# 基于层次联邦与动态权重的卫星网络异常检测方法

牛渲文[1]，杜晔[1,2*]，杨明松[3]，李昂[3]，黎妹红[1,2]

（1.北京交通大学智能交通数据安全与隐私保护技术北京市重点实验室，北京 100044；
2.北京交通大学国家经济安全预警工程北京实验室，北京 100044；3.北京交通大学詹天佑学院，北京 100044）

**摘　要：**随着全球卫星网络的发展与覆盖，卫星网络攻击的影响逐渐扩大，开展卫星网络攻击或异常行为检测研究，对保障空天地一体化网络安全至关重要。针对联邦学习（FL）在卫星网络分布式异常检测中存在通信连接不稳定、聚合时间过长的问题，提出一种基于层次 FL 与改进动态半异步聚合算法的卫星网络异常检测方法。首先，融合层次 FL 进行分布式异常检测模型训练与分层聚合，提出一种 3 层架构的空天地协同异常检测框架，将高空通信平台站（HAPS）作为边缘计算层用于局部聚合，解决星地通信范围有限的问题；然后，针对 FL 在卫星网络中存在的通信连接不稳定、聚合时间过长的问题，提出并实现一种改进动态半异步联邦聚合算法，结合卫星状态信息构造改进聚合时机序列和动态权重，缓解由于星地通信间歇性而导致的聚合时间过长、模型精度受影响的问题。在 STIN 和 CIC-IDS-2017 数据集上的对比实验结果表明，该方法在保证良好的异常检测模型性能的同时，有效提高了卫星网络分布式异常检测中的 FL 聚合效率。

**关键词：**层次联邦学习；动态权重；卫星网络；异常检测；近地轨道

**中图分类号：**TP309　　**文献标志码：**A　　**DOI：**10.19678/j.issn.1000-3428.0069214

# Anomaly Detection Method for Satellite Networks Based on Hierarchical Federation and Dynamic Weights

NIU Xuanwen[1], DU Ye[1,2*], YANG Mingsong[3], LI Ang[3], LI Meihong[1,2]

(1.Beijing Key Laboratory of Security and Privacy in Intelligent Transportation, Beijing Jiaotong University, Beijing 100044, China;
2.Beijing Laboratory of National Economic Security Early-warning Engineering, Beijing Jiaotong University, Beijing 100044, China;
3.Jeme Tienyow Honors College, Beijing Jiaotong University, Beijing 100044, China)

**【Abstract】**Satellite network attacks have gradually increased with the development and widespread coverage of global satellite networks. Research on satellite network attacks or anomaly behavior detection is paramount for ensuring the security of space-air-ground integrated networks. Considering the issues of unstable communication and prolonged aggregation time in the application of Federated Learning (FL) for distributed anomaly detection in satellite networks, this paper proposes a satellite network anomaly detection method based on hierarchical FL and an improved dynamic semi-asynchronous aggregation algorithm. First, by integrating the hierarchical FL for distributed anomaly detection model training and hierarchical aggregation, a three-tier architecture for a space-air-ground collaborative anomaly detection framework is proposed. The proposed framework utilizes High-Altitude Platform Stations (HAPS) as an edge computing layer for local aggregation, addressing the limited satellite-ground communication range. Subsequently, to address unstable communication and prolonged aggregation times in FL within satellite networks, an improved dynamic semi-asynchronous federated aggregation algorithm is proposed and implemented. This algorithm constructs an improved aggregation timing sequence and dynamic weights by incorporating satellite status information, thereby mitigating the issues of prolonged aggregation time and compromised model accuracy caused by intermittent satellite-ground communication. Comparative experiments on the STIN and CIC-IDS-2017 datasets reveal that the proposed method effectively enhances FL aggregation efficiency in distributed anomaly detection for satellite networks while maintaining the excellent performance of the anomaly detection model.

**【Key words】**hierarchical Federated Learning (FL); dynamic weights; satellite network; anomaly detection; Low Earth Orbit (LEO)

## 0　引言

近年来，为实现网络的全球覆盖与接入，卫星网络在通信、导航、遥感等关键领域的应用日益广泛[1]。卫星网络是由一定数量的卫星以及相应的地面设施共同构成的一种新型网络，其旨在提供实时

**收稿日期：**2024-01-12　　**修回日期：**2024-07-15

**基金项目：**北京市自然科学基金（L254063）；中央引导地方科技发展资金（246Z0705G）；中央高校基本科研业务费专项资金（2024JBZX018）。

**通信作者 E-mail：*** ydu@bjtu.edu.cn

计算机工程 www.ecice06.com

信息处理、带宽互联网接入等通信服务[2]。其中,由近地轨道(LEO)卫星[3]组成的互联网以其抗毁性强、覆盖能力好、链路损耗低等优势,成为全球卫星互联网的发展热点,Starlink、OneWeb 等典型低轨宽带星座的相继建成[4],正在加速推进全球卫星网络的发展。然而,卫星网络作为关键基础设施,一旦遭到网络攻击,攻击者可通过控制卫星或相应地面设备以窃取机密信息,严重威胁国家国防安全与太空发展权益。因此,对卫星网络中的攻击或入侵行为进行有效检测,作出及时预警与响应,对于构建卫星网络安全防护体系至关重要[5]。

传统的异常检测方法往往采用集中检测模式,该模式无法适用于卫星网络这类高动态的大规模网络,因此,卫星网络异常检测通常采用星地协同的分布式架构[6]。卫星节点将原始特征数据下传至部署于地面站(GS)的中央服务器,由中央服务器训练异常检测模型,并将训练后的模型上传至卫星节点进行分布式检测。在检测过程中,对于未知恶意流量,卫星节点会向地面下传原始特征,在传输过程中特征数据量冗杂,易造成链路拥塞,且存在信息泄露风险。将联邦学习(FL)引入分布式卫星网络异常检测[7],卫星与地面站只需传送参数,不仅大幅缩减了数据传输量,经全局聚合后的模型还能够有效地应对不同卫星节点的多种网络攻击。

为提高卫星网络中 FL 的聚合效率,保证异常检测模型的性能,本文提出了一种基于层次 FL 与改进动态半异步聚合的空天地协同异常检测方法。首先,引入搭载高性能边缘计算平台的高空通信平台站(HAPS)[8]作为中间层,连接卫星与地面站,有效缓解星地通信范围有限、通信链路不稳定等问题;然后,提出一种适应该框架的改进动态半异步聚合方法(FedIDSS),结合卫星状态信息构造改进聚合时机序列与动态权重,采用分层半异步方式进行聚合,以保证模型的异常检测精度;最后,通过实验证明基于 FedIDSS 算法的卫星网络异常检测方法在保证检测准确率、减少聚合时间等方面的有效性。

## 1 相关工作

由于卫星网络由海量动态且异构的参与节点组成,面临的威胁多为分布式拒绝服务攻击(DDoS)等大规模分布式协同攻击,卫星网络异常检测目前通常采用分布式架构。文献[9]提出了一种基于区块链的分布式卫星互联网入口防御框架(DCED),对多类 DDoS 攻击进行识别与拦截。文献[10]提出了一种基于区块链和智能合约的卫星通信网络入侵检测与访问控制框架(ACID),防止非法用户访问基于区块链的卫星通信网络,并通过监控交易执行路径和方法调用上下文来检测恶意攻击。分布式卫星网络异常检测框架有效缓解了星地链路带宽有限、网络结构复杂等问题,但在实际检测过程中,卫星向地面站下传的原始特征数据面临泄露风险,且存在卫星节点间数据不共享、无法对其他节点数据进行有效检测等问题。

