方法，能够全面客观评估该物联网轻量级入侵侦测方法的实际性能，为其改进优化提供依据。

实验选用当前主流的Bot-IoT和UNSW-NB15共2个数据集进行比对评价（见表1和表2）。Bot-Iot数据集在识别分布式阻断服务攻击（DDoS）与阻断服务（DoS）攻击方面展现出卓越性能。UNSW-NB15数据集基于正规化后数值，表示出基础的深度学习模型，在网络攻击分类任务中展现出卓越的性能，尤其是在多类别攻击辨识方面表现出色。

表1　Bot-IoT数据集评价

模型	参数	FLOPs/M	大小/KB	训练时间/s	推理时间/s
DNN	10692	4.354	45.7	529.0	6.3
BiLSTM	16132	7.143 9	68.8	673.4	7.1
RNN	16204	7.150 8	68.3	575.3	7.3
CNN	18372	9.319 9	83.5	1 189.6	7.5
DL-BiLSTM	1654	0.610 7	28.3	755.2	6.3

表2　UNSW-NB15数据集评价

模型	参数	FLOPs/M	大小/KB	训练时间/s	推理时间/s
DNN	42952	31.322 2	184.1	1 513.4	7.1
BiLSTM	15608	6.802 4	65.8	718.8	8.4
RNN	21128	9.202	88.4	765.8	6.5
CNN	13928	6.07	59.9	793.6	8.2
DL-BiLSTM	1988	0.627	36.5	709.4	6.5

实验结果显示，相较于传统深度学习模型，基于深度学习与动态量化的方法能显著减小模型大小。本研究所提的DL-BiLSTM模型与传统模型相比，压缩率可达66.1%，体积缩减80.2%。得益于动态量化技术，该模型通过降低参数精度，在几乎不损失性能的前提下大幅减少储存需求，适合部署于储存空间有限的物联网设备。在计算复杂度方面，传统CNN每次推论约需9.32 MFLOPs，DL-BiLSTM仅需0.61 MFLOPs，计算量下降93.5%。这源于动态量化后可在低位元整数运算单元执行推论，且精选特征维度避免了冗余计算，保证模型在资源受限的物联网终端快速完成检

测，满足即时性要求。随着输入数据规模的增大，传统模型计算复杂度增长远快于本方法。综上，该物联网轻量级入侵侦测方法轻量化能力优秀，在保证检测性能的同时有效降低资源需求，证明“深度学习+动态量化”可实现模型尺寸缩减66%~80%、FLOPs减少93%~98%，还能缩短训练与推论时间，为资源受限的物联网场景提供有力支持。

物联网设备日益普及，但因其资源有限和网络复杂，其安全性常常面临挑战，易遭网络攻击。本研究提出创新混合深度学习模型—DL-BiLSTM，该模型结合DNN与BiLSTM的优势，能够从复杂的网络数据中提取非线性特征和双向长距离依赖特征。其中，DNN擅长深层次层次表示，BiLSTM可捕捉数据前后向序列关系，全面分析网络行为上下文信息，提升入侵侦测的精准度，减少误报漏报情况的发生[18]。针对物联网设备的运算和内存限制，本研究引入IPCA算法进行降维。IPCA算法能增量更新主成分，适合处理流数据，在不损失重要信息的前提下降低运算需求。此外，本研究还采用动态量化技术优化模型结构，通过降低权重和激活值精度、修剪冗余连接等方式，减少内存使用并加速推理，使模型参数量大多处于0.2~0.6 M，对应32-bit浮点为0.8~2.4 MB，量化后可压缩至低于2 MB，在确保高效侦测的同时减轻设备的负担，实现了该模型在实际物联网设备上部署的可行性。本研究所提出的DL-BiLSTM模型实现了高效精准的入侵侦测，兼顾物联网设备实际限制，通过特征降维与模型优化提升实用性，为物联网安全提供了可行方案，也为后续研究打下了基础。

参考文献：

[1] SHIEH C S, LIN W W, NGUYEN T T, et al. Detection of Unknown DDoS Attacks with Deep Learning and Gaussian Mixture Model[J]. Applied Sciences, 2021, 11(11): 5213.

