基于异步个性化联邦学习的DDoS攻击检测与缓解

朱海婷[1),2)] 魏明岗[1)] 刘丰宁[1)] 何高峰[1)] 张 璐[3)]

[1)](南京邮电大学物联网学院 南京 210003)

[2)](东南大学计算机网络和信息集成教育部重点实验室 南京 210096)

[3)](南京审计大学计算机学院 南京 211815)

摘 要 网络流量分类在网络管理和安全中至关重要,尤其是精准识别分布式拒绝服务(Distributed Denial of Service,DDoS)攻击这一威胁。DDoS攻击会导致服务中断、资源耗尽和经济损失,严重影响服务质量(QoS)。尽管集中式模型在DDoS攻击检测中取得了一定成效,但在实际应用中存在挑战:数据分布不均、数据集中传输困难,以及异构设备和动态网络环境的限制,从而难以实现实时检测。为应对这些问题,本文提出了一种基于异步个性化联邦学习的DDoS攻击检测与缓解方法AdaPerFed(Adaptive Personalized Federated Learning)。首先,通过定制的ResNet架构高效处理一维流量数据,并集成Net模块增强特征提取能力。然后,通过软件定义网络(SDN,Software-Defined Networking)模拟复杂动态网络环境,并引入完善的缓解系统应对多样化攻击场景。个性化联邦学习框架有效处理了非独立同分布(Non-IID,Non-Independent and Identically Distributed)数据问题,并通过异步学习机制适应异构设备和网络条件的差异,提升了系统的鲁棒性和扩展性。实验结果表明,AdaPerFed在CICDDoS2019、CIC-IDS2017和InSDN等数据集上均优于其他联邦学习算法,在不同客户端数量下展现出更快的收敛速度和更强的鲁棒性,DDoS检测准确率提升了15%~20%。消融实验进一步验证了个性化聚合模块对系统性能的显著提升。

关键词 联邦学习;分布式拒绝服务(DDoS);深度学习;ResNet;软件定义网络(SDN)

中图法分类号 TP309 **DOI号** 10.11897/SP.J.1016.2025.00808

DDoS Attack Detection and Mitigation Based on Asynchronous Personalized Federated Learning

ZHU Hai-Ting[1),2)] WEI Ming-Gang[1)] LIU Feng-Ning[1)] HE Gao-Feng[1)] ZHANG Lu[3)]

[1)](School of Internet of Things, Nanjing University of Posts and Telecommunications, Nanjing 210003)

[2)](Key Laboratory of Computer Network and Information Integration, Ministry of Education, Southeast University, Nanjing 210096)

[3)](School of Computer Science, Nanjing Audit University, Nanjing 211815)

Abstract Network traffic classification serves as a fundamental component of both network management and cybersecurity, playing a pivotal role in ensuring the stability and security of modern communication infrastructures. Among various network security threats, the accurate identification of Distributed Denial of Service (DDoS) attacks remains particularly crucial, as such attacks have the potential to severely compromise system availability and overall network

收稿日期:2024-11-15;在线发布日期:2025-02-13。本课题得到国家自然科学基金面上项目(62272237)、国家自然科学基金青年科学基金项目(52105553,61802207)、江苏省高等学校自然科学研究重大项目(22KJA520005)、计算机网络和信息集成教育部重点实验室(东南大学)开放课题(K93-9-2023-04)、江苏高校'青蓝工程'资助。**朱海婷**,博士,讲师,中国计算机学会(CCF)会员,主要研究领域为网络测量、网络管理、网络安全等。E-mail:htzhu@njupt.edu.cn。**魏明岗**,硕士研究生,主要研究领域为网络安全。**刘丰宁**,硕士研究生,主要研究领域为联邦学习。**何高峰**,博士,副教授,研究方向为网络安全、物联网安全等。**张 璐**(通信作者),博士,副教授,研究方向为数据挖掘、网络空间安全等。E-mail:luzhang@nau.edu.cn。

reliability. DDoS attacks can cause significant disruptions to network services by overwhelming targeted systems with an excessive volume of malicious traffic, leading to service outages, rapid depletion of computational and network resources, and substantial financial losses. These consequences critically impair the Quality of Service (QoS), affecting both end users and service providers by degrading network performance and reducing operational efficiency. While centralized machine learning models have demonstrated notable success in detecting DDoS attacks by leveraging vast amounts of labeled data for training, their deployment in real-world network environments is hindered by several intrinsic challenges. One of the most critical issues is the highly imbalanced distribution of network traffic data, where attack patterns and normal traffic exhibit significant variations across different clients. Furthermore, the centralized collection and transmission of large-scale network data not only introduce severe privacy and security concerns but also pose substantial bandwidth and storage constraints, making traditional data aggregation approaches impractical. Additionally, heterogeneous network devices—ranging from high-performance servers to resource-constrained edge devices—operate under diverse computational capabilities and network conditions, while the constantly evolving nature of network traffic dynamics further complicates the feasibility of real-time DDoS detection and mitigation strategies. To effectively address these challenges and enhance the adaptability and efficiency of DDoS attack detection in dynamic network environments, this paper introduces AdaPerFed (Adaptive Personalized Federated Learning), an asynchronous personalized federated learning-based approach designed to detect and mitigate DDoS attacks while overcoming the inherent limitations of centralized detection frameworks. First, we develop a customized ResNet-based deep learning architecture that is specifically optimized for efficiently processing one-dimensional network traffic data, enabling the extraction of rich temporal and spatial features crucial for DDoS detection. Additionally, we integrate a dedicated Net module within the architecture to further enhance feature extraction capabilities, allowing the model to capture complex attack patterns more effectively and distinguish malicious traffic from benign network activities with higher precision and robustness. Subsequently, we leverage Software-Defined Networking (SDN) to construct a highly flexible and programmable network environment, allowing us to simulate realistic, large-scale, and dynamically changing network conditions where diverse attack scenarios can be systematically evaluated. To complement our detection framework, we incorporate a comprehensive mitigation system, which dynamically adjusts network security policies and defensive mechanisms in response to evolving attack patterns, ensuring proactive protection against a wide range of DDoS threats. The personalized federated learning framework employed in AdaPerFed effectively addresses the fundamental challenge of Non-Independent and Identically Distributed (Non-IID) data, a common issue in federated learning where clients possess highly diverse and unbalanced datasets. By incorporating an asynchronous learning mechanism, our approach ensures that each client autonomously updates and fine-tunes its model based on local data distributions, thereby enhancing personalization and improving overall model generalization. Furthermore, this asynchronous and adaptive learning strategy enables the system to accommodate heterogeneous devices with varying computational resources and network conditions, significantly improving the robustness, scalability, and practical deployment potential of the proposed framework. Extensive experimental evaluations conducted on three widely-used benchmark datasets—CICDDoS2019, CIC-IDS2017, and InSDN—demonstrate that AdaPerFed significantly outperforms state-of-the-art federated learning algorithms in terms of both detection accuracy and learning efficiency. Across various experimental settings, our method consistently

exhibits faster convergence rates, enabling the model to achieve optimal performance with fewer training iterations, even as the number of participating clients increases. Furthermore, AdaPerFed achieves a remarkable 15%-20% improvement in DDoS detection accuracy compared to existing federated learning approaches, highlighting its superior ability to effectively identify and mitigate DDoS attacks across diverse and complex network environments. Additionally, ablation studies further validate the critical role of the personalized aggregation module in enhancing overall system performance.

Keywords federated learning; Distributed Denial of Service (DDoS); deep learning; ResNet; Software-Defined Networking (SDN)

1 引 言

网络流量分类是网络管理中的一项基础任务，其主要目标之一是保障网络安全[1]。鉴于DDoS攻击对网络安全构成的威胁，准确识别这种攻击在流量分类中成为一个重大挑战。DDoS攻击通过资源耗尽、服务中断、攻击者匿名性及经济损失，严重威胁和挑战网络安全及其基础设施的稳定性[2]。这类攻击通过向目标服务器或网络发送大量流量，将其淹没，从而使其无法正常为合法用户提供服务[3]。随着车联网和物联网网络的普及，到2026年，物联网设备的连接数预计将增长至约264亿，这将扩大潜在的攻击面[4]。被攻陷的设备可能会被利用来对全球分布的边缘服务器发起大规模的DDoS攻击，不仅威胁到个人用户，还危及更广泛的数字生态系统[5]。因此，实施有效的DDoS攻击防御策略和技术对于维护网络安全至关重要。

多种机器学习框架已广泛应用于DDoS攻击检测，其中包括K近邻（KNN）、支持向量机（SVM）、随机森林（RF）和朴素贝叶斯（NB）等传统方法[6]。这些方法通过分析和分类网络流量模式来检测异常行为。然而，传统机器学习方法在复杂攻击场景下的表现存在局限，尤其在处理大规模和动态变化的流量数据时，检测性能不够理想[7]。

近年来，研究重心逐渐转向深度学习，以提升DDoS攻击检测的准确性和鲁棒性[8]。深度学习模型能够捕捉复杂的数据模式和非线性关系，对未知威胁具有更强的泛化能力[9]。然而，随着网络深度的增加，传统深度神经网络面临梯度消失和网络退化等问题。这些问题可能导致模型训练过程中的梯度更新减缓甚至停滞，影响网络的收敛速度和最终性能[10]。此外，深度模型参数众多且复杂，容易产生过拟合现象，尤其是在数据分布不均或特征冗余的情况下。因此，如何在提升检测精度的同时，克服梯度消失和网络退化等挑战，成为DDoS攻击检测研究中的关键问题。此外，现实世界的网络环境复杂多变，网络流量动态性强，数据分布会随着时间和环境不断变化，使得模型难以依赖静态数据集进行全面学习和泛化[11]，进一步增加了DDoS攻击检测的难度。

尽管集中式模型在DDoS攻击检测中展现出一定的效果，但在实际应用中仍面临诸多挑战。首先，现实世界的数据分布普遍存在非均衡性，网络流量中不同来源的数据量与类别可能存在显著差异。这种不平衡性易导致模型偏向于样本量较大的类别，从而降低对小类别异常行为的检测能力，影响整体检测性能。此外，集中式模型依赖于将所有数据集中化进行训练，然而在现实环境中，由于数据隐私保护要求、法规限制（如General Data Protection Regulation），以及设备的地理分布和异构性，集中数据传输和存储难以实现[12]。

其次，不同设备之间的计算能力和网络条件差异明显。例如，物联网设备、边缘服务器和云服务器的性能差距显著，使得部分设备无法承载高计算负载，限制了集中式模型的应用范围。此外，设备的网络连接状态在实际环境中往往不稳定，一些节点可能频繁离线或延迟上传数据，进一步加剧了集中训练的不确定性与延迟。在异构设备与动态网络环境下，集中式模型的鲁棒性和扩展性受到限制，难以满足复杂网络环境中的实时检测需求。

为了解决上述挑战，本文提出了一种基于异步个性化联邦学习的DDoS攻击检测与缓解方法。首先，引入定制化的ResNet架构来高效处理一维流量数据，并通过集成Net模块增强特征提取能力。其次，采用软件定义网络模拟复杂且动态的网

