基于联邦增量学习的SDN环境下DDoS攻击检测模型

刘延华[1),2),4),5)] 方文昱[1),4),5)] 郭文忠[1),2),4),5)]
赵宝康[3)] 黄 维[1),4),5)]

[1)](福州大学计算机与大数据学院 福州 350108)
[2)](福州大学至诚学院 福州 350002)
[3)](国防科技大学计算机学院 长沙 410073)
[4)](大数据智能教育部工程研究中心 福州 350108)
[5)](福建省网络计算与智能信息处理重点实验室(福州大学) 福州 350108)

摘 要 SDN是一种被广泛应用的网络范式.面对DDoS攻击等网络安全威胁,在SDN中集成高效的DDoS攻击检测方法尤为重要.由于SDN集中控制的特性,集中式DDoS攻击检测方法在SDN环境中存在较高的安全风险,使得SDN的控制平面安全性受到了巨大挑战.此外,SDN环境中流量数据不断增加,导致复杂流量特征的更复杂化、不同实体之间严重的Non-IID分布等问题.这些问题对现有的基于联邦学习的检测模型准确性与鲁棒性的进一步提高造成严重阻碍.针对上述问题,本文提出了一种基于联邦增量学习的SDN环境下DDoS攻击检测模型.首先,为解决集中式DDoS攻击检测的安全风险与数据增量带来的Non-IID分布问题,本文提出了一种基于联邦增量学习的加权聚合算法,使用动态调整聚合权重的方式个性化适应不同子数据集增量情况,提高增量聚合效率.其次,针对SDN环境中复杂的流量特征,本文设计了一种基于LSTM的DDoS攻击检测方法,通过统计SDN环境中流量数据的时序特征,提取并学习数据的时序关特征的相关性,实现对流量特征数据的实时检测.最后,本文结合SDN集中管控特点,实现了SDN环境下的DDoS实时防御决策,根据DDoS攻击检测结果与网络实体信息,实现流规则实时下发,达到有效阻断DDoS攻击流量、保护拓扑重要实体并维护拓扑流量稳定的效果.本文将提出的模型在增量式DDoS攻击检测任务上与FedAvg、FA-FedAvg和FIL-IIoT三种方法进行性能对比实验.实验结果表明,本文提出方法相比于其他方法,在DDoS攻击检测准确率上提升5.06%~12.62%,$F1$-Score提升0.0565~0.1410.

关键词 联邦学习;联邦增量学习;网络安全;DDoS攻击检测;软件定义网络
中图法分类号 TP309 **DOI号** 10.11897/SP.J.1016.2024.02852

Federated Incremental Learning Based DDoS Attack Detection Model in SDN Environment

LIU Yan-Hua[1),2),4),5)] FANG Wen-Yu[1),4),5)] GUO Wen-Zhong[1),2),4),5)]
ZHAO Bao-Kang[3)] HUANG Wei[1),4),5)]

[1)](*College of Computer and Data Science, Fuzhou University, Fuzhou* 350108)
[2)](*Zhicheng College, Fuzhou University, Fuzhou* 350002)
[3)](*College of Computer, National University of Defense Technology, Changsha* 410073)

收稿日期:2024-01-18;在线发布日期:2024-09-19. 本课题得到国家自然科学基金重点项目(U21A20472,U22B2005)、国家自然科学基金青年科学基金项目(62406070)、国家重点研发计划项目(2021YFB3600503)、福建省自然科学基金项目(2021J01625,2021J01616)、福建省科技重大专项(2021HZ022007)、福建省技术创新重点攻关及其产业化项目(2024G018)、福州市科技重大项目(2023-ZD-003)资助.
刘延华,博士,教授,中国计算机学会(CCF)高级会员,主要研究领域为网络空间安全、智能计算及应用等. E-mail: lyhwa@fzu.edu.cn. **方文昱**,硕士研究生,主要研究领域为联邦学习、网络空间安全等. **郭文忠**,博士,教授,博士生导师,主要研究领域为多媒体智能信息处理、网络计算与分析、数据挖掘等. **赵宝康**,博士,副教授,主要研究领域为互联网、网络空间安全等. **黄 维**,博士,讲师,主要研究领域为联邦学习、城市计算等.

[4](*Engineering Research Center of Big Data Intelligence, Ministry of Education, Fuzhou* 350108)
[5](*Fujian Key Laboratory of Network Computing and Intelligent Information Processing (Fuzhou University), Fuzhou* 350108)

Abstract Software-Defined Networking (SDN) is a widely adopted network paradigm characterized by the separation of the control plane from the data plane. In light of network security threats, particularly Distributed Denial of Service (DDoS) attacks, the integration of effective DDoS attack detection methods within SDN is of paramount importance. The centralized control characteristic of SDN presents significant security risks when employing centralized DDoS attack detection methods, thereby posing considerable challenges to the security of the control plane in SDN environments. Furthermore, the growing volume of traffic data in SDN environments results in challenges related to more intricate traffic characterization and a pronounced Non-Independent and Identically Distributed (Non-IID) distribution among various entities. These issues present significant barriers to enhancing the accuracy and robustness of current federated learning-based detection models. The separation of management and control in SDN facilitates the creation of new flow rules by users, which enhances the efficiency of message routing control. However, current methodologies for flow detection face difficulties in preserving the knowledge of original features while simultaneously adapting to the distribution of newly generated features within the SDN environment. This challenge contributes to a phenomenon known as data forgetting. Furthermore, the imposition of flow rules restricts the forwarding targets of messages, resulting in variability in the data messages that can be collected by different host entities. The Non-IID distribution problem significantly undermines the performance and robustness of DDoS attack detection models that utilize artificial intelligence. To address these challenges, we propose a federated incremental learning-based model for DDoS attack detection within an SDN environment. This model integrates incremental learning and federated learning to accommodate new data inputs through incremental model updates, thereby eliminating the need for global re-training of the entire model. To mitigate the security risks associated with centralized DDoS attack detection methods and to address the Non-IID distribution issues arising from data increments, we introduce a weighted aggregation algorithm grounded in federated incremental learning. This algorithm personalizes adaptation to different sub-dataset increments by dynamically adjusting aggregation weights, thereby enhancing the efficiency of incremental aggregation. Additionally, in response to the complex traffic features inherent in SDN networks, we propose a DDoS attack detection methodology that employs Long Short-Term Memory (LSTM) networks. This approach enables real-time detection of traffic features by extracting and learning the temporal correlations present in the data, utilizing statistical analysis of the temporal characteristics of traffic data within SDN networks. Finally, by integrating the unique characteristics of SDN networks, we facilitate real-time decision-making for DDoS defense. This integration combines the results of DDoS attack detection with information pertaining to network entities, enabling the real-time deployment of flow rules. Concurrently, this approach effectively mitigates malicious DDoS attack traffic, safeguards critical entities, and ensures the stability of network topology. In this study, we evaluate the performance of the proposed method against existing techniques, including FedAvg, FA-FedAvg, and FIL-IIoT, in the context of an incremental DDoS attack detection task. The experimental results indicate that the proposed method enhances the accuracy of DDoS attack detection by an improvement range of 5.06% to 12.62% and increases the F1-Score by 0.0565 to 0.1410 when compared to alternative methods.

Keywords federated learning; federated incremental learning; cybersecurity; DDoS attack detection; software-defined networks

1 引 言

DDoS(Distributed Denial of Service, DDoS)攻击是一种通过控制大量僵尸机器向目标主机发起的分布式攻击[1],会导致目标实体出现宕机、服务不可用等问题,给网络通信带来巨大损失[2-3]. SDN(Software-Defined Networking, SDN)作为一种现代网络范式,被广泛应用到物联网、工业互联网等领域中[4]. SDN通过采用网络虚拟化技术,将控制平面与数据平面分离开来,使网络流量控制变得更加灵活,为实现DDoS防御策略实时部署提供了集中式的可行解决方案[5-6].

然而,SDN集中控制的特性使SDN中心控制器在公开网络中更容易成为恶意攻击的目标. 因此,针对SDN的DDoS攻击活动,往往会造成控制平面受损、策略失效、数据流篡改等问题[6-7]. 这使SDN的安全性面临巨大挑战,主要包括以下三个方面:

(1)SDN环境下的集中控制方式,对DDoS攻击具有更高的脆弱性. 目前基于集中式机器学习的DDoS攻击检测方法,在SDN环境下需要选择特定的训练中心与检测中心[6],而这个训练中心与检测中心则更容易成为恶意攻击的目标,从而导致SDN环境中的DDoS攻击检测系统出现整体瘫痪. 因此,基于集中式机器学习的DDoS攻击检测方法,在SDN环境下难以发挥作用.

