异构数据分布下的跨域联邦入侵检测模型

张尚哲
（中国联合网络通信有限公司哈尔滨市分公司，黑龙江 哈尔滨 150001）

摘　要：5G/6G时代的高速移动通信网络和物联网广泛互联，使网络环境更加开放复杂，各类网络入侵威胁也日益严峻。传统入侵检测系统大多采用集中式模型，需要将各域数据汇集到中心进行分析，存在数据孤岛和隐私泄露隐患，且难以适应跨运营域、跨网络场景的多样化威胁。为此，提出了一种基于联邦学习（federated learning，FL）的跨域入侵检测系统（intrusion detection system，IDS）模型框架Cross-FL-IDS，通过在各网络域本地训练入侵检测模型、全球聚合更新参数，实现不同域协同检测新兴威胁。在保护各域数据隐私的前提下，Cross-FL-IDS引入跨域特征共享与个性化融合机制，提升了模型对异构流量模式的泛化能力。

关键词：联邦学习；网络安全；入侵检测；跨域协同
中图分类号：TN915.08；TP393
文献标志码：A
doi: 10.11959/j.issn.1000−0801.2026043

Cross-domain federated intrusion detection model under heterogeneous data distribution

Zhang Shangzhe
China United Network Communications Co., Ltd. Harbin Branch, Harbin 150001, China

Abstract: In the 5G/6G era, owing to the widespread interconnection of high-speed mobile communication networks and the Internet of things, network environments are rendered more open and complex, and the severity of diverse network intrusion threats is heightened. Traditional intrusion detection systems are predominantly based on centralized architectures, under which data from each domain are required to be aggregated at a central site for analysis; as a result, risks of data silos and privacy leakage are introduced, and adaptation to diverse threats across operator domains and networks is hindered. To address these issues, a federated learning based cross-domain intrusion detection system model framework (Cross-FL-IDS) was proposed, in which intrusion detection models were trained locally within each network domain and model parameters were globally aggregated and updated, by which collaborative detection of emerging threats across domains was achieved. Under the premise that the privacy of each domain's data was preserved, cross-domain feature-sharing and personalized fusion mechanisms were introduced in Cross-FL-IDS, through which the model's generalization to heterogeneous traffic patterns was improved.

Key words: federated learning, network security, intrusion detection, cross-domain collaboration

收稿日期：2025−09−01；修回日期：2025−12−02
通信作者：张尚哲，2665495833@qq.com

0 引言

随着无线通信技术迈入5G及未来6G时代，网络架构日趋复杂，万物互联带来的安全挑战愈发突出[1]。一方面，5G/6G网络支持海量异构设备接入和超高带宽应用，如智能家居、自动驾驶车辆、工业物联网等，这些场景下网络流量呈现跨域、异构的特征，各子网络或域（如5G网络中的不同切片）之间流量分布差异明显；另一方面，高速网络环境下攻击手段演进迅速，新型分布式拒绝服务攻击、物联网僵尸网络攻击等层出不穷，给传统网络安全防护带来巨大挑战。入侵检测系统（intrusion detection system，IDS）作为安全防御的重要组成部分，近年来从依赖攻击特征库的签名检测逐步转向利用机器学习的异常检测，以期发现未知威胁[2]。然而，现有许多基于机器学习/深度学习的IDS往往假定训练数据集中存放在单一地点，由中央服务器统一训练模型。这种集中式架构在当前背景下面临以下两大瓶颈。

（1）隐私与合规：各运营商或组织出于数据安全和法规要求，难以直接共享原始网络流量数据用于统一训练，集中收集数据可能导致敏感信息泄露。

（2）数据孤岛与泛化：不同网络域的流量和攻击分布不尽相同，如果仅依赖单一域的数据训练IDS模型，往往对其他域的攻击检测效果不佳，而简单地将所有数据集中训练，又会因域间差异使模型性能下降。因此，如何在保护各域数据隐私的前提下，实现跨域协同的入侵检测，提升模型对不同网络环境的适应性，成为当前网络安全领域的重要课题。

