文章编号：1003-0530(2024)04-0706-13

基于收缩自编码器的无人机GPS欺骗攻击协同检测方法

佘丁辰[1] 王 威*[1] 王加琪[1] 晋本周[1] 刘敬颐[2] 吴启晖[1]

（1. 南京航空航天大学电子信息工程学院，江苏南京 211106；
2. 中国电信股份有限公司江苏分公司，江苏南京 210037）

摘 要： GPS欺骗攻击是一种通过改变GPS信号来诱导接收机导航系统的恶意攻击，它会使无人机产生偏离运行轨迹、飞入禁飞区、强制降落等异常行为。当前对GPS欺骗攻击的检测仍存在模型训练效率较低、检测性能不高等问题，基于此，本文提出了一种无人机GPS欺骗攻击协同检测方法。该方法采用联邦学习框架，多个基站通过本地接收的无人机运行数据协同训练异常检测模型并计算异常检测阈值，进而检测无人机是否存在GPS欺骗攻击。此外，为了防止在联邦学习过程中不同基站本地训练数据分布差异过大导致模型训练效果降低的问题，本文采用收缩自编码器作为异常检测模型。与自编码器相比，收缩自编码器通过在损失函数中加入新的损失项，将训练数据样本的低维表示压缩到更小的范围内，从而使模型在训练过程中能够更好地学习训练数据样本的低维特征，提高了模型区分正常数据和异常数据的能力。基于公开数据集的实验结果表明，本文提出的方法对无人机GPS欺骗攻击的准确率、查准率和召回率分别达到了96.49%、96.03%和93.85%，比原始的自编码器提高了1.63%、0.8%和4.62%，且与采用集中式学习框架相比，本文提出的协同检测方法能够显著提高模型的训练效率。同时，本文提出的联邦学习收缩自编码器受平衡系数改变的影响最小，在异常检测阈值计算不准确的情况下仍然能够达到较好的检测结果。

关键词： 无人机GPS欺骗攻击；联邦学习；收缩自编码器；协同检测

中图分类号： TN925 **文献标识码：** A **DOI：** 10.16798/j.issn.1003-0530.2024.04.009

引用格式： 佘丁辰，王威，王加琪，等. 基于收缩自编码器的无人机GPS欺骗攻击协同检测方法[J]. 信号处理，2024，40(4)：706-718. DOI：10.16798/j.issn.1003-0530.2024.04.009.

Reference format： SHE Dingchen，WANG Wei，WANG Jiaqi，et al. Collaborative detection method of UAV GPS spoofing attack based on shrink autoencoder[J]. Journal of Signal Processing，2024，40(4)：706-718. DOI: 10.16798/j.issn.1003-0530.2024.04.009.

Collaborative Detection Method of UAV GPS Spoofing Attack Based on Shrink Autoencoder

SHE Dingchen[1] WANG Wei*[1] WANG Jiaqi[1] JIN Benzhou[1] LIU Jingyi[2] WU Qihui[1]

（1. College of Electronic and Information Engineering，Nanjing University of Aeronautics and Astronautics，Nanjing，Jiangsu 211106，China；
2. China Telecom Corporation Limited Jiangsu Branch，Nanjing，Jiangsu 210037，China）

收稿日期：2023-11-14；修回日期：2024-01-17

*通信作者：王威 wei_wang@nuaa.edu.cn *Corresponding Author：WANG Wei，wei_wang@nuaa.edu.cn

基金项目：国家自然科学基金(62371231)；江苏省重点研发计划(产业前瞻与关键核心技术)重点项目(BE2022068，BE2023027)；江苏省前沿引领技术基础研究重大项目课题(BK20222001)；中国科协青年人才托举工程(YESS20200207)

Foundation Items：The National Natural Science Foundation of China (62371231)；The Jiangsu Provincial Key Research and Development Program (BE2022068，BE2023027)；The Natural Science Foundation on Frontier Leading Technology Basic Research Project of Jiangsu (BK20222001)；The Young Elite Scientist Sponsorship Program，China Association for Science and Technology (YESS20200207)