络环境，并配备完善的缓解系统以应对多样化的攻击场景。此外，本文通过个性化联邦学习框架解决非独立同分布数据问题，确保每个设备根据自身数据特点获得个性化模型[13]。与此同时，异步学习机制有效应对异构设备之间计算能力和网络条件的差异，使系统能够在不依赖同步通信的情况下高效运行。该方法通过动态调整本地与全局模型之间的权重，增强了模型在真实环境中的适应性，实现了鲁棒且高效的DDoS攻击检测与防御。

与传统的DDoS攻击检测方法不同，本文提出的方法在个性化模型生成、处理非独立同分布数据、异步更新机制和动态自适应模型更新方面展现出独特优势。传统方法采用统一的全局模型，难以适应不同设备或网络环境的特征，而本文通过个性化联邦学习框架，为每个设备生成适应本地数据特点的模型，显著提升检测精度和泛化能力。此外，本文能够有效处理非独立同分布数据，解决了传统方法假设数据（Independent and Identically Distributed，IID）的局限；异步学习机制灵活应对设备间的计算和网络延迟差异，提高了训练效率和实时性；而动态自适应的模型更新策略则能根据不同的攻击类型和网络环境调整模型，提高防御新型DDoS攻击的能力。通过这些创新，本文的方法在复杂动态的网络环境中展现出比传统方法更强的鲁棒性和效率。

综上所述，本文提出了一种基于异步个性化联邦学习的DDoS攻击检测模型，有效应对了非独立同分布数据、异构设备性能差异以及网络动态变化等现实挑战。通过引入定制化ResNet架构与Net模块，提升了模型在一维流量数据处理和特征提取方面的性能。采用软件定义网络环境对复杂网络场景进行模拟，验证了模型在真实环境中的鲁棒性和高效性。此外，异步训练机制降低了设备间对同步通信的依赖，使各客户端能够根据其自身状态灵活参与训练，提高了系统的容错性和运行效率[14]。该模型在CICDDoS2019、CIC-IDS2017和InSDN多个数据集上的表现优于现有先进方法。通过异步个性化策略，模型实现了全局优化与本地定制之间的平衡，显著提升了DDoS攻击的检测与防御效果。

本文的主要工作如下：

（1）通过定制的ResNet提升模型性能：设计并优化了ResNet架构以适应一维流量数据的特征处理，增强了模型的特征提取能力，并有效缓解了传统深度神经网络中的梯度消失和网络退化问题。这一改进确保了模型在复杂流量模式下的检测准确性，并减少了计算资源的消耗。

（2）提出了异步和个性化联邦学习框架：该框架针对现实环境中的非独立同分布数据和设备性能差异问题，采用个性化策略为每个客户端定制模型参数，从而提升本地检测性能。通过异步训练机制，降低了设备间对同步通信的依赖，确保客户端能够根据自身状态灵活参与训练，增强了系统的鲁棒性和适应性。

（3）在SDN环境下实现了高效的DDoS攻击缓解：利用SDN的灵活性，模拟复杂的网络环境，并结合动态信任值机制、速率限制和黑名单策略，实现了实时高效的DDoS攻击检测与缓解。当检测到异常流量时，动态调整攻击者的信任值，并逐步采用速率限制措施，防止服务中断。一旦信任值降低到阈值以下，恶意IP将被列入黑名单，从而有效阻止进一步攻击。这一综合策略确保了网络的安全性和服务的稳定性。

2　相关工作

在过去的几年里，DDoS攻击已经成为网络安全领域中的一大挑战。传统的DDoS攻击检测方法多依赖于集中式架构，但随着网络规模的扩大和攻击方式的日益复杂，这些方法面临着诸多挑战[15]。近年来，软件定义网络和联邦学习（Federated Learning，FL）作为两种重要的技术手段，在DDoS攻击检测中展现出了较为显著的优势。

2.1　SDN环境下的DDoS检测研究

SDN通过集中控制平面和数据平面的分离，能够实时监控并动态调整网络流量，为DDoS攻击的检测和缓解提供了新思路[16-18]。Dan Tang[19]通过多维流量分析、时间序列分析和特征提取实现SDN中LDoS攻击的检测和缓解，但主要集中在传输层攻击，对其他层的攻击缺乏关注。

此外，深度学习技术逐渐成为SDN环境中DDoS检测的主流方法。Gadallah等人[20]采用深度学习技术检测SDN中的DDoS攻击，在控制平面和数据平面分别进行检测，取得了较高的检测准确率，表明深度学习在处理复杂网络流量时的潜力。随后，Bazzi[21]使用ResNet-50模型提取网络流量特征并进行SYN Flood DDoS攻击分类，在公共和专有数据集上展示了较高的准确性，证明了深度神经网络在特征提取和分类任务中的优势。类似地，Hnamte等人[22]针对SDN环境检测和缓解DDoS攻

击，在多个数据集上取得接近100%的检测准确率，并展示了良好的扩展性和适应性，这反映了深度学习技术在SDN中的强大表现。

尽管这些研究集中在提高DDoS攻击检测的准确性和适应性，仍面临两个主要挑战：一是许多方法只能处理特定类型的攻击，难以应对动态攻击环境；二是部分方法依赖于传统的同步学习，缺乏对非独立同分布（Non-IID）数据和异步网络环境的适应性。

2.2 基于联邦学习的DDoS攻击检测

联邦学习作为一种分布式学习方法，通过保持数据在本地，提高隐私保护并降低通信成本。Doriguzzi-Corin等人[23]使用自适应联邦学习在CICDDoS2019数据集上检测DDoS攻击，结果显示检测准确率和收敛时间优于现有FL方法，突出了自适应机制在提高模型训练效率和精度方面的潜力。与此类似，Li等人[24]基于联邦学习和雾/边缘计算进行DDoS防御，在UNSW NB15数据集上实现了接近集中式模型的检测准确率，同时缓解响应时间减少72%，攻击成本提高3.7倍，证明了该方法在边缘计算环境中的优势。

Fotse等人[25]进一步提出了基于联邦学习的FedLAD架构，适用于多控制器SDN，确保了隐私保护，并在CICDDoS2019等数据集上实现了超过98%的检测精度。该方法不仅具有低资源消耗的特点，还在高准确率的同时有效减少了计算开销，适应了分布式网络环境中对计算资源的限制。Zhang[26]则提出了一种基于联邦学习的DDoS攻击检测模型，结合K-Means聚类和SMOTEENN重采样技术，显著提高了CICDDoS2019数据集上的检测精度，并通过减少通信轮次，进一步提升了联邦学习方法的效率，检测精度比FedAvg方法提高了4%。

Liu等人[27]提出了一种基于联邦增量学习（Incremental Learning）的DDoS攻击检测模型，结合动态权重聚合和LSTM网络，在SDN环境中有效解决了Non-IID数据问题。实验结果显示，该方法在检测准确率上比FedAvg方法提高了5.06%-12.62%，F1-Score提升了0.0565-0.1410，展示了增量学习在应对不断变化的数据环境中的优势。与此同时，Yin等人[28]提出了一种基于联邦学习的多域DDoS检测方法，通过分布式知识库和区块链技术，在CICDDoS2019数据集上实现了高达95%以上的检测准确率。该方法利用区块链评估恶意参与者的信任度，从而有效防御数据中毒攻击，进一步提升了系统的鲁棒性和安全性。

最后，Dimolianis等人[29]提出了一种隐私保护的联邦学习架构，由可信第三方协调，在多域环境下实现实时的DDoS攻击过滤。显著提高了检测准确率，验证了联邦学习在分布式环境中的实际应用潜力。

这些研究表明，基于联邦学习的DDoS攻击检测方法通过自适应机制、增量学习、边缘计算和区块链技术，显著提升了检测准确性、实时性和系统适应性，同时优化了通信和计算效率，解决了传统集中式方法中的高延迟和计算资源瓶颈。

2.3 个性化联邦学习

随着现实场景中数据的非独立同分布特性对传统联邦学习算法提出挑战，个性化联邦学习（Personalized Federated Learning，pFL）应运而生。它通过个性化更新机制，有效解决客户端数据分布的不一致性，尤其在应对复杂攻击模式时，能更好地适应每个客户端的需求。

在个性化联邦学习的研究中，Chen等人[30]通过迁移学习，将全局模型迁移到客户端生成个性化模型。Wu等人[31]提出基于云-边协同的个性化联邦学习框架，以提升智能物联网（IoT）应用的适应性并降低通信开销。Fallah等人[32]和Jiang等人[33]则采用元学习方法，将全局模型训练视为元训练，客户端局部模型训练视为元测试，从而优化个性化模型。Dinh等人[34]通过解耦全局与局部模型参数，找到两者之间的平衡，提升个性化调整效果。

在网络安全领域，个性化联邦学习也展现了巨大潜力。Thin等人[35]提出的PFL-IDS系统，通过logit调整损失和恶意客户端检测机制，解决了数据不平衡问题并防止中毒攻击。Su和Zhang[36]的APFed框架通过个性化更新和共享全局分类器，提升了模型在全局和个性化场景下的泛化能力。Luo等人[37]提出基于Transformer的IoT恶意流量检测框架，利用个性化联邦学习和多点协作，提高了检测性能。

尽管现有基于SDN和联邦学习的DDoS检测方法已取得进展，但在应对客户端异构和非独立同分布（Non-IID）数据时仍存在不足。本论文提出的方法AdaPerFed通过引入性能向量驱动的个性化更新机制和异步学习策略，有效解决了客户端数据分布不一致和高延迟问题。

3　模　型

本节详细介绍本文提出的基于异步个性化联邦学习的DDoS攻击检测模型，包括以下三个核心部分：定制化ResNet架构、个性化联邦学习框架，以及在SDN环境中的应用与动态缓解策略。通过定制化ResNet模型，本研究增强了对一维流量数据的特征提取能力，有效解决了传统深度模型中的梯度消失和网络退化问题。个性化联邦学习框架旨在应对非独立同分布（Non-IID）数据和设备间性能差异，利用异步机制降低同步通信需求，提升系统在异构网络环境中的适应性。此外，通过SDN模拟复杂的网络环境，并结合动态信任值、速率限制和黑名单策略，实现了DDoS攻击的高效检测与缓解，保障网络的安全性和稳定性。

3.1　ResNet

我们对ResNet进行了定制化修改，将其调整为适用于一维流量数据的模型，通过引入1D卷积层替换原有的2D卷积，以更好地处理时间序列数据[38]。为进一步增强特征提取能力，我们添加了一个Net模块，Net模块由三个全连接层组成。通过与ResNet结合使用，以捕捉更细微的恶意流量特征。这些改进不仅有效缓解了梯度消失和网络退化问题，还提升了模型在非独立同分布（Non-IID）数据上的鲁棒性和检测精度，使其更适用于复杂的网络环境。模型如图1所示。所添加的Net模块如图2所示。