针对上述挑战，本文提出采用联邦学习（federated learning，FL）技术来构建跨域入侵检测模型。FL是一种分布式机器学习框架，允许多个节点在本地数据上训练模型，并通过加权聚合形成全局模型，不需要集中共享原始数据。这一范式非常适合各参与方共同构建安全模型的需求。一些前沿研究已开始探索将FL用于入侵检测。例如，文献[3]提出在资源受限设备上利用深度神经网络和FL进行异常检测，但假设所有客户端数据同分布，未解决实际非独立同分布（independent identically distributed，IID）流量问题。文献[4]将FL用于物联网环境训练分类器检测攻击，类似地忽略了不同设备数据源异构的情况。文献[5]在FL框架下构建基于注意力机制的图神经网络IDS，取得了较好性能，但仍局限于单域数据分布的建模。文献[6]提出通过共享数据密度函数而非原始数据来增强隐私，但对异构数据的全局泛化挑战缺乏明确应对。可见，现有FL+IDS研究在一定程度上证明了分布式检测的可行性，但普遍存在对跨域数据差异适应不足的问题，这限制了全局模型在不同网络域环境下的检测效果。

1 相关研究现状

1.1 联邦学习在入侵检测中的应用

联邦学习由于其“数据不出本地”的特点，近年来在数据敏感领域得到广泛关注，将其应用于网络入侵检测已成为一个新兴方向。传统IDS通常需要将各节点的流量日志集中到安全管理中心进行分析，这不但增加了中心服务器的负担，也带来了隐私风险。谷歌于2017年率先提出利用联邦学习构建移动设备键盘个性化模型，在保障用户隐私方面展示了巨大潜力。受此启发，研究人员开始尝试将FL技术引入IDS领域，通过FL，各网络节点（如路由器、交换机、物联网网关等）可以在本地训练检测模型，只需要将模型参数上传至中央服务器进行聚合，既实现了全局知识共享，又避免了原始数据集中。

近年来，已有若干工作探索了不同FL架构和算法在入侵检测中的效果。例如，文献[7]将联邦学习按照客户端数据分布特性分为横向FL、纵

向FL和联邦迁移学习这3类。大多数网络安全场景采用横向联邦学习（horizontal federated learning，HFL），即各客户端拥有相同特征空间但不同样本（不同流量记录），这与分布式学习最为接近。在HFL框架下，多篇研究证明了神经网络模型在联邦入侵检测系统（federated intrusion detection system，FIDS）中的有效性。由于深度学习对海量数据和算力有要求，将训练任务分散到客户端可以缓解中心节点的计算瓶颈，提高模型的训练效率。

具体方案方面，文献[8]早期在5G无线通信网络环境中部署了FL的IDS原型，用博弈论分析带宽欺骗攻击的检测，对抗联邦训练中的恶意行为。文献[9]提出基于FL的分布式异常检测系统，设计了使用生成对抗网络（generative adversarial network，GAN）进行数据增强来应对通信数据不平衡问题的方案。文献[10]则关注FL过程中的攻击抵抗，如模型中毒攻击和后门攻击防御。FL-IDS方向的研究表明，在保证各参与方数据隐私的同时，联邦模型的检测性能接近于集中式模型，某些情况下甚至优于各自孤立训练的模型。然而，这些工作的共同假设往往是参与各方的数据分布相近，即使存在不平衡，也主要通过算法调优来处理，对不同域数据分布差异导致的模型偏差关注较少。这为跨域联邦入侵检测的研究留下了空间。

1.2　跨域入侵检测

跨域入侵检测指的是在多个彼此独立的网络域（如不同的组织、运营商网络，或同一运营商下不同地理区域/网络切片）之间开展协同的威胁检测。每个域内可能有各自的流量模式和攻击类型，单一模型难以兼顾所有域的差异，因此需要在协同过程中保留域间差异信息。这实际上与机器学习中的非IID问题密切相关，也是联邦学习面临的主要挑战之一。针对跨域数据差异，一些研究开始引入个性化联邦学习或联邦迁移学习的思路。在网络安全领域，文献[11]提出的动态采样联邦入侵检测系统（dynamic sampling-federated intrusion detection system，DS-FedIDS）架构利用动态采样技术，缓解各客户端类别不平衡和分布差异，对每个客户端采用自适应采样来突出少数类别攻击的学习。同时，引入本地个性化层的方法也被证明有效，即模型的前几层在客户端间共享以学习通用特征，而末几层为各客户端独有，以学习域特定模式。这种“共享+专有”的模型有助于跨域知识的部分泛化与保留。

另一个相关方向是跨域知识蒸馏或迁移学习。文献[12]提出的框架在服务器端集成跨域结构引导机制，利用公开的跨域数据训练一个全局指导模型，将不同域的结构知识融合来提升本地模型训练效果。这说明，通过巧妙地共享高层抽象知识（而非原始数据或低层特征），确实可以提升跨域模型的泛化性能。