Abstract: As a malicious attack by manipulating the received GPS signal of an unmanned aerial vehicle (UAV), a GPS spoofing attack may cause severe abnormal behaviors in UAVs, such as deviating from the intended path, flying into the no-fly zone, and forced landing. Therefore, to ensure the safety of UAVs, it is urgently demanded to investigate the GPS spoofing attack detection methods. Currently, the detection of GPS spoofing attacks still suffers from low model training efficiency and low detection performance. To tackle this problem, a collaborative UAV GPS spoofing attack detection scheme is proposed in this paper. Specifically, a federated learning framework is adopted, where multiple base stations (BSs) train the anomaly detection model and calculate the anomaly detection threshold with locally received UAV operation data, to detect whether the UAV suffers a GPS spoofing attack. To mitigate the performance deterioration resulting from uneven data distribution in the federated learning model, the shrink autoencoder is used. Compared with conventional autoencoders, a new loss term is added to the loss function in the shrink autoencoder, which can compress the low-dimensional representation of the training data sample into a smaller range. Thus, the low-dimensional features of the training data can be captured more easily, and the distinguishing capability of abnormal data can be improved. Experimental results with an open data set show that the accuracy rate, precision rate, and recall rate with the proposed scheme can reach up to 96.49%, 96.03%, and 93.85%, respectively, which are 1.63%, 0.8%, and 4.62% higher, respectively, than the original autoencoder. It has been proven that the shrink autoencoder can improve the detection performance of the collaborative detection method. Compared with the centralized learning framework, the proposed collaborative detection method can improve training efficiency. Moreover, the proposed shrink autoencoder, within a federated learning framework, shows the least sensitivity to changes in the balance coefficient, maintaining good detection results even with an inaccurate anomaly detection threshold. In conclusion, simulation experiments prove that the collaborative UAV GPS spoofing attack detection scheme proposed in this paper can achieve better detection performance and higher model training efficiency on open data sets.

Key words: UAV GPS spoofing attack; federated learning; shrink autoencoder; collaborative detection

1　引言

无人机已经广泛应用于农林保护[1]、军事作战[2]、工业生产[3]等多个领域，执行监测、救援[4]、遥感、运输和网络中继[5]等关键的任务，其重要性日益突出。然而，无人机容易受到GPS欺骗攻击的威胁[6]。由于在GPS欺骗攻击中，攻击者会通过改变GPS信号来对接收机的导航系统进行诱导[7]。因此，受到GPS欺骗攻击的无人机会产生偏离运行轨迹、飞入禁飞区或强制降落等异常行为[8]，从而影响无人机的运行安全。

针对无人机GPS欺骗攻击的检测，目前的研究工作主要分为基于规则的检测方法和基于机器学习的检测方法两种类型。基于规则的检测方法主要是根据一定的数学规则来计算特定的参数，如无人机相对距离、位置偏差等，依据所计算的相关参数来判断无人机是否产生了异常。Qu等人提出了无人机协同定位系统[9]。该系统设立一组参考无人机，通过机载的RDF接收器收到的待测无人机的几何方位角和相对倾角来计算无人机的相对位置，将计算所得的位置与无人机实际所处位置进行对比，从而检测无人机是否受到GPS欺骗攻击。在文献[10]中，提出了一种利用分布式雷达地面站局部跟踪器的无人机GPS欺骗攻击检测方法。该方法将无人机和局部跟踪器链接到融合节点，将无人机通过扩展卡尔曼滤波框架估计自身的状态信息作为主数据，将局部跟踪器对无人机时变运动的估计数据作为辅助数据，结合主数据与辅助数据与GPS的定位数据进行比较，来检测GPS欺骗攻击。文献[11]中的作者通过计算无人机运行过程中不同物理参数泊松分布的Kullback-Leibler散度，来检测无人机受GPS欺骗攻击所导致的异常。文献[12]提出了一种视觉传感器和IMU结合的无人机GPS欺骗攻击检测方法，通过将IMU和视觉传感器测得的无人机速度信息进行融合，并与无人机GPS接收机获得的速度信息进行比较，来检测无人机是否受到GPS欺骗攻击。

