基于深度学习的物联网入侵检测系统综述*

周品希，沈　岳，李　伟
（湖南农业大学　信息与智能科学技术学院，湖南　长沙　410000）

摘　要：物联网中智能设备的互联互通在推动社会进步的同时，也因设备异构性、协议多样性和资源受限性导致安全威胁日益复杂化。传统入侵检测系统依赖特征匹配和规则定义，在面对新型攻击和动态攻击模式时表现出局限性。系统梳理了深度学习技术在物联网入侵检测系统中的应用进展，通过对比分析发现：基于深度学习的模型在检测精度和实时性上优于传统方法，在处理空间特征、捕捉时序依赖等方面表现突出；无监督学习和集成方法通过生成对抗样本、融合多模型优势，有效提升了小样本场景下的检测鲁棒性；当前研究仍面临数据标注成本高、边缘计算资源受限、动态攻击适应性不足等挑战。总结探讨了未来研究应聚焦轻量化、跨模态数据融合等方向，为构建高效、自适应的物联网安全防护体系提供理论支撑。

关键词：网络安全；物联网；入侵检测；深度学习
中图分类号：TP393.08　　**文献标识码：**A　　**DOI：**10.19358/j.issn.2097-1788.2025.06.001
引用格式：周品希，沈岳，李伟. 基于深度学习的物联网入侵检测系统综述［J］. 网络安全与数据治理，2025，44(6)：1-10.

A review of IoT intrusion detection systems based on deep learning

Zhou Pinxi，Shen Yue，Li Wei
（College of Information and Intelligence，Hunan Agricultural University，Changsha 410000，China）

Abstract：While the interconnection of smart devices in the Internet of Things promotes social progress，it also leads to increasingly complex security threats due to device heterogeneity，protocol diversity and resource constraints. Traditional intrusion detection systems rely on feature matching and rule definition，and show limitations when facing new attacks and dynamic attack patterns. This paper systematically sorts out the application progress of deep learning technology in the intrusion detection system of the Internet of Things. Through comparative analysis，it is found that the model based on deep learning is superior to traditional methods in detection accuracy and real-time performance，and has outstanding performance in processing spatial features and capturing temporal dependencies. Unsupervised learning and integration methods effectively improve the detection robustness in small sample scenarios by generating adversarial samples and integrating the advantages of multiple models. Current research still faces challenges such as high data annotation costs，limited edge computing resources，and insufficient adaptability to dynamic attacks. This paper summarizes and discusses the directions that future research should focus on，such as lightweight and cross-modal data fusion，to provide theoretical support for building an efficient and adaptive Internet of Things security protection system.

Key words：network security；Internet of Things；intrusion detection；deep learning

0　引言

物联网（Internet of Things，IoT）的快速发展正深刻地改变着人们的生活方式和社会的运行模式。目前，物联网应用已经覆盖了智能家居、医疗健康、工业控制、智慧农业等各个领域。然而，物联网设备的广泛部署和互联互通也带来了严重的安全隐患。由于物联网设备资源受限、异构性强、通信协议多样等原因，以往的网络安全防护手段难以适应这一复杂的环境，导致物联网系统频繁成为网络攻击的目标，严重威胁着个人隐私、企业利益及国家安全[1-2]。

入侵检测系统（Intrusion Detection System，IDS）凭借其能够实时监控网络流量，检测并响应异常行为，被广

*基金项目：湖南省教育厅基金项目（22B0204）

泛应用于物联网安全领域中。早期的 IDS 主要依赖于特征匹配[3]和规则定义[4]，然而随着网络规模的大幅扩张以及网络处理节点数量的激增，重要数据在不同的网络节点之间生成和共享，同时旧攻击发生突变或产生大量新型攻击，数据传输量的剧增和攻击方式的多变使其检测效果满足不了当前需求。

近年来，随着深度学习在众多领域的广泛应用，研究人员探索了多种深度学习模型，以应对物联网环境中复杂多变的安全威胁。在物联网入侵检测中，深度学习可以从大量的网络流量和设备行为中挖掘隐蔽的模式，自动学习攻击特征，减少对人工规则的依赖。

1　物联网概述

物联网是由通过互联网相互通信的互联设备组成的庞大生态系统。这些设备的范围从简单的传感器和执行器到复杂的系统，如智能家居设备、工业机械，甚至可穿戴设备。物联网的主要特征之一是其能够自主地从环境中收集数据，并提供实时反馈。例如，安装在农田中的物联网传感器可以监测土壤湿度、温度和作物健康状况，帮助农民做出有关灌溉和作物管理的决策[5]。同样，家庭中的智能电表通过物联网技术跟踪能源消耗情况，优化能源使用并降低成本[6]。

物联网架构通常包括三个关键阶段：采集阶段、传输阶段和处理阶段[7]。在采集阶段，物联网系统通过传感器节点从物理环境中感知并收集数据，同时捕获和监控设备间的通信信息。在传输阶段，采集到的数据通过各种通信技术，如以太网、蓝牙、Wi-Fi、混合光纤同轴或数字用户线等传输至指定的应用程序或用户[8]。最后，在处理阶段，提取出与物理网络相关联的关键信息，并基于这些信息采取必要的控制和管理措施。物联网基本架构如图 1 所示。

然而，随着物联网设备和应用场景的不断增加，物联网环境的安全性问题日益严峻。物联网设备通常部署在开放的环境中，容易受到物理攻击、网络攻击、设备劫持等多方面威胁。由于物联网设备种类繁多、功能复杂、处理能力和安全防护能力有限，确保数据安全、隐私保护及实时监控成为亟待解决的挑战。

在此背景下，基于深度学习的入侵检测方法因其强大的数据处理和模式识别能力，逐渐成为物联网安全研究的热点。深度学习能够在海量数据中自动提取特征，并有效识别复杂的攻击模式。特别是在物联网环境下，深度学习方法能够应对大规模、异构、动态的数据流，识别不同类型的攻击行为，从而为物联网提供更为精确、智能的安全防护。