2　跨域联邦入侵检测模型设计

2.1　本地特征提取与模型初始化

跨域联邦入侵检测模型Cross-FL-IDS的结构示意图如图1所示。该模型包含本地入侵检测模型、联邦聚合服务器，以及跨域知识融合模块等部分。

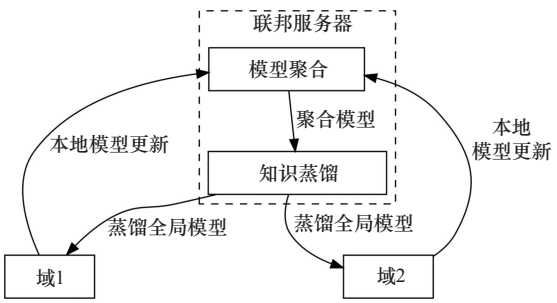


图1　模型Cross-FL-IDS的结构示意图

Cross-FL-IDS框架采用经典的联邦学习客户端–服务器架构，包括N个客户端（网络域）和1个中央服务器。每个客户端代表一个独立的网

络域，内部部署有实时流量监测和入侵检测模型。例如，不同行政单位的网络、运营商的不同区域网络或5G网络中的不同切片，都可视作独立客户端。各客户端可以是运行在多接入边缘计算（multi-access edge computing，MEC）节点的IDS实例，也可以是本地网关设备。中央服务器则可由云端的协调服务器或边缘云节点担当，负责协调联邦训练过程并融合跨域知识。

在联邦训练开始前，每个客户端需要对其本地网络流量进行预处理和特征提取，用于训练初始的入侵检测模型。考虑不同域可能采用不同的检测模型类型，本文在框架中统一采用深度神经网络模型作为基础分类器[13]。

2.2 联邦训练与模型聚合

联邦训练流程如图2所示。联邦训练过程按照迭代的通信轮次进行，每轮包含本地训练和全局聚合两个阶段，具体流程如下。

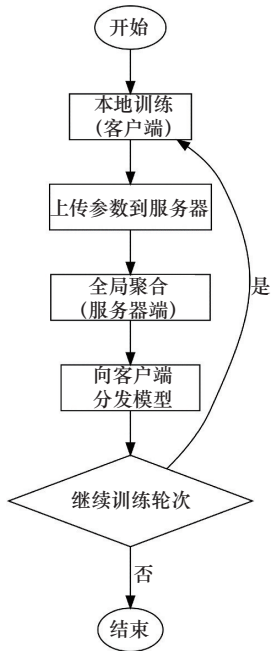


图2 联邦训练流程

（1）本地训练：在第r轮（r=1,2,…）开始时，中央服务器将当前全局模型的参数$\boldsymbol{W}^{(r)}$广播给选定的一批客户端（可以是全部N个域，也可以是随机抽取的部分域，以平衡通信开销）。客户端收到全局模型后，加载前述共享层权重，并在本地数据中继续训练一定轮次（本地epoch数可为1个或数个），更新模型参数得到$\boldsymbol{W}_i^{(r)}$，其中i表示客户端。训练优化目标采用交叉熵损失或其他适合分类的损失函数，通过随机梯度下降（stochastic gradient descent，SGD）或Adam优化器迭代。对于多分类的入侵检测，将正常流量和各种攻击类型作为不同类别进行训练。

（2）模型聚合：当本地训练完成后，客户端将模型更新（梯度或新参数）发送回中央服务器。为减少通信量，通常只传输模型的权值参数差量$\Delta\boldsymbol{W}_i^{(r)}=\boldsymbol{W}_i^{(r)}-\boldsymbol{W}^{(r)}$。服务器在收集到来自$m$个参与客户端的更新后，使用联邦平均（FedAvg）算法进行参数聚合：

$$\boldsymbol{W}^{(r+1)}\leftarrow\frac{1}{\sum_{i=1}^{m}n_i}\sum_{i=1}^{m}n_i\boldsymbol{W}_i^{(r)} \tag{1}$$

其中，n_i是客户端i用于训练的数据样本数，其作为加权系数，用以体现数据量大的客户端对全局模型的贡献更高。聚合后得到新的全局模型参数$\boldsymbol{W}^{(r+1)}$。接着进入下一轮训练，重复上述过程，直到全局模型在验证集上收敛或达到预设的轮次。