基于 FL 框架的异常检测[11-12]目前已成为卫星网络分布式异常检测的研究重点之一,可有效提高模型的准确性与泛化性。文献[13]结合水平联邦学习(HFL)与星地一体化网络(STIN),提出一种分布式入侵检测系统,并设计了一种卫星网络拓扑优化算法,降低卫星网络中频繁切换链路时恶意数据包的追踪难度;文献[14]提出了一种结合 FL 与循环神经网络(RNN)的分布式智能卫星网络入侵检测系统(DFSat),其能够显著区分基于物联网的卫星网络中复杂的网络攻击,并有效评估卫星系统的安全性;文献[15]提出一种基于深度联邦学习(DFL)的卫星网络入侵检测模型,采用基于差分隐私(DP)的去中心化数据预处理机制,并集成深度自编码器(DAE)和 FL 构建分布式入侵检测模型,有效识别卫星网络中的零日攻击等异常流量。然而,在上述研究工作中,卫星节点的动态性使得星地链接存在时间窗口期,每个时间点只有少部分节点在通信范围内,若位于地面的中央服务器在接收所有节点参数后再进行同步聚合,将导致聚合周期过长的问题。

为使 FL 在卫星网络中的性能更优,目前许多研究结合卫星网络特点,从服务器部署位置与聚合周期等不同角度进行适应性改进。文献[16]提出一种适用于密集低轨卫星星座的联邦学习算法(FedISL),将中央服务器部署于北极点的地面站或中轨卫星(MEO)上,利用星间链路(ISL)和卫星运行的可预测性来优化聚合策略,大幅减少了训练时间和通信成本;文献[17]对不同轨道上的卫星进行分组,以解决数据非独立同分布的问题,并将参数服务器部署于高空通信平台,设计了一种结合卫星内部模型接力传播与陈旧度折扣的异步联邦算法(AsyncFLEO),缓解了因卫星与参数服务器之间不稳定连接和不规则访问导致的聚合时间过长问题;文献[18]提出一种半异步联邦算法(FedSpace),设计了考虑卫星轨道等数据的动态模型聚合调度算法,有效平衡了同步聚合中空闲等待与异步聚合中

计算机工程 www.ecice06.com

模型陈旧的问题。

针对卫星网络动态性高、隐私性强等特点，需要设计一种面向卫星网络的分布式异常检测方法，有效提升卫星网络中异常检测精度与联邦聚合效率，同时保护数据隐私。

## 2 基于层次联邦的空天地协同异常检测框架

FL[19]是一种旨在保护数据隐私的分布式深度学习框架，在 FL 中，当使用海量数据集进行模型训练或训练任务对时效性要求较高时，传统两层 FL 并不适用。针对上述问题，文献[20]提出层次联邦学习(HierFAVG)，该框架采用云服务器-边缘服务器-客户端协同分层聚合机制，有效缓解了传统两层 FL 框架中的中央服务器聚合压力大、设备与中央服务器之间通信链路距离长和延迟高等问题。星地链路的长距离通信使得传输延迟较大，且传输稳定性和可靠性易受各种自然因素的干扰和影响，在卫星网络中引入层次 FL，降低了卫星节点与中央服务器间的通信开销，但由于卫星网络与地面网络之间存在显著差异，高动态节点和多变网络拓扑影响了层次 FL 的收敛效率与模型性能，需要对其加以改进以适用于卫星网络。

本文提出了一种基于层次联邦学习的空天地协同异常检测框架，框架包含卫星节点层、边缘计算层、中央服务器层 3 个部分，如图 1 所示(彩色效果见《计算机工程》官网 HTML 版，下同)。

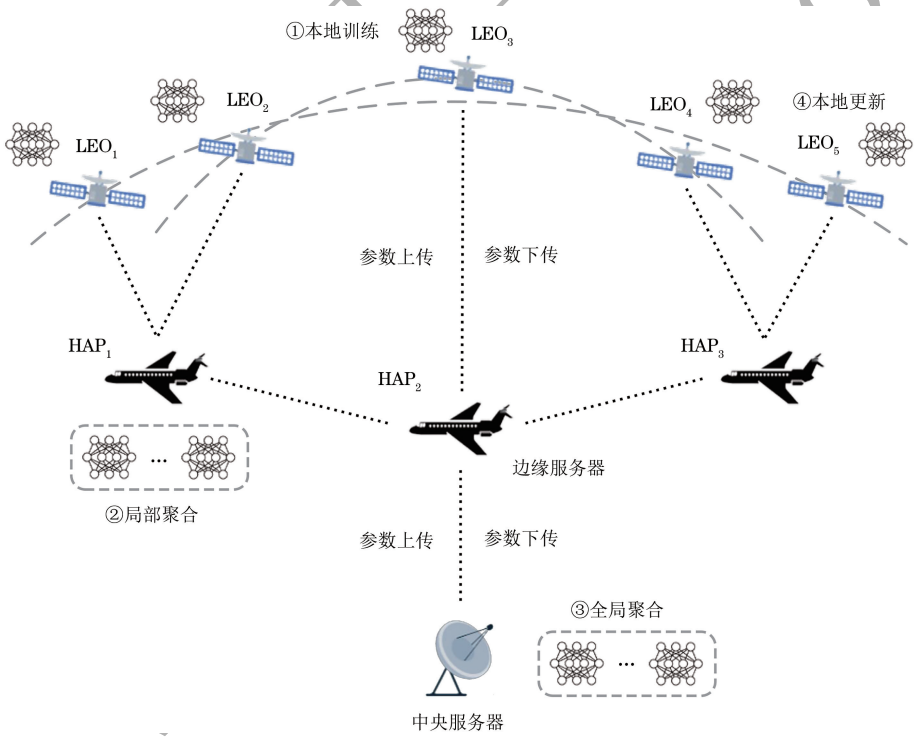



**图 1 空天地协同异常检测框架层次结构**

**Fig. 1 Hierarchical structure of the space-air-ground collaborative anomaly detection framework**

卫星节点层由 LEO 卫星组成，允许卫星与同一轨道相邻卫星通过 ISL 通信，各卫星节点进行异常检测、特征处理、本地模型更新。边缘计算层引入搭载高性能边缘计算平台的 HAPS 连接卫星与地面站，HAPS 为静态部署在地面站上空的平流层飞艇、固定翼无人机等，与通信范围内的卫星节点进行连接，通过 HAPS-卫星链路(HSL)[21]发送或接收模型参数，进行局部聚合。中央服务器层由部署于 GS 的中央服务器构成，其进行全局聚合，与主 HAPS 连接并发送全局模型或接收局部聚合模型参数。

异常检测流程分为模型的离线训练与在线检测两部分，考虑到星上计算资源有限等情况，在地面以离线方式分布式训练模型，直至达到指定精度后将模型上传至卫星进行在线检测与更新。首先，卫星节点将特征处理后的流量数据输入到经过训练的本地模型中，输出异常检测结果，若为正常流量则将继续向其他节点转发该数据，若为恶意流量数据则进行告警，更新本地数据库并训练本地模型；接着，卫星动态进入 HAPS 的通信范围，HAPS 与其连接并接收卫星下传的本地模型参数进行局部聚合；最后，HAPS 向地面站下传局部模型参数，由地面站进行全局聚合，重复上述步骤直至达到指定轮次或精度。模型训练与异常检测流程如图 2 所示。