(2)SDN环境下不断产生新的流规则和流量数据,对机器学习模型将导致明显的数据遗忘问题和Non-IID(Non-Independent and Identically Distributed)分布问题. 针对上述场景,目前已有的DDoS攻击检测方法难以兼顾不断产生的新特征分布与原有特征分布的知识,从而容易导致产生数据遗忘问题[8-9]. 此外,不同主机实体能够接收的数据报文各不相同,这使得不同实体之间将会产生数据的统计性异构问题,即Non-IID分布问题[10]. 因此,基于人工智能的DDoS攻击检测模型,需要在计算性能及鲁棒性等方面克服上述问题,进一步提升检测能力.

(3)SDN环境存在更多复杂流量特征需要分析与学习. 在SDN环境下,由于控制器、流表以及对应的控制协议等的实现,相比于非SDN环境,要处理的网络流量特征则更加复杂和多样化,这使得DDoS攻击检测模型需要进行更多轮次的迭代与拟合,加重了训练DDoS攻击检测模型的成本负担. 因此,SDN环境下的DDoS攻击检测模型,需要考虑复杂流量特征的简约化.

针对上述若干挑战,联邦学习(Federated Learning, FL)[11]模型提供了良好的解决途径. FL具有数据不离开本地的分布式训练方式,相较于集中式学习节约了数据通信成本、保护数据隐私. FL能够广泛地学习不同网络实体的流量特征和流表特征,以提高SDN环境下DDoS攻击检测和控制平面决策准确性[12]. 因此,使用FL模型实现DDoS攻击检测的相关研究成果逐渐增加[13-15].

针对FL模型的数据遗忘问题和Non-IID问题,联邦增量学习(Federated Incremental Learning, FIL)给出可行解决方法. FIL结合了增量学习和联邦学习,能在不重新训练整个模型的情况下,通过增量式的模型更新方式来适应新的数据输入[16]. 在工业物联网和区块链等领域,已提出了面向不同场景的FIL方法[17-20].

借鉴上述研究思路,本文提出了一种基于FIL的SDN环境下DDoS攻击检测模型. 针对SDN流量数据进行特征抽取与统计,通过FIL方法聚合分布各异的网络实体的训练模型,并对DDoS攻击流量进行检测和决策,提高DDoS攻击检测的准确性和实时性. 本文主要工作如下:

(1)针对挑战(1)与挑战(2),本文提出了一种基于联邦增量学习的加权聚合算法. 面向SDN环境内分布式DDoS攻击检测,针对数据增量导致的数据遗忘问题和Non-IID问题,提出有效的模型聚合方案. 根据不同实体能够捕获到的数据增量与积累情况,使用动态权重式的联邦聚合策略,对不同实体的训练模型实现有效聚合.

(2)针对挑战(3),本文提出了一种基于LSTM的DDoS攻击检测方法,提取分析SDN中复杂得流量数据的时间关联性特征,实现对流量特征数据的实时检测. 本文使用CICFlowMeter[21]提取SDN流量数据中的时间统计特征,实时捕获与抽取SDN环境中流量数据的流表特征与一般流量特征. 本文使用LSTM进行复杂数据流量特征的关联性分析与学习,以实现流量数据特征和IP信息匹配的快速分析与处理.

(3)在上述工作的基础上,本文实现了SDN环境下的DDoS实时防御决策. 结合上述DDoS攻击检测结果与网络实体信息的精确匹配,实现了流规则实时下发技术,达到有效阻断DDoS恶意攻击流

量、保护拓扑重要实体的效果.

2　相关工作

2.1　SDN环境下DDoS攻击检测研究

SDN集中管控的特性简化了DDoS攻击检测模型构建的复杂性，使得多视角、全局性的DDoS攻击识别及防御成为可能[22-25].

针对SDN的外部DDoS攻击检测问题，李传煌等人[26]提出了一种基于深度学习混合模型的DDoS攻击检测方法DCNN-DSAE，该方法在构建深度学习模型时，输入特征除了从数据平面提取的21个流量特征字段外，并手动标记了用于区分流类型的5个额外特征. 针对SDN中低速率拒绝服务攻击(Low-rate Denial of Service，LDoS)的检测问题，Tang等人[27]提出了一种轻量级的实时框架，以较低的系统成本实现实时攻击检测和缓解. Mousavi等人[28]则基于SDN的集中控制模式，提出了一种基于目的IP地址熵变化的DDoS攻击检测方案.

为了降低DDoS攻击对网络全局的影响，Hormozi等人[29]使用SDN控制器来引导DDoS攻击流，使DDoS攻击对网络拓扑的影响达到最小，保证了网络其余部分的安全. Dumka等人[30]分析了DDoS攻击对SDN通信性能的影响，进而提出了一种提高网络性能的新算法，该算法通过对IP地址的跟踪，实现了对洪泛型DDoS攻击的有效防范，保证了网络系统的稳定性. Najar等人[31]提出了一种基于平衡随机采样和卷积神经网络的DDoS攻击检测方法，提高了SDN中DDoS攻击检测的准确率.

针对SDN中的流量特征学习，Tang等人[32]提出了一种基于Learning-To-Rank (LtR)的方案，用于缓解针对流表的低速DDoS攻击. Gadallah等人[33]针对SDN控制平面和数据平面的DDoS攻击，提出了一种面向流量特征提取的深度学习模型学习方法，解决了针对SDN的特殊DDoS攻击检测困难的问题.

分析上述已有研究工作，SDN环境下的DDoS攻击检测中广泛应用了深度学习与流量特征统计技术.

2.2　基于联邦学习的DDoS攻击检测研究

流量特征分析，需要收集不同用户的流量数据，这对用户信息隐私安全存在潜在威胁. 若不能收集较为全面的流量数据，基于深度学习的DDoS攻击检测模型，则不能学习到完整的数据空间分布特征[34]，检测准确率难以保证. FL模型在不需要数据离开本地的情况下，能够对各网络实体开展分布式训练，可以有效克服上述问题. 因此，基于FL的DDoS攻击检测方法受到广泛关注.

Li等人[35]提出了一种基于FL的DDoS攻击检测模型，并结合模糊计算技术，提高了检测精度. Zhang等人[36]提出了FLDDoS模型，它是一种基于FL的DDoS攻击检测模型，针对数据集分布不平衡问题，提出了基于K-Means分层聚合算法和数据重采样方法. Yin等人[37]提出了一种基于FL的可信多域DDoS攻击检测方法，在保护各域数据隐私的前提下，实现了更全面的DDoS攻击检测. Narmadha等人[38]提出了一种新的FL隐私保护方法，有效提升DDoS防御能力. Dimolianis等人[39]提出了一种用于DDoS攻击检测的FL框架，通过引入可信实体，实现检测模型中敏感信息的隐私保护. Pourahmadi等人[40]开发了一种新颖的跨孤岛FL框架，旨在更好解决数据孤岛问题，实现高精度的智能DDoS攻击检测. 梁俊威等人[41]针对工业领域中的数据孤岛和隐私泄露问题，提出了一种适用于工业物理系统的安全协作入侵检测方法，实现了对各种类型攻击的有效检测. Abou等人[42]为了保护不同SDN域实体之间的隐私安全，提出了一种基于FL与区块链的全局入侵检测模型，实现了跨域的安全威胁检测.

针对低速DDoS攻击检测，Ali等人[43]提出了一种采用加权FL的DDoS攻击检测方法，为低速DDoS攻击检测提供了新思路. Liu等人[44]研究了一种基于双向LSTM和注意力机制的异步FL仲裁框架，以节约低速DDoS攻击检测中的通信开销.

2.3　联邦增量学习研究

FIL是一种将FL与增量学习相结合的分布式学习技术，在解决据遗忘问题和Non-IID分布问题上，具备更好的性能优势[45-46]. FIL已在相关领域取得了一些研究进展，但在DDoS攻击检测方面尚未发现具有代表性的研究成果.

针对Non-IID分布问题，崔腾等人[18]提出了一种结构与参数并行优化的联邦增量迁移学习方法，通过FIL，建立了基于模型输出信息的联邦共识组织，并利用横向FL进行模型增强. 面向工业物联网中的数据异构问题，刘晶等人[20]提出一种基于FIL的工业物联网数据共享方法，根据参与方等级值动态调整参与子集，通过计算参与方的增量聚合权重，实现对新增数据的有效学习. 为了缓解AI模型训

练流式数据存在模型性能差、训练效率低等问题，姜慧等人[19]提出了一种面向异构流式数据的高性能联邦持续学习算法，以提升模型对旧数据的分类能力.

此外，有不少研究者聚焦于优化聚合权重分配[47-50]，如引入模型贡献度、信誉机制等，自适应地产生不同局部模型的聚合权重. 也有部分研究者在训练过程引入注意力机制等，来动态产生模型聚合权重，以达到适应数据量变化的目的[51-52].