在这个过程中，由于各客户端的数据非IID，传统的FedAvg可能面临收敛变慢或模型偏置的问题。为此，需要在聚合阶段引入以下改进策略。

- 动态加权：服务器可根据每轮各客户端模型的性能（如本地验证集精度）来调整聚合权重，使得表现较好的模型更新占比略增，防止某些极端分布的数据过度影响全局模型。
- 模型正则化：在聚合时对更新幅度进行限制，如采用K异步聚合或梯度剪裁，避免异常更新扰乱全局模型训练。

- 安全聚合：采用安全多方计算对模型更新进行加密聚合，防止服务器从单个更新中反推出客户端的敏感信息。这属于隐私保护措施之一，但由于不直接影响检测性能，这里不展开阐述。

2.3　跨域知识融合机制

本文的重点创新在于服务器端的跨域知识融合模块。直观而言，单纯依靠FedAvg聚合只能平均不同域的模型参数，无法充分提取域与域之间可能共有的深层次模式信息。不同网络域的流量虽然在分布上存在差异，但潜在仍可能共享某些结构性质或攻击行为模式，如分布式拒绝服务（distributed denial of service，DDoS）攻击在不同网络中的流量突发特征可能类似。这些共性模式如果能被提炼为全局知识，将有助于提升模型对新域的泛化能力。受文献[14]启发，本文在联邦训练过程中增加了跨域公共数据的指导训练：中央服务器维护一个小规模的公共数据集（不含各域私密数据，可来自公开数据源或模拟生成的流量片段），用于辅助训练一个全局指导模型。

具体而言，在每轮聚合后，服务器利用该公共数据集执行跨域知识蒸馏。令$p_i(y|x)$表示第i个客户端模型对公共数据集中样本x属于类别y的预测概率。通过对m个客户端模型的预测取平均，本文得到集成的输出分布：

$$p_{\text{ens}}(y|x)=\frac{1}{m}\sum_{i=1}^{m}p_i\ (y|x) \tag{2}$$

接下来，服务器更新全局指导模型参数W_g，使其对x的输出分布$p_i(y|x)$与上述集成分布$p_{\text{ens}}(y|x)$尽可能接近。中央服务器维护一个小规模的公共数据集（记为D_{pub}，不含各域私密数据，可来自公开数据源或模拟生成的流量片段），用于辅助训练一个全局指导模型。优化目标可以定义为两者之间的Kullback-Leibler（KL）散度：

$$\min W_g \sum_{x\in D_{\text{pub}}} \text{KL}(p_{\text{ens}}(\cdot|x)\|p_g(\cdot|x)) \tag{3}$$

通过这一知识蒸馏过程，服务器获得了融合各域知识的“蒸馏”全局模型。相比直接参数平均，该模型在公共数据集上的行为受到了所有客户端模型的共同约束，因此，能够捕获各域之间的共有模式。

同时，本文在模型架构上引入本地个性化层来结合跨域知识与域内特征。具体来说，模型的前几层作为共享层在客户端间同步更新，而最后一层保留为各客户端独有，不参与全局聚合。这种“共享+专有”的模型设计使每个域都能保留针对自身流量模式的最后调整。联邦训练中，客户端仅上传共享层的参数更新，本地个性化层参数保留在本地，不上传至外部。全局聚合和公共数据蒸馏主要更新共享层的参数，各客户端再将更新后的共享层与自己的个性化层结合，形成最终模型。通过将全局知识的注入和本地个性化调整相结合，Cross-FL-IDS可以在域间差异显著的情况下学习到既兼顾共性又保留个性的入侵检测模型。

2.4　在线检测与持续学习

一旦联邦训练完成并收敛得到最终的全局模型，各客户端即可将该模型部署用于在线入侵检测。在线检测过程中，每个域的新流量数据首先经过预处理转化为模型可接受的特征向量，然后输入本地模型进行分类判断。由于保留了本地个性化层，各客户端在最终模型的基础上还可针对自身数据做少量微调，以获得最佳检测效果。对于检测到的可疑流量或攻击事件，各域可按照预定策略上报告警。此外，如果在实际运行中某个域出现了全新类型的攻击样本，可将其记录下来，并在下一联邦训练周期中纳入训练数据，从而实现模型的持续进化学习。