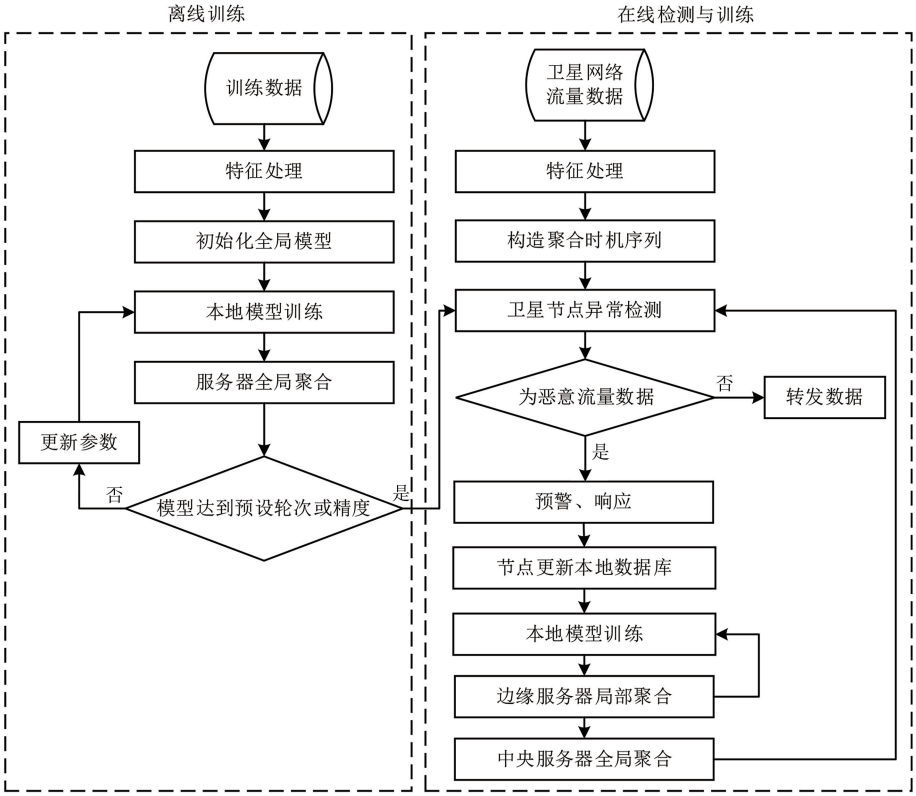



**图 2 模型训练和检测流程**

**Fig. 2 Model training and detection process**

由多个局部聚合服务器构成的中间层，能够有效解决在多个卫星直接与唯一中央服务器通信时所出现的问题。具体而言，在原通信模式下，多个卫星持续直接与中央服务器通信，会不断占用中央服务器的网络接口以监控卫星返回的参数，进而耗费大量带宽资源。而该中间层的引入，在分散 GS 通信压力的同时，也缓解了通信资源浪费的状况。由于卫星相对于 GS 的可视范围有限，星地连接存在时间窗口期，且每个时间点只有少部分卫星节点在通信范围内，严重影响了模型的聚合效率，而采用 HAPS 作为局部聚合服务器并进行分层半异步聚合的框架，扩大了 GS 与卫星通信的可视范围，使得一次聚合过程中的参与节点数量显著增加，从而加速了聚合过程，更加适应动态环境。

## 3 改进的动态半异步联邦聚合算法 FedIDSS

### 3.1 基础算法简介

层次联邦学习采用分层 FL 架构，具有一个云服务器与多个边缘服务器。首先，由云服务器初始化全局模型 $\omega_{t-1}$，将其下发给所有客户端后，参与节点 $i$ 使用本地数据集 $D_i$ 训练模型；然后，部分参与节点将更新后的本地模型参数 $\omega_{t,i}$ 上传至边缘服务器，经局部聚合得到参数 $\omega_{t,l}$，各边缘服务器再将局部模型参数上传至云服务器进行全局聚合，得到新一轮全局模型 $\omega_t$。聚合方法通常采用加权平均聚合算法 FedAvg[22] 进行同步聚合，聚合公式如式(1)所示：

$$\omega_{t,l}=\sum_{i=1}^{n}\frac{D_i}{D}\omega_{t,i} \tag{1}$$

式中：$t$ 为全局聚合轮次；$n$ 为边缘服务器 $l$ 下参与模型训练的节点总数；$D_i$ 为第 $i$ 个客户端上的数据集；$D=\bigcup_{i=1}^{n}D_i$ 为总训练数据集。模型训练的主要目标是优化全局模型参数 $\omega_t$，使得全局损失函数达到最小值，优化目标函数如式(2)和式(3)所示：

$$\min_{\omega_t}F(\omega_t) \tag{2}$$

$$F(\omega_t)=\frac{\sum_{i}^{l}|D_i|F_i(\omega_t)}{|D|} \tag{3}$$

式中：$|D|$ 为训练数据样本的总数；$|D_i|$ 为第 $i$ 个客户端上训练数据样本的数量。由于随机选择客户端具有不确定性，且客户端数量庞大，因此某些客户端将出现因长时间未加入聚合过程而导致模型过时等问题。为降低陈旧模型对全局模型的影响，文献[23]提出了临时加权聚合算法，为客户端增加时间戳 $t_i^{\text{timestamp}}$，聚合方法如式(4)所示：

$$\omega_t=\sum_{i=1}^{n}\frac{D_i}{D}\left(\frac{\mathrm{e}}{2}\right)^{-(t-t_i^{\text{timestamp}})}\omega_{t,i} \tag{4}$$

式中：e 为自然对数的底；$t_i^{\text{timestamp}}$ 表示第 $i$ 个客户端最近一次参与的聚合轮次。采用该方法聚合时，在参与节点本地数据集大小相同的情况下，更新更加频繁的模型将在聚合中拥有更高的权重，从而限制陈旧模型对全局模型的负面影响。

上述研究通过改进聚合权重，强化了高性能的模型参数在聚合中的比重，但在卫星网络应用场景下，聚合过程中除模型过时的问题以外，还存在由于不同卫星的运行周期、计算能力和通信资源不同，部分参与节点训练速度过慢，导致聚合效率与模型性能受到显著影响，对此，需要结合卫星动态信息对聚合策略进行进一步改进。

### 3.2 动态半异步聚合权重

由于各卫星节点计算能力、运行周期、本地数据等存在差异，采用异步聚合[24]时某些卫星节点可能在很长一段时间内都未参与到聚合过程中，其本地模型参数与全局模型参数存在较大差异，可能会对聚合后的全局模型造成影响。为进一步限制陈旧模型对全局模型的影响，对局部聚合方法进行改进，引入临时加权聚合算法，对所有参与节点增加时间戳，将其作为陈旧度折扣因子 $s_i$，并引入精确召回分数 $f_i$ 和本地数据集比重 $D_i/D$ 作为动态权重 $\alpha$，如式(5)~式(7)所示：

$$f_i=\frac{(1+\beta^2)\cdot P_{t-1,i}\cdot R_{t-1,i}}{\beta^2\cdot P_{t-1,i}+R_{t-1,i}} \tag{5}$$

$$s_i=\left(\frac{\mathrm{e}}{2}\right)^{-(t-t_i^{\text{timestamp}})} \tag{6}$$

$$\alpha=s_i\cdot f_i\cdot\frac{D_i}{D}=\left(\frac{\mathrm{e}}{2}\right)^{-(t-t_i^{\text{timestamp}})}\cdot\frac{(1+\beta^2)\cdot P_{t-1,i}\cdot R_{t-1,i}}{\beta^2\cdot P_{t-1,i}+R_{t-1,i}}\cdot\frac{D_i}{D} \tag{7}$$