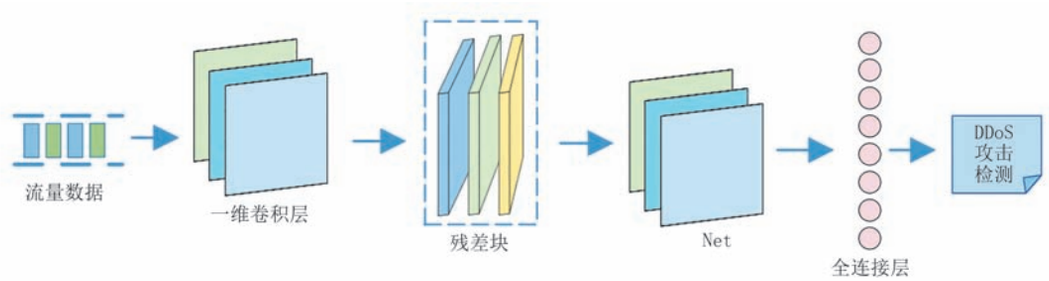


图1　ResNet模型图

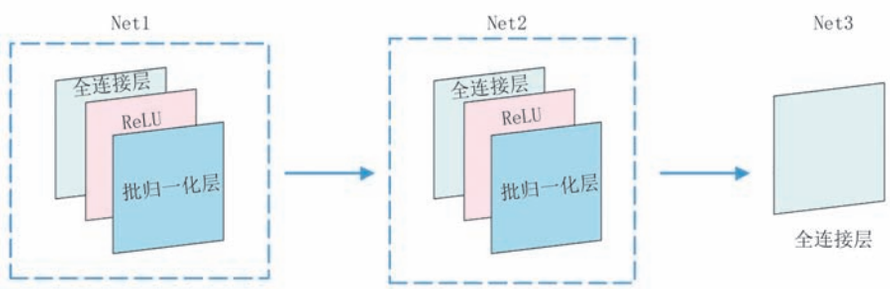


图2　Net结构图

3.2　异步个性化联邦学习框架

在传统联邦学习中，客户端异构性（如计算能力、网络条件差异）和非独立同分布（Non-IID）数据给全局模型训练带来了极大挑战。此外，现实环境中的客户端可能无法始终在线参与训练，传统的同步联邦学习方法要求所有客户端同时在线，这在实际网络中难以实现。为了解决这些问题，我们提出了支持随机在线客户端的异步个性化联邦学习算法。

在非独立同分布（Non-IID）数据环境中，不同客户端的本地训练数据特性存在差异，直接聚合各客户端的模型可能会导致全局模型在整体数据上的性能下降。为了应对这一挑战，我们提出了一种基于性能向量的个性化更新算法，通过量化客户端模型与全局模型之间的性能差距，动态分配每个客户端模型的权重，以实现更精准的个性化更新。

该方法基于客户端模型的多项性能指标（F1-Score、损失值、精确率、召回率和准确率），构建性能向量，并以欧氏距离为度量标准，量化全局模型与客户端模型在性能上的差异性。对于欧氏距离较小的客户端模型，增加其对全局知识的吸收程度；反之，对于差异较大的模型，则更大程度地保留其个性化特性，从而实现差异化的联邦知识融合策略。通过

这种方式，既保证了全局模型的泛化能力，又能够有效利用本地模型的个性化特性，从而在保持全局一致性的同时，满足每个客户端的个性化需求。

欧氏距离用于衡量全局模型与客户端的性能向量之间的差距，如公式(1)：

$$d\left(v_g, v_c^i\right)=\sqrt{\sum_{k=1}^{n}\left(v_g-v_c^i\right)^2} \tag{1}$$

其中，n为性能向量的维度，v_g表示全局性能向量，v_c表示客户端性能向量。i表示第i个客户端。k表示第k个性能向量。

为了避免极端值对模型聚合过程的影响，并确保每个客户端的模型对全局模型的贡献更加稳定和合理。使用反正切(arctan)函数来平滑数据因子。权重的计算公式(2)如下：

$$\omega_c=\alpha\times\arctan\left(\frac{1}{d\left(v_g, v_c^i\right)+\varepsilon}\right) \tag{2}$$

α是平衡因子，用于控制全局与个性化模型融合，ε是极小值，防止分母为0。

在聚合之前，需要对每个客户端的个性化权重ω_c进行归一化，确保所有客户端的权重和为1。如公式(3)所示。

$$\omega_c\leftarrow\frac{\omega_c}{\sum_{i=1}^{n}\omega_i} \tag{3}$$

在聚合过程中，服务器会基于客户端的权重ω_c以及上传的模型参数M_c^i，对全局模型M_g进行更新。如公式(4)所示。

$$M_g\leftarrow\sum_{i=1}^{n}\omega_c\times M_c^i \tag{4}$$

M_c^i是第i个客户端上传的本地模型。ω_c是该客户端的权重，反映了他对全局模型的贡献。服务器按权重对所有客户端模型进行加权求和，生成新的全局模型。目的是更高质量的客户端模型对全局模型的影响更大；表现差异大的客户端模型则贡献较小，避免偏离全局优化方向。

每个客户端在接收到服务器下发的更新后的全局模型M_g后，需要根据个性化权重ω_c调整本地模型。如公式(5)所示。

$$M_c^i\leftarrow M_c^i+\omega_c\left(M_g^i-M_c^i\right) \tag{5}$$

M_c^i表示客户端的第i个参数。M_g^i表示全局模型的第i个参数。ω_c是个性化权重，用于决定客户端吸收多少全局模型的知识。

算法1. 基于性能向量的个性化更新算法

输入：全局模型参数M_g，每个客户端的本地模型参数M_c，全局性能向量v_g，客户端性能向量v_c，冻结层数L_f，平衡因子α，客户端数量n

输出：个性化更新后的客户端模型M_c^{new}，聚合后的全局模型M_g^{new}

1. FUNCTION 获取$d\left(v_g, v_c^i\right)$
2. 初始化距离矩阵d
3. FOR v_c^i IN v_c DO
4. FOR v_gDO
5. $d\left(v_g, v_c^i\right)=\sqrt{\sum_{k=1}^{n}\left(v_g-v_c^i\right)^2}$
6. END FOR
7. END FOR
8. 返回$d_{v_g v_c}$
9. FUNCTION 获取客户端个性化权重ω_c
10. 设置ω_c为长度为n的空列表
11. FOR $i\leftarrow$1 TO n DO
12. $W_c^i=\alpha\times\arctan\left(\frac{1}{d\left(v_g, v_c^i\right)+\varepsilon}\right)$
13. $\omega_c\leftarrow\{\omega_1, \cdots, \omega_n\}$
14. $\omega_c\leftarrow\frac{\omega_c}{\sum_{i=1}^{n}W_c^i}$
15. END FOR
16. 返回ω_c
17. FUNCTION 聚合全局模型M_g^{new}
18. FOR M_c^i IN M_c DO
19. FOR $i\leftarrow$1 TO n DO
20. $M_g\leftarrow\sum_{i=1}^{n}W_c^i\times M_c^i$
21. END FOR
22. 返回M_g^{new}
23. FUNCTION 获取客户端模型M_c^{new}
24. FOR $i\leftarrow$1 TO n DO
25. FOR layer = frozen_layers TO total_layers DO
26. $M_c^i\leftarrow M_c^i+W_c^i\left(M_g^i-M_c^i\right)$
27. END FOR
28. END FOR
29. 返回个性化更新后的客户端模型M_c^{new}

该算法通过性能驱动的动态权重调整、全局与个性化的平衡、和冻结机制，在复杂的非独立同分布(Non-IID)数据环境中实现了鲁棒、高效的联邦学习模型更新，确保了模型的整体性能和个性化需求。它不仅提升了系统的适应性和灵活性，同时降低了通信开销，为大规模、异构数据环境中的联邦学习提供了强有力的支持。算法过程如图3所示。

传统的同步联邦学习要求所有客户端在同一轮内完成训练并上传模型，服务器才能进行模型的聚

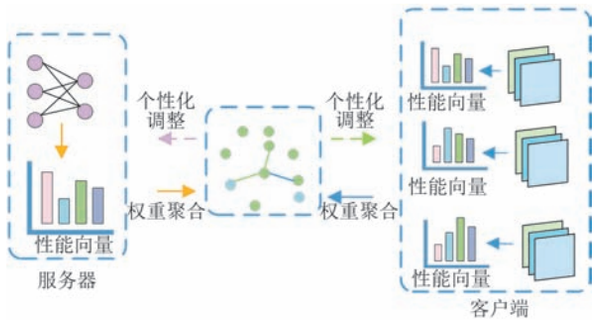


图3　基于性能向量的个性化更新算法过程图

合与更新。然而，在实际场景中，各客户端的设备性能不一致，部分设备可能运算能力弱、网络延迟高，甚至出现掉线，导致同步联邦学习难以有效运行。整体训练速度受限于最慢的客户端（“慢设备瓶颈”），拖慢整个模型更新的节奏。一旦某些设备掉线，无法按时完成上传，整个训练过程可能中断或延迟。性能好的客户端在等待慢设备完成训练时，无法高效利用计算资源，增加系统的闲置成本。

为了解决这些问题，我们设计了一种异步联邦学习算法，允许客户端按照各自的节奏上传模型，并根据服务器的反馈进行个性化更新。如算法2所示。

为了确保模型能够准确收敛，我们引入了时间戳与最大延迟控制机制，每个客户端的模型更新都携带一个时间戳，标记该更新的生成时间。服务器根据时间戳判断各客户端更新的有效性。如果某个客户端的更新超出了设定的最大延迟阈值（max_delay），该更新将被丢弃，不参与本轮的全局模型聚合。通过这一机制，我们能够确保低延迟客户端的更新能够优先被处理，而过期的更新则会被自动排除，从而避免高延迟客户端的过期更新对全局模型的收敛性和准确性产生负面影响。同时，为了减小通信延迟带来的影响，客户端在上传模型更新之前进行一定次数的局部训练，从而确保上传的更新质量，并减少因网络延迟带来的性能波动。

算法2.　异步联邦学习算法

输入：客户端集合C，轮次总数R，重连概率$P_{reconnect}$，掉线概率$P_{disconnect}$，重连间隔interval

输出：客户端在线状态

1. 初始化在线客户端集合：
2. C_online←{c_1，c_2，•••，c_n}#初始时所有客户端在线
3. FOR r = 1 TO R DO
4. 　　C_selected⊆C_online
5. 　　FOR c∈C_online：
6. 　　IF 随机数<$P_{disconnect}$：
7. 　　将c从C_online移除
8. 　　END FOR
9. 　　FOR c∉C_online：
10. 　　IF（随机数<$P_{reconnect}$）AND（r % interval == 0）：
11. 　　将c加入C_online
12. 　　END IF
13. 　　FOR c∈C_selected执行：
14. 　　训练本地模型M_c
15. 　　上传模型参数到服务器
16. END FOR
17. 在每轮训练结束时：
18. 　　更新全局模型和客户端模型

相比于传统的同步联邦学习，异步联邦学习更适应设备异构性和网络不稳定环境。它通过个性化更新和动态权重聚合机制，在保证全局模型性能的同时，支持客户端的个性化优化需求。最终，这一设计有效提升了系统的鲁棒性与灵活性，使联邦学习在复杂多变的环境中也能高效、稳定地进行。

3.3　SDN环境下DDoS检测与缓解

在完成上述工作后，我们在SDN环境下进行了DDoS实时监测与缓解。控制器通过OpenFlow协议集中管理数据流。利用Ryu控制器和OVS交换机进行DDoS攻击检测、流量管理。