3 实验设计与结果分析

3.1 实验环境与数据集

实验使用Python语言和联邦学习框架PySyft搭建了仿真环境。服务器和客户端的训练在一台配备Intel i5 CPU、32 GB内存的工作站上进行模拟（通过多线程模拟通信时延），采用同步的联邦训练模式。联邦训练的最大通信轮次设为R=100，可根据模型收敛情况提前终止或继续。优化器采用Adam，初始学习率为0.001，并在训练过程中按需衰减。除非特别说明，联邦聚合采用等权重平均（各域样本数相近）。跨域公共数据指导的系数λ初始设为0.1，经过少量预实验确定为较优值。

实验选择了2个经典的入侵检测数据集，并对其进行划分，以模拟跨域场景。具体如下。

（1）NSL-KDD数据集：该数据集是KDD Cup 99数据集的改进版，去除了冗余记录并重新平衡了类别分布，是网络入侵检测研究的标准基准数据集之一。该数据集包含训练集和测试集，共125 973条网络连接记录，每条记录提取41维特征[15]。实验将NSL-KDD全部数据打乱后按3个不同网络域进行划分，分别为Domain A、Domain B、Domain C。划分策略基于攻击类型和流量模式分组，使每个域的流量分布存在明显差异。

（2）CIC-IDS 2017数据集：该数据集由加拿大通信安全机构发布，涵盖了2017年某周内真实背景下的正常流量和攻击流量。本文使用其提取的流量特征数据，总计约280万条记录，每条有80维特征。考虑数据量巨大且分布复杂，本文选取其中2天（周二和周四）的数据作为实验数据源，以确保包含多种攻击类型且数据规模便于处理。每个域的数据约有几十万条记录，并按8∶2的比例切分训练集和测试集。不同时段（不同天）的流量统计特性差异较大，可视为不同网络环境下的数据，因此非常适合用于验证跨域方案[16]。

上述划分确保了不同域间攻击类别分布和流量模式均存在差异，体现出非IID特征。例如，在NSL-KDD的划分中，各域攻击/正常（attack/normal）流量比例和攻击类型频次不同；在CIC-IDS 2017的划分中，不同时段的数据包含的攻击种类和频率也不同。这为评估联邦模型的泛化性能提供了有挑战性的平台。此外，在入侵检测场景中，查全率和误报率两个指标尤为关键，漏报一次攻击可能造成严重后果，而过高的误报率会影响系统的可用性。比较各种方法时，本文重点关注这些指标之间的平衡关系。

3.2 跨域联邦模型与基线比较

本节比较了Cross-FL-IDS与若干基线方法在各数据集上的检测性能，选取的基线方法如下。

（1）单域独立训练（Local）：即每个域各自用本地数据训练模型，不进行跨域合作。

（2）传统联邦平均（FedAvg）：不使用跨域知识融合的FL，仅使用FedAvg聚合全局模型。

NSL-KDD数据集和CIC-IDS 2017数据集上各方法的检测性能分别见表1、表2，结果以全局模型在所有域整体测试集上的宏平均指标计。

表1 NSL-KDD数据集上各方法的检测性能

方法	准确率	查准率	查全率	$F1$分数	误报率
Local	79.0%	80.5%	73.0%	76.6%	3.5%
FedAvg	87.0%	88.2%	80.1%	83.9%	2.3%
Cross-FL-IDS	90.4%	91.0%	85.3%	88.1%	2.1%

表2 CIC-IDS 2017数据集上各方法的检测性能

方法	准确率	查准率	查全率	$F1$分数	误报率
Local	84.1%	85.0%	78.2%	81.4%	3.0%
FedAvg	89.5%	90.4%	83.5%	86.8%	1.7%
Cross-FL-IDS	93.1%	91.2%	88.5%	89.8%	1.5%

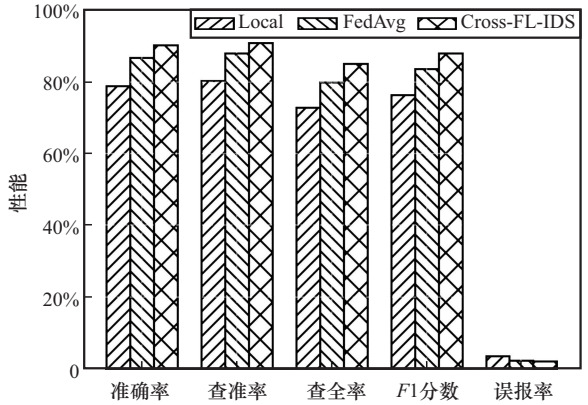
在准确率方面，Cross-FL-IDS在NSL-KDD数据集上达到90.4%，在CIC-IDS2017数据集上达到93.1%，相较Local分别提升了约14.4%和10.7%，相较仅有FedAvg的联邦模型也有约4%