3 基于联邦增量学习的DDoS攻击检测模型

3.1 威胁建模与解决方法

本文结合相关研究工作，对SDN环境中可能存在的潜在威胁进行威胁建模. 本文主要聚焦SDN网络内部恶意用户对不同实体产生的攻击，具体包括：

(1)对内部正常用户的DDoS攻击. 这类攻击是指由SDN环境中恶意用户实体对特定的正常用户实体发起的DDoS攻击，攻击目的是使被攻击的正常用户实体功能瘫痪.

(2)对DDoS攻击检测中心的DDoS攻击. 这类攻击是指SDN环境中恶意实体对DDoS攻击检测中心发起的攻击行为，攻击目的是使检测中心停止服务，即DDoS攻击检测功能失效.

针对上述攻击威胁，本文提出一种基于FIL的SDN环境下DDoS攻击检测模型，并进一步实现对DDoS攻击的防御决策.

为检测针对内部正常用户的DDoS攻击，本文研究基于CICFlowMeter的特征提取方法与基于LSTM的深度学习模型，对网络内用户接收到的历史流量数据进行时序统计特征提取，进而对获得的特征数据进行分析与学习，实现高效的DDoS攻击检测.

为检测针对DDoS攻击检测中心的DDoS攻击，本文采用基于FIL的模型聚合与模型部署，采用分布式的模型训练和部署方式，增强检测模型在局部本地DDoS攻击检测的模型性能，避免集中式DDoS攻击检测中心存在的潜在风险.

进一步，本文结合基于ODL-API的流规则控制方法，实现对SDN环境下的DDoS攻击的实时防御决策.

3.2 模型概述

本文提出的基于FIL的SDN环境下DDoS攻击检测模型框架如图1所示. 本文框架中主要包括了以下四种实体：

(1)正常用户

正常用户，是指正常使用网络与其他网络实体进行通信，以获取远程服务的良好用户实体. 正常用户在请求的通信内容、通信数据大小与请求频率等各方面，均难以对网络通信功能造成严重破坏或负担. 在本文框架中，正常用户还可以通过部署DDoS攻击检测模型，以实现分布式的DDoS攻击检测.

(2)恶意用户群体

恶意用户群体，是指企图通过对正常用户实体进行DDoS攻击，以达到令被攻击实体无法正常提供服务能力的用户实体集合. 恶意用户群体可以组织高频率、数据量大的DDoS攻击，对正常用户实体或网络通信造成破坏和负担.

(3)聚合服务器

聚合服务器实体，是指为SDN网络拓扑中参与FIL的用户实体提供模型聚合服务的功能性实体. 聚合服务器可以收集来自各个用户实体的局部模型、聚合权重参数，以实现对局部模型的模型聚合，最终生成全局模型. 此外，由于本文使用FIL，聚合服务器可以对各个用户实体进行多轮的增量式模型聚合，以实现对SDN环境中新增流量数据的持续学习.

(4)SDN控制器

SDN控制器，是指用于对SDN网络拓扑内的链路连通性、路由转发等功能进行可编程控制的实体. 在本文框架中，SDN控制器依据DDoS攻击检测的结果以及相应的防御决策，控制拓扑中指定链路或实体的通信活动.

如图1所示，本检测模型通过五个步骤实现对SDN环境下DDoS攻击的分布式实时检测，具体描述如下：

步骤①，参与FIL的正常用户在所能够收集到的局部历史流量数据上进行训练，得到各自的局部模型. 正常用户将最近一次模型聚合期间的新增数据量、最新局部模型性能指标等，作为模型聚合的权重参数与局部模型一同上传到聚合服务器.

步骤②，聚合服务器收集来自参与FIL用户上传的局部模型以及聚合权重参数，执行FIL聚合算法，对各局部模型进行增量聚合，得到最新的全局模型. 然后，参加FIL的正常用户重新从聚合服务器更新最新的模型参数.

步骤③，针对实时捕获的流量数据，正常用户使

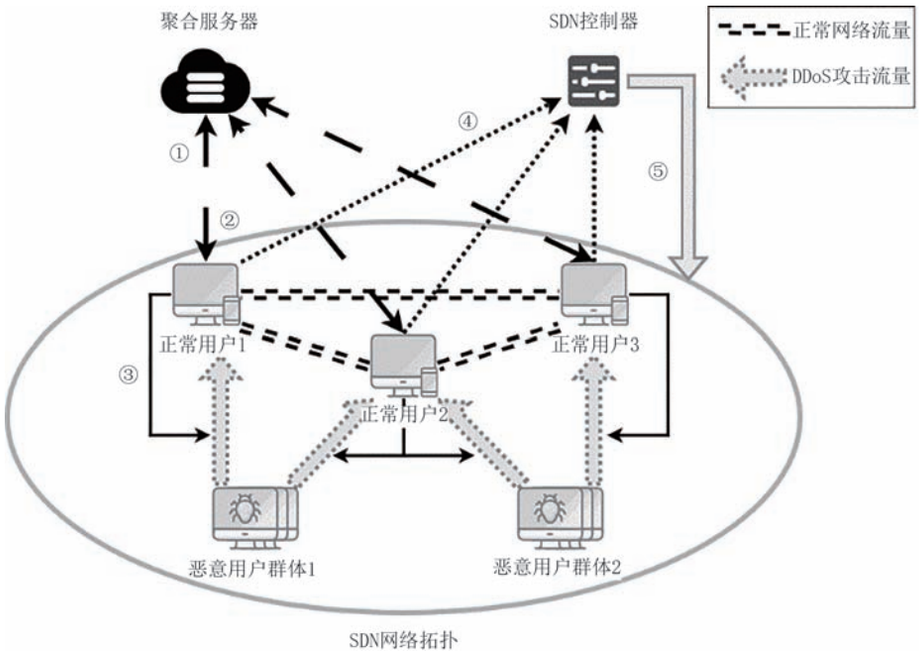

图1　基于FIL的SDN环境下DDoS攻击检测模型

用基于CICFlowMeter的特征提取方法与基于LSTM的深度学习模型，对一定时隙内的流量数据进行DDoS攻击的实时检测.

步骤④与步骤⑤，则是当正常用户检测到DDoS攻击时，本身及时做出对应的防御决策，同时上传到SDN控制器，进而实现对周边恶意用户群体的DDoS攻击流量进行防御处理.

3.3　联邦增量聚合

针对新增流规则和流量特征变化导致的数据遗忘以及不同实体间的Non-IID问题，本文提出一种基于联邦增量学习的加权聚合算法，降低从不同流量数据分布获得的局部模型对全局模型鲁棒性的影响. 加权聚合算法的过程如图2所示，算法参数释义表如表1所示.

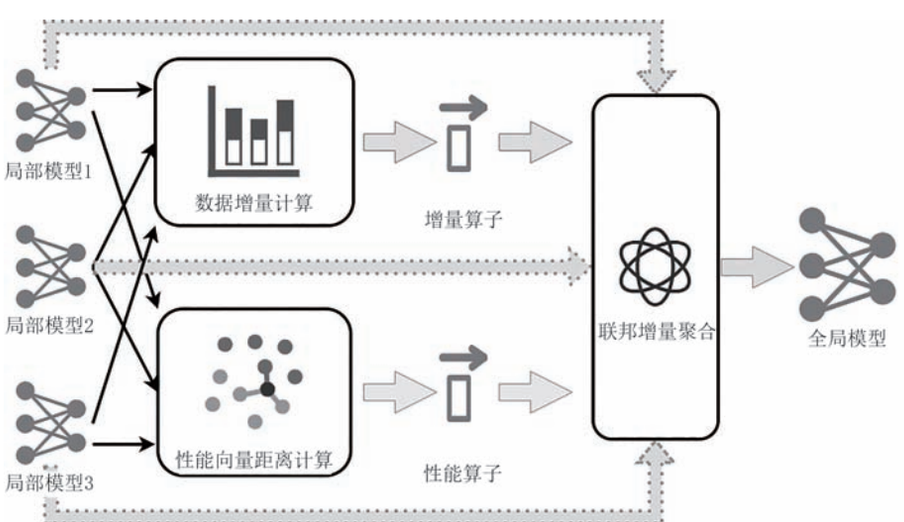

图2　基于联邦增量学习的加权聚合算法

如图所示，本文提出的聚合算法权重主要由增量算子与性能算子两部分构成.