上述基于规则的检测方法虽然能够简化异常检测模型的构建过程，但检测性能不够精确。此外，由于其按照固定的规则来进行检测，只适用于特定的攻击场景，泛化性不强。为了弥补上述缺点，许多研究人员提出采用机器学习的方法来进行无人机GPS欺骗攻击检测。G. Aissou等人[13]比较了RF、Gradient Boost、XGBoost和LightGBM四种基于树的机器学习模型对无人机GPS欺骗攻击的检测性能，通过对包含正常和异常标签的数据样本

进行训练和测试，最终比较得到XGBoost较其他模型的检测性能最好。Dang等人[14]根据无人机GPS欺骗攻击的特点，将无人机与基站间的理论路径损失与实际路径损失之间的偏差作为训练数据，通过多层感知器（MLP）学习路径损失偏差在正常情况下和无人机受GPS欺骗攻击情况下的特征，来实现对GPS欺骗攻击的检测。文献[15]提出了一种结合三维无线电地图和机器学习的蜂窝连接无人机GPS欺骗攻击检测方法。该方法利用RNN、CNN、MLP等机器学习方法，通过分析无人机或基站上报的实际接收信号强度（RSS）值和由三维无线电地图提供的理论接收信号强度值之间的偏差，来检测无人机是否受到GPS欺骗攻击。

由于基于监督的机器学习方法需要对数据集进行标记来进行训练，而数据集的标记需要耗费大量的工作，增加了模型训练的时间成本；此外，在缺乏先验知识的情况下，对于接收到的无人机相关数据，难以有效提取出可供标记的异常数据。为了避免以上问题，不少研究工作采用无监督学习的方式进行攻击检测。在文献[16]中，作者提出了一种利用无人机正常状态数据的知识进行GPS欺骗攻击检测的方法。该方法通过One Class SVM对无人机正常状态数据进行训练来构造一个决策边界，通过这个边界判断测试的数据与训练数据的相似度，将超出边界的数据判断为异常。文献[17]作者使用LSTM来检测GPS欺骗攻击，该方法学习无人机已有的相关运行数据来预测无人机之后的运行路径，通过计算预测路径与GPS信号给出的路径之间的偏差来检测异常。在文献[18]中，作者建立了一个由堆叠自编码器组成的异常检测模型。该模型的训练数据为从无人机正常运行的飞行日志中提取的一组特征数据。通过学习输入数据的潜在特征来重建输入，并计算重建损失，根据训练数据计算所得的重建损失确定检测阈值。在异常检测过程中，将测试数据输入模型计算得到的重建损失与设定的阈值进行比较，来检测无人机是否出现异常。

上述基于机器学习的异常检测方法采用集中式学习来训练异常检测模型。与分布式学习方法相比，集中式学习往往需要较长的训练时间。并且由于集中式学习只通过一个节点对接收到的数据进行训练，无法保证模型的检测效果。为了提高模型的训练效率和检测性能，本文在文献[18]所作工作的基础上考虑无人机GPS欺骗攻击的分布式检测场景，通过联邦学习使多个监测节点在本地对不同无人机的运行数据进行并行训练，来得到异常检测模型，实现对无人机的协同检测。在异常检测模型协同训练过程中，不同监测节点用于本地训练的无人机运行数据分布差异较大，导致训练得到的异常检测模型的检测性能降低。为了解决这一问题，本文采用收缩自编码器作为异常检测模型。该模型通过将各检测节点接收到的训练数据的低维分布强制收缩到一定范围，来减小联邦学习中局部训练数据间的分布差异，从而使训练得到的全局模型能够更好地区分正常数据和异常数据，达到提高全局模型异常检测性能的效果。本文所作贡献如下：

1）提出了针对无人机GPS欺骗攻击的协同检测方法，通过引入联邦学习来协同训练无人机GPS欺骗攻击检测模型。

2）在针对受GPS欺骗攻击的无人机协同检测场景中，提出将收缩自编码器作为异常检测模型。解决了联邦学习训练过程中并行训练的数据分布差异较大导致所训练的全局模型性能下降的问题。