2　物联网 IDS 分类

深度学习通过构建多层神经网络，自动提取高维数据中的潜在特征，实现从原始数据到高层语义信息的映射[9]。多种深度学习网络，如卷积神经网络（Convolutional Neural Network，CNN）、生成对抗网络（Generative Adversarial Network，GAN）、循环神经网络（Recurrent Neural Network，RNN）、图神经网络（Graph Neural Network，GNN）和长短期记忆网络（Long Short－Term Memory Network，LSTM）等被广泛应用于不同领域与环境的物联网入侵检测中。

根据学习方式和策略的不同，基于深度学习的物联网 IDS 分类如图 2 所示。

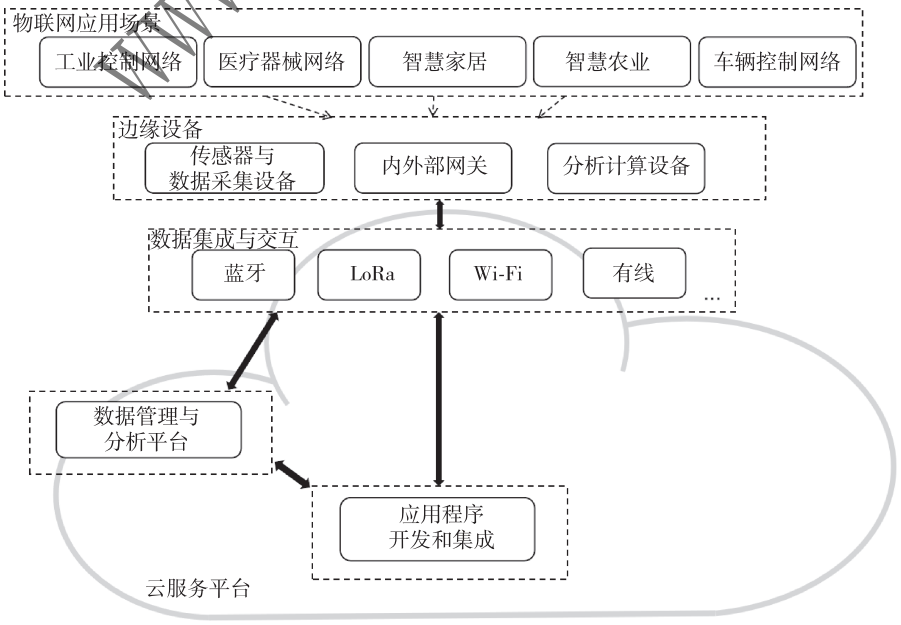

图 1　物联网基本架构图

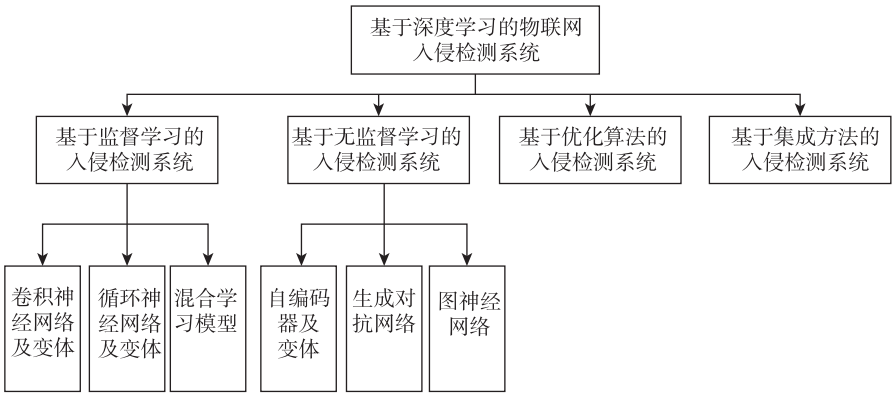

图 2　基于深度学习的物联网 IDS 分类图

监督学习依赖已标注的训练数据集来训练模型，模型通过学习输入特征与已知标签之间的映射关系，从而实现对未知数据的预测和分类。CNN 通过稀疏连接、参数共享以及方差表示等，减少网络中的数据参数和层间连接，提高模型的扩展性和计算效率。由于物联网设备产生的大量网络流量数据具有复杂的空间特征，CNN 处理这些结构化数据时表现出色。RNN 及其变体 LSTM、门控循环单元（Gated Recurrent Unit，GRU）等在捕捉网络流量中的时间依赖关系方面具有优势，能够有效地处理物联网设备生成的时序数据。混合学习模型将不同的神经网络结构结合，利用各自的优势进行联合学习，以提升物联网入侵检测的整体性能。

无监督学习无需标签数据，能够在物联网环境中自动识别潜在的攻击行为。无监督深度学习方法利用物联网生成的海量数据，分析数据中的隐藏模式和异常行为，具有良好的泛化能力和适应性。自编码器通过将输入压缩为低维表示，然后重建原始输入，从而学习数据的内在结构，在处理高维网络流量数据、检测异常行为方面效果较好。GAN 通过生成器和判别器之间的对抗过程，学习数据的真实分布，进而生成高质量的网络流量样本检测异常。GNN 近年来在复杂网络分析中广泛应用，能够高效处理具有图结构的数据，在通用网络和物联网环境下，GNN 擅长捕捉节点间的关系，用于识别异常流量。

优化算法应用于参数调优、特征选择、模型架构优化等不同层次，实现模型性能的增强。近年来大量的研究将优化算法引入到深度学习的物联网 IDS 中，利用启发式和智能搜索算法自动优化攻击数据维度以及检测模型的各类参数和结构。

集成方法通过多个弱分类器或不同类型的模型进行组合，克服单一模型局限，利用多深度学习模型的优势结合与互补，优化决策过程并降低误报率和漏报率。

物联网 IDS 通过分析设备行为、网络流量和系统活动，检测和识别潜在的入侵行为，防止恶意攻击者利用物联网设备进行数据窃取、网络瘫痪或其他破坏性活动[10]。物联网 IDS 采用多种检测方法和部署策略，确保在广泛多样的设备环境中提供有效的安全防护。应用于物联网的 IDS 的分类如图 3 所示。