由于DDoS攻击的复杂性和多样性，单一的缓解策略难以应对所有场景。因此，结合多种缓解技术可以显著提升系统的抗攻击能力。通过智能分析与行为检测相结合的方法，能够进一步提高DDoS防护的精准度和效果。为缓解DDoS攻击，我们采用了速率限制、IP封禁和信任值动态管理等综合策略进行缓解。具体的缓解算法如算法3所示。

算法3.　DDoS攻击缓解

输入：检测到的攻击者IP和受害者IP，初始信任值

输出：DDoS攻击缓解结果

1. 初始化信任值
2. 初始化blacklist = {}和trust_values = {}
3. FOR each detected attacker IP DO
4. 　　IF attacker IP ∈ blacklist THEN
5. 　　记录日志"攻击者已在黑名单中"跳过该攻击者
6. 　　CONTINUE
7. 　　END IF
8. 　　IF attacker IP ∉ trust_values THEN
9. 　　首次将attacker IP的信任值设置为 initial_trust_value
10. 　　否则trust_values[attacker IP]−1
11. 　　END IF
12. 　　IF trust_values[attacker IP] ⩽ 0 THEN

13. Block traffic from attacker IP
14. Add attacker IP to blacklist
15. 记录日志“攻击者IP已加入黑名单，流量已被阻止”
16. ELSE
17. 对攻击者IP应用速率限制；记录日志“对攻击者IP应用了速率限制”
18. END IF
19. END FOR

4 实验与分析

4.1 数据集

在本研究中，我们选用了三个不同的网络安全数据集：CICDDoS2019、CIC-IDS2017和InSDN，以全面评估和验证所提出的DDoS攻击检测方法。每个数据集都有其独特的特点和应用场景，能够为模型的泛化能力和适应性提供充分的测试支持。

CICDDoS2019[39]数据集是一个为网络安全研究设计的公共数据集，旨在帮助研究人员深入分析和理解分布式拒绝服务（DDoS）攻击。该数据集涵盖了多种常见的DDoS攻击类型，如UDP洪泛攻击、TCP SYN洪泛攻击等，模拟了真实网络环境下的多种攻击场景，包含详细的流量特征和标签，为DDoS检测研究提供了丰富的数据支持。

CIC-IDS2017[40]是一个广泛应用于网络入侵检测系统（IDS）评估和研究的数据集。该数据集涵盖了多种常见的网络攻击类型，包括端口扫描、网络钓鱼、Brute-force等，模拟了企业级网络环境中的正常流量和恶意流量，提供了多种流量特征和数据标签，以支持对入侵检测系统的全面评估。

InSDN[41]数据集则专注于软件定义网络（SDN）的入侵检测，专为检测和缓解DDoS攻击而设计。该数据集模拟了SDN环境中的真实网络流量，包括内部和外部来源的多种攻击类型，如DoS攻击、洪泛攻击等，同时记录了网络拓扑信息和流量统计特征，适用于研究在SDN环境下的攻击检测和防御方法。

4.2 实验环境与评估指标

本文实验环境是在CPU为Intel core i7-8700CPU @ 3.20 GHz 12核。GPU为NVIDIA RTX A4000，大小为16 G。内存的大小为298 G的服务器上进行一系列的评估实验。本文使用的编程语言是Python，版本为3.8，服务器使用的深度学习框架为Pytorch，版本为2.3.0。

此外，SDN实验环境使用Mininet 2.3.1进行配置，虚拟网络交换机运行Open vSwitch（OVS）版本3.4.0。网络控制器使用Ryu版本4.34实现，提供网络流量的集中管理。网络拓扑由五个交换机和十五个主机构成，模拟分布式DDoS攻击场景，使用hping发动DDoS攻击。

实验所选用的评估指标为准确率和F1-score。如公式（6）和公式（9）所示。

$$Accuracy=\frac{TP+TN}{TP+FP+TN+FN} \tag{6}$$

$$Precision=\frac{TP}{TP+FP} \tag{7}$$

$$Recall=\frac{TP}{TP+FN} \tag{8}$$

$$F1\text{-}score=2\times\frac{Precision\times Recall}{Precision+Recall} \tag{9}$$

TP（True Positives）表示真正例数；FN（False Negatives）表示假反例数；FP（False Positives）表示假正例数；TN（True Negatives）表示真反例数。

4.3 实验结果与分析

本实验利用CICDDoS2019、CIC-IDS2017和InSDN三个数据集构建了非独立同分布（Non-IID）数据集，旨在模拟真实网络环境中数据分布的不均匀性，以测试模型在异构数据条件下的适应性。为了实现这一目标，我们采用了Dirichlet分布来将数据分配至多个客户端。Dirichlet分布能够有效地模拟客户端之间在数据量和标签分布上的差异，反映出网络环境中不同流量类型的不均匀性。

具体而言，Dirichlet[42]分布被用来为每个客户端分配样本，其中客户端之间的数据标签比例存在显著差异。例如，某些客户端主要接收到高频率的DDoS攻击流量，而其他客户端则以正常业务流量为主。此外，客户端间的标签比例也不均衡，这种分配方式能够真实地反映出网络环境中的流量多样性。在数据量差异方面，部分客户端仅包含少量样本，而其他客户端则承担大量流量，从而有效地测试模型在数据量不均衡条件下的鲁棒性。

针对每个数据集，我们构建了15种不同的数据分布，并将这些数据分配给15个客户端。实验中，选取了5个、10个和15个客户端进行后续实验，以考察不同客户端数量下模型的表现。数据的具体分布和样本数量差异如表1所示。其中比例是指DDoS占总样本的比例。

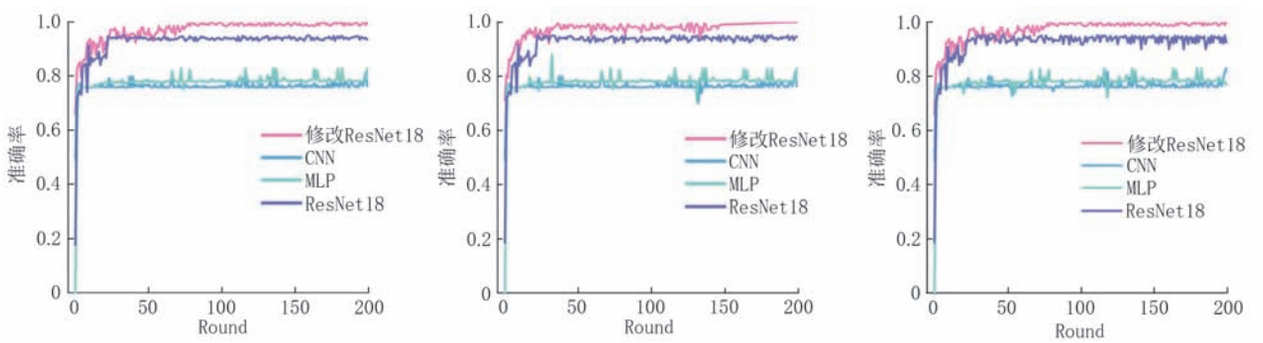
我们进行了多个实验，包括模型对比、联邦学习算法对比、异步性验证、消融实验、不同平衡因子的验证、多分类验证以及在SDN环境中的实验，以全面评估和验证AdaPerFed算法的性能与适应性。

表1　数据分布表

客户端	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
比例	1	0.75	0.5	0.25	0	0.2	0.3	0.4	0.05	0.1	0.6	0.15	0.8	0.9	0.5
正常流量	0	1500	4250	3750	5500	2400	2800	1200	5700	6300	3200	1700	600	400	2500
DDoS	4000	4500	4250	1250	0	600	1200	800	300	700	4800	300	2400	3600	2500

4.3.1　模型对比

为了验证我们改进后的ResNet18模型的性能，我们将其与CNN、MLP和未修改的ResNet18模型进行了对比。所有模型均采用我们提出的异步个性化联邦学习算法进行训练与评估，以确保在异构数据环境下对各模型的表现进行全面测试和验证。效果如图4所示。具体的实验结果如表2所示。



（a）CICDDoS2019数据集不同模型对比结果　（b）InSDN数据集不同模型对比结果　（c）CIC-IDS2017数据集不同模型对比结果

图4　不同深度学习模型对比图

表2　不同深度学习模型结果

模型	准确率		
	CICDDoS2019	CIC-IDS2017	InSDN
修改ResNet18	0.9990	0.9987	0.9992
CNN	0.7757	0.8132	0.8275
MLP	0.7817	0.8806	0.8278
ResNet18	0.9500	0.9532	0.9483

从表2可以看出，修改后的ResNet18模型在CICDDoS2019、CIC-IDS2017和InSDN数据集上的准确率均接近99%，显著优于原始ResNet18、CNN和MLP模型，表现出极高的稳定性和适应性。这表明对ResNet18模型的修改非常成功，使其在DDoS检测和入侵检测任务中效果显著提升。

实验结果显示，改进后的ResNet18模型在所有数据集上表现出显著优势，准确率在较高水平上稳定收敛，特别是在前30轮内便能快速达到稳定状态。而相比之下，原始ResNet18模型的收敛速度相对较慢，准确率略低。此外，CNN和MLP模型的准确率波动更为明显，表明它们在特征提取和泛化能力上较为不足。

这些结果表明，改进后的ResNet18深层结构更适合复杂的网络攻击检测任务，能够更有效地捕捉数据集中的多样化特征。因此，我们修改和定制的ResNet18模型不仅在收敛速度和准确率上超越了原始ResNet18模型，还在不同数据集上实现了更好的泛化性能，为高效、精准的攻击检测提供了可靠的技术支撑。

4.3.2　联邦学习算法对比

在本节中，我们将对比多种联邦学习算法在网络攻击检测任务中的性能，包括FedAvg[43]、FLAD[44]、FedALA[45]以及我们提出的AdaPerFed算法。FedAvg是一种经典的联邦学习算法，通过简单平均客户端模型权重实现聚合，但在异构数据环境下表现有限。FLAD引入了自适应动态调整机制，能够针对客户端的差异化数据特性优化聚合，提高模型的泛化性能。FedALA采用同步个性化策略，使得全局模型能够更好地适应客户端的个性化需求，在同步训练中平衡个体和全局性能。而我们设计的AdaPerFed算法在此基础上进一步优化，通过动态自适应聚合机制，更高效地处理异构数据和

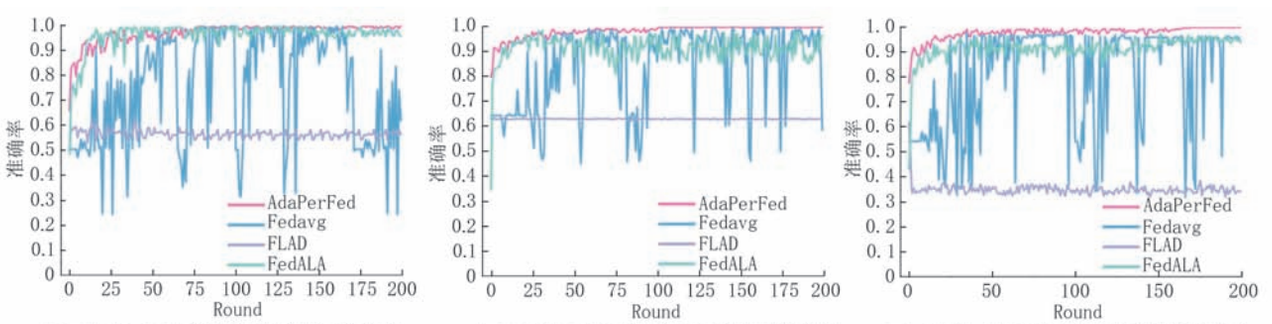
动态客户端环境，提升了模型的收敛速度和检测精度。通过实验，我们将验证这些算法在多个数据集上的性能差异，并突出AdaPerFed在泛化能力、个性化处理和模型鲁棒性方面的优势。