改进后的聚合公式如式(8)所示：

$$\omega_t=(1-\alpha)\omega_{t-1}+\alpha\omega_{t,i}=\left(1-\left(\frac{\mathrm{e}}{2}\right)^{-(t-t_i^{\text{timestamp}})}\cdot\frac{(1+\beta^2)\cdot P_{t-1,i}\cdot R_{t-1,i}}{\beta^2\cdot P_{t-1,i}+R_{t-1,i}}\cdot\frac{D_i}{D}\right)\omega_{t-1}+\left(\left(\frac{\mathrm{e}}{2}\right)^{-(t-t_i^{\text{timestamp}})}\cdot\frac{(1+\beta^2)\cdot P_{t-1,i}\cdot R_{t-1,i}}{\beta^2\cdot P_{t-1,i}+R_{t-1,i}}\cdot\frac{D_i}{D}\right)\omega_{t,i} \tag{8}$$

式中：$P_{t-1,i}$ 为第 $i$ 个参与节点的精确率；$R_{t-1,i}$ 为召回率；$\beta$ 为精确率的权重。模型的精确率与召回率是分类性能的重要评判指标，两者通常情况下呈负相关。精确召回分数 $f_i$ 用于调节精确率与召回率的影响，较为全面地评价模型的性能，在本文中设置为 0.8，也就是精确率的权重高于召回率。陈旧度折扣因子 $s_i$ 是对模型陈旧度的判断分数，参与节点更新越频繁时 $s_i$ 的值越大，因此，在聚合中更新更加频繁、综合性能更高的模型参数将获得更高的权重。

### 3.3 改进聚合时机序列

在采用同步聚合方法进行聚合时，聚合周期多为固定间隔，而文献[25]提出采用固定聚合时机序列并不能使模型达到最优性能，更优的聚合时机序列是公差为负的等差数列，也就是聚合频率逐渐增加的聚合方式，更优聚合时机序列如式(9)所示：

$$\min_{I_T=\{a_0,a_1,\cdots,a_R\}} f(\omega)$$
$$\text{s.t. } 0=a_0<a_1<\cdots<a_R=T \tag{9}$$

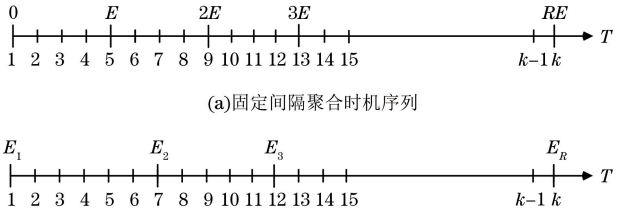
式中：$R$ 为通信轮数；$a_R$ 为第 $R$ 轮的聚合时机；$T$ 为总迭代次数；$E=T/R$ 为固定聚合间隔。固定聚合时机序列为 $I_T=\{0,E,2E,\cdots,RE\}$，更优聚合时机序列为 $\varepsilon_T=\{E_1,E_2,\cdots,E_R\}$，该序列是首项为 $E_1$、公差为 $d_\varepsilon$、和为 $T$ 的等差数列。因此，要构造该序列，首先需要确定公差与首项。根据等差序列求和公式可得式(10)：

$$d_\varepsilon=\frac{2(E_1-E)}{R-1} \tag{10}$$

根据条件 $\Delta\leqslant E_i$，假设 $H\cdot\Delta<E_i$，可得式(11)：

$$E<E_1<\frac{2(R-1+H)}{R-1+2H}E \tag{11}$$

固定间隔聚合时机序列和更优聚合时机序列的示意图如图 3 所示。




(a)固定间隔聚合时机序列

(b)更优聚合时机序列

**图 3 聚合时机序列**

**Fig. 3 Aggregation timing sequence**

卫星网络中节点始终处于动态运行状态，因此应用于地面网络的聚合策略对星地协同架构中的聚合效率存在限制[26]。采用固定间隔同步聚合时，训练前期模型准确率低，聚合后模型性能提升缓慢，而在训练后期本地模型准确率提高，聚合后模型性能更优。此外，由于部分卫星节点算力有限或周期较长，使得聚合时间过长，或长期未参与聚合，导致本地模型陈旧，对全局模型产生负面影响。卫星网络中采用固定聚合时机序列示意图如图 4 所示。

计算机工程 www.ecice06.com

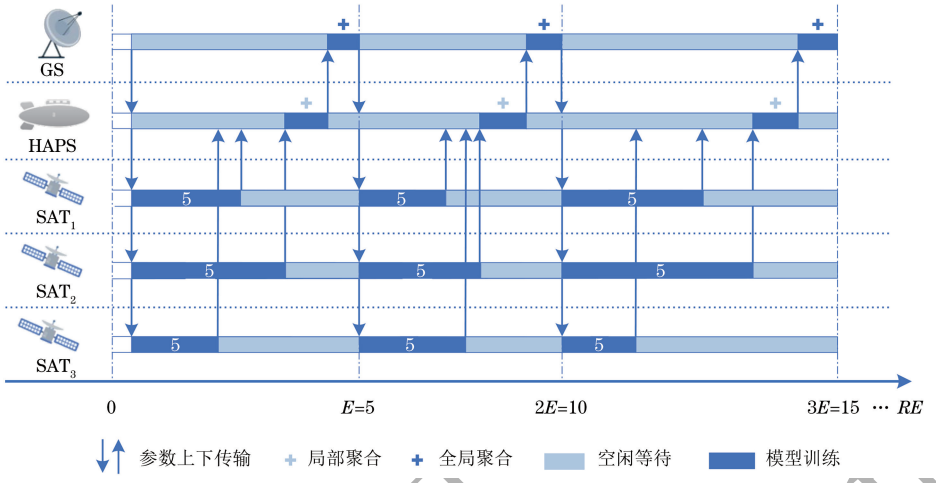



**图 4 卫星网络中采用固定聚合时机序列的示意图**

**Fig. 4 Schematic diagram of fixed aggregation timing sequence in satellite network**

针对上述问题，为有效平衡卫星网络中的聚合效率与模型性能，结合卫星算力与通信信息，构造改进聚合时机序列 $\varepsilon_T=\{E_1,E_2,\cdots,E_R\}$。假设在采用圆轨道的 Waker-Delta[27] 星座中，轨道和卫星以相同间隔均匀分布，卫星动态进入 HAPS 的通信范围，通信存在窗口期[28]。在卫星运行过程中，尽管卫星节点间以及轨道之间的间隔相同，但不同卫星与同一 HAPS 或同一卫星与不同 HAPS 之间的通信连接时间并不相同。由于卫星节点完成一次参数接收、模型训练、参数下传过程的时间至少为一个窗口期，将 2 次聚合间参与节点本地模型迭代次数 $E$ 作为固定聚合间隔，$E$ 的计算方法如式(12)所示：

$$E=\frac{t_l-t_{ts}-t_p+nt_z}{t_{tr}}(n\geqslant 0) \tag{12}$$

式中：$t_l$ 为通信保持时间；$t_{ts}$、$t_p$、$t_z$ 分别为数据传输时延、传播时延[29]、卫星轨道周期。$t_{ts}$、$t_p$ 计算方法分别如式(13)和式(14)所示：

$$t_{ts}=\frac{L_{\text{packet}}}{R_{\text{send}}} \tag{13}$$

$$t_p=\frac{d(i,j)}{v_s} \tag{14}$$

式中：$L_{\text{packet}}$ 为数据包长度，单位为 bit；$R_{\text{send}}$ 为当前节点转发速度，单位为 bit/s；$d(i,j)$ 为卫星节点 $i$ 和 HAPS 节点 $j$ 之间的距离；$v_s$ 为无线电波传播速度，取 $3\times10^8$ m/s。