(1)增量算子$factor_{data}$

针对数据增量的数据遗忘问题，本文在聚合中引入增量算子. 该算子根据不同实体的新增数据量，评估具有不同增量数据的实体在模型聚合中的影响能力. 在联邦增量训练过程中，本文计算不断变化的局部流量数据中新旧数据样本的比例，评估目前用户实体所拥有局部流量数据的聚合重要性. 并将量化的评估结果归一化，进而计算得到加权聚

表1 基于联邦增量学习的加权聚合算法参数释义表

符号	释 义
λ	数据样本增量的比例参数
$factor_{data}$	模型聚合权重计算中的增量算子
$\Delta data$	新增数据样本数目
$total\_data$	总数据样本数量
$factor_{capability}$	模型聚合权重计算中的性能算子
$\boldsymbol{v}_i$	参与训练的第i个局部模型的性能向量
$\boldsymbol{d}$	局部模型的性能向量距离矩阵
w	局部模型的聚合权重集合

合算法中的增量算子$factor_{data}$，具体的计算如公式(1)和公式(2)所示．其中，$\Delta data$、$total_data$分别代表新增数据样本数量、总数据样本数量．

$$\lambda=1-\frac{\Delta data}{total\_data} \tag{1}$$

$$factor_{data}=1-\frac{2}{\pi}\arctan(\lambda) \tag{2}$$

(2)性能算子$factor_{capability}$

针对不同用户间存在的Non-IID分布问题，本文对于不同用户训练得到的局部模型，先通过计算$F1$-Score、损失值、Kappa-Score等因子大小，进而评估相应局部模型的聚合重要性．具体地，本文将(F1-Score，损失值，Kappa-Score)作为局部模型对应的性能向量，通过计算性能向量之间的欧氏距离，量化不同模型之间的性能差距．最终，通过对各模型的性能差距进行统计，计算得到加权聚合算法中的性能算子$factor_{capability}$，具体计算如公式(3)～公式(4)所示．其中，v_i、v_j分别表示两个局部模型的性能向量($i,j=1,2,\cdots,n$)．

$$\boldsymbol{d}_{i,j}=\sqrt{\sum_{k=1}^{n}(\boldsymbol{v}_{i,k}-\boldsymbol{v}_{j,k})^2} \tag{3}$$

$$factor_{capability_i}=\frac{\sum_{j=1}^{n}\boldsymbol{d}_{i,j}}{\sum_{i=1}^{n}\sum_{j=1}^{n}\boldsymbol{d}_{i,j}} \tag{4}$$

本文提出的基于联邦增量学习的加权聚合算法如算法1所示．该算法对新增流量情况和局部模型进行综合评价，为不同的局部模型赋予不同的聚合权重，动态调节不同局部模型对全局模型的影响程度．

算法1 基于联邦增量学习的加权聚合算法

输入：新增样本数$=\{\Delta data_1,\Delta data_2,\cdots,\Delta data_n\}$，总样本数$=\{total_data_1,total_data_2,\cdots,total_data_n\}$，性能向量$\mathrm{V}=\{v_1,v_2,\cdots,v_n\}$

输出：模型聚合权重$w=\{w_1,w_2,\cdots,w_n\}$

1. FUNCTION 获取$factor_{data}$
2. $\lambda\leftarrow 1-\frac{\Delta data}{total\_data}$
3. $factor_{data}\leftarrow 1-\frac{2}{\pi}\arctan(\lambda)$
4. 返回$factor_{data}$
5. FUNCTION 获取$factor_{capability}$
6. 初始化距离矩阵$\boldsymbol{d}$
7. FOR $\boldsymbol{v}_i$ IN V DO
8. FOR $\boldsymbol{v}_j$IN V DO
9. $\boldsymbol{d}_{i,j}\leftarrow\sqrt{\sum_{k=1}^{3}\left(\boldsymbol{v}_{i,k}-\boldsymbol{v}_{j,k}\right)^2}$
10. END FOR
11. END FOR
12. 设置$factor_{capability}$为长度为n的空列表
13. FOR $i\leftarrow 1$ TO n DO
14. $factor_{capability\,i}\leftarrow\frac{\sum_{j=1}^{n}\boldsymbol{d}_{i,j}}{\sum_{i=1}^{n}\sum_{j=1}^{n}\boldsymbol{d}_{i,j}}$
15. END FOR
16. 返回$factor_{capability}$
17. FUNCTION 获取模型聚合权重
18. 设置$factor_{data}$为长度为n的空列表
19. FOR $i\leftarrow 1$ TO n DO
20. $factor_{data\,i}\leftarrow$ 获取$factor_{data}(\Delta data_i,total_{data_i})$
21. END FOR
22. $factor_{capability}\leftarrow$获取$factor_{capability}$(V)
23. 设置w为长度为n的空列表
24. FOR $i\leftarrow 1$ TO n DO
25. $w_i\leftarrow\frac{factor_{data\,i}}{factor_{capability\,i}}$
26. END FOR
27. FOR $i\leftarrow 1$ TO n DO
28. $w_i\leftarrow\frac{w_i}{sum(w)}$
29. END FOR
30. 返回w

由上述权重算法，计算得到模型聚合权重，使用加权聚合的方式聚合得到增量后最新的全局模型．

3.4 DDoS攻击检测

针对SDN环境中存在更多复杂流量特征的问题，本文提出了一种基于LSTM的DDoS攻击检测方法，对复杂流量数据进行时间关联性特征提取，有效降低特征数据规模，提升了攻击检测的实时性．

3.4.1 检测模型

由于报文发送时间上的连续性，使得特定IP的报文数据在时间序列上具有较强的关联性[1]．这一关联性，可以作为判别特定时隙内相关流量是否具

有恶意攻击性的重要依据．因此，本文采用了LSTM结构作为进行DDoS攻击检测的模型结构．本文使用Pytorch构造模型结构，主要分为特征提取器和分类器两部分．特征提取器包含基本的若干LSTM基础单元层，对每层输出都设置有Dropout层，对参数进行随机遗忘，以防止模型过拟合．分类器设置为全连接层，根据特征提取器计算的特征参数，对样本进行分类．模型结构如图3所示．

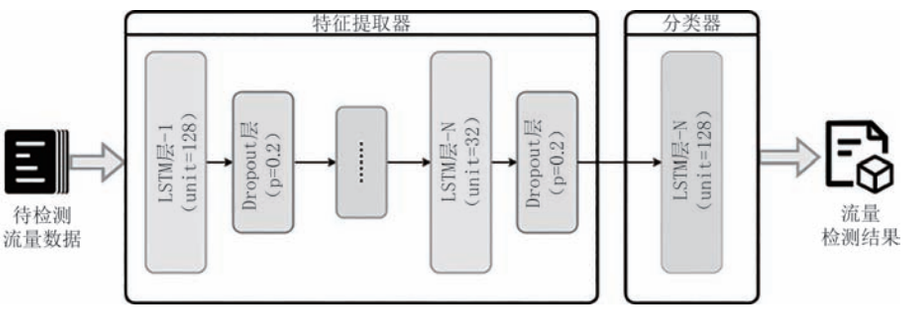

图3　基于LSTM的检测模型结构

3.4.2　攻击检测算法

本文基于CICFlowMeter和上述联邦增量聚合算法训练得到LSTM检测模型，提出了一种DDoS攻击检测算法．检测算法包括流量数据实时捕获、特征统计提取和DDoS攻击检测等部分，相关的算法参数释义表如表2所示．

表2　DDoS攻击检测算法主要参数释义表

符号	释义
$D_{features}$	经特征提取得到的数据样本集合
D_{ip}	数据样本集合中的IP信息
D_{other}	数据样本集合中的其余特征数据
S_{ip}	需要DDoS防御决策的IP集合
M	当前全局模型

如图4所示，本文对于实时捕获的流量数据，使用CICFlowMeter对一定时间内的不同通信流量进行独立统计，以提取流量数据的时序统计特征．用户实体从聚合服务器下载最新的全局模型参数，替换原有模型参数，并对流量数据攻击检测．若检测结果认为不存在DDoS攻击，则重新返回流量捕获过程；若检测结果认为存在DDoS攻击，则判定为DDoS攻击数据．对于每次检测，进一步结合流量数据中的网络实体信息，确定需要实施DDoS防御决策的DDoS IP列表．攻击检测的过程如算法2所示．

算法2　DDoS攻击检测算法

输入：特征提取得到的一定时间段流量数据$D_{features}$，最新模型M

输出：生成DDoS IP集合S_{ip}

1. 将$D_{features}$中IP信息单独提取为D_{ip}，其余流表特征等数据特征为D_{other}
2. 设置S_{ip}为空集合
3. $res \leftarrow M(D_{other})$
4. IF res显示为DDoS攻击数据
5. 　　在D_{ip}中找到对应IP信息，并加入S_{ip}