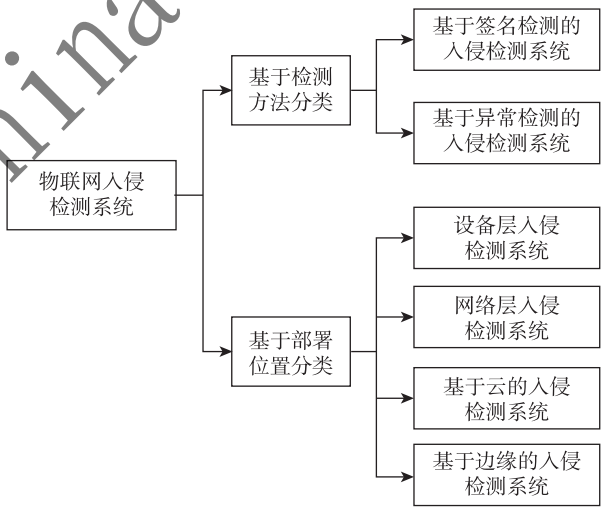

图 3　物联网 IDS 分类图

3　基于检测方法的物联网 IDS 分类

3.1　基于签名检测的 IDS

基于签名检测的 IDS（Name-based IDS，NIDS）通过对网络流量与已知的攻击模式或签名进行比对，当检测到匹配的模式时，系统触发警报。这种方法依赖于维护一个不断更新的签名数据库，其中包含了已知的攻击特征，如特定的攻击包结构、异常的协议使用等。文献［11］提出了一种基于签名的物联网 IDS，该系统混合使用集中式和分布式的放置策略，用于检测来自外部网络以及内部受感染节点的入侵，将入侵模型部署在边界路由器进行恶意节点的判断。文献［12］提出了一个过滤模型用于自动检测新的攻击签名并更新攻击数据库，该

模型将大型签名库分为最频繁签名库和互补签名库，通过相似性因子和 IP 黑名单来检测新攻击并更新签名库。文献［13］提出一个基于签名的 NIDS 性能自适应框架，框架使用基于信任的黑名单数据包过滤器减少数据包匹配阶段的工作负载，并结合独占签名匹配方案，构建误报过滤器提取数据包特征以降低误报率。

NIDS 在检测已知威胁方面非常有效。然而由于物联网设备的多样性，攻击模式可能随着新设备和新应用的出现而变化，针对未出现过的新型攻击和已知攻击的变体形式，该方法检测效果表现不佳，因此需要频繁更新攻击签名数据库，致使其维护和更新成本较高。

3.2 基于异常检测的 IDS

基于异常检测的 IDS（Anomaly-based IDS，AIDS）通过使用标记为正常或假设大部分数据代表正常行为的数据来训练网络正常行为模型，并将网络数据与基准模型进行比较，当检测网络数据中存在不符合预期行为的模式时，系统则将其标记为潜在的入侵攻击。与 NIDS 相比，AIDS 的主要优势在于，通过基于正常行为模式对未知攻击进行学习，超出正常行为阈值则识别为异常流量[14]。文献［15］提出了一种改进的 AIDS，系统使用递归特征消除技术为特征分配权重，根据特征重要性排序后选择最优特征子集，在 NSL-KDD 数据集上取得了较高的二元分类和多分类准确率。文献［16］提出了一种基于成本敏感深度学习和集成算法的多层检测系统，第一层采用成本敏感网络分离正常和可疑流量，第二层采用极端梯度增强算法针对可疑样本进行攻击流量数的进一步分类。

在物联网环境中，AIDS 不仅关注外部攻击，还能识别来自内部的异常威胁。但缺点是物联网中网络数据的高数目以及高维度导致该方法面临误报率高、计算资源需求高、实时性挑战等问题[17]。

4 基于部署位置的物联网 IDS 分类

在多层次的物联网架构中，有效精准的安全防护是至关重要的。根据检测范围、性能要求以及适用场景的不同，物联网 IDS 可以分为设备层 IDS、网络层 IDS、云层 IDS 以及基于边缘计算的 IDS，具体部署架构如图 4 所示。

4.1 设备层 IDS

设备层 IDS 部署在物联网设备或传感器节点上，持续监测设备的运行状态和数据流量活动。此类 IDS 主要针对单个设备或传感器的攻击，如恶意软件植入、设备劫持、未经授权的访问等，通过本地监控及时检测和响应入侵行为，其主要特点包括：

（1）设备层安全防护体系通过轻量化模型部署实现

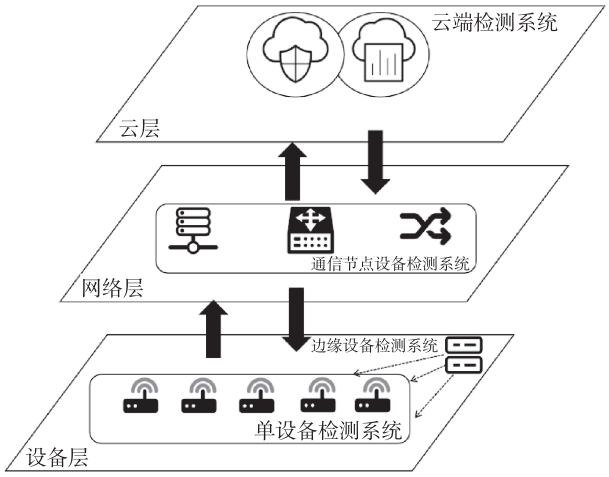

图 4 物联网 IDS 部署架构图

终端设备自主防御能力。文献[18]通过主机 - 网络分布式代理架构，基于预定义签名库进行流量初筛，并利用协议预解析技术将原始流量压缩实现性能提升。嵌入式模型优化聚焦于神经网络轻量化改造，文献[19]在 Arduino Uno 部署多层感知器（MLP），为低功耗设备提供能耗 - 精度平衡的检测方案。

（2）基于无监督学习框架利用无标签数据构建异常检测基线。文献［20］基于 Raspberry Pi 4 构建轻量监控设备，通过核函数映射构建正常流量超平面边界，实现无标签依赖的异常检测。文献［21］通过 HWT（Haar Wavelet Transform）增强时频特征表达、动态硬阈值记忆机制和时空建模，解决了物联网流量异常检测中特征表达不足和模型泛化能力差的问题。

（3）在受限设备条件下，通过优化算法提升资源利用效率。混合优化算法方面，文献［22］通过改进传统布谷鸟搜索算法和通过分层的神经元网络结构，处理不同抽象级别的特征，提升对隐蔽攻击的识别能力。文献［23］融合混合 shuffled shepherd 优化算法与模拟退火的局部优化，通过全局 - 局部双阶段优化增强模型对异构攻击的鲁棒性。