2 研究场景

在无人机GPS欺骗攻击协同检测场景中，采用联邦学习训练异常检测模型，如图1所示。

在该场景中，假设共有N架无人机和M座配备监测设备的基站，分别表示为$U=\{U_1,\cdots,U_i,\cdots,U_N\}$和$B=\{B_1,\cdots,B_k,\cdots,B_M\}$。每架无人机$U_i$向基站$B_k$发送自身的运行数据。基站通过配备的监测设备接收无人机发送的运行数据，来进行模型训练和异常检测。在联邦学习过程中，所有监测基站作为训练客户端共同训练一个异常检测模型。假设联邦学习的全局聚合轮数为r，在每一轮的全局模型训练过程中，中央服务器首先初始化所要训练的异常检测模型参数$\boldsymbol{W}_t, t=0,1,\cdots,r$，并将其发送给所有基站。每一个基站根据其接收的无人机正常运行数据进行本地训练，并将训练后的局部更新参数$\boldsymbol{W}_t^k$上传中央服务器。中央服务器在接收到所有基站上传的更新参数后，通过聚合算法对全局模型进行更新，并将更新后的全局模型参数$\boldsymbol{W}_{t+1}$重新发送给各个基站，来进行下一轮的全局训练。在达到设定的全局聚合轮数r后，中央服务器将训练完成的异常检测模型发送给各个基站，各基站将自身的本地训练数据输入异常检测模型中得到局部异常检测阈值$\mathrm{th}_{\mathrm{local}\,k}$，并将其上传给中央服务器。中央服务器根据接收到的所有基站的局部异常检测阈值$\mathrm{th}_{\mathrm{local}\,k}$计算全局异常检测阈值$\mathrm{th}_{\mathrm{local}}$，并将其发布给各个基