的提升。这说明联邦协同确实带来了额外的信息增益，而跨域融合机制进一步改善了模型对不同分布数据的适应性。

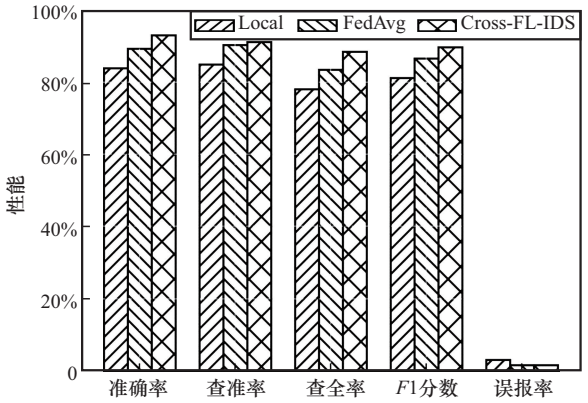
在查全率方面，本文模型在两个数据集上均表现较好，且优于其他方法。联邦方法尤其是结合个性化和跨域融合的方案能够更有效地捕获各域的攻击，提高整体查全率。

在误报率方面，Cross-FL-IDS 同样保持在较低水平（NSL-KDD 数据集约 2.1%，CIC-IDS2017 数据集约 1.5%）。这意味着联合训练并未以牺牲过多误报为代价来提升检测率，本文方法在漏报与误报之间实现了更好的平衡。这对实际部署非常关键，因为过高的误报率会导致运维人员对警报失去信任。

多模型性能比较如图 3 所示，并与表 1 和表 2 的数据相互印证。



（a）NSL-KDD数据集



（b）CIC-IDS 2017数据集

图3　多模型性能比较

不同模型的受试者工作特征（receiver operating characteristic，ROC）曲线对比如图 4 所示。由图 4 可知，Cross-FL-IDS 的 ROC 曲线整体位于其他模型之上，这意味着在相同误报率下本模型能够取得更高的检测率。换言之，Cross-FL-IDS 在检测率与误报率的权衡上明显优于各基线模型，其 ROC 曲线下面积（AUC）也更大，体现了其整体性能优势。