（4）设备层 IDS 集成策略兼顾资源限制与复杂攻击检测需求。文献［24］中 Lambda 架构的引入实现了历史批处理与实时流处理的统一，通过滑动窗口机制平衡检测精度与响应速度，结合多数投票和加权集成优化，为物联网安全提供了兼顾高精度与实时性的解决方案。针对数据不均衡难题，文献［25］采用 Bagging 集成方法自举采样生成多个子数据集，训练带有类权重的 DNN 基估计器模型，平滑掉个别基学习器对多数类的过度偏向。

表 1 展示了例举设备层 IDS 所用模型和数据集及评价指标。

表 1　设备层 IDS 比较

文献	模型及算法	数据集及指标
[18]	COLIDE	Cooja Simulated TrafficDataset MemoryOverhead(RAM overhead) = 368; MemoryOverhead(ROM overhead) = 274
[19]	MLP	NSL-KDD: Acc = 97.5%, Pre = 97.3%, Cov = 97.2%, *F*1 = 97.2%
[20]	OC-SVM	Raspberry Pi 4 DoS AttackTrafficDataset Acc = 96.9%, Pre = 85.0%, Rec = 99.3%, *F*1 = 91.6%
[21]	HaarAE	KDDCUP99: Rec = 99.7%, Pre = 97.5%, *F*1 = 98.6%; Comprehensive Data: Rec = 94.4%, Pre = 95.9%, *F*1 = 95.2%
[22]	HNA-NN; IWP-CSO	SIRD: Acc = 95%, Pre = 96%; SORD: Acc = 94%, Pre = 95%; MIRD: Acc = 93%, Pre = 94%; MORD: Acc = 92%, Pre = 93%
[23]	TCNN; SSO-SA	Security camera XC1003: Pre = 99.4%, Rec = 99.4%, *F*1 = 99.4%
[24]	LSTM + CNN + ANN	IOT-23: Acc = 99.6%
[25]	Multi-DNN	NSL-KDD: Acc = 98.90%, Pre = 99.90%, Rec = 98.71%, *F*1 = 99.31%; UNSW_NB15: Acc = 96.70%, Pre = 98.90%, Rec = 98.67%, *F*1 = 98.78%; CICIDS2017: Acc = 98.74%, Pre = 99.77%, Rec = 99.96%, *F*1 = 99.86%; BoT-IoT: Acc = 98.99%, Pre = 98.90%, Rec = 91.30%, *F*1 = 94.95%

4.2　网络层 IDS

网络层 IDS 部署在物联网网络的通信节点或路由器上，负责监控和分析网络流量，检测拒绝服务攻击、零日攻击、暴力破解等网络层面的攻击活动以及异常通信行为，当前网络层 IDS 围绕检测架构、算法效能和实时性三个方向进行优化，应对物联网场景下的动态攻击防护需求。

在检测架构方面，网络层 IDS 突破传统单点检测模式，实现多阶段过滤与强化学习。文献［26］采用三级检测引擎：首层部署轻量级 Z-score 滤波器实现流量初筛；中间层通过改进 Hessian 矩阵解析协议字段突变特征；顶层构建 Deep Q-Learning 决策模型实现攻击类型细粒度分类。

算法效能优化呈现多模态技术融合的趋势。针对监督学习场景，文献［27］的双通道 CNN 架构通过分离式卷积核提升特征提取效率，在 IoT-Botnet2020 数据集达到 99.85% 召回率。文献［28］基于组合卷积网络的方法，同时使用 CNN 从输出层平均激活率中自动学习高信息量特征以及实现攻击检测。在无监督检测领域，文献［29］通过多个损失函数的对抗性训练学习网络流量底层分布，加权判别器输出与重构距离生成异常分数，结合核密度估计动态调整攻击阈值。文献［30］通过 TCN（Temporal Convolutional Network）结合通道注意力机制，使用注意力机制赋予权重来提升网络对重要特征的关注。

实时性提升通过优化算法与部署协同得以实现。文献［31］在蜂群算法中引入雇佣蜂 - 旁观蜂协同搜索机制，优化 DCNN（Deep Convolutional Neural Network）参数更新路径，避免局部最优。文献［32］使用鲸鱼优化算法（WOA）优化 LSTM 的时间步长和隐藏层结构，从而增强了模型的时序建模效率。在集成部署方面，文献［33］中三组异构 CNN 集成架构组合 SHAP 和 LIME 模型解释工具揭示了特征对模型决策的影响，在 ToN-IoT 数据集实现高分类性能与可解释性平衡。

表 2 展示了例举网络层 IDS 所用模型和数据集及评价指标。

表 2　网络层 IDS 比较

文献	模型及算法	数据集及指标
[26]	LightNetHMS	NSL-KDD: Rec = 96.9%, Pre = 96.6%, Spe = 96.8%
[27]	TCNN	Bot-IoT: Acc = 99.89%, Pre = 99.26%, Rec = 96.21%, *F*1 = 98.65%
[28]	CNN	IoT-Botnet2020: Acc = 98.04%, Pre = 98.09%, Rec = 99.85%, *F*1 = 98.96%, FPR = 1.92%
[29]	FlowGAN	UNSW-NB15: *F*1 = 83.8%, AUC = 85.3%
[30]	IResTAE2A	NSL-KDD: Acc = 92.3%, Pre = 94.0%, Rec = 88.7%, *F*1 = 91.3%; CICIDS2017: Acc = 99.7%, Pre = 99.3%, Rec = 99.7%, *F*1 = 99.5%; CICIDS2018: Acc = 99.6%, Pre = 99.7%, Rec = 99.7%, *F*1 = 99.7%
[31]	DCNN; NSBPSO	UNSW-NB15: Rec = 99.03%, Spe = 95.32%, Acc = 98.86%
[32]	LSTM; WOA	CIDDS-001: Acc = 99.3%, Sen = 98.3%, Spe = 99%; UNSW-NB15: Acc = 99.1%, Sen = 98%, Spe = 98.89%; NSL-KDD: Acc = 99.5%, Sen = 98.7%, Spe = 98.45%
[33]	Multi-CNN	ToN-IoT (Binary) Acc = 99.69%, Pre = 100.0%, Rec = 100.0%, *F*1 = 100.0%; (Multi) Acc = 99.63%, Pre = 99.8%, Rec = 99.2%, *F*1 = 99.5%