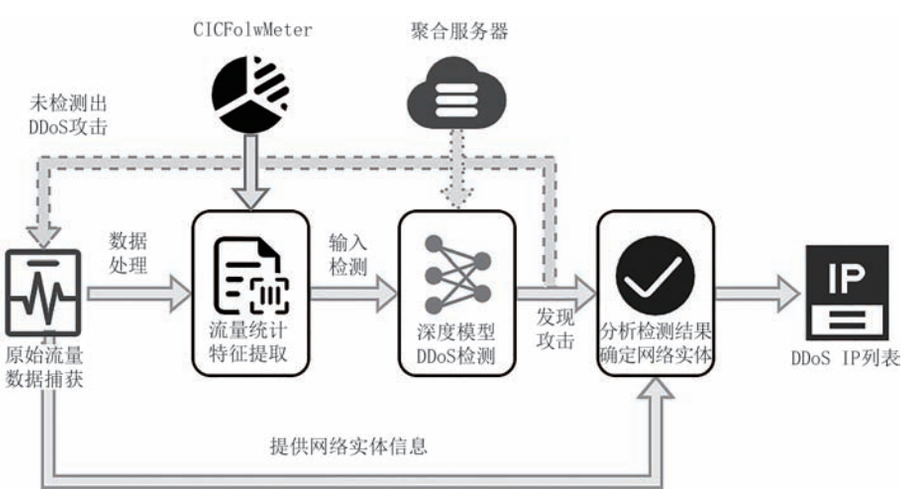

图4　SDN环境下的DDoS攻击检测算法

6. END IF

7. 返回生成的IP集合S_{ip}

3.5 DDoS防御决策

在上述工作的基础上，本文实现了SDN环境下的实时DDoS防御决策. 结合SDN集中控制的架构特性，本文使用OpenDaylight远程控制器，通过对与特定主机相连的交换机下发DDoS防御流表（以下简称流表），实现DDoS防御的分布式决策.

本文提出的DDoS防御决策算法的过程如图5所示，具体步骤如算法3所示，相关算法参数表如表3所示.

如图5所示，根据从检测算法获取的DDoS IP列表，提取其中DDoS攻击有关的源IP、目的IP，实时生成对应流表. 通过查找主机直连交换机的关系映射表，确定需要下发流表的目标交换机.

基于上述决策信息，通过调用ODL-API完成对目标交换机流表的实时下发，实现对指定主机下达防御动作的能力.

表3 DDoS防御决策算法主要参数释义表

符号	释 义
S_{ip}	需要DDoS防御决策的IP集合
Θ	生成的流表
θ_i	IP集合中第i个IP信息对
H	需要下发流表主机集合
params	待下发的流表参数
P_{switch}	主机-交换机对应关系集合

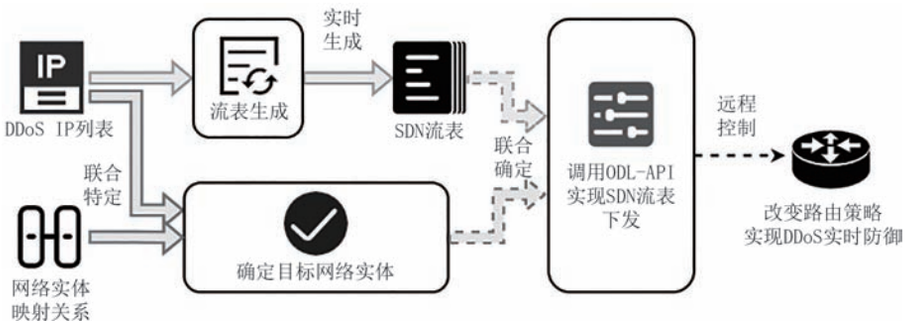

图5 SDN环境下的DDoS防御决策的过程

算法3 DDoS防御决策算法

输入：DDoS IP集合S_{ip}，主机-交换机对应关系集合P_{switch}

输出：生成DDoS防御流表Θ

1. FOR θ_i INS$_{ip}$ DO
2. 通过IP信息对θ_i确定需要下发流表主机集合H
3. FOR h IN H DO
4. 根据当前拓扑流量情况确定流表参数*params*
5. Θ←实时生成流表(θ_i, h, *params*)
6. 通过查找主机-交换机对应关系集合P_{switch}确定相邻交换机s
7. 调用ODL-API，实现对s实时下发流表Θ，并回报下发结果
8. END FOR
9. END FOR

4 实验与分析

本节对所提出的算子有效性、检测模型的性能与鲁棒性进行实验验证和性能分析，并与相关方法进行对比实验验证，最后对DDoS防御决策的有效性进行验证.

4.1 环境设置

4.1.1 拓扑仿真模拟

实验中，使用Mininet模拟所需要的拓扑结构，并采用Python脚本实现拓扑结构的构建，所生成的拓扑结构如图6所示. 在拓扑结构中，主机*h1*、*h2*、*h3*、*h4*均仅收集与自身相关的报文数据，且各自存储并维护相互独立的局部数据集.

4.1.2 数据捕获与预处理

在不同主机上使用Wireshark分别捕获实时报文数据，并将捕获的报文数据存储为相互独立的PCAP文件. 进而，使用CICFlowMeter方法对时间段内报文数据的PCAP文件进行数据特征提取与统计，得到包括源、目的IP、源端口、目的端口、协议、每秒速率和SDN中的流表特征等，共计82维数据特征.

将上述特征数据记录，去除源IP、目的IP以及时间戳，并根据采集时间段，制作样本标签，作为各主机的局部训练集. 若进行DDoS攻击检测，则不会对数据制作样本标签，并将另外保存数据源IP、目的IP.

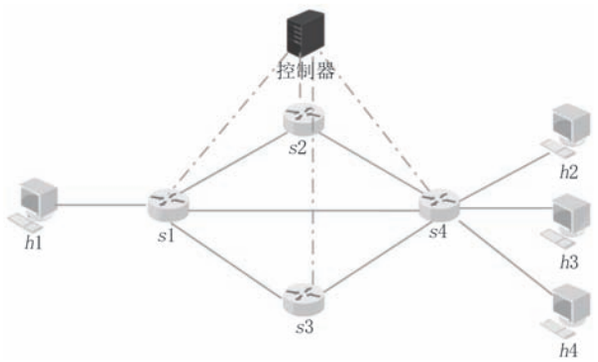

图6　仿真的拓扑结构

4.1.3　实验环境与实验数据

实验中，数据分布被分为基础数据分布与增量数据分布两种，实验训练参数设置如表4所示.

表4　训练参数表

参数	数值选择
局部训练轮数	100
全局训练轮数	5
学习率	1×10^{-4}

对于基础数据分布，本文在实际运行的拓扑中预先收集了一些流量数据，作为各主机初始的基础局部数据集，包括HTTP流量、FTP流量、SYN攻击流量和UDP攻击流量. 不同子数据集初始样本比例如表5所示，设置的数据样本空间分布相对均匀.

表5　子数据集初始样本比例

子数据集编号	良性数据样本数目	DDoS数据样本数目
1	3006	1001
2	2680	853
3	3051	1018
4	3251	1084

对于增量数据分布，本文在FIL的全局训练中设置不同子数据集的增量变化特点，并使用基于联邦增量学习的加权聚合算法进行全局聚合. 为验证所提出DDoS攻击检测模型的有效性，本文设置不同主机间的正常数据与DDoS攻击数据增量比例、增量数据种类各不相同. 多轮训练将导致不同主机间的数据分布逐渐出现较大的差异，最终形成Non-IID分布环境. 各子数据集数据增量如表6所示，由于多次实时采集数据样本数目之间存在一定波动，表中给出了不同主机实体的数据样本均值及波动值.

表6　子数据集数据增量特点分布

子数据集编号	良性数据样本增量	DDoS数据样本增量
1	1596 ± 96	0
2	1225 ± 14	402 ± 36
3	805 ± 56	798 ± 28
4	0	1608 ± 54

多轮训练将导致不同主机间的数据分布逐渐出现较大的差异，最终形成Non-IID分布环境. 同时，为更好仿真Non-IID分布环境，本文令不同主机捕获的增量数据分布中，良性样本和DDoS攻击样本比例符合一定规律. 子数据集1的增量分布中，良性样本占比为1，DDoS攻击样本占比为0；子数据集2的增量分布中，良性样本占比为0.75，DDoS攻击样本占比为0.25；子数据集3的增量分布中，良性样本和DDoS攻击样本各占比为0.5；子数据集4的增量分布中，良性样本占比为0，DDoS攻击样本占比为1.

4.2　算法实验与分析

4.2.1　算子有效性实验

本节实验对所提出的增量算子和性能算子的有效性进行验证. 针对上述两种算子，以FL经典聚合算法FedAvg[11]作为基准线，并分别以准确率(Accuracy)以及$F1$-Score作为评价指标，分别进行有效性实验. 实验结果如图7、图8所示.