$t_{tr}$ 为卫星节点模型平均训练时间，与数据集大小 $|D_i|$、处理单个数据样本所需的 CPU 周期数 $c_i$ 和卫星节点的 CPU 频率 $v_i$ 成正比，其计算方法如式(15)所示：

$$t_{i,tr}=\frac{c_i|D_i|}{v_i} \tag{15}$$

根据式(11)和式(12)可构造首项，如式(16)所示：

$$\frac{t_l-t_{ts}-t_p+nt_z}{t_{tr}}<E_1<\frac{2(R-1+H)}{R-1+2H}\cdot\frac{t_l-t_{ts}-t_p+nt_z}{t_{tr}} \tag{16}$$

由此可构造改进聚合序列，如式(17)所示：

$$\varepsilon_T=\{E_1,E_2,\cdots,E_R\}=\{E_1,E_1-d_\varepsilon,\cdots,E_1-(R-1)d_\varepsilon\}=\left\{E_1,E_1-\frac{2}{R-1}\left(E_1-\frac{t_l-t_{ts}-t_p+nt_z}{t_{tr}}\right),\cdots,E_1-2\left(E_1-\frac{t_l-t_{ts}-t_p+nt_z}{t_{tr}}\right)\right\} \tag{17}$$

采用改进聚合时机序列进行聚合的示意图如图 5 所示。

### 3.4 FedIDSS 算法流程

首先，采用离线方式在地面设备中训练异常检测模型；然后，通过空天地协同异常检测框架进行在线特征处理和异常检测，参与节点根据改进后的聚合时机序列参与聚合，服务器使用动态聚合权重对接收的节点本地模型参数进行聚合，以提高卫星网络中联邦学习聚合效率、保证异常检测精度。FedIDSS 算法伪代码如下：

**算法 1** FedIDSS 算法

**输入** 本地数据集 $D_i=\{x_j,y_j\}_{j=1}^{|D_i|}$，初始模型权重 $\omega_0$

**输出** 全局模型权重 $\omega_t$

1. Begin
2. Initialize all clients with parameter $\omega_0$ //全局模型初//始化
3. $\varepsilon_T\leftarrow$Initial_Interval() //构造聚合时机序列
4. For each communication round r = 1, 2,…, R do

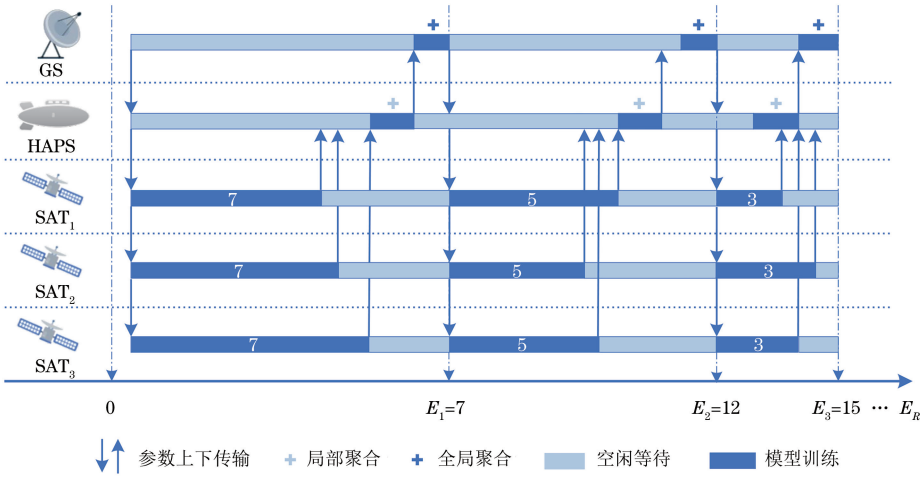



**图 5 卫星网络中采用改进聚合时机序列的示意图**

**Fig. 5 Schematic diagram of improved aggregation timing sequence in satellite network**

5. For each satellite i = 1, 2,…, N in parallel do
6. $\omega_i(r) \leftarrow \omega_i(r-1) - \eta \nabla F_i(\omega_i(r-1))$
7. End for
8. For each $I_r$ in $\varepsilon_T$ do
9. For each HAPS l = 1, 2,…, N in parallel do
10. t←t+1
11. $\omega_t^l(r) \leftarrow \text{LocalAggregation}(\omega_i^l(r)_{i\in\ell})$
12. If t=$I_r$ then
13. HAPS transmit $\omega_t^l(r)$ to GS
14. End if
15. End for
16. $\omega(r) \leftarrow \text{GlobalAggregation}(\omega^l(r)_{l=1}^{\ell})$
17. End for

## 4 实验及结果分析

### 4.1 数据集及预处理

为验证模型的有效性，本文使用公开的星地融合网络流量数据集 STIN 与地面网络流量数据集 CIC-IDS-2017。STIN 数据集划分与攻击类型如表 1 所示。

**表 1 STIN 数据集部分特征**

**Table 1 Partial characteristics of STIN dataset**

| 特征 | 描述 |
|---|---|
| fw_pk | 前向数据包总数 |
| l_fw_pkl | 前向数据包总长度 |
| pkl_len_min | 数据流最小长度 |
| pkl_len_max | 数据流最大长度 |
| bw_pkt_S | 每秒传输后向数据包数 |
| fl_byt_s | 每秒传输字节数 |
| syn_cnt | SYN 数据包数 |
| urg_cnt | URG 数据包数 |

STIN 是 2020 年公布的星地网络良性与恶意流量特征数据集，分为卫星网络数据集 SAT20 与地面网络数据集 TER20，均为 15 维网络流量特征。其中，SAT20 包含 2 种针对卫星网络 DTN 协议的 DDoS 攻击，分别为 SYN_DDoS 和 UDP_DDoS，TER20 包含 7 种针对地面网络的攻击，分别为后门攻击、僵尸网络、Web 攻击以及 4 种 DDoS 攻击。CIC-IDS-2017 是 2017 年采集公布的网络流量数据集，包含 DDoS、僵尸网络、Web 攻击、暴力 FTP 等多种网络攻击，本文使用其中的 DDoS、僵尸网络、Web 攻击 3 种攻击类型与正常类型的流量数据。

在数据预处理时，首先删除特征中的强相关特征与无关特征，剔除重复、缺失的异常数据，将文本类型的特征转换为数值类型，并对其进行 One-Hot 编码与归一化处理。接着，对数据进行特征选择，对处理后的数据使用随机森林算法计算特征的重要度评分，选取评分最高的 8 个特征。最后，将打乱后的数据按照 6∶4的比例划分为训练集和测试集。处理后的 STIN 数据集共包含 51 050 条数据，其中训练集包含 30 630 条数据，测试集包含 20 420 条数据；CIC-IDS-2017 数据集共包含 51 140 条数据，其中训练集包含 30 756 条数据，测试集包含 20 384 条数据。