在本实验中，我们设置了不同数量的客户端来评估各个联邦学习算法的性能。为了深入探讨算法在不同数据规模和客户端数量下的表现，我们分别使用了5、10和15个客户端进行测试。这些客户端的数据为非独立同分布(Non-IID)。此外，实验中考虑了多个性能指标，涵盖了客户端和全局模型的各项表现。所有的算法均采用我们定制的ResNet18作为基础模型，以保证结果的公平性。

在CICDDoS2019数据集上的结果如图4，表3所示。从图5可以看出AdaPerFed在不同客户端数量下均表现出更高的准确率和更快的收敛速度。与FedAvg相比，准确率高约20%，波动减少；较FLAD高30%以上，泛化更好；较FedALA高10%-15%，波动更低。

表3 不同客户端在CICDDoS2019数据集上的结果

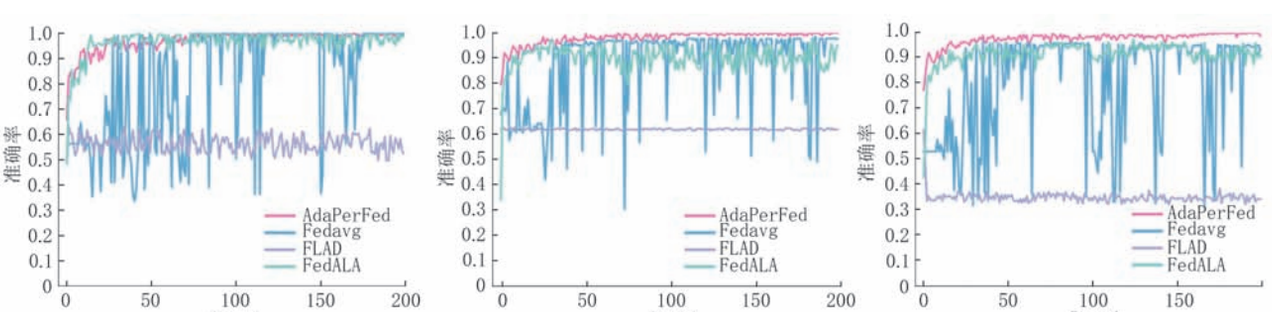
算法	准确率		
	5	10	15
AdaPerFed	0.9990	0.9970	0.9985
Fedavg	0.9986	0.9963	0.9400
FLAD	0.6612	0.6692	0.3420
FedALA	0.9973	0.9247	0.9435



(a) CICDDoS2019数据集5个客户端准确率 (b) CICDDoS2019数据集10个客户端准确率 (c) CICDDoS2019数据集15个客户端准确率

图5 不同客户端在CICDDoS2019数据集上的结果

在CIC-IDS2017数据集上的结果如图6、表4所示。总体来看，AdaPerFed在不同客户端数量下均表现出优异的准确率和稳定性，迅速收敛并保持在0.9以上，展现了出色的泛化能力和扩展性。相比之下，FedAvg波动较大，尤其在多客户端环境下不稳定；FLAD表现稳定但准确率偏低，一直在0.5到0.6之间；FedALA随客户端增加波动性加剧。AdaPerFed在各场景下相比其他算法准确率提升15%-30%，收敛更快、波动更小，展现了更好的稳定性和适应性。



(a) CIC-IDS2017数据集5个客户端总体准确率 (b) CIC-IDS2017数据集10个客户端准确率 (c) CIC-IDS2017数据集15个客户端准确率

图6 不同客户端在CIC-IDS2017数据集上的结果

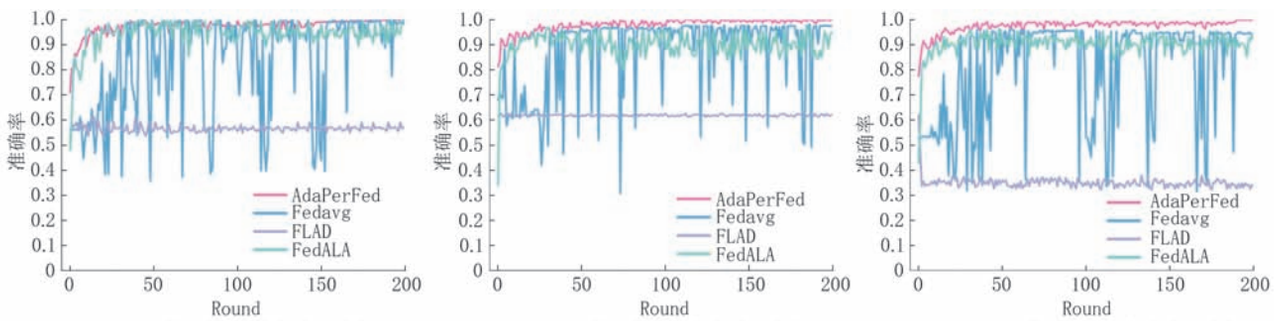
在InSDN数据集上的结果如图7、表5所示。从图6(a)可以看出AdaPerFed在不同客户端数量下均优于其他算法，相比FedAvg提升5%-10%，收敛更快，且在大规模客户端环境中展现了更好的稳定性和自适应性。综上所述，AdaPerFed相较于其他算法具备15%-20%的准确率提升，并能有效减少波动，展现出更强的自适应性和泛化能力，适合处理大规模异构数据场景。

表4　不同客户端在CIC-IDS2017数据集上的结果

算法	准确率		
	5	10	15
AdaPerFed	0.9987	0.9986	0.9995
Fedavg	0.9923	0.9776	0.9468
FLAD	0.5535	0.6187	0.3462
FedALA	0.9959	0.9517	0.9121

的F1分数，且随着客户端数量的增加，模型的稳定性和准确率未显著下降。

算法成功平衡了全局泛化与本地个性化需求，展现出在多客户端异构环境中的高度适应性和鲁棒性。无论是在客户端数量较少还是较多的情况下，算法都能稳定地保持高性能，并且在面对非独立同分布（Non-IID）数据时，依然能够有效处理数据分布差异，确保全局模型的准确性和稳定性。同时，个性化策略使得每个客户端能够在保证全局一致性的同时，更好地适应自身的特定需求，从而提升了整体系统的鲁棒性和灵活性。



（a）InSDN数据集5个客户端准确率　（b）InSDN数据集10个客户端准确率　（c）InSDN数据集15个客户端准确率

图7　不同客户端在InSDN数据集上的结果

表5　不同客户端在InSDN数据集上的结果

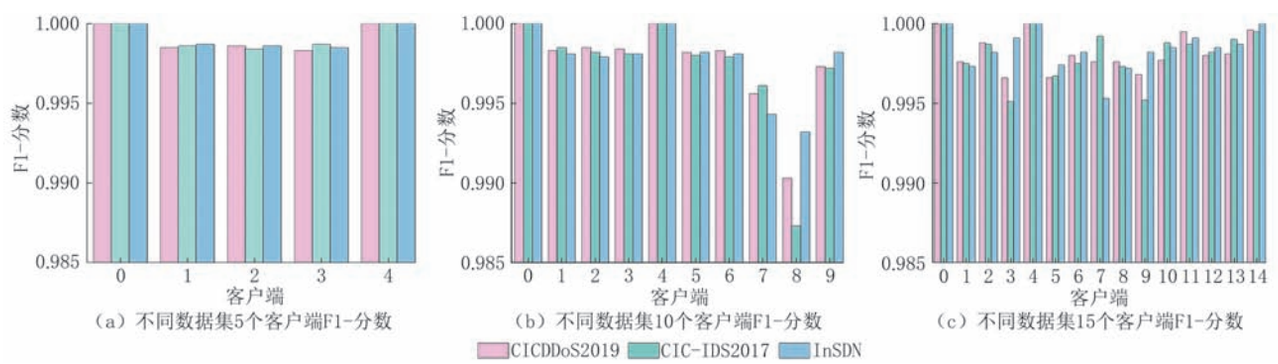
算法	准确率		
	5	10	15
AdaPerFed	0.9992	0.9993	0.9993
Fedavg	0.9843	0.9762	0.9443
FLAD	0.5690	0.6205	0.3252
FedALA	0.9936	0.9508	0.9247

AdaPerFed不仅在保证全局模型性能方面表现优异，还充分考虑了各客户端的个性化需求。在所有客户端上，全局模型展现出卓越的泛化能力和稳定性，具体结果如图8所示。AdaPerFed在不同数量的客户端和多个数据集（CICDDoS2019、CIC-IDS2017和InSDN）上的实验结果进一步验证了其全局和个性化能力的优越性。即使在非独立同分布（Non-IID）数据场景中，AdaPerFed依然保持了较高

4.3.3　异步性验证

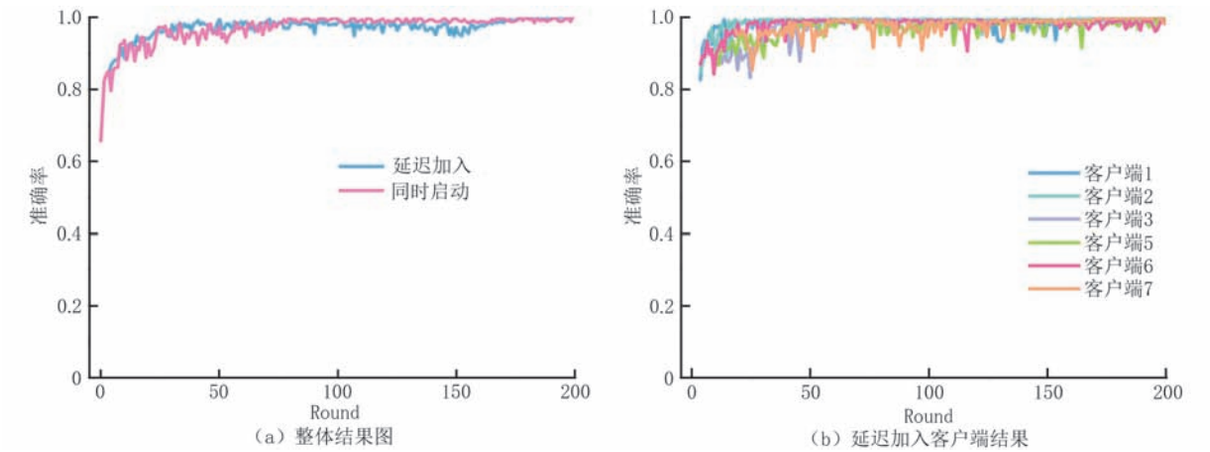
在本节中，我们验证了AdaPerFed在异步场景下的性能表现，重点关注了客户端断线、重连以及部分客户端永久下线的情况。针对这些挑战，我们设计了多种场景进行实验，以测试算法在真实网络环境中的鲁棒性和适应性。为了避免极端情况的影响，我们在下面的实验中没有选择客户端0和客户端4，选择了客户端1、2、3、5、6、7。