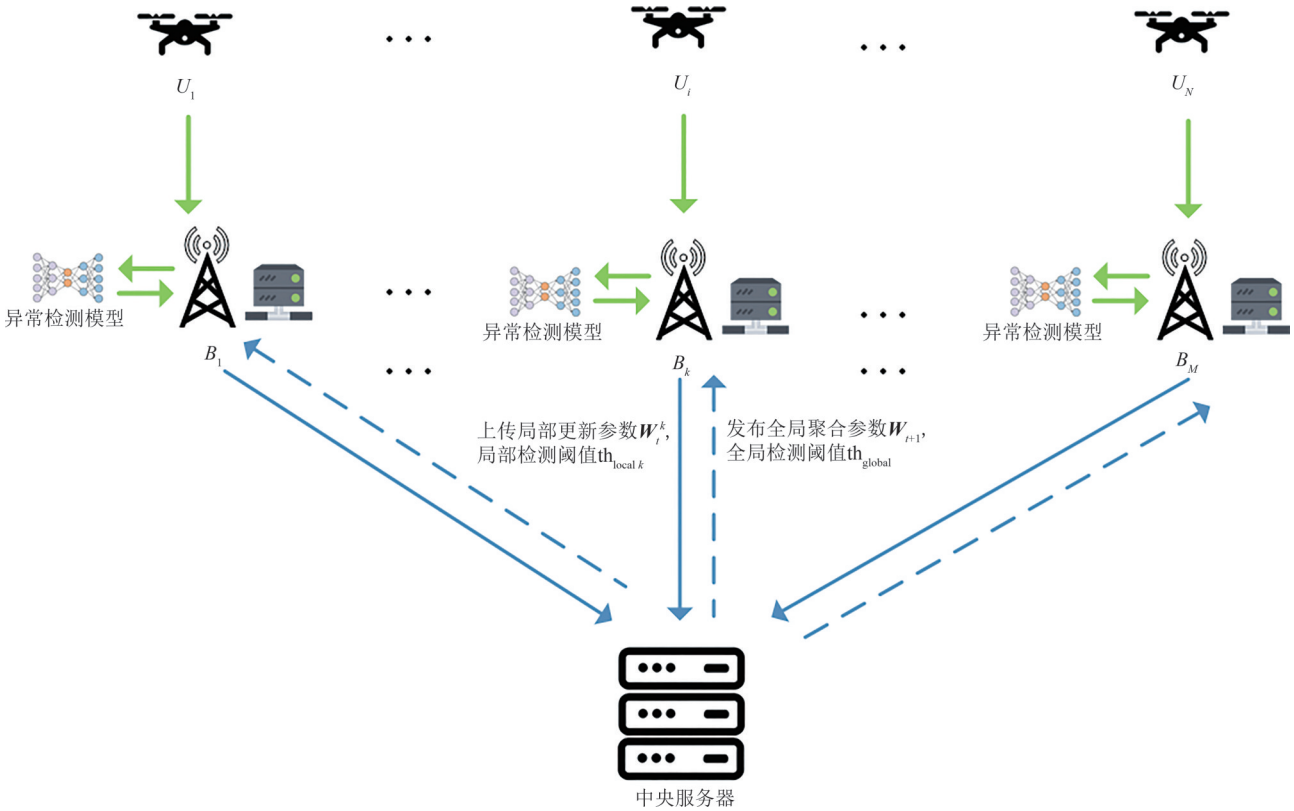


图 1　无人机GPS欺骗攻击协同检测场景

Fig. 1　UAV GPS spoofing attack collaborative detection scenario

站。在无人机GPS欺骗攻击检测过程中，各基站通过自身配备的监测设备将接收到的无人机运行数据输入训练好的异常检测模型中，将模型的输出结果与全局异常检测阈值进行比较，若超过阈值，则说明输入的数据异常，即可认为该基站所接收的运行数据对应的无人机受到了GPS欺骗攻击。

3　所提方法

本节分析和描述了本文提出的无人机GPS欺骗攻击协同检测方法。首先介绍了本文所提的收缩自编码器模型，分析了选用收缩自编码器作为异常检测模型的原因并介绍了其数学模型；之后描述了基于收缩自编码器的无人机GPS欺骗攻击协同检测算法流程。

3.1　收缩自编码器异常检测模型

本文采用收缩自编码器作为无人机受GPS欺骗攻击的异常检测模型。收缩自编码器是自编码器的一种变体，在协同训练条件下，与自编码器模型相比，它能够改进模型训练后的异常检测效果[19]。为了分析收缩自编码对模型检测效果的改进，首先介绍采用自编码器进行异常检测的基本原理。自编码器是一种无监督的神经网络模型，它的基本结构如图2所示。

根据图2可知，在自编码器的基本结构中，包含编码器和解码器两部分。输入向量在进入编码器后，通过编码器压缩到低维向量，之后再将压缩的低维向量作为输入，经过解码器重新扩张到与输入向量相同维度的高维向量中，以达到重建输入向量的目的。在自编码器的训练过程中，其目标是通过梯度下降等参数优化算法进行迭代训练来减小通过自编码器输出的重建向量与输入向量之间的重建损失，从而使通过自编码器输出的重建向量更接近输入的真实向量[20]。自编码器的基本数学表示如下[21]：

$$\boldsymbol{z}_i = e(\boldsymbol{x}_i) = \sigma_e(\boldsymbol{W}_e \boldsymbol{x}_i + \boldsymbol{b}_e) \tag{1}$$

$$\hat{\boldsymbol{x}}_i = d(\boldsymbol{z}_i) = \sigma_d(\boldsymbol{W}_d \boldsymbol{z}_i + \boldsymbol{b}_d) \tag{2}$$

其中，$e(\boldsymbol{x})$和$d(\boldsymbol{z})$分别表示编码器和解码器；$\boldsymbol{x}_i$为输入的特征向量，$\boldsymbol{z}_i$为经过编码器输出的输入向量$\boldsymbol{x}_i$的低维表示，$\hat{\boldsymbol{x}}_i$为解码器输出的重建向量；$\boldsymbol{W}_e$，$\boldsymbol{b}_e$和$\boldsymbol{W}_d$，$\boldsymbol{b}_d$分别为训练编码器和解码器的相关参数，其中$\boldsymbol{W}$表示权重矩阵，$\boldsymbol{b}$表示偏置矩阵；σ_e，σ_d为激活函数。自编码器所要优化的目标函数为：