4.3 基于云的 IDS

云层 IDS 部署在云平台上，利用云计算处理能力，对大量数据进行集中分析，适合广域物联网环境中的大规模、多点攻击入侵检测。因此，云端安全防护体系依托云计算资源实现大规模威胁智能分析。

云层监督方法中，侧重于对序列数据的全局建模。文献［34］在传统自动编码器中添加 LSTM 层对序列数据进行编码，提取时间依赖特征，随后在解码过程中，重构出低维表示以降低数据维度，实现训练时间的减少与检测性能的提高。

面向未知攻击检测需求，依赖云端资源，无监督方法在云端流量数据处理中呈现出高效性。文献［35］通过 GRU 捕获时序依赖，通过贝叶斯推理优化高斯分量选择，实现潜在空间多模态分布的高效学习。文献［36］构建多阶段 GAN-AE 框架，首阶段 AE 最小化正常流量重构误差，次阶段将 AE 作为生成器进行对抗训练，提升 MQTT 协议下未知入侵的判别能力。

智能优化算法为云端高维数据处理和模型架构搭建提出了新的解决思路。文献［37］和［38］的特征选择机制，通过自然优化算法的位置更新机制优化特征选择以符合目标函数的条件，从高维特征向量中选择具有代表性的特征子集。混合优化框架方面，文献［39］通过使用改进的帝王蝶优化算法对 RK-CNN（Recurrent Kernel Convolutional Neural Network）进行参数配置优化，结合卷积和循环核层的优势，实现深度提取数据时空特征。

针对云端多源异构数据难题，云层集成模型优化突破了传统堆叠模型限制。文献［40］利用残差注意力增强局部特征交互，Transformer 捕捉全局上下文关联，BiLSTM 建模长期流量依赖，在 NSL-KDD 等数据集实现高精度检测。文献［41］使用深度自编码器（DAE）将输入特征进行高维特征映射，再结合多独立概率神经网络 EPNN 形成深度堆叠集成结构，模型的泛化能力与鲁棒性得到提升。

表 3 展示了例举云层 IDS 所用模型和数据集及评价指标。

4.4 基于边缘的 IDS

边缘计算是一种将数据计算和存储资源部署在靠近数据源或用户的网络边缘的分布式计算架构[42]。基于边缘计算的 IDS 专注于在网络边缘处理和分析数据，从而在 IoT 环境中提供实时和低延迟的安全防护。基于此特性，边缘 IDS 研究主要围绕特定场景下有、无监督检测，轻量化模型和协同检测框架四个方向展开。

面向工业控制、智慧农业等场景的传感器与网络流量协同分析需求，研究者提出多种混合模型。针对序列特征优化问题，文献［43］提出了一种混合工业物联网入侵检测方法，通过 Inception-CNN 优化注意力机制提取

表 3 云层 IDS 比较

文献	模型及算法	数据集及指标
［34］	LAE-BLSTM	Bot-IoT：MCC（Binary）=93.17%，MCC（Multi）=97.29%
［35］	GGU-VAE	IntelDataset：Acc=97.9%，Pre=99.2%，Rec=92.3%，*F*1=95.6%，AUC=95.9%； YahooDataset：Acc=96.1%，Pre=92.3%，Rec=92.3%，*F*1=92.3%，AUC=94.8%； ProcessMinerDataset：Acc=84.3%，Pre=81.2%，Rec=68.7%，*F*1=68.7%，AUC=79.1%
［36］	GAN-AE	MQTT-IOT-IDS2020：Acc=96.9%，Pre=97.7%，Rec=97.6%，*F*1=97.6%
［37］	MDBN；ISSA	UNSW-NB15： ACC（Binary）=99.79%，FAR（Binary）=0.204%； ACC（Multi）=99.84%，FAR（Multi）=0.158%
［38］	CNN；RSA	NSL-KDD：Acc=76.107%，Pre=82.171%，Rec=76.107%，*F*1=71.731%； Bot-IoT：Acc=99.020%，Pre=99.098%，Rec=99.038%，*F*1=99.070%； CICIDS2017：Acc=99.911%，Pre=99.907%，Rec=99.911%，*F*1=99.888%
［39］	RKCNN；MMBO	N-BaIoT：Acc=99.96%，Pre=99.85%，Rec=99.91%，*F*1=99.88%，Spe=99.95%； CICIDS2017：Acc=99.95%，Pre=99.35%，Rec=99.35%，*F*1=99.35%，Spe=99.93%
［40］	Res-TranBiLSTM	NSL-KDD：Acc=90.99%，Pre=91.39%，Rec=90.94%，*F*1=90.89%； CICIDS2017：Acc=99.15%，Pre=99.15%，Rec=99.14%，*F*1=99.14%
［41］	DAE-EPNN	N-BaIoT：Acc=99.696%

的序列特征，综合改进 BiGRU 模型提升检测精度。文献［44］提出一种针对智慧农业领域的边缘－雾协同框架，框架中传感器层的硬件设备采集农业环境数据后传输至雾计算层进行数据处理与分析，雾计算层部署融合 CNN 与注意力 BiGRU 的入侵检测系统，并根据识别特征重要性引入权重系数查找关键特征。

边缘层无监督 IDS 关注轻量化生成模型以降低计算开销以及局部图结构的分析。文献［45］提出基于 TCN 和自关注机制的 GAN 架构，利用 TCN 块捕获长短期依赖，自注意力块增强全局建模能力，从多维度提升对抗生成质量。文献［46］通过多头注意力机制构建物联网网络图，利用图同构网络进行边分类与特征泛化，目的是提升物联网网络中边缘表示能力。

边缘层 IDS 主要通过优化算法进行参数微调，实现资源受限环境下的模型轻量化及增效。文献［47］开发协同混合框架，通过改进遗传算法动态调整神经网络参数，优化特征选择以最大化边缘节点资源利用率。文献［48］结合灰狼优化算法（GWO）与迁移学习，对 CNN 模型的学习率、权重等超参数进行微调，在 ToN-IoT 等数据集上实现检测性能与泛化能力的双重提升。