### 4.2 实验评估指标

实验采用准确率（Accuracy，$A$）、精确率（Precision，$P$）、召回率（Recall，$R$）、F1 值（F1，$F_1$）作为指标对模型性能进行评估，并引入聚合时间与通信成本作为方法代价的评价指标，当算法 1 与算法 2 达到相同的准确率时，算法 2 与算法 1 训练轮次的比值即为相对通信成本。评价指标的计算方法分别如式(18)～式(21)所示，其中，$N_{TP}$、$N_{TN}$、$N_{FP}$、$N_{FN}$ 分别表示真正例、真反例、假正例、假反例。

www.ecse06.com 计算机工程

$$A=\frac{N_{TP}+N_{TN}}{N_{TP}+N_{FP}+N_{TN}+N_{FN}} \tag{18}$$

$$R=\frac{N_{TP}}{N_{TP}+N_{FN}} \tag{19}$$

$$F_1=\frac{2\times P\times R}{P+R} \tag{20}$$

$$T_{total}=\sum_{t=1}^{r_{rounds}}(T_{local}+T_{communication}) \tag{21}$$

### 4.3 实验环境与参数设置

本文在 Windows 11 系统上使用 PyTorch 搭建实验运行环境，具体软硬件环境如表 2 所示。

表 2 硬件与软件环境参数

Table 2 Hardware and software environment parameters

| 配置项 | 配置 |
|---|---|
| CPU | 11th Gen Intel® Core™ i5-11400H @2.70 GHz |
| 内存 | 16.0 GB RAM |
| 操作系统 | Windows 11 64 位 |
| 编程语言 | Python 3.7.6 |
| 软件环境 | PyCharm 2019.3.3，STK 11.6.0 64 位，torch 1.8.1 |

实验仿真环境采用卫星星座分析软件 STK（Systems Tool Kit）模拟 Walker-Delta 星座，包含 4 个均匀分布的轨道平面，每个轨道以相同间隔分布 5 颗卫星，星座具体参数设置如表 3 所示。HAPS 静态部署在距地面 50 km 处，部署位置为均匀间隔分布、卫星过境时间最长的现有地面站上空，中央服务器所在的地面站位于中国北京。

表 3 Walker-Delta 星座仿真环境

Table 3 Simulation environment of Walker-Delta constellation

| 参数名称 | 参数设置 |
|---|---|
| 卫星类型 | LEO |
| 轨道数目/个 | 4 |
| 卫星数目/个 | 20 |
| 轨道高度/km | 1 400 |
| 轨道倾角/(°) | 60 |
| 卫星绕地球飞行周期/min | 约 114 |
| HAPS 高度/km | 50 |

在上述参数设置的基础上，数据传输速率设置为 1.0 Mb/s，卫星与 HAPS 的通信连接保持时间为 10.75 min，仿真环境结构如图 6～图 8 所示。

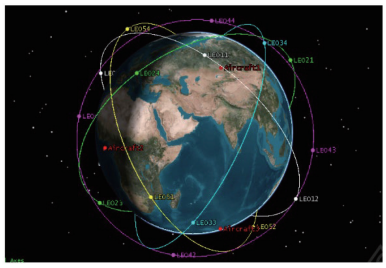


图 6 Walker-Delta 星座与 HAPS 结构

Fig.6 Walker-Delta constellation and HAPS structure

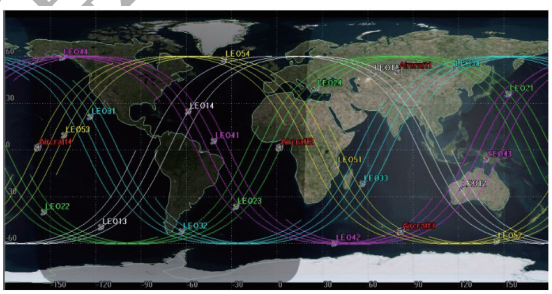


图 7 Walker-Delta 星座卫星轨道周期

Fig.7 Orbital period of the Walker-Delta constellation satellite

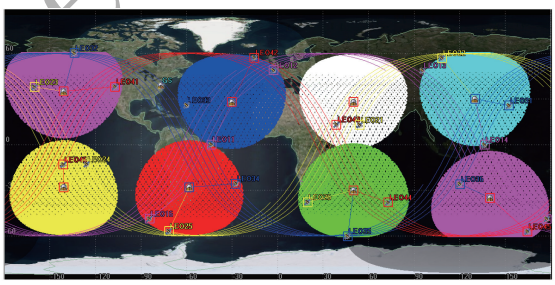


图 8 HAPS 与卫星连接全覆盖示意图

Fig.8 Schematic diagram of full coverage for HAPS and satellite connections

### 4.4 实验结果分析

BP 神经网络因其具有分类能力好、模型体量小的特点，在异常检测领域被广泛应用，因此，本文采用 BP 神经网络作为异常检测模型。在训练阶段，使用 SGD 优化器，学习率 $\eta=0.01$，批量大小为 64，损失函数为 Cross-Entropy，数据为非独立同分布（Non-IID）。实验主要包括两部分：一是与基于传统联邦学习算法的异常检测模型进行对比，以验证 FedIDSS 算法能够保证对星地融合网络异常流量的检测精度；二是与现有联邦学习聚合算法和卫星网络中的改进联邦学习聚合算法进行对比，以评估 FedIDSS 算法在优化聚合效率方面的有效性。

#### 4.4.1 异常检测性能分析

为验证异常检测模型在检测性能上的表现，分别在不同数据集上进行多分类实验，其中包括 Botnet、DDoS、Backdoor、Web Attack 这 4 种攻击类以及正常类的数据。对通信 100 轮的异常检测模型的检测准确率、召回率和 F1 值进行统计，如表 4、表 5 所示。

计算机工程 www.ecice06.com

表 4 STIN 数据集上异常检测模型的多分类实验结果

Table 4 Results of multi-classification experiment of anomaly detection model on STIN dataset

| 数据集 | 数据类型 | Accuracy | Recall | F1 |
|---|---|---|---|---|
| STIN | DDoS | 0.80 | 0.78 | 0.79 |
| | Backdoor | 0.91 | 0.81 | 0.87 |
| | Botnet | 0.96 | 0.92 | 0.92 |
| | Normal | 0.82 | 0.89 | 0.85 |

表 5 CIC-IDS-2017 数据集上异常检测模型的多分类实验结果

Table 5 Results of multi-classification experiment of anomaly detection model on CIC-IDS-2017 dataset

| 数据集 | 数据类型 | Accuracy | Recall | F1 |
|---|---|---|---|---|
| CIC-IDS-2017 | DDoS | 0.98 | 0.98 | 0.98 |
| | Web Attack | 0.99 | 0.97 | 0.98 |
| | Botnet | 0.99 | 0.99 | 0.98 |
| | Normal | 0.98 | 0.99 | 0.99 |

在 STIN 数据集上，FedIDSS 对卫星网络中的 DDoS 攻击的检测准确率可达 0.80，召回率达 0.78，对于 Backdoor、Botnet 攻击的检测准确率分别为 0.91 和 0.96；在 CIC-IDS-2017 数据集上，FedIDSS 对于各类攻击的检测准确率和召回率均在 0.98 左右。在星地融合数据集上的检测结果相比地面网络数据集而言不太稳定，这可能是由于星地网络融合数据的样本数量有限，且特征与地面网络数据存在一定差异。尽管如此，从实验结果中还是可以明显看出，基于 FedIDSS 算法的异常检测模型在提高聚合效率的基础上，仍能对大部分攻击类别取得较高的检测性能。

为更直观地评估模型的异常检测性能，采用混淆矩阵表示模型分类性能，由图 9 和图 10 可知，本文模型在 STIN 和 CIC-IDS-2017 数据集上对不同攻击类型均能保证有效的分类性能。