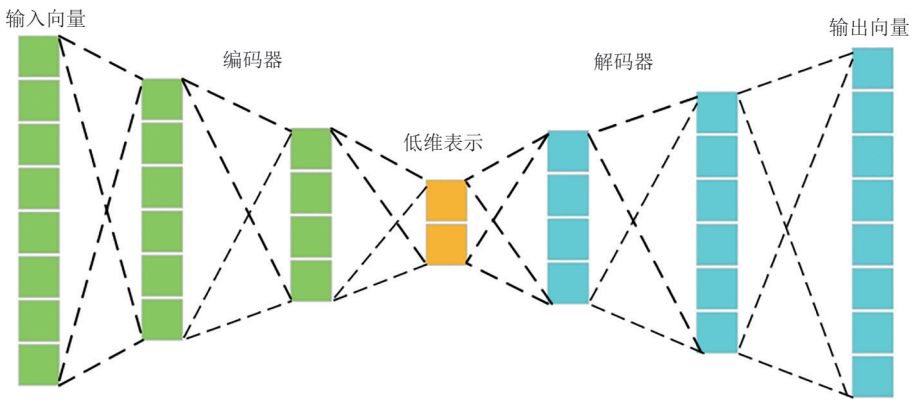


图2 自编码器

Fig. 2 Autoencoder

$$\text{Minimize Loss} = \text{dist}(\boldsymbol{x},\hat{\boldsymbol{x}}) \tag{3}$$

从目标函数中可知，训练自编码器的目的是通过优化模型参数使输入自编码器得到的损失函数达到最小。式中，$\boldsymbol{x}$和$\hat{\boldsymbol{x}}$分别表示自编码器的输入数据和输出的重建数据，dist为二者的距离度量函数，通常采用MSE或MAE。在本文中，采用MAE作为自编码器输入与输出的距离度量函数，则损失函数表示为：

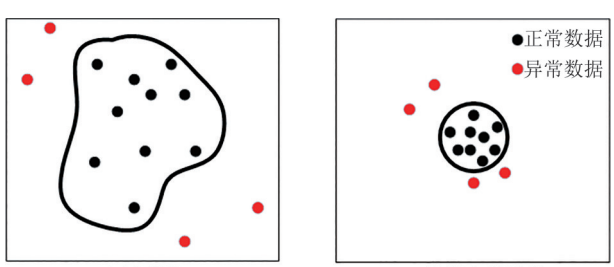
$$\text{Loss} = \frac{1}{n}\sum_{i=1}^{n}\left|\hat{\boldsymbol{x}}_i - \boldsymbol{x}_i\right| \tag{4}$$

式中，n表示训练数据集中共有n个样本。由于自编码器的实质是将输入向量压缩到低维，通过学习输入样本的潜在特征来重构输入，使得输出向量与输入向量间的重建损失达到最小。根据它的特性，可以将其作为无人机异常数据的检测模型。采用自编码器检测无人机异常运行数据的基本思想为：通过将无人机正常运行时的数据作为训练数据集输入自编码器进行训练，可以使训练所得的自编码器对训练数据集的重建损失达到最小。在训练得到用于异常检测的自编码器模型后，根据训练数据样本输入自编码器的损失函数计算异常检测阈值。由于自编码器是通过无人机正常运行数据进行训练的，因此当输入经过训练后的自编码器的数据为异常数据时，计算得到的重建损失会比正常数据得到的重建损失大[22]，若其超过设定的异常检测阈值，则说明该数据为异常数据，即代表所对应的无人机受到了GPS欺骗攻击。

根据第2节所述，本文通过联邦学习来训练异常检测模型。在联邦学习的协同训练场景中，由于采集对象、采集时间以及采集地点的不同，不同基站用于本地训练的无人机正常数据样本可能具有较大的分布差异，从而影响联邦学习对异常检测模型的训练效果。为了解决这一问题，本文采用收缩自编码器作为异常检测模型。收缩自编码器的损失函数表达如下[23]：

$$\text{Loss}_{\text{SAE}} = \frac{1}{n}\sum_{i=1}^{n}\left|\hat{\boldsymbol{x}}_i - \boldsymbol{x}_i\right| + \lambda\frac{1}{n}\left\|\boldsymbol{z}_i\right\|^2 \tag{5}$$