边缘层 IDS 资源分散且相互关联的特点，推动了基于时空特征融合与异构多模型联合的集成模型的构建。文献［49］利用多边缘节点联合训练本地模型，通过联邦参数聚合更新中央服务器模型，在降低数据泄露风险的同时提升资源利用率。文献［50］利用 SAE（Stacked Autoencoder）的无监督、非线性特征缩减优势与 CarBoost 的重要性排序方法，实现集成特征选择，Transformer-CNN-LSTM 集成模型实现全局、局部和时序依赖的综合信息考量。

表 4 展示了例举边缘层 IDS 所用模型和数据集及评价指标。

表 4　边缘层 IDS 比较

文献	模型及算法	数据集及指标
［43］	Attention-BiGRU	Edge-IIoTset：Acc＝94.7%，Rec＝94.7%，Pre＝94.8%，*F*1＝94.6%； CICIDS2017：Acc＝99.3%，Rec＝99.3%，Pre＝99.3%，*F*1＝99.3%； CICIoT2023：Acc＝99.5%，Rec＝99.5%，Pre＝99.5%，*F*1＝99.5%
［44］	CNN-BiGRU-Attention	APA-DDoS：Acc＝99.35%，Pre＝99.90%，*F*1＝99.08%，Rec＝98.99%； ToN-IoT：Acc＝99.71%，Pre＝99.89%，*F*1＝99.85%，Rec＝99.05%
［45］	DGAN	CICDDoS2019： （TCN Block）Acc＝97.07%，Pre＝97.05%，Rec＝97.10%，*F*1＝97.07%； （Self-Attention Block）Acc＝96.82%，Pre＝96.82%，Rec＝96.82%，*F*1＝96.82%
［46］	GINE	AWID：Acc＝97.28%，Pre＝95.08%，Rec＝97.29%，*F*1＝96.20%； 5G-NIDD：Acc＝99.00%，Pre＝97.11%，Rec＝99.16%，*F*1＝98.12%； Bot-IoT：Acc＝97.11%，Pre＝94.50%，Rec＝97.74%，*F*1＝96.10%
［47］	LSTM；GA	BoT-IoT：Acc＝99.41%，Pre＝98.50%，Rec＝99.78%，FAR（Multi）＝2.56%
［48］	OCNN-LSTM；GWO	ToN-IoT：Acc＝94.4%，Pre＝92.7%，Rec＝55.0%，*F*1＝45.1%； UNW-NB15：Acc＝92.7%，Pre＝94.2%，Rec＝92.3%，*F*1＝92.3%
［49］	DNN；CNN；LSTM	IoTID20，IoT23，N-BaIoT： Acc＝99%，Rec＝98.8%，*F*1＝98.9%
［50］	Transformer-CNN-LSTM	NSL-KDD：Acc（Binary）＝99.5%，Acc（Multi）＝99.7%，*F*1（Binary）＝99.4%，*F*1（Multi）＝99.6%； UNSW-NB15：Acc（Binary）＝99.6%，Acc（Multi）＝99.1%，*F*1（Binary）＝99.6%，*F*1（Multi）＝99.1%； AWID：Acc（Binary）＝99.9%，Acc（Multi）＝99.8%，*F*1（Binary）＝99.9%，*F*1（Multi）＝99.8%

5 挑战与展望

5.1 数据标注困难及不平衡问题

物联网网络中的数据呈现多样化，不同设备、协议和应用产生的流量特征存在较大差异[51]。由于数据的标记和分类成本高昂，许多深度学习模型依赖的大量高质量标注数据在实际应用中难以获得。此外，攻击流量在整体数据流中占比往往较小，攻击模式和正常行为之间界限模糊，导致难以有效区分。

因此针对流量数据的泛化与少数类样本生成是值得投入研究的方向。一个主要的思路是迁移学习，模型在跨域数据中进行知识转移，减少对大规模标注数据的依赖。此外，传统采样技术通过线性插值生成少数类样本，容易导致生成样本呈现单一性，造成类别边界上产生混淆样本。GAN 技术可以动态生成符合原始分布的样本数据，从而在提高模型对少见攻击类型的检测能力的同时，减少对少数类的过拟合风险。

5.2 计算资源与能耗限制问题

在物联网环境中，深度学习模型的复杂性和对计算资源的高需求使得其在边缘设备上运行时面临困难，在资源受限的环境中，传统深度学习模型可能导致延迟过高，影响实时检测的性能[52]。

未来可以考虑采用轻量化模型设计，如移动端优化的卷积神经网络（如 MobileNet 等）或剪枝与量化技术，以降低模型的计算负担。同时，边缘计算与云计算的混合架构可以在边缘设备上进行简单的特征提取和初步分析，将复杂计算任务转移到云端处理[53]，从而提升整体系统的实时性和效率。

5.3 动态攻击威胁

物联网环境中的设备和流量具有高度的动态性[54]，使得攻击模式和流量行为不断演变，传统模型在面对新的攻击时可能出现显著的性能下降。此外，部署环境中的设备变化和网络条件也会影响数据分布，导致模型在实际应用中无法保持稳定的检测效果。

当前针对动态环境适应性的研究仍然较为薄弱，未来可探索在线学习和自适应深度学习技术，通过实时监控和快速学习新的攻击模式，自动调整深度学习架构以增强模型检测能力。同时，结合多模态数据源而不仅限于数据流，通过多层信息融合，实现检测流量异常的同时，及时发现网络架构异常。

6 结论

本文从检测方法与部署位置两个维度对基于深度学习的物联网 IDS 进行了系统性分类评述。研究发现：（1）监督学习模型（如 TCNN、Res-TranBiLSTM）虽在标注充分的数据集上表现优异，但面临物联网数据标注成本高昂的瓶颈；（2）无监督方法（如 GAN-AE、ARGA）通过生成对抗训练和自编码器重构，在零日攻击检测中展现出潜力，但需解决生成样本多样性不足的问题；（3）边缘计算场景下，轻量化模型与联邦学习结合可兼顾实时性与隐私保护，但跨设备模型一致性仍需优化；（4）动态攻击应对方面，基于注意力机制的 LSTM 模型能够捕捉协议层异常，但对物理层攻击特征提取能力有限。

本文总结提出三点改进方向：首先，构建物联网攻击图谱数据库，通过主动学习减少标注需求；其次，设计异构边缘计算框架，利用边缘节点分布式训练提升响应速度；最后，开发多模态融合检测算法，综合流量特征、设备日志和物理环境数据提升检测覆盖率。研究结果表明，深度学习为物联网安全提供了新的技术路径，但需在模型轻量化、数据高效利用和适应性方面持续突破。

参考文献

[1] MARSHALL C, PRIOR M. Cyber security: global food supply chain at risk from malicious hackers [EB/OL]. (2022 - 05 - 20). https://www.bbc.com/news/science-environment - 61336659.