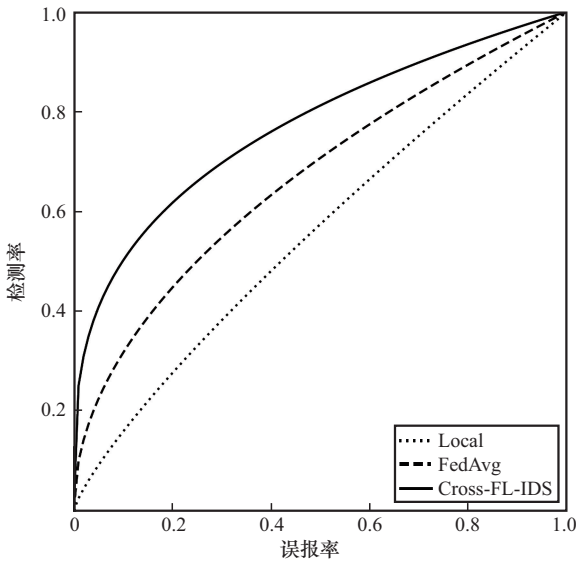


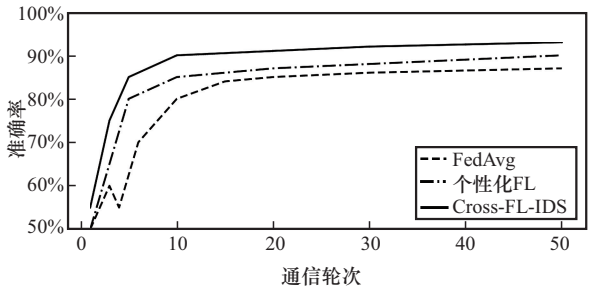
图4　不同模型的ROC曲线对比

3.3　非IID场景下的收敛分析

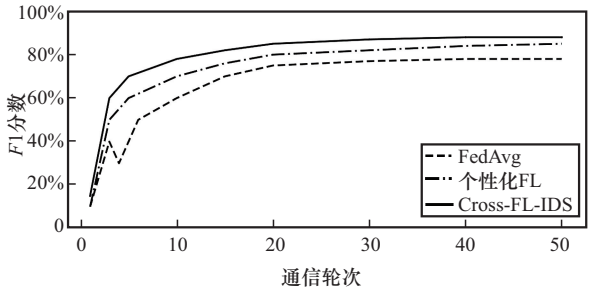
本文比较了在非 IID 数据环境下 3 种联邦学习方法的收敛性能，包括传统联邦平均 FedAvg（无个性化和跨域融合策略）、个性化 FL（在 FedAvg 基础上每个客户端保留独立的最后一层参数）以及本文提出的 Cross-FL-IDS 模型（在 FedAvg 基础上结合跨域公共知识蒸馏和本地个性化）。非 IID 场景中的收敛曲线如图 5 所示。

由图 5 可知，纯 FedAvg 在数据异构条件下收敛速度较慢，模型精度在初始几轮波动较大，约 20 轮后准确率稳定在 85% 左右，并出现平台期，50 轮时 $F1$ 分数约为 78%，之后提升趋缓。这与已知的 FL 在非 IID 条件下收敛困难的现象一致。

引入本地个性化层后，收敛速度有所加快，约30轮时准确率已接近88%，*F*1分数达到82%。这表明个性化策略在一定程度上缓解了不同数据分布之间的冲突，使各客户端能够部分保留自身的优化方向，从而加快全局收敛。



（a）不同通信轮次上的模型准确率



（b）不同通信轮次上的F1分数

图5　非IID场景中的收敛曲线

相比之下，Cross-FL-IDS的收敛速度和精度进一步提升。在相同通信轮次下，本文所提方法的准确率比纯FedAvg提高了4%~5%，且震荡幅度更小。训练过程更加稳定，这得益于引入跨域知识对全局模型进行正则约束，使模型每轮更新不会因某些偏异域的数据而发生大的偏离。总体而言，跨域知识融合和本地个性化机制的结合，有效改善了非IID场景下联邦训练的收敛性能和稳定性。

3.4　跨域融合机制的作用验证

为量化跨域知识融合模块的贡献，本文进行了消融实验。实验分别移除“跨域公共数据指导”和“本地个性化层”两项策略，观察模型性能的变化。CIC-IDS 2017数据集上的消融实验结果见表3。

表3　CIC-IDS 2017数据集上的消融实验结果

模型	准确率	查准率	查全率	*F*1分数	误报率
Cross-FL-IDS	93.1%	91.2%	88.5%	89.8%	1.5%
FedAvg+个性化	91.6%	90.5%	86.5%	88.0%	1.7%
移除个性化层	90.8%	89.7%	86.8%	87.8%	1.8%
纯FedAvg	89.0%	87.0%	82.2%	84.5%	2.1%

从表3可以看到，移除“跨域公共数据指导”（等价于仅有FedAvg +个性化）后，全局准确率降低约1.6%（由93.1%降至91.6%），查全率下降约2.3%（由88.5%降至86.5%），*F*1分数下降约2.0%（由89.8%降至88.0%）。这说明缺少跨域公共知识的注入时，模型对各异构模式的掌握略有下降，主要体现在查全率指标变差，即对某些域的少见攻击检出率降低。移除个性化层（仅FedAvg + 公共指导，全共享模型）后，准确率下降更明显，降低约2.5%（由93.1%降至90.8%），查准率下降约1.6%（由91.2%降至89.7%），*F*1分数下降约2.2%（由89.8%降至87.8%）。可见，没有本地定制、完全共享的模型在兼顾所有域模式时表现欠佳，一定程度上验证了个性化层的重要作用——它使模型能够针对域差异进行最后的调整，从而保证查准率等指标不因不同域数据的混杂而受损。

当同时移除两者（退化为纯FedAvg）时，性能降幅最大。准确率由93.1%降至89.0%（下降幅度约4.4%），查准率由91.2%降至87.0%（下降约4.6%），查全率由88.5%降至82.2%（下降约7.1%），这与前文对比的FedAvg基线结果一致。由此验证了本文提出的跨域知识融合模块（包括公共数据指导和本地个性化层）对提升联邦模型性能的显著作用。