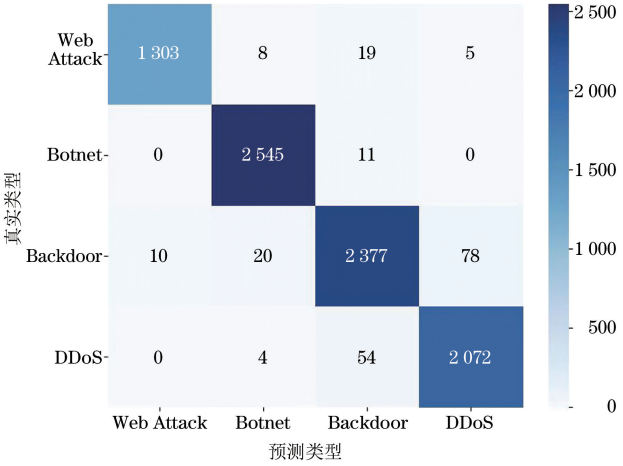



图 9 基于 STIN 数据集的异常检测混淆矩阵

Fig.9 Anomaly detection confusion matrix based on STIN dataset

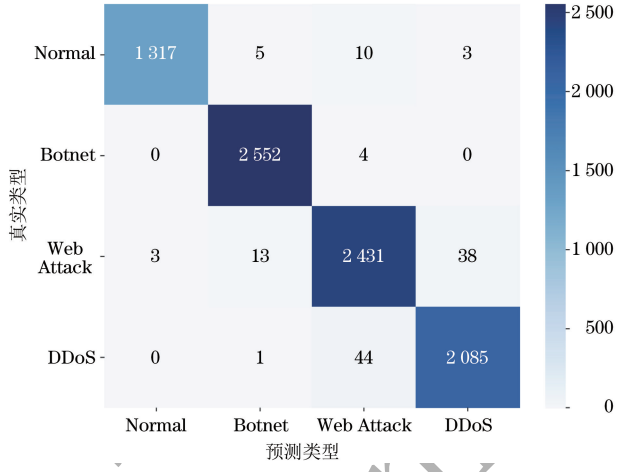



图 10 基于 CIC-IDS-2017 数据集的异常检测混淆矩阵

Fig.10 Anomaly detection confusion matrix based on CIC-IDS-2017 dataset

4.4.2 联邦学习算法性能对比分析

为验证 FedIDSS 算法在优化聚合效率方面的有效性，将其与联邦学习同步聚合算法和卫星网络中的改进联邦学习聚合算法进行实验对比。实验使用相同的合轮数和异常检测模型，分别在 STIN 和 CIC-IDS-2017 数据集上评估不同联邦学习算法的聚合效率和聚合后的模型性能。将每个数据集下 HierFAVG 的通信成本记为 1，实验结果如表 6、表 7、图 11 和图 12 所示。

表 6 STIN 数据集上不同 FL 算法的性能对比

Table 6 Performance comparison of different FL algorithms on STIN dataset

| FL 算法 | Accuracy/% | Recall/% | 聚合时间/h | 通信成本 |
|---|---|---|---|---|
| FedAvg | 60.56 | 67.15 | 36.00+ | 2.44 |
| HierFAVG | 77.70 | 79.35 | 36.00+ | 1.00 |
| FedISL | 42.17 | 52.22 | 36.00+ | 4.31 |
| FedIDSS | 80.17 | 85.11 | 32.31 | 0.95 |

表 7 CIC-IDS-2017 数据集上不同 FL 算法的性能对比

Table 7 Performance comparison of different FL algorithms on CIC-IDS-2017 dataset

| FL 算法 | Accuracy/% | Recall/% | 聚合时间/h | 通信成本 |
|---|---|---|---|---|
| FedAvg | 63.20 | 65.10 | 36.00+ | 1.62 |
| HierFAVG | 79.60 | 81.71 | 36.00+ | 1.00 |
| FedISL | 43.62 | 52.15 | 36.00+ | 5.31 |
| FedIDSS | 81.65 | 84.12 | 31.83 | 0.97 |

在表 6 和图 11 中，对比了 FedAvg、HierFAVG、FedISL 以及本文算法 FedIDSS 在 STIN 数据集上的性能，实验结果显示，FedAvg 需要超过 36 h 才能收敛，这是因为同步聚合时大部分连接处于空闲状态，等待时间过长导致收敛速度缓慢；

计算机工程 www.ccjc06.com

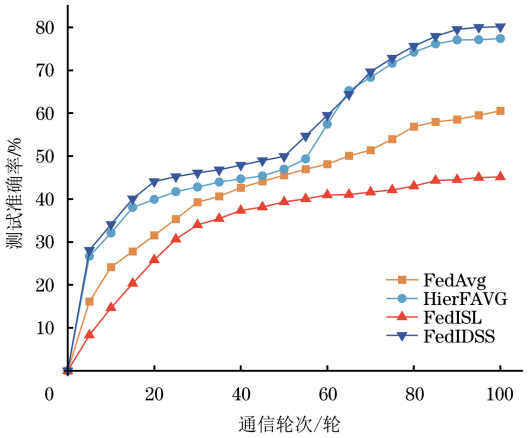



图 11 STIN 数据集上不同 FL 算法的准确率曲线

Fig. 11 Accuracy curves of different FL algorithms on STIN dataset

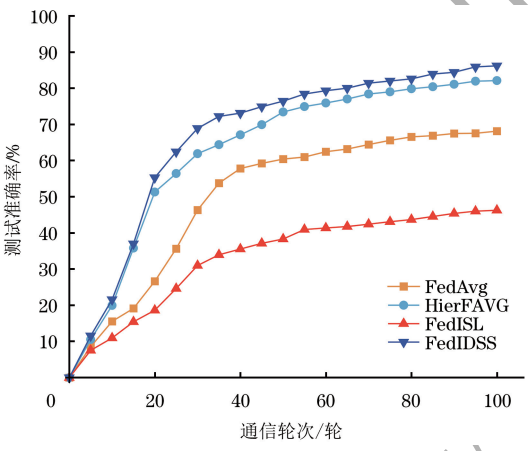



图 12 CIC-IDS-2017 数据集上不同 FL 算法的准确率曲线

Fig. 12 Accuracy curves of different FL algorithms on CIC-IDS-2017 dataset

HierFAVG 相较于 FedAvg 在准确率上有所提升，但同样受制于空闲连接，聚合时间超过 36 h；在中央服务器位于北极点这一理想设置下，FedISL 聚合时间可达到 3.5 h，但在非理想条件下准确率约为 45.17%，且聚合时间仍超过 36 h；FedIDSS 在训练 32.3 h 后准确率达 80.17%，相对通信成本为 0.95，在聚合速度与检测性能方面相较于对比算法实现了显著提升。由表 7 和图 12 可知，本文算法在 CIC-IDS-2017 数据集上也具有良好的聚合效率和异常检测性能。

## 5 结束语

本文对卫星网络中的层次联邦学习框架和动态半异步聚合算法进行优化，提出一种卫星网络分布式异常检测方法，以解决卫星网络中由于卫星可见范围有限使得聚合速度过慢、模型检测精度受影响等问题。该方法首先融合层次联邦学习架构，提出空天地协同异常检测框架，引入高空通信平台作为边缘计算层进行分层聚合与协同训练，扩大星地通信范围；然后，提出改进的动态半异步聚合算法，构造改进聚合时机序列，用于平衡收敛速度与模型性能，同时增加陈旧度折扣因子、精确召回分数等动态权重，保证模型检测精度。实验结果表明，FedIDSS 相较于其他对比算法收敛速度更快、综合性能更稳定，能够在提升卫星网络中联邦聚合效率的基础上，保证模型异常检测性能。在未来，可考虑采用启发式算法等方式对星地融合网络数据进行特征选择，进一步提高检测精度，以及引入同态加密等隐私保护方法，加强对数据传输协议和加密算法的研究。

## 参考文献

[1] KODHELI O, LAGUNAS E, MATURO N, et al. Satellite communications in the new space era: a survey and future challenges[J]. IEEE Communications Surveys & Tutorials, 2021, 23(1): 70-109.