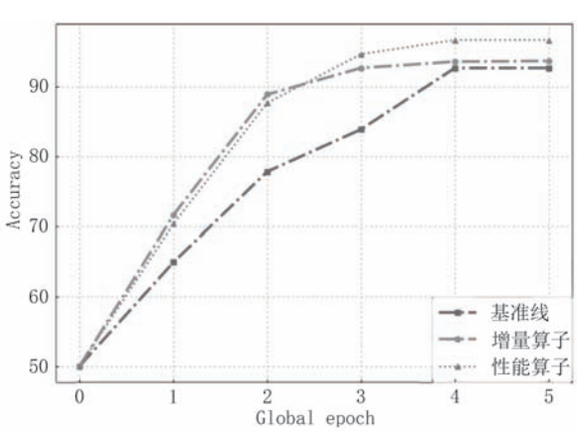

图7　以准确率作为评价指标的算子有效性实验

其中，横轴表示FIL的全局训练轮数、纵轴分别表示准确率Accuracy和$F1$-Score评价指标数值.

分析结果，应用了增量算子的模型训练中，准确率和$F1$-Score分别平均提升5.71%、0.0755，最终准确率和$F1$-Score分别提升了1.02%、0.009. 而应用了性能算子的模型训练中，准确率和$F1$-Score分别平均提升6.82%、0.0685，最终准确率和$F1$-

Score分别提升了4.03%、0.0248.

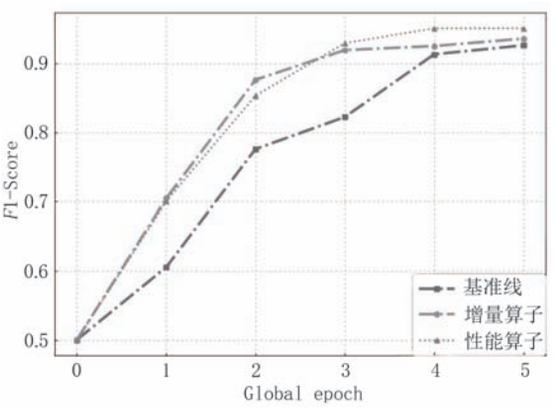

图8 以$F1$-Score作为评价指标的算子有效性实验

实验结果表明,本文提出的两种算子,都有助于促进模型较早期趋向于性能收敛,且对模型学习数据分布特征具有一定的性能提升.

4.2.2 模型性能对比实验

本节实验将所提出的基于联邦增量学习的加权聚合算法与其他FL方法进行对比实验,对不同方法在DDoS攻击检测准确率、$F1$-Score结果进行对比.实验结果如图9、图10所示,与其他方法的平均评价指标、最终评价指标的具体数值如表7所示.

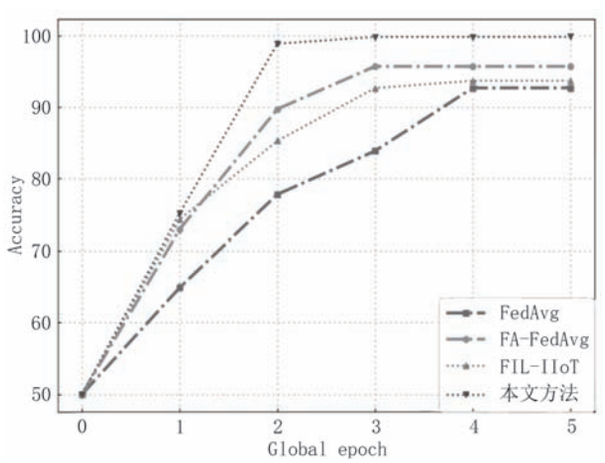

图9 本文方法与其他方法准确率对比实验

实验中的对比算法FA-FedAvg、FIL-IIoT,与本文方法相似,都采用了动态调整局部模型权重的做法,来实现聚合模型在数据不平衡或数据增量场景下分类性能的提升.

分析实验结果,FedAvg算法表现较平均,尤其是最终收敛性能指标,原因可能是由于FedAvg在训练后期出现了较为明显的数据遗忘,导致准确率、$F1$-Score收敛数值都较低.相较于FedAvg

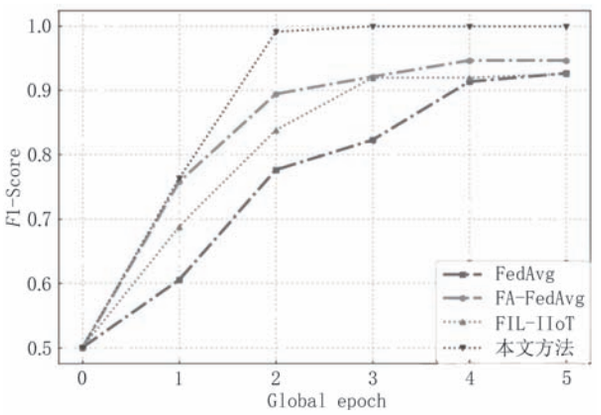

图10 本文方法与其他方法$F1$-Score对比实验

表7 对比实验性能指标数值

方法	最终准确率	平均准确率	最终F1-Score	平均F1-Score
FedAvg	92.68	82.38	0.9266	0.8088
FA-FedAvg[53]	95.72	89.94	0.9451	0.8933
FIL-IIoT[20]	93.55	87.92	0.9256	0.8583
本文方法	**99.45**	**95.00**	**0.9931**	**0.9498**

算法,FA-FedAvg和FIL-IIoT算法在平均评价指标、最终评价指标上表现较为相似,均有一定幅度提升.

与上述三种方法相比,本文方法在平均评价指标、最终评价指标上均表现最优.在平均准确率上分别提升12.62%、5.06%、7.08%;在最终准确率上分别提升6.77%、3.73%、5.90%;在平均$F1$-Score上分别提升0.1410、0.0565、0.0915;在最终$F1$-Score分别提升0.0665、0.0480、0.0675.

实验结果表明,本文所提出方法在DDoS流量数据增量与数据分布不平均的场景下,相较于其他方法,在更早期全局训练轮次就实现了模型性能的高准确率收敛,也具有更好的检测性能表现.

4.2.3 鲁棒性对比实验

本节实验将采用所训练生成的最终FIL检测模型,对不同主机实体的不同数据分布流量数据进行DDoS攻击检测,并与其他FL方法进行性能表现对比,以验证本文方法的鲁棒性.实验结果如图11、图12所示.

实验结果表明,FedAvg与FA-FedAvg在不同主机上的检测准确率、$F1$-Score值都呈现出一定程度的性能表现波动与不平衡.相比较上述两个方法,本文方法在不同主机的检测性能具有更高的鲁棒性,且在各局部数据集上准确率、$F1$-Score的相对方差均小于1%,性能指标上也表现

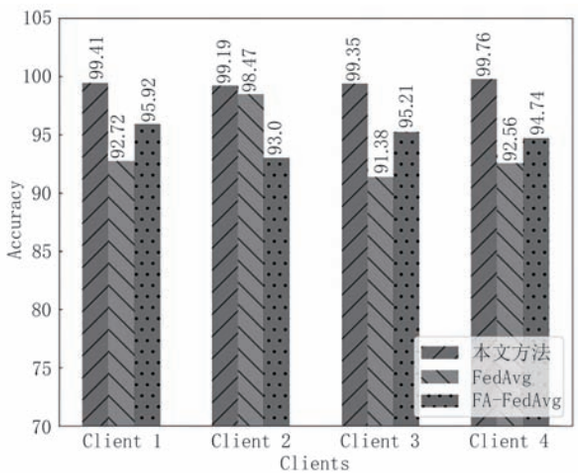

图11　不同主机DDoS攻击检测准确率鲁棒性实验

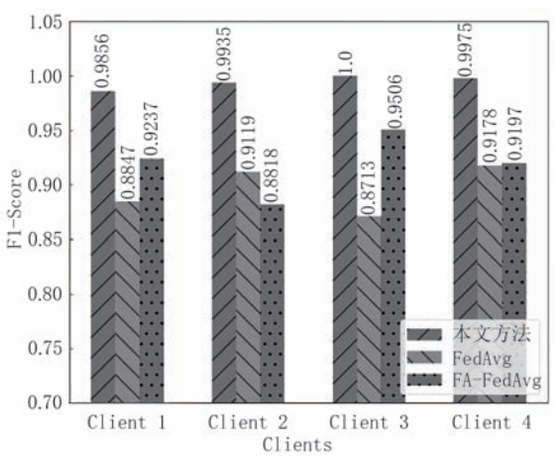

图12　不同主机DDoS攻击检测$F1$-Score鲁棒性实验

更好.