首先是延迟加入场景，我们选取的6个客户端，在训练开始后在随机轮次后加入实验。随机轮次的范围为[3,20]，结果如图9、表6所示。



（a）不同数据集5个客户端F1-分数　（b）不同数据集10个客户端F1-分数　（c）不同数据集15个客户端F1-分数

图8　客户端性能结果



（a）整体结果图 （b）延迟加入客户端结果

图9 延迟加入场景

表6 延迟加入结果

模型	准确率
全局	0.9989
延迟加入全局	0.9961
客户端1	0.9974
客户端2	0.9969
客户端3	0.9957
客户端5	0.9951
客户端6	0.9940
客户端7	0.9942

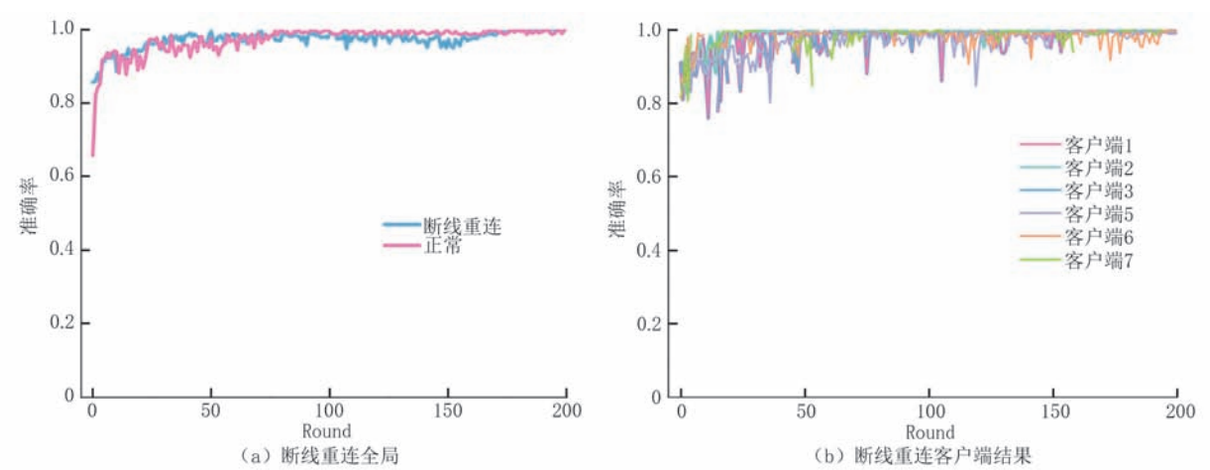
图9(a)展示了延迟加入与同时启动两种场景下的整体训练效果。虽然延迟加入的客户端在初期收敛速度较慢，但在约150轮后迅速达到与同时启动的结果几乎一致。这说明即便有客户端晚加入，模型仍能迅速适应，保持稳定的性能表现。

图9(b)展示了延迟加入客户端的具体表现。各客户端在训练初期虽有波动，但最终准确率均稳定在0.9以上，表明延迟加入不会对整体性能产生显著影响。

表6显示延迟加入全局模型的准确率为0.9961，略低于同步加入的全局模型(0.9989)，但差距非常小。所有客户端的性能最后均稳定在0.99以上，显示出较高的性能。说明延迟加入不会影响整体性能。

接着是断线重连验证，我们选取的6个客户端断线重连的概率为0%到25%，意味着有的客户端不会进行断线重连，断线重连的间隔设置为[3, 20]，结果如图10、表7所示。图10(a)展示了断线重连与正常训练情况下的全局模型表现。尽管存在客户端的断线和重连，全局模型的准确率仍稳定在0.9以上，表明系统具有较强的鲁棒性和对网络波动的适应能力。与正常训练相比，断线重连的曲线虽有波动，但最终结果趋于一致，说明客户端的断线不会显著影响全局模型的收敛效果。

图10(b)聚焦于客户端的准确率表现。初期各客户端的准确率有所波动，但随着训练轮次增加，即使在多次断线重连的情况下，各客户端准确率最终



（a）断线重连全局 （b）断线重连客户端结果

图10 断线重连结果图

表7　断线重连结果

模型	准确率
全局	0.9991
断线重连全局	0.9982
客户端1	0.9984
客户端2	0.9980
客户端3	0.9981
客户端5	0.9988
客户端6	0.9995
客户端7	0.9988

都收敛至稳定水平。这表明系统在异步环境中能够有效同步客户端状态，确保个性化模型的需求得到满足，同时断线不会对最终准确率产生重大影响。

表7显示全局模型在断线重连的情况下准确率为0.9982，与正常情况下的0.9991相近。客户端的结果也都稳定在0.998以上，显示出良好的适应性。

在永久断线中，我们设置客户端一开始全员在线，训练5轮后开始执行永久断线操作，永久断线的概率为0%-25%。结果如图11、表8所示。

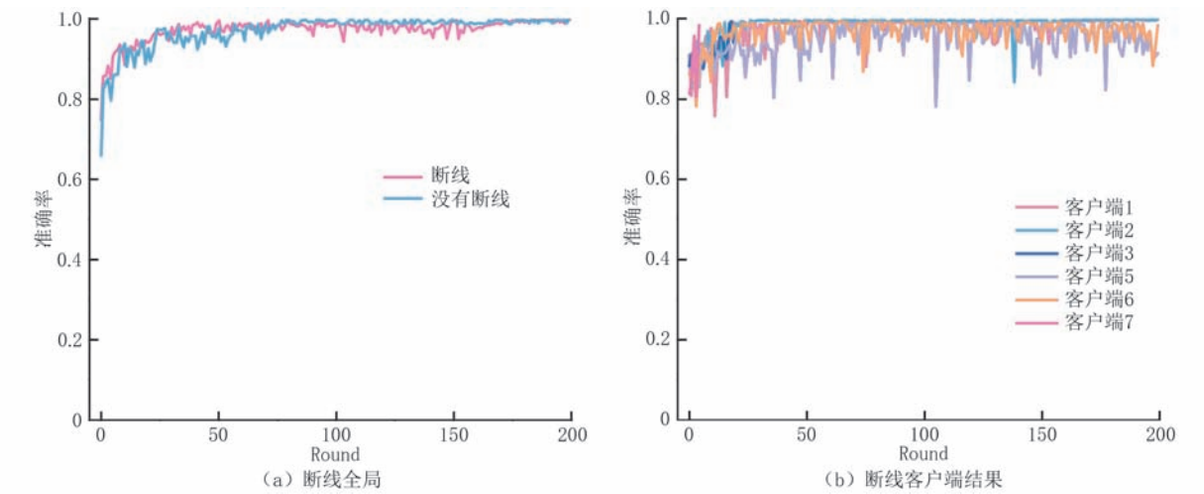


图11　永久断线结果图

表8　永久断线结果

模型	准确率
全局	0.9996
永久断线全局	0.9989
客户端1	0.9994
客户端2	0.9982
客户端3	0.9306
客户端5	0.9992
客户端6	0.9996
客户端7	0.9837

图11(a)展示了全局模型在部分客户端永久断线与无断线情况下的表现。即使客户端3、7未能参与完整训练，全局模型的准确率仍稳定在0.998以上，与无断线情况相近，显示出系统在部分客户端缺失时的良好收敛性和鲁棒性。

图11(b)展示了客户端个体表现。尽管客户端3和客户端7在永久断线后准确率较低，但其余客户端的准确率依然保持在0.998以上，表明剩余客户端的模型表现未受显著影响。

表8数据进一步验证了这一点。全局模型的准确率达到0.9989，与全员在线的情况几乎一致；这表明系统在客户端永久掉线的情况下，能够稳定其他客户端的表现，不影响整体模型的收敛和准确性。

总体而言，AdaPerFed在部分客户端永久掉线的异步环境中展现出卓越的适应性，能够在保证在线客户端性能稳定的同时，维持全局模型的鲁棒性和一致性。

本节实验通过延迟加入、断线重连和永久断线三种典型异步场景，系统性验证了AdaPerFed算法的鲁棒性与适应性。结果显示，无论客户端的加入时机或网络连接状态如何，AdaPerFed均能够实现高准确率，且在模型性能上保持较高的稳定性。

延迟加入实验表明，即便客户端在训练启动后延迟加入，系统依然能够迅速收敛，并达到与同时启动场景相近的性能水平。断线重连实验进一步证明了系统的适应能力，即使客户端在训练过程中频繁掉线并重新连接，系统的全局模型与个性化模型的准确率也未受显著影响。对于永久断线场景，即便部分客户端在训练中永久下线，系统依然维持整体模型的高准确率与鲁棒性。

综上所述，AdaPerFed在异步训练环境中展现出显著的鲁棒性和适应性，能够有效应对各种网络波动和客户端状态的动态变化，确保全局模型和个性化模型的稳定性和一致性，适应异步联邦学习的复杂应用需求。

4.3.4 消融实验

为了验证我们提出的基于性能向量的个性化更新算法的有效性，我们设计了两组消融实验，以评估AdaPerFed算法与传统加权平均方法的性能对比，以及Net模块在修改版ResNet18中的作用。在第一个实验中，我们去除了由性能向量驱动的个性化更新模块，仅使用加权平均方法进行模型聚合，从而评估个性化更新模块对整体系统性能的贡献。在第二个实验中，两个版本均采用AdaPerFed算法，旨在验证Net模块在提升模型性能中的作用。实验结果如图12所示。

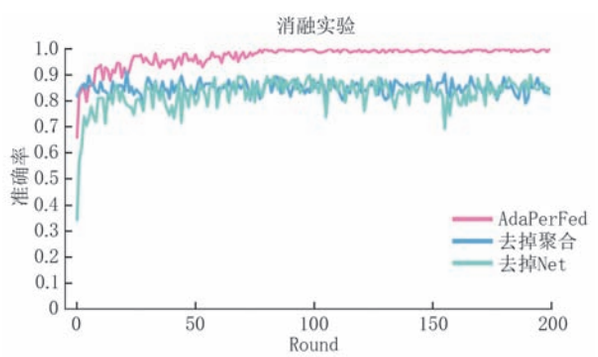


图12 消融实验

根据图12的结果，完整的AdaPerFed算法在全局准确率上明显优于去掉个性化聚合模块和去掉Net模块的版本，并且在训练过程中展现出更小的波动幅度。这表明，个性化更新、聚合模块以及Net模块在提升模型性能方面发挥了至关重要的作用，显著增强了AdaPerFed算法在异构数据环境中的适应性和稳定性。这一结果验证了基于性能向量的个性化更新策略和Net模块在异构联邦学习场景中的有效性与优越性。

4.3.5 不同平衡因子的验证

为了评估平衡因子对模型收敛性和稳定性的影响，我们设计了该实验，探究不同平衡因子(0.2、0.5、0.7和0.9)对模型准确率的作用。通过调整平衡因子，我们希望验证模型在处理非独立同分布数据时的稳健性与一致性表现。