[2] ARGHIRE I. Telegram zero-day enabled malware delivery [EB/OL]. [2024 - 07 - 23]. https://www.securityweek.com/telegram-zero-day-enabled-malware-delivery.

[3] LUNTEREN J V. High-performance pattern-matching for intrusion detection [C]//Proceedings IEEE INFOCOM 2006, 25th IEEE International Conference on Computer Communications. IEEE, 2006: 1 - 13.

[4] TAJBAKHSH A, RAHMATI M, MIRZAEI A. Intrusion detection using fuzzy association rules [J]. Applied Soft Computing, 2009, 9 (2): 462 - 469.

[5] ALI A, ALSHMRANY S. Internet of Things (IoT) embedded smart sensors system for agriculture and farm management [J]. International Journal of Advanced and Applied Sciences, 2020, 7 (10): 38 - 45.

[6] HAFEEZ G, WADUD Z, KHAN I U, et al. Efficient energy management of IoT-enabled smart homes under price-based demand response program in smart grid [J]. Sensors, 2020, 20 (11): 3155.

[7] KHRAISAT A, GONDAL I, VAMPLEW P, et al. Survey of intrusion detection systems: techniques, datasets and challenges [J]. Cybersecurity, 2019, 2 (1): 1 - 22.

[8] MAIER M. Fiber-wireless (FiWi) broadband access networks in an age of convergence: past, present, and future [J]. Advances in Optics, 2014, 2014 (1): 945364.

[9] BELLO M, NÁPOLES G, SÁNCHEZ R, et al. Deep neural net-

work to extract high-level features and labels in multi-label classification problems [J]. Neurocomputing, 2020, 413: 259 – 270.

[10] HEIDARI A, JABRAEIL JAMALI M A. Internet of Things intrusion detection systems: a comprehensive review and future directions [J]. Cluster Computing, 2023, 26 (6): 3753 – 3780.

[11] IOULIANOU P, VASILAKIS V, MOSCHOLIOS I, et al. A signature-based intrusion detection system for the Internet of Things [J]. Information and Communication Technology Forum, Session 2, Paper SESSION02_ 3, 2018.

[12] AlYOUSEF M Y, ABDELMAJEED N T. Dynamically detecting security threats and updating a signature-based intrusion detection system's database [J]. Procedia Computer Science, 2019, 159: 1507 – 1516.

[13] MENG W, KWOK L F. Enhancing the performance of signature-based network intrusion detection systems: an engineering approach [J]. HKIE Transactions, 2014, 21 (4): 209 – 222.

[14] JYOTHSNA V, PRASAD R, PRASAD K M. A review of anomaly based intrusion detection systems [J]. International Journal of Computer Applications, 2011, 28 (7): 26 – 35.

[15] KANNARI P R, CHOWDARY N S, BIRADAR R L. An anomaly-based intrusion detection system using recursive feature elimination technique for improved attack detection [J]. Theoretical Computer Science, 2022, 931: 56 – 64.

[16] GUPTA N, JINDAL V, BEDI P. CSE-IDS: using cost-sensitive deep learning and ensemble algorithms to handle class imbalance in network-based intrusion detection systems [J]. Computers & Security, 2022, 112: 102499.

[17] ALSOUFI M A, RAZAK S, SIRAJ M M, et al. Anomaly-based intrusion detection systems in IoT using deep learning: a systematic literature review [J]. Applied Sciences, 2021, 11 (18): 8383.

[18] ARSHAD J, AZAD M A, ABDELTAIF M M, et al. An intrusion detection framework for energy constrained IoT devices [J]. Mechanical Systems and Signal Processing, 2020, 136: 106436.

[19] DE ALMEIDA FLORENCIO F, MORENO E D, MACEDO H T, et al. Intrusion detection via MLP neural network using an arduino embedded system [C]//2018 VIII Brazilian Symposium on Computing Systems Engineering (SBESC). IEEE, 2018: 190 – 195.

[20] WHITE J, LEGG P. Unsupervised one-class learning for anomaly detection on home IoT network devices [C]//2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA). IEEE, 2021: 1 – 8.

[21] XIE X, LI X, XU L, et al. HaarAE: an unsupervised anomaly detection model for IoT devices based on Haar wavelet transform [J]. Applied Intelligence, 2023, 53 (15): 18125 – 18137.

[22] SHITHARTH S. An enhanced optimization based algorithm for intrusion detection in SCADA network [J]. Computers & Security, 2017, 70: 16 – 26.

[23] ALWESHAH M, ALKHALAILEH S, Beseiso M, et al. Intrusion detection for IoT based on a hybrid shuffled shepherd optimization algorithm [J]. The Journal of Supercomputing, 2022, 78 (10): 12278 – 12309.

[24] ALGHAMDI R, BELLAICHE M. An ensemble deep learning based IDS for IoT using Lambda architecture [J]. Cybersecurity, 2023, 6 (3): 1 – 17.

[25] THAKKAR A, LOHIYA R. Attack classification of imbalanced intrusion data for IoT network using ensemble-learning-based deep neural network [J]. IEEE Internet of Things Journal, 2023, 10 (13): 11888 – 11895.

[26] OTOUM Y, NAYAK A. AS-IDS: anomaly and signature based IDS for the Internet of Things [J]. Journal of Network and Systems Management, 2021, 29 (3): 23.

[27] AIJUMAH A. IoT-based intrusion detection system using convolution neural networks [J]. PeerJ Computer Science, 2021, 7: e721.