4　结束语

本文面向复杂网络环境，提出了一种融合跨域联邦学习的入侵检测模型框架Cross-FL-

IDS。通过联邦学习机制，各网络域在本地完成模型训练并共享参数，在保护数据隐私的同时实现协同检测；通过在服务器端引入跨域公共知识指导和在客户端设计个性化层，增强了全局模型对异构网络流量的泛化能力。相关数据集上的实验结果验证了本文所提方案的有效性。相较传统集中式或各自为战的检测方法，Cross-FL-IDS 在保持较低误报率的前提下，显著提高了对多种攻击的检测率，综合性能接近于数据集中训练的理想模型水平。同时，该方案天然满足各参与方“数据不出本地”的安全要求，非常适合于多运营主体或多部门联合防御网络威胁的场景。

参考文献：

[1] IMT-2030(6G)推进组. 6G总体愿景与潜在关键技术白皮书[R]. 北京: IMT-2030(6G)推进组, 2020.
IMT-2030 (6G) Promotion Group. 6G overall vision and potential key technology white paper[R]. Beijing: IMT-2030 (6G) Promotion Group, 2020.

[2] Bace R, Mell P. Intrusion detection systems (IDSv1.0) [R]. Gaithersburg: U.S. National Institute of Standards and Technology, 2001.

[3] Li Y C, Ma R, Jiao R H. A hybrid malicious code detection method based on deep learning[J]. International Journal of Security and its Applications, 2015, 9(5): 205-216.

[4] Aldweesh A, Derhab A, Emam A Z. Deep learning approaches for anomaly-based intrusion detection systems: a survey, taxonomy, and open issues[J]. Knowledge-Based Systems, 2020, 189: 105124.

[5] Zhang C Y, Patras P, Haddadi H. Deep learning in mobile and wireless networking: a survey[J]. IEEE Communications Surveys & Tutorials, 2019, 21(3): 2224-2287.

[6] Hodo E, Bellekens X, Hamilton A, et al. Shallow and deep networks intrusion detection system: a taxonomy and survey[PP]. arXiv (2017-01-09) [2025-05-01] arXiv: arXiv.1701.02145.

[7] Tang F X, Mao B M, Fadlullah Z M, et al. On a novel deep-learning-based intelligent partially overlapping channel assignment in SDN-IoT[J]. IEEE Communications Magazine, 2018, 56(9): 80-86.

[8] Mothukuri V, Parizi R M, Pouriyeh S, et al. A survey on security and privacy of federated learning[J]. Future Generation Computer Systems, 2021, 115: 619-640.

[9] Taheri R, Shojafar M, Alazab M, et al. Fed-IIoT: a robust federated malware detection architecture in industrial IoT[J]. IEEE Transactions on Industrial Informatics, 2021, 17(12): 8442-8452.

[10] 张磊, 姜鸽, 蒲冰倩, 等. 联邦学习中的模型中毒攻击防御策略综述[J]. 计算机科学与探索, 2025: 1-26.
Zhang L, Jiang G, Pu B Q, et al. Model poisoning attack defense strategies in federated learning: a survey[J]. Journal of Frontiers of Computer Science and Technology, 2025: 1-26.

[11] Youm S, Kim T. Enhancing federated intrusion detection with class-specific dynamic sampling[J]. Applied Sciences, 2025, 15(9): 5067.

[12] Li B B, Wu Y H, Song J R, et al. DeepFed: federated deep learning for intrusion detection in industrial cyber-physical systems[J]. IEEE Transactions on Industrial Informatics, 2021, 17(8): 5615-5624.

[13] Lin Z P, Yang J, Lian Y B, et al. Optimization design of cross border intelligent marketing management model based on multi layer perceptron-grey wolf optimization convolutional neural network[J]. Scientific Reports, 2025, 15: 5150.

[14] De S, Wang W, Zhou Y C, et al. Analysing environmental impact of large-scale events in public spaces with cross-domain multimodal data fusion[J]. Computing, 2021, 103(9): 1959-1981.

[15] Iftikhar N, Rehman M U, Ali Shah M, et al. Intrusion detection in NSL-KDD dataset using hybrid self-organizing map model[J]. Computer Modeling in Engineering & Sciences, 2025, 143(1): 639-671.

[16] Da Silva Ruffo V G, Lent D M B, Carvalho L F, et al. Generative adversarial networks to detect intrusion and anomaly in IP flow-based networks[J]. Future Generation Computer Systems, 2025, 163: 107531.

[作者简介]

张尚哲（2002–），男，中国联合网络通信有限公司哈尔滨市分公司工程师，主要研究方向为计算机网络与信息安全。