实验结果如图13所示。无论平衡因子取值如何，模型均展现出良好的收敛性和高稳定性，准确率在训练初期迅速提升并趋于稳定。特别是在平衡因子为0.7时，模型准确率稍高且波动较小，表现出最佳性能。总体来看，模型在不同平衡因子下均展现出较强的稳健性，即使面对异构数据分布，仍能保持稳定且一致的准确率水平。这表明合理设置平衡因子能够增强模型的适应性和稳定性。

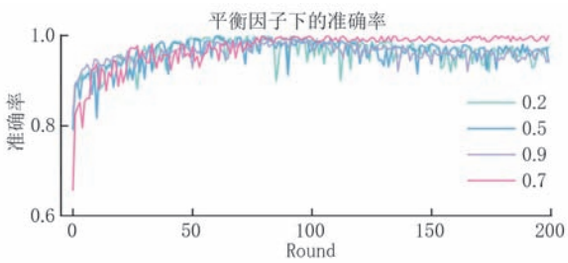


图13 平衡因子准确率图

4.3.6 多分类验证

为了验证多分类任务的效果，我们选取了CICDDoS2019数据集中的8类DDoS流量数据，进行了不均衡数据条件下的实验，实验结果如下图14所示。

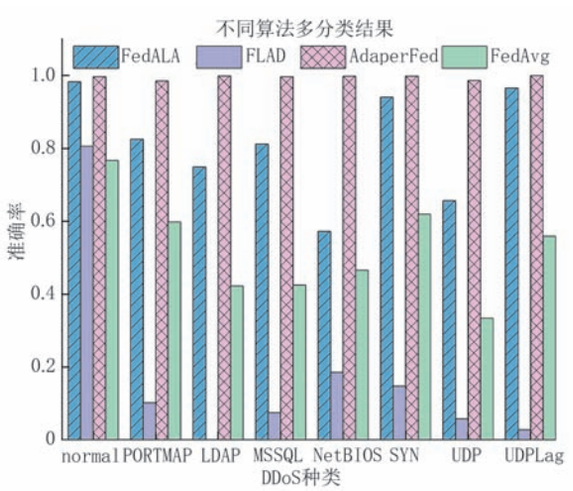


图14 多分类实验结果

在本次实验中，AdapterFed方法表现出色，在不均衡数据的挑战下依然展现了强大的分类能力。相比其他方法，AdapterFed能够更有效地适应数据的分布差异，提供了更高的分类准确率，特别是在较少样本的攻击类型上也能保持稳定的表现。这说明AdapterFed不仅能够捕捉多种类型DDoS流量的特征，还能在联邦学习环境中有效应对数据不均衡的情况，为多分类任务提供了更加鲁棒的解决方案。

4.3.7　SDN中的实验

在软件定义网络环境中，检测和防御DDoS攻击是至关重要的环节。SDN作为一种新型的网络架构，通过将网络的控制平面与数据平面分离，实现了网络资源的集中管理与灵活配置。通过集中式的控制器，SDN能够实时监控网络流量、分析网络状态，并在网络遭遇攻击时做出快速反应。这一架构使得网络管理员可以动态地调整流量策略和优化网络行为，特别是在面对复杂且突发的DDoS攻击时，具有显著优势。

在本文提出的框架中，当训练好的神经网络检测到DDoS攻击时，它会将攻击的特征和相关信息即时传递给SDN控制器。控制器根据接收到的检测结果，迅速生成并下发适当的DDoS缓解策略，如调整路由路径、隔离攻击源或修改流量过滤规则。通过这种机制，SDN控制器能够实时协调网络资源，执行精确的流量调度，从而有效缓解DDoS攻击带来的负面影响。相比传统的网络防御方法，SDN的集中控制能力使其能够快速适应网络环境的动态变化，提供更加高效和灵活的攻击响应方案。

为验证AdaPerFed算法在SDN环境中的有效性与适应性，我们设计了一个由十五个主机构成的实验，具体配置和流程如下：

实验拓扑如图15所示。在训练阶段，前十个主机（h1至h10）接收混合的正常流量和DDoS攻击流量，以增强模型对不同流量特征的辨别能力。主机h15则仅接收正常流量，以保证模型能区分纯净流量的特征。剩余四个主机（h11至h14）被配置为潜在攻击源，模拟网络环境中的DDoS攻击者。通过这种配置，模型可以在多源异构流量环境下进行训练，学习如何识别攻击流量与正常流量的差异。

在验证阶段，我们进一步测试模型在面对突发攻击时的检测与防御效果。在实验的前20秒内，指挥h11和h12向h15发送正常流量，正常流量的发送速率为每0.01秒发送一个数据包，确保模型建立对纯净流量的基线响应。在第20秒时，h13开始向h15发起DDoS攻击，DDoS攻击流量被设置为每0.001秒发送一个数据包，模拟突发攻击场景。此时我们监测模型的响应，评估其检测到异常流量并采取适当防御措施的能力。

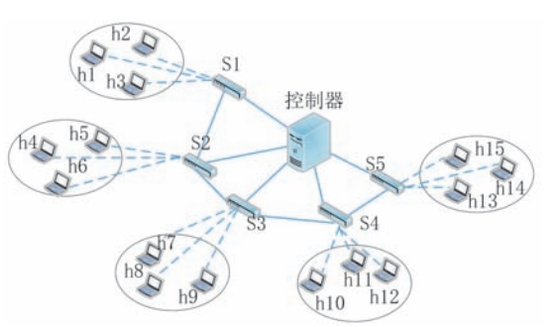


图15　实验拓扑图

实验结果如图16所示。结果显示，尽管h15在训练阶段仅学习了正常流量特征，但在实验进行到第20秒时，系统成功检测到h13发起的DDoS攻击，并通过联邦学习模型迅速启用缓解措施。在触发缓解策略后，流量在40秒后迅速下降并恢复到正常水平，表明系统在检测和防御突发攻击方面表现出色。

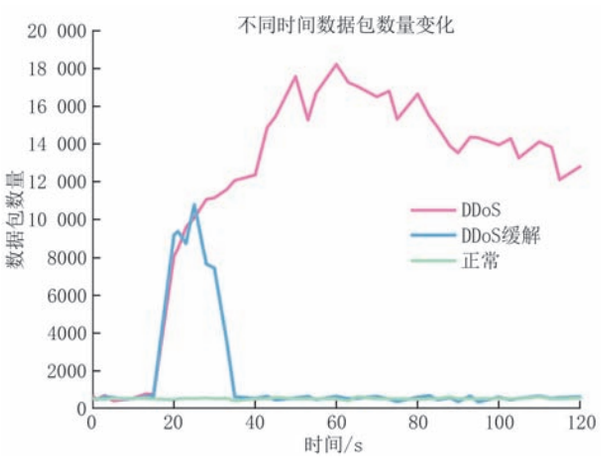


图16　数据包数据图

这一实验结果验证了AdaPerFed在SDN环境中的有效性和适应性，特别彰显了联邦学习框架的优势。即使h15在训练过程中未直接接触过DDoS流量，依托于联邦模型中由其他主机共享的学习成果，h15依然能够在突发攻击情境下快速识别威胁并采取有效的防御措施。这表明系统不仅能够适应异构数据环境，还能在未见过的攻击场景中保持高效的检测和缓解能力，为实际网络环境中的应用提供了有力的支持。

4.3.8　计算资源与通信开销评估

在联邦学习中，模型的计算资源消耗和通信开销是影响性能的重要因素。为了全面评估不同算法的效率，我们对修改版ResNet18和原始ResNet18进行了计算资源消耗的对比分析，结果如表9所示。

修改版ResNet18通过将原始的二维网络结构

表9 计算资源对比结果表

名称	计算资源消耗
修改版ResNet18	7.4%
ResNet18	17.4%

转化为一维网络，相比于原始ResNet18显著降低了计算资源消耗，从17.4%减少至7.4%。这种优化主要得益于一维卷积操作在计算复杂度上的降低，从而减少了每层的计算量和模型参数，进而降低了训练和推理过程中的计算负担。

同时对FedAvg、FLAD、FedALA以及我们提出的AdaPerFed算法的通信开销进行了比较。结果如图17所示。AdaPerFed通过冻结层和动态客户端选择策略，显著降低了通信开销。在算法设计上，冻结层减少了传输的模型参数数量，而动态选择客户端则避免了过多无效更新的传输。相较于传统的联邦学习算法（如FedAvg）和其他优化算法（如FLAD），AdaPerFed的通信开销更加精简，具有更高的通信效率。

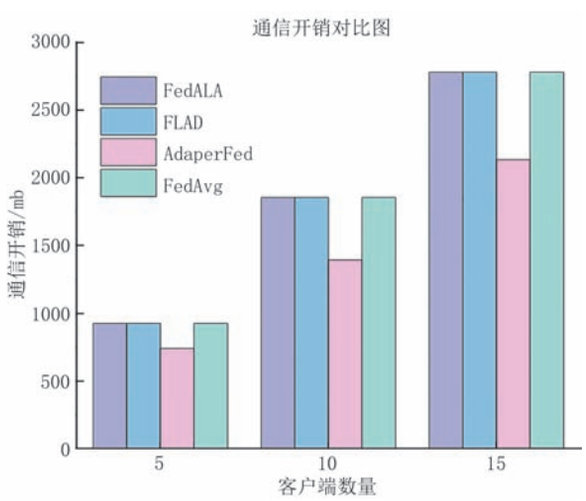


图17 不同联邦学习通信开销图

5 结 论

本文提出了一种基于异步个性化联邦学习的DDoS攻击检测与缓解方法，该方法通过定制化ResNet架构、高效的个性化联邦学习框架以及SDN环境中的动态缓解策略，全面提升了DDoS检测与防御的性能。在此方法中，我们通过1D卷积改进ResNet结构以更好地适应一维流量数据，同时通过引入Net模块提高特征提取能力，从而提高了DDoS攻击检测的精度。个性化联邦学习框架在解决非独立同分布（Non-IID）数据和设备异构性方面发挥了重要作用，通过异步机制减轻了同步通信的负担，提升了模型在真实网络环境中的适应性。此外，SDN环境中的缓解策略通过动态信任值管理、速率限制和黑名单机制，实现了对DDoS攻击的实时监测与高效防御。

实验结果表明，AdaPerFed在CICDDoS2019、CIC-IDS2017和InSDN等多个数据集上均优于传统联邦学习算法，在不同客户端数量和异步环境下展现出更快的收敛速度和更高的检测准确率。通过消融实验验证了个性化聚合模块的有效性，同时异步性实验表明，AdaPerFed在应对网络波动和客户端异步加入方面具有卓越的鲁棒性。在SDN环境中，AdaPerFed实现了对DDoS攻击的高效防御，证明了该模型的实际应用潜力。

总之，本研究通过异步个性化联邦学习方法成功应对了复杂网络环境中的数据异质性、网络不稳定和计算差异等挑战，为未来大规模分布式网络中的DDoS检测与防御提供了高效、可靠的解决方案。

参 考 文 献

[1] Mankawade A M, Kolpe P D, Pote A M, et al. A dynamic framework for DDoS attack detection and mitigation in software-defined network using machine learning//Proceedings of the 2024 International Conference on Intelligent Systems for Cybersecurity (ISCS), Gurugram, India, 2024: 1-7

[2] Agrawal N, Tapaswi S. Defense mechanisms against DDoS attacks in a cloud computing environment: State-of-the-art and research challenges. IEEE Communications Surveys & Tutorials, 2019, 21(4): 3769-3795