[28] ALABSI B A, ANBAR M, RIHAN S D A. CNN-CNN: dual convolutional neural network approach for feature selection and attack detection on Internet of Things networks [J]. Sensors, 2023, 23 (14): 6507.

[29] LI Z, WANG P, WANG Z, et al. Flowgananomaly: flow-based anomaly network intrusion detection with adversarial learning [J]. Chinese Journal of Electronics, 2024, 33 (1): 58 – 71.

[30] TONG J, ZHANG Y. A real-time label-free self-supervised deep learning intrusion detection for handling new type and few-shot attacks in IoT networks [J]. IEEE Internet of Things Journal, 2024 (19): 11.

[31] BANIASADI S, ROSTAMI O, MMARTÍN D, et al. A novel deep supervised learning-based approach for intrusion detection in IoT systems [J]. Sensors, 2022, 22 (12): 4459.

[32] JOTHI B, PUSHPALATHA M. WILS-TRS—a novel optimized deep learning based intrusion detection framework for IoT networks [J]. Personal and Ubiquitous Computing, 2023, 27 (3): 1285 – 1301.

[33] MOUSA'B M S, HASAN M K, SULAIMAN R, et al. An explainable ensemble deep learning approach for intrusion detection in industrial Internet of Things [J]. IEEE Access, 2023, 11: 115047 – 115061.

[34] POPOOLA S I, ADEBISI B, HAMMOUDEH M, et al. Hybrid deep learning for botnet attack detection in the Internet-of-Things networks [J]. IEEE Internet of Things Journal, 2020, 8 (6): 4944 – 4956.

[35] GUO Y, JI T, WANG Q, et al. Unsupervised anomaly detection in IoT systems for smart cities [J]. IEEE Transactions on Net-

work Science and Engineering, 2020, 7 (4): 2231 – 2242.

[36] BOPPANA T K, BAGADE P. GAN-AE: an unsupervised intrusion detection system for MQTT networks [J]. Engineering Applications of Artificial Intelligence, 2023, 119: 105805.

[37] SARKAR N, KESERWANI P K, GOVIL M C. A better and fast cloud intrusion detection system using improved squirrel search algorithm and modified deep belief network [J]. Cluster Computing, 2024, 27 (2): 1699 – 1718.

[38] DAHOU A, ABD ELAZIZ M, CHELLOUG S A, et al. Intrusion detection system for IoT based on deep learning and modified reptile search algorithm [J]. Computational Intelligence and Neuroscience, 2022, 2022 (1): 6473507.

[39] OM KUMAR C U, MARAPPAN S, MURUGESHAN B, et al. Intrusion detection model for IoT using recurrent kernel convolutional neural network [J]. Wireless Personal Communications, 2023, 129 (2): 783 – 812.

[40] WANG S, XU W, LIU Y. Res-TranBiLSTM: an intelligent approach for intrusion detection in the Internet of Things [J]. Computer Networks, 2023, 235: 109982.

[41] TSOGBAATAR E, BHUYAN M H, TAENAKA Y, et al. DeL-IoT: a deep ensemble learning approach to uncover anomalies in IoT [J]. Internet of Things, 2021, 14: 100391.

[42] ELRAWY M F, AWAD A I, HAMED H F A. Intrusion detection systems for IoT-based smart environments: a survey [J]. Journal of Cloud Computing, 2018, 7 (1): 1 – 20.

[43] YANG K, WANG J M, LI M J. An improved intrusion detection method for IIoT using attention mechanisms, BiGRU, and Inception-CNN [J]. Scientific Reports, 2024, 14 (1): 19339.

[44] KEHINENI K, PRADEEPINI G. Intrusion detection in Internet of Things-based smart farming using hybrid deep learning framework [J]. Cluster Computing, 2024, 27 (2): 1719 – 1732.

[45] DE ARAUJO-FILHO P F, NAILI M, KADDOUM G, et al. Unsupervised GAN-based intrusion detection system using temporal convolutional networks and self-attention [J]. IEEE Transactions on Network and Service Management, 2023, 20 (4): 4951 – 4963.

[46] JIANG Z, LI J, HU Q, et al. Scalable graph-aware edge representation learning for wireless IoT intrusion detection [J]. IEEE Internet of Things Journal, 2024, 11 (16): 26955 – 26969.

[47] SAHEED Y K, ABDULGANIYU O H, TCHAKOUCHT T A. Modified genetic algorithm and fine-tuned long short-term memory network for intrusion detection in the Internet of Things networks with edge capabilities [J]. Applied Soft Computing, 2024, 155: 111434.

[48] LILHORE U K, MANOHARAN P, SIMAIYA S, et al. HIDM: hybrid intrusion detection model for industry 4.0 networks using an optimized CNN-LSTM with transfer learning [J]. Sensors, 2023, 23 (18): 7856.

[49] FENANIR S, SEMCHEDINE F. Smart intrusion detection in IoT edge computing using federated learning [J]. Revue d'Intelligence Artificielle, 2023, 37 (5): 1133 – 1145.

[50] TAWFIK M. Optimized intrusion detection in IoT and fog computing using ensemble learning and advanced feature selection [J]. PLoS ONE, 2024, 19 (8): e0304082.

[51] TAHAEI H, AFIFI F, ASEMI A, et al. The rise of traffic classification in IoT networks: a survey [J]. Journal of Network and Computer Applications, 2020, 154: 102538.

[52] KAMATH V, RENUKA A. Deep learning based object detection for resource constrained devices: systematic review, future trends and challenges ahead [J]. Neurocomputing, 2023, 531: 34 – 60.

[53] ANDRIULO F C, FIORE M, MONGIELLO M, et al. Edge computing and cloud computing for Internet of Things: a review [C]//Informatics, 2024, 11 (4).

[54] AFZAL B, ALVI S A, SHAH G A, et al. Energy efficient context aware traffic scheduling for IoT applications [J]. Ad Hoc Networks, 2017, 62: 101 – 115.

（收稿日期：2024 – 12 – 30）

作者简介：

周品希（2001 – ），男，硕士研究生，主要研究方向：信息安全。

沈岳（1968 – ），男，教授，主要研究方向：农业信息化。

李伟（1988 – ），通信作者，男，博士，讲师，主要研究方向：信息安全。E-mail：liwei@ hunau. edu. cn。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部