[2] CHEN J Y, YANG A. Intelligent Agriculture and Its Key Technologies Based on Internet of Things Architecture[J]. IEEE Access, 2019, 7: 77134-77141.

[3] KHAN M, SILVA N, HAN K. Internet of Things Based Energy Aware Smart Home Control System[J]. IEEE Access, 2016, 4(99): 7556-7566.

[4] GOPE P, SIKDAR B. Lightweight and Privacy-Preserving Two-Factor Authentication Scheme for IoT Devices[J]. IEEE Internet of Things Journal, 2019, 6(1): 580-589.

[5] CHRISTIN A, GISELLE C, ALMOBAIDEEN W, et al. A Comprehensive Survey for IoT Security Datasets Taxonomy, Classification and Machine Learning Mechanisms[J]. Computers & Security, 2023, 132(9): 103283.

[6] HOSSEININOORBIN S, LAYEGHY S, SARHAN M, et al. Exploring edge TPU for network intrusion detection in IoT[J]. Journal of Parallel and Distributed Computing, 2023, 179(9): 104712.

[7] HARBI Y, ALIOUAT Z, REFOUFI A, et al. Recent Security Trends in Internet of Things: A Comprehensive Survey[J]. IEEE Access, 2021, 9: 113292-113314.

[8] SHARMA S, VERMA V K. Security explorations for routing attacks in low power networks on Internet of things[J]. The Journal of Supercomputing, 2020, 77(5): 1-35.

[9] SARUMATHI M, JAMALIPOUR A. A Lightweight Intrusion Detection for Sybil Attack Under Mobile RPL in the Internet of Things[J]. IEEE Internet of Things Journal, 2020, 7(1): 379-388.

[10] LI K H, MA W G, DUAN H W, et al. Multi-source refined adversarial domain adaptation with transfer complementarity infusion for IoT intrusion detection under limited samples[J]. Expert Systems With Applications, 2024, 254: 32.

[11] ALBULAYHI K, SMADI A A, SHELDON F T, et al. IoT Intrusion Detection Taxonomy, Reference Architecture, and Analyses[J]. Sensors, 2021, 21(19): 6432-6432.

[12] QIAO T, LI J M, LIU H B. A Method for Guaranteeing Wireless Communication Based on a Combination of Deep and Shallow Learning.[J]. IEEE Access, 2019, 7: 38688-38695.

[13] MASDARI M, KHEZRI H. Towards fuzzy anomaly detection-based security: a comprehensive review[J]. Fuzzy Optimization and Decision Making, 2020, 20(1): 1-49.

[14] FU Y, DU Y, CAO Z, et al. A deep learning model for network intrusion detection with imbalanced data[J]. Electronics, 2022, 11(6): 898.

[15] BRIDGES R A, GLASS-VANDERLAN T R, IANNACONE M D, et al. A Survey of Intrusion Detection Systems Leveraging Host Data[J]. ACM Computing Surveys (CSUR), 2019, 52(6): 1-35.

[16] YU Z, LIU Y, LI R, et al. LIDS: A Lightweight Intrusion Detection System for Controller Area Network[J]. IEEE Transactions on Computer-Aided Design of Integrated Circuits and Systems, 2025: 1-1.

[17] RAZA S, WALLGREN L, VOIGT T. SVELTE: Real-time intrusion detection in the Internet of Things[J]. Ad Hoc Networks, 2013, 11(8): 2661-2674.

[18] AHMAD M S, SHAH S M. A lightweight mini-batch federated learning approach for attack detection in IoT[J]. Internet of Things, 2024, 25: 101088.

作者简介：

吴志祥，毕业于吉林大学，高级工程师，硕士，主要从事面向网络空间安全的人工智能融合应用及效能提升研究工作；陆文红，毕业于哈尔滨工业大学，高级工程师，硕士，主要从事信息安全管理和数据安全管理等工作；曲谱，毕业于哈尔滨工业大学，工程师，学士，主要从事网络安全防护、风险评估及安全事件分析等工作。