[3] Ahuja N, Singal G, Mukhopadhyay D, et al. Automated DDOS attack detection in software defined networking. Journal of Network and Computer Applications, 2021, 187: 103108-103124

[4] Rath K C, Khang A, Roy D. The role of Internet of Things (IoT) technology in Industry 4.0 economy//Proceedings of the Advanced IoT Technologies and Applications in the Industry 4.0 Digital Economy. Boca Raton, USA: CRC Press, 2024: 1-28

[5] Anley M B, Genovese A, Agostinello D, et al. Robust DDoS attack detection with adaptive transfer learning. Computers & Security, 2024, 144: 103962-103972

[6] Banitalebi Dehkordi A, Soltanaghaei M R, Boroujeni F Z. The DDoS attacks detection through machine learning and statistical methods in SDN. The Journal of Supercomputing, 2021, 77(3): 2383-2415

[7] Bazzi H S, Nassar A H, Haidar I M, et al. ResNet-based detection of SYN flood DDoS attacks//Proceedings of the 2024

IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT), Greater Noida, India, 2024: 1142-1147

[8] Bhayo J, Shah S A, Hameed S, et al. Towards a machine learning-based framework for DDoS attack detection in software-defined IoT (SD-IoT) networks. Engineering Applications of Artificial Intelligence, 2023, 123: 106432-106439

[9] Bhuvaneswari Amma N G, Selvakumar S. A statistical class center based triangle area vector method for detection of denial of service attacks. Cluster Computing, 2021, 24: 393-415

[10] Qi T, Zhang H, Zhao H, et al. Research on ECG Signal Classification Based on Hybrid Residual Network. Applied Sciences, 2024, 14(23): 11202-11217

[11] Cao Y, Jiang H, Deng Y, et al. Detecting and mitigating DDoS attacks in SDN using spatial-temporal graph convolutional network. IEEE Transactions on Dependable and Secure Computing, 2021, 19(6): 3855-3872

[12] Wabi A A, Idris I, Olaniyi O M, et al. Ddos attack detection in sdn: method of attacks, detection techniques, challenges and research gaps. Computers & Security, 2023, 139: 103652-103685

[13] Li J, Zhang Z, Li Y, et al. FIDS: Detecting DDoS through federated learning based method//Proceedings of the 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications. Shenyang, China, 2021: 856-862

[14] McMahan B, Moore E, Ramage D, et al. Communication-efficient learning of deep networks from decentralized data//Proceedings of the Machine Learning Research. Amsterdam, Netherlands, 2017: 1273-1282

[15] Lu X, Xiao L, Li P, et al. Reinforcement learning-based physical cross-layer security and privacy in 6G. IEEE Communications Surveys & Tutorials, 2022, 25(1): 425-466

[16] Pillai S E V S, Polimetla K. Mitigating DDoS attacks using SDN-based network security measures//Proceedings of the 2024 International Conference on Integrated Circuits and Communication Systems (ICICACS), Raichur, India, 2024: 1-7

[17] Pillai S E V S, Polimetla K. Integrating network security into software-defined networking (SDN) architectures//Proceedings of the 2024 International Conference on Integrated Circuits and Communication Systems (ICICACS), Raichur, India, 2024: 1-6

[18] Ayodele B, Buttigieg V. SDN as a defence mechanism: a comprehensive survey. International Journal of Information Security, 2024, 23(1): 141-185

[19] Ding D, Savi M, Siracusa D. Tracking normalized network traffic entropy to detect DDoS attacks in P4. IEEE Transactions on Dependable and Secure Computing, 2021, 19(6): 4019-4031

[20] GadallahWaheed G, IbrahimHosny M, OmarNagwa M. A deep learning technique to detect distributed denial of service attacks in software-defined networks. Computers & Security, 2024, 137:103588-103594

[21] Bazzi H S, Nassar A H, Haidar I M, et al. ResNet-based detection of SYN flood DDoS attacks//Proceedings of the 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT), Greater Noida, India, 2024: 1142-1147

[22] Hnamte V, Najar A A, Nhung-Nguyen H, et al. DDoS attack detection and mitigation using deep neural network in SDN environment. Computers & Security, 2024, 138: 103661-103680

[23] Doriguzzi-Corin R, Siracusa D. FLAD: adaptive federated learning for DDoS attack detection. Computers & Security, 2024, 137: 103597-103610

[24] Li J, Lyu L, Liu X, et al. FLEAM: A federated learning empowered architecture to mitigate DDoS in industrial IoT. IEEE Transactions on Industrial Informatics, 2021, 18(6): 4059-4068

[25] Zhang J, Yu P, Qi L, et al. FLDDoS: DDoS attack detection model based on federated learning//Proceedings of the 2021 IEEE 20th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom), Shenyang, China, 2021: 635-642

[26] Fotse Y S N, Tchendji V K, Velempini M. Federated Learning Based DDoS Attacks Detection in Large Scale Software-Defined Network. IEEE Transactions on Computers, IEEE Transactions on Computers, 2025, 74(1): 101-115

[27] Liu Yanhua, Fang Wenyu, Liu Ximeng, et al. DDoS Attack Detection Model in SDN Environment Based on Federated Incremental Learning. Chinese Journal of Computers, 2024, 47(12):2852-2866
(刘延华,方文昱,刘西蒙,等.基于联邦增量学习的SDN环境下DDoS攻击检测模型.计算机学报, 2024,47(12):2852-2866)

[28] Yin Z, Li K, Bi H. Trusted multi-domain DDoS detection based on federated learning. Sensors, 2022, 22(20): 7753-7778

[29] Dimolianis M, Kalogeras D K, Kostopoulos N, et al. DDoS attack detection via privacy-aware federated learning and collaborative mitigation in multi-domain cyber infrastructures//Proceedings of the 2022 IEEE 11th International Conference on Cloud Networking (CloudNet). Paris, France, 2022: 118-125

[30] Chen Y, Qin X, Wang J, et al. Fedhealth: A federated transfer learning framework for wearable healthcare. IEEE Intelligent Systems, 2020, 35(4): 83-93

[31] Wu Q, He K, Chen X. Personalized federated learning for intelligent IoT applications: A cloud-edge based framework. IEEE Open Journal of the Computer Society, 2020, 1: 35-44

[32] Fallah A, Mokhtari A, Ozdaglar A. Personalized federated learning with theoretical guarantees: A model-agnostic meta-learning approach. Advances in Neural Information Processing Systems, 2020, 33: 3557-3568

[33] Liang J, Cheng W, Sun L, et al. Federated meta-learning with fast convergence and efficient communication//Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery & Data Mining (KDD). Anchorage, USA, 2019: 1015-1023

[34] Dinh CT, Tran N, Nguyen J. Personalized federated learning

with moreau envelopes. Advances in Neural Information Processing Systems, 2020, 33: 21394-21405

[35] Thein T T, Shiraishi Y, Morii M. Personalized federated learning-based intrusion detection system: Poisoning attack and defense. Future Generation Computer Systems, 2024, 153: 182-192

[36] Su X, Zhang G. APFed: Adaptive personalized federated learning for intrusion detection in maritime meteorological sensor networks, Digital Communications and Networks, 2024, 134:1-13

[37] Luo Y, Chen X, Sun H, et al. Securing 5G/6G IoT Using Transformer and Personalized Federated Learning: An Access-Side Distributed Malicious Traffic Detection Framework. IEEE Open Journal of the Communications Society, 2024, 5: 1325-1339

[38] Nair A S, Hoffrogge P, Czurratis P, et al. 1D-ResNet Framework for Ultrasound Signal Classification//International Symposium for Testing and Failure Analysis. ASM International, 2022, 84437: 21-27

[39] Sharafaldin I, Lashkari A H, Hakak S, Ghorbani A A. Developing realistic distributed denial of service (DDoS) attack dataset and taxonomy//Proceedings of the 2019 International Carnahan Conference on Security Technology (ICCST), Chennai, India, 2019: 1-8

[40] Elsayed M S, Le-Khac N-A, Jurcut A D. InSDN: A novel SDN intrusion dataset. Sensors, 2020, 8: 165263-165284

[41] Sharafaldin I, Lashkari A H, Ghorbani A A. Toward generating a new intrusion detection dataset and intrusion traffic characterization//Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP), Funchal, Portugal, 2018

[42] Kim G, Kim J, Han B. Communication-efficient federated learning with accelerated client gradient//Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR), Seattle, USA, 2024: 12385-12393

[43] McMahan B, Moore E, Ramage D, et al. Communication-efficient learning of deep networks from decentralized data//Proceedings of the 20th International Conference on Artificial Intelligence and Statistics (AISTATS), Fort Lauderdale, USA, 2017: 1273-1282

[44] Doriguzzi-Corin R, Siracusa D, FLAD: Adaptive Federated Learning for DDoS attack detection, Computers & Security, 2024, 137:103597-103610

[45] Zhang J, Hua Y, Wang H, et al. FedALA: Adaptive local aggregation for personalized federated learning//Proceedings of the 37th AAAI Conference on Artificial Intelligence (AAAI), Washington, USA, 2023, 37(9): 11237-11244

ZHU Hai-Ting, Ph. D., lecturer. Her primary research areas include network measurement, network management, and network security.

WEI Ming-Gang, M. S. candidate. His research interest is network security.

LIU Feng-Ning, M. S. candidate. Her research interest is federated learning.

HE Gao-Feng, Ph. D., associate professor. His research interests include network traffic analysis and IoT security.

ZHANG Lu, Ph. D., associate professor. His research interests include data mining and cybersecurity.

Background

This study focuses on DDoS attack detection within network traffic classification. DDoS attacks, which flood targets with traffic and disrupt services, pose a serious threat to network security. With the rise of IoT and vehicular networks, the number of IoT devices is expected to reach 26.4 billion by 2026, increasing the risk of attacks. Effective DDoS defense strategies are crucial for maintaining network security.

Although traditional machine learning methods (such as KNN, SVM) have shown some effectiveness in DDoS detection, they face limitations with complex, large-scale traffic data. Deep learning improves detection accuracy but suffers from issues such as vanishing gradients, network degradation, and overfitting, especially with imbalanced data. Centralized detection models also encounter challenges in real-world applications, such as privacy, security, and device performance differences, limiting their applicability in dynamic network environments.

To address these challenges, this study proposes an asynchronous personalized federated learning method for DDoS detection and mitigation, incorporating a customized ResNet architecture and Net module to enhance feature extraction. Using software-defined networking (SDN) to simulate complex environments, the asynchronous learning mechanism effectively handles variations in device computing power and network conditions, enabling efficient and robust DDoS

detection. The proposed model outperforms existing methods on datasets such as CICDDoS2019, demon-strating excellent detection performance and adaptability.

This work was supported by the Foundation: National Natural Science Foundation of China (No. 62272237), Youth Fund of National Natural Science Foundation of China (No. 52105553, No. 61802207), the Key Project of Natural Science Research in Jiangsu Provincial Colleges and Universities (No. 22KJA520005), Open Project of Key Laboratory of Computer Networks and Information Integration of the Ministry of Education (Southeast University) (K93-9-2023-04), and the QingLan Project of Jiangsu Province.