[2] GUO H Z, LI J Y, LIU J J, et al. A survey on space-air-ground-sea integrated network security in 6G[J]. IEEE Communications Surveys & Tutorials, 2022, 24(1): 53-87.

[3] YAO H P, WANG L Y, WANG X D, et al. The space-terrestrial integrated network: an overview[J]. IEEE Communications Magazine, 2018, 56(9): 178-185.

[4] 蒋长林, 李清, 王羽, 等. 天地一体化网络关键技术研究综述[J]. 软件学报, 2024, 35(1): 266-287.
JIANG C L, LI Q, WANG Y, et al. Survey on key technologies in space-ground integrated network[J]. Journal of Software, 2024, 35(1):266-287. (in Chinese)

[5] CAO H, WU L L, CHEN Y, et al. Analysis on the security of satellite Internet[EB/OL]. [2023-10-05]. https://link.springer.com/chapter/10.1007/978-981-33-4922-3_14.

[6] ASHRAF I, NARRA M, UMER M, et al. A deep learning-based smart framework for cyber-physical and satellite system security threats detection[J]. Electronics, 2022, 11(4): 667.

[7] AGRAWAL S, SARKAR S, AOUEDI O, et al. Federated learning for intrusion detection system: concepts, challenges and future directions[J]. Computer Communications, 2022, 195: 346-361.

[8] ZHAO J Y, ZOU J X, LI Z P, et al. High Altitude Platform (HAP) communication system based on satellite communication theory[C]//Proceedings of the 22nd IEEE International Conference on Communication Technology (ICCT). Washington D. C., USA: IEEE Press, 2022: 446-450.

[9] GUO W, XU J, PEI Y K, et al. A distributed collaborative entrance defense framework against DDoS attacks on satellite Internet[J]. IEEE Internet of Things Journal, 2022, 9(17): 15497-15510.

[10] CAO S, DANG S X, ZHANG Y, et al. A blockchain-based access control and intrusion detection framework for satellite communication systems[J]. Computer Communications, 2021, 172: 216-225.

[11] LAVAUR L, PAHL M O, BUSNEL Y, et al. The evolution of federated learning-based intrusion detection and mitigation: a survey[J]. IEEE Transactions on Network and Service Management, 2022, 19(3): 2309-2332.

[12] 刘金硕, 詹岱依, 邓娟, 等. 基于深度神经网络和联邦学习的网络入侵检测[J]. 计算机工程, 2023, 49(1): 15-21, 30.

www.cicone.com

LIU J S, ZHAN D Y, DENG J, et al. Network intrusion detection based on deep neural network and federated learning[J]. Computer Engineering, 2023, 49(1): 15-21, 30. (in Chinese)
[13] LI K, ZHOU H C, TU Z, et al. Distributed network intrusion detection system in satellite-terrestrial integrated networks using federated learning[J]. IEEE Access, 2020, 8: 214852-214865.
[14] MOUSTAFA N, KHAN I A, HASSANIN M, et al. DFSat: deep federated learning for identifying cyber threats in IoT-based satellite networks[J]. IEEE Transactions on Industrial Informatics, 2024, 8: 1-8.
[15] SALIM S, MOUSTAFA N, HASSANIAN M, et al. Deep-federated-learning-based threat detection model for extreme satellite communications[J]. IEEE Internet of Things Journal, 2024, 11(3): 3853-3867.
[16] RAZMI N, MATTHIESEN B, DEKORSY A, et al. On-board federated learning for dense LEO constellations[C]// Proceedings of the IEEE International Conference on Communications. Washington D. C., USA: IEEE Press, 2022: 4715-4720.
[17] ELMAHALLAWY M, LUO T, IBRAHEM M I. Secure and efficient federated learning in LEO constellations using decentralized key generation and on-orbit model aggregation[C]// Proceedings of the 2023 IEEE Global Communications Conference. Washington D. C., USA: IEEE Press, 2023: 5727-5732.
[18] SO J, HSIEH K, ARZANI B, et al. FedSpace: an efficient federated learning framework at satellites and ground stations[EB/OL]. [2023-12-21]. https://doi.org/10.48550/arXiv.2202.01267.
[19] MCMAHAN B, MOORE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data[EB/OL]. [2023-12-21]. https://proceedings.mlr.press/v54/mcmahan17a/mcmahan17a.pdf.
[20] LIU L M, ZHANG J, SONG S H, et al. Client-edge-cloud hierarchical federated learning[C]//Proceedings of the 2020 IEEE International Conference on Communications (ICC). Washington D.C., USA: IEEE Press, 2020: 1-6.
[21] MEI C L, GAO C, XING Y X, et al. An energy consumption minimization optimization scheme for HAP-satellites edge computing[C]//Proceedings of the 22nd IEEE International Conference on Communication Technology (ICCT). Washington D. C., USA: IEEE Press, 2022: 857-862.
[22] LI T, SAHU A K, ZAHEER M, et al. Federated optimization in heterogeneous networks[J]. Proceedings of Machine Learning and Systems, 2020, 2: 429-450.
[23] CHEN Y, SUN X Y, JIN Y C. Communication-efficient federated deep learning with layerwise asynchronous model update and temporally weighted aggregation[J]. IEEE Transactions on Neural Networks and Learning Systems, 2020, 31(10): 4229-4238.
[24] XIE C, KOYEJO S, GUPTA I. Asynchronous federated optimization[EB/OL]. [2023-12-21]. https://arxiv.org/abs/1903.03934.
[25] ZHANG H, WU T T, CHENG S Y, et al. Aperiodic local SGD: beyond local SGD[C]// Proceedings of the 51st International Conference on Parallel Processing. Washington D.C., USA: IEEE Press, 2022: 1-10.
[26] 张泰江, 李勇军, 赵尚弘. 基于 GEO/LEO 双层卫星网络的路由算法优化设计[J]. 计算机工程, 2020, 46(7): 198-205.
ZHANG T J, LI Y J, ZHAO S H. Optimization design of routing algorithm based on GEO/LEO double-layer satellite network[J]. Computer Engineering, 2020, 46(7): 198-205. (in Chinese)
[27] VEMURI S S, DAPPURI B. Walker-Delta constellation design for LEO-based navigation using small satellites[J]. IET Conference Proceedings, 2022, 2022(1): 250-253.
[28] 郑鹏飞, 陈宏宇, 郭崇滨. 低轨巨型链形星座解析设计及效能分析[J]. 西北工业大学学报, 2022, 40(1): 148-157.
ZHENG P F, CHEN H Y, GUO C B. Analytical design and performance analysis of LEO mega chain satellite constellation[J]. Journal of Northwestern Polytechnical University, 2022, 40(1): 148-157. (in Chinese)
[29] DAKIC K, CHAN C C, AL HOMSSI B, et al. On delay performance in mega satellite networks with inter-satellite links[C]// Proceedings of the 2023 IEEE Global Communications Conference. Washington D. C., USA: IEEE Press, 2023: 4896-4901.

编辑 吴云芳

计算机工程 www.ecice06.com