4.2.4　DDoS防御决策有效性实验

本节对采用本文方法的DDoS防御决策的有效性进行实验验证. 本文使用hping3模拟DDoS攻击流量，从主机2对主机1、主机3对主机1、主机4对主机1进行时长为2.5 s的DDoS模拟攻击，并实时捕获其流量数据. 使用所提出的DDoS攻击检测模型进行检测，并实现防御决策判定，最终分别下发不同主机到主机1方向的流表. 实验结果以有无进行流表下发决策的链路流量来表示，如图13至图15所示. 其中，横轴表示检测链路流量速率的时间，纵轴表示链路流量速率，实验从500 ms处开始进行DDoS攻击流量实验.

以图13为例分析实验结果，由主机2对主机1的流量变化可知，在没有防御决策的情况下，随着DDoS攻击流量的注入，链路流量速率明显增大，最高流量速率达到约1000 KB/s. 而采用了防御决策后，则针对DDoS攻击流量下发防御流表，成功使链路流量速率得到了有效控制.

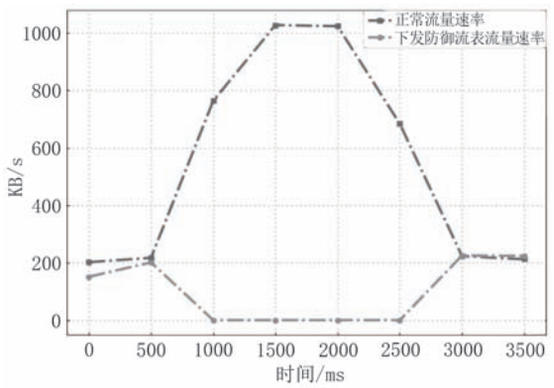

图13　主机2对主机1DDoS防御决策有效性验证

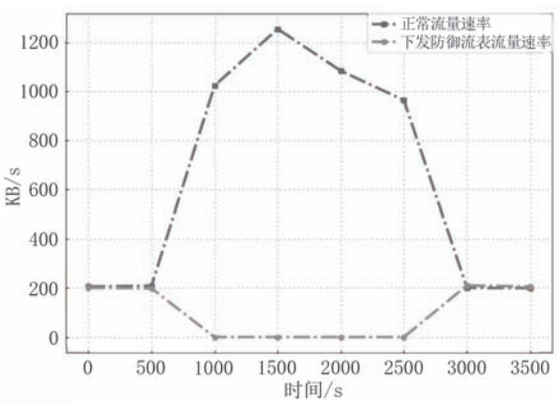

图14　主机3对主机1DDoS防御决策有效性验证

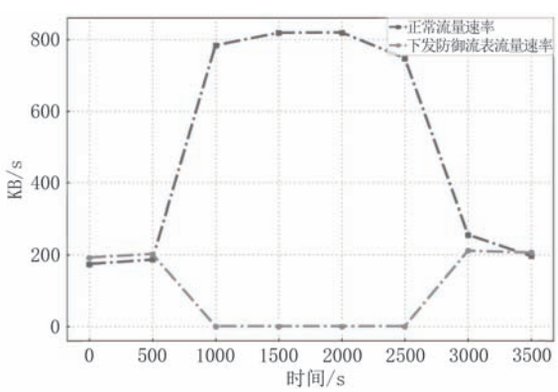

图15　主机4对主机1DDoS防御决策有效性验证

5　结束语

本文围绕SDN环境下DDoS攻击检测问题，针对数据增量导致的数据Non-IID问题，提出了一种基于FIL的SDN环境下DDoS攻击检测模型，包括了基于FIL的加权聚合算法、DDoS攻击检测算法及防御决策方法. 经对比实验验证，所提出的模型方法具备一定性能优势和更高鲁棒性.

在未来研究工作中，将进一步探索FIL在数据增量环境下不同恶意攻击检测的创新方法．同时，也将考虑更多的网络拓扑应用场景，研究数据样本自动标签技术、小样本学习技术等，更好提升基于FIL的检测模型的实际可用性．

致 谢 我们向对本文工作给予支持和宝贵建议的评审老师和同行表示衷心的感谢!

参 考 文 献

[1] Vishwakarma R, Jain A K. A survey of DDoS attacking techniques and defence mechanisms in the IoT network. Telecommunication Systems, 2020, 73(1): 3-25

[2] Wang D, Zhou J, Masdari M, et al. Security in wireless body area networks via anonymous authentication: Comprehensive literature review, scheme classification, and future challenges. Ad Hoc Networks, 2023, 153: 1-27

[3] Eliyan L F, Di Pietro R. Dos and DDoS attacks in software defined networks: A survey of existing solutions and research challenges. Future Generation Computer Systems, 2021, 122: 149-171

[4] Urrea C, Benitez D. Software-defined networking solutions, architecture and controllers for the industrial internet of things: A review. Sensors, 2021, 21(19): 6585-6605

[5] Karnani S, Agrawal N, Kumar R. A comprehensive survey on low-rate and high-rate DDoS defense approaches in SDN: Taxonomy, research challenges, and opportunities. Multimedia Tools and Applications, 2023, 83: 1-54

[6] Swami R, Dave M, Ranga V. Software-defined networking-based DDoS defense mechanisms. ACM Computing Surveys, 2019, 52(2): 1-36

[7] Singh J, Behal S. Detection and mitigation of DDoS attacks in SDN: A comprehensive review, research challenges and future directions. Computer Science Review, 37, 2020:1-25

[8] 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

[9] Fallah M, Mohammadi P, NasiriFard M, et al. Optimizing QoS metrics for software-defined networking in federated learning. Mobile Information Systems, 2023,21: 1-10

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

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

[12] Zhang C, Xie Y, Bai H, et al. A survey on federated learning. Knowledge-Based Systems, 2021, 216: 106775-106775

[13] Zainudin A, Akter R, Kim D S, et al. FedDDoS: An efficient federated learning-based DDoS attacks classification in SDN-enabled IIoT networks//Proceedings of the 13th International Conference on Information and Communication Technology Convergence. Jeju Island, Republic of Korea, 2022: 1279-1283

[14] Issa W, Moustafa N, Turnbull B, et al. Blockchain-based federated learning for securing internet of things: A comprehensive survey. ACM Computing Surveys, 2023, 55(9): 1-43

[15] Agrawal S, Sarkar S, Aouedi O, et al. Federated learning for intrusion detection system: Concepts, challenges and future directions. Computer Communications, 2022, 195:346-361

[16] Wang X, Liang Z, Koe A S V, et al. Secure and efficient parameters aggregation protocol for federated incremental learning and its applications. International Journal of Intelligent Systems, 2022, 37(8): 4471-4487

[17] Kumar Y, Singla R. Federated learning systems for healthcare: Perspective and recent progress. Federated Learning Systems: Towards Next-Generation AI, 2021, 2021: 141-156

[18] Cui T, Zhang H J, Dai W, et al. Federated incremental transfer learning based on distributed consensus. Chinese Journal of Computers, 2024, 47(4): 821-841.(in Chinese)
(崔腾,张海军,代伟.基于分布共识的联邦增量迁移学习.计算机学报, 2024, 47(4), 821-841)

[19] Jiang H, He T L, Liu M, et al. High-performance federated continual learning algorithm for heterogeneous streaming data. Journal on Communications, 2023, 44(05): 123-136.(in Chinese)
(姜慧,何天流,刘敏等.面向异构流式数据的高性能联邦持续学习算法.通信学报,2023,44(05):123-136)

[20] Liu J, Dong Z H, Zhang Z Y, et al. Data sharing method of industrial internet of things based on federal incremental learning. Journal of Computer Applications, 2022, 42(4): 1235-1243.(in Chinese)
(刘晶, 董志红, 张喆语等. 基于联邦增量学习的工业物联网数据共享方法. 计算机应用, 2022, 42(4): 1235-1243.)

[21] Lashkari A H, Seo A, Gil G D, et al. Cic-ab: Online ad blocker for browsers//Proceedings of the 2017 International Carnahan Conference on Security Technology.Madrid, Spain, 2017: 1-7

[22] Alhijawi B, Almajali S, Elgala H, et al. A survey on DOS/DDoS mitigation techniques in SDNs: Classification, comparison, solutions, testing tools and datasets. Computers and Electrical Engineering, 2022, 99: 107706-107724

[23] Santos R, Souza D, Santo W, et al. Machine learning algorithms to detect DDoS attacks in SDN. Concurrency and Computation: Practice and Experience, 2020, 32(16): 1-14

[24] Balarezo J F, Wang S, Chavez K G, et al. A survey on DOS/DDoS attacks mathematical modelling for traditional, SDN and virtual networks. International Journal of Engineering Science and Technology, 2022, 31: 101065-101080

[25] Gaurav A, Gupta B B, Alhalabi W, et al. A comprehensive survey on DDoS attacks on various intelligent systems and it's defense techniques. International Journal of Intelligent Systems, 2022, 37(12): 11407-11431

[26] Li C H, Wu Y, Qian Z Z, et al. DDoS attack detection and defense based on hybrid deep learning model in SDN. Journal on Communications, 2018, 39(7): 176-187 (in Chinese)
(李传煌,吴艳,钱正哲等.SDN下基于深度学习混合模型的DDoS攻击检测与防御.通信学报,2018,39(07):176-187)

[27] Tang D, Yan Y, Zhang S, et al. Performance and features: Mitigating the low-rate TCP-targeted dos attack via SDN. IEEE Journal on Selected Areas in Communications, 2021, 40 (1): 428-444

[28] Mousavi S M, St-Hilaire M. Early detection of DDoS attacks against SDN controllers//Proceedings of the 2015 International Conference on Computing, Networking and Communications. California, USA,2015: 77-81

[29] Hormozi M, Erfani S H. An SDN-based DDoS defense approach using route obfuscation. Concurrency and Computation: Practice and Experience, 2023, 35(1): 1-21

[30] Dumka A, Ashok A, Verma P. Performance analysis of DDoS attack on SDN and proposal of cracking algorithm. International Journal of Information Technology Project Management, 2020, 11(4): 1-12

[31] Najar A A, Naik S M. Cyber-secure SDN: A CNN-based approach for efficient detection and mitigation of DDoS attacks. Computers & Security, 2024, 139: 103716-103739

[32] Tang D, Yan Y, Gao C, et al. Ltrft: Mitigate the low-rate data plane DDoS attack with learning-to-rank enabled flow tables. IEEE Transactions on Information Forensics and Security, 2023, 18: 3143-3157

[33] Gadallah W G, Ibrahim H M, Omar N M. A deep learning technique to detect distributed denial of service attacks in software-defined networks. Computers & Security, 2023, 137: 103588-103600

[34] Kaur S, Sandhu A K, Bhandari A. Investigation of application layer DDoS attacks in legacy and software-defined networks: A comprehensive review. International Journal of Information Security, 2023, 22(6): 1949-1988

[35] 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

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

[37] Yin Ziwei, Li Kun, Bi Hongjun. Trusted multi-domain DDoS detection based on federated learning. Sensors, 2022, 22: 7728-7753

[38] Narmadha K, Varalakshmi P. Federated learning in healthcare: A privacy preserving approach//Proceedings of the Medical Informatics Europe Conference. Nice, France, 2022: 194-198

[39] 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. Paris, France, 2022: 118-125

[40] Pourahmadi V, Alameddine H A, Salahuddin M A, et al. Spotting anomalies at the edge: Outlier exposure-based cross-silo federated learning for DDoS detection. IEEE Transactions on Dependable and Secure Computing, 2022, 20: 4002-4015

[41] Liang J W, Yang G, Ma M D. Secure federated distillation gan for CIDS in industrial CPS. Journal on Communications, 2023, 44(12): 230-244 (in Chinese)
(梁俊威, 杨耿,马懋德. 基于安全联邦蒸馏 GAN 的工业 CPS 协作入侵检测系统. 通信学报, 2023, 44(12): 230-244)

[42] Abou El Houda Z, Hafid A S, Khoukhi L. Mitfed: A privacy preserving collaborative network attack mitigation framework based on federated learning using SDN and blockchain. IEEE Transactions on Network Science and Engineering, 2023, 10 (4): 1985-2001

[43] Ali M N, Imran M, din M S, et al. Low rate DDoS detection using weighted federated learning in SDN control plane in IoT network. Applied Sciences, 2023, 13(3): 1431-1452

[44] Liu Z, Guo C, Liu D, et al. An asynchronous federated learning arbitration model for low-rate DDoS attack detection. IEEE Access, 2023, 11: 18448-18460

[45] Konečný J. Federated learning: Strategies for improving communication efficiency. arXiv preprint arXiv: 1610.05492, 2016: 1-10

[46] Zhang W, Lu Q, Yu Q, et al. Blockchain-based federated learning for device failure detection in industrial IoT. IEEE Internet of Things Journal, 2020, 8(7): 5926-5937

[47] Bai J, Sajjanhar A, Xiang Y, et al. Fedewa: Federated learning with elastic weighted averaging//Proceedings of the 2022 International Joint Conference on Neural Networks. Padua, Italy, 2022: 1-8

[48] Deng Y, Lyu F, Ren J, et al. Fair: Quality-aware federated learning with precise user incentive and model aggregation//Proceedings of the IEEE Conference on Computer Communications. Virtual, 2021: 1-10

[49] Ye R, Xu M, Wang J, et al. Feddisco: Federated learning with discrepancy-aware collaboration//Proceedings of the International Conference on Machine Learning.Hawaii, USA, 2023: 39879-39902

[50] Tang Z, Shao F, Chen L, et al. Optimizing federated learning on non-iid data using local Shapley value//Proceedings of the Artificial Intelligence: 1st CAAI International Conference. Hangzhou, China, 2021: 164-175

[51] Wu H, Wang P. Fast-convergent federated learning with adaptive weighting. IEEE Transactions on Cognitive Communications and Networking, 2021, 7(4): 1078-1088

[52] Mou Y, Geng J, Welten S, et al. Optimized federated learning on class-biased distributed data sources//Proceedings of the Joint European Conference on Machine Learning and Knowledge Discovery in Databases. Bilbao, Spain, 2021: 146-158

[53] Geng D Q, He H W, Lan X C, et al. Bearing fault diagnosis based on improved federated learning algorithm. Computing, 2022, 104: 1-19

LIU Yan-Hua, Ph. D., professor. His research interests include cyberspace security, intelligent computing and application.

FANG Wen-Yu, M. S., candidate. His research interests include federated learning and cyberspace security.

GUO Wen-Zhong, Ph. D., professor. His research interests include multimedia intelligent information processing, network computing and analysis, and data mining.

ZHAO Bao-Kang, Ph. D., associate professor. His research interests include Internet and cyberspace security.

HUANG Wei, Ph. D., lecturer. Her research interests include federated learning and urban computing.

Background

DDoS attack is a kind of distributed attack launched to the target host by controlling a large number of zombie machines, which brings huge losses to the network communication. SDN, as a modern network paradigm, has been applied to a wide range of network domains. By separating the control plane from the data plane, SDN adopts a flexible architecture to gradually optimize and replace the traditional network structure, and provides a centralized and feasible solution for real-time deployment of DDoS defense policies.

However, also because of the centralized control characteristics of SDN, its central controller in the open network is more likely to become the target of malicious attacks. As a result, DDoS attacks against SDN networks have begun to appear, which often result in damage to the control plane, policy failure, data stream tampering and other problems. This leads to a great challenge to the security of SDN networks.

According to the research on DDoS attack detection in SDN environment, there are three main challenges:

(1) Centralized control of SDN networks is vulnerable to DDoS attacks. Currently available centralized machine learning in SDN networks often also need to select a specific detection center, which will become the central hub of the DDoS attack detection function.

(2) The data forgetting problem and Non-IID distribution problem caused by the constant generation of new flow rules and traffic data in SDN networks. The existing flow detection methods are difficult to retain the knowledge of the original features while learning the new feature distributions generated in the SDN network, which leads to the data forgetting problem. In addition, since the flow rules restrict the forwarding target of the messages, the data messages that can be collected by different host entities are different. The Non-IID (Non-Independent and Identically Distributed) distribution problem will have a serious negative impact on the model performance and robustness of DDoS attack detection models using machine learning, and robustness will have serious negative impact.

(3) There are more complex traffic features to be analyzed and learned in SDN networks. In SDN networks, packets are forwarded through controllers, flow tables and corresponding control protocols. Compared with non-SDN networks, a large number of complex traffic features need to be processed and learned.

We adopt Federated Incremental Learning (FIL) to solve the above problems. FIL, as an emerging distributed learning technique, combines well with incremental learning and federated learning, and can adapt to new data inputs through incremental model updating without retraining the whole model globally.

This paper mainly proposes a DDoS attack detection model based on FIL in SDN environment. Feature extraction and statistics are carried out for SDN network traffic data, and the training model of network entities with different distributions is aggregated by FIL method, and the DDoS attack traffic is detected and decided, so as to improve the accuracy and real-time performance of DDoS attack detection.

This work is supported by the National Natural Science Foundation of China under Grant No. U21A20472, No. U22B2005 and No. 62406070, the National Key Research and Development Program of China under Grant No. 2021YFB3600503, the Natural Science Foundation of Fujian Province under Grant No. 2021J01625 and No. 2021J01616, the Science and Technology Major Program of Fujian Province under Grant No. 2021HZ022007, the Technological Innovation Key Research and Industrialization Program of Fujian Province under Grant No. 2024G018 and the Science and Technology Major Program of Fuzhou City under Grant No. 2023-ZD-003.