式中，$\boldsymbol{z}_i$为输入数据的低维表示，λ用于控制两个损失项之间的权衡。根据式(5)可知，与自编码器相比，收缩自编码器在损失函数中引入了新的损失项$\lambda\frac{1}{n}\left\|\boldsymbol{z}_i\right\|^2$。在异常检测模型训练过程中，该损失项能够减小输入模型的不同训练样本之间的低维分布差异。图3(a)和(b)分别表示了输入数据经过自编码器和收缩自编码器所得到的低维分布。根据图中可知，与自编码器相比，收缩自编码器将训练的正常数据的低维表示映射到更小的范围之内。由于在本文的异常检测过程中，异常检测模型通过学习正常数据压缩到低维的潜在特征来重建正常数据，并通过计算得到的重建损失来判断异常。因此，当所训练的数据样本的分布差异较大时，采用收缩自编码器将训练数据的低维表示压缩到一定范围内能够更好地学习训练数据的低维特征，增大



(a) 自编码器 (b) 收缩自编码器

图3 输入数据的低维分布

Fig. 3 Low dimensional distribution of input data

无人机正常运行数据与异常数据在低维空间的分布差异，从而在无人机GPS欺骗攻击检测过程中通过计算输入数据的重建损失来更好地区分正常数据与异常数据。

根据上述收缩自编码器的特点，本文实验中构建的收缩自编码器模型为对称的7层神经网络结构。它由输入层、隐藏层和输出层组成。在该网络中，输入层和输出层的神经元数量为16，代表输入特征向量的维数，中间的五层为隐藏层，其神经元个数分别为20、15、5、15、20。其中，隐藏层3对应输入向量经过编码器输出的低维向量，隐藏层4、隐藏层5对应解码器，输出层的结果为输入特征向量经过自编码器学习得到的重建向量。实验中用于训练的收缩自编码器的数学模型如下：

$$\boldsymbol{h}_1=\sigma(\boldsymbol{W}_1\boldsymbol{x}+\boldsymbol{b}_1) \tag{6}$$

$$\boldsymbol{h}_2=\sigma(\boldsymbol{W}_2\boldsymbol{h}_1+\boldsymbol{b}_2) \tag{7}$$

$$\boldsymbol{h}_3=\sigma(\boldsymbol{W}_3\boldsymbol{h}_2+\boldsymbol{b}_3) \tag{8}$$

$$\boldsymbol{h}_4=\sigma(\boldsymbol{W}_4\boldsymbol{h}_3+\boldsymbol{b}_4) \tag{9}$$

$$\boldsymbol{h}_5=\sigma(\boldsymbol{W}_5\boldsymbol{h}_4+\boldsymbol{b}_5) \tag{10}$$

$$\hat{\boldsymbol{x}}=\sigma(\boldsymbol{W}_6\boldsymbol{h}_5+\boldsymbol{b}_6) \tag{11}$$

$$\mathrm{Loss}_{\mathrm{SAE}}=\frac{1}{n}\sum_{i=1}^{n}\left|\hat{\boldsymbol{x}}_i-\boldsymbol{x}_i\right|+\lambda\frac{1}{n}\left\|\boldsymbol{z}_i\right\|^2 \tag{12}$$

其中，$\boldsymbol{x}$，$\hat{\boldsymbol{x}}$分别表示输入的无人机运行数据和输出的重建数据；$\boldsymbol{h}_k(k=1,2,\cdots,5)$为对应隐藏层的输出；$\boldsymbol{W}_j,\boldsymbol{b}_j(j=1,2,\cdots,6)$代表神经网络中每一层的权重和偏置，其中$\boldsymbol{W}_j$即为本文提出的协同训练场景中所要更新的模型参数；$\sigma$为激活函数，本模型中采用sigmoid函数。在式(12)中，$\boldsymbol{z}_i$对应输入样本通过编码器输出的低维表示，即$\boldsymbol{z}_i=\boldsymbol{h}_{3i}$。

3.2　无人机GPS欺骗攻击协同检测算法

本文采用联邦学习对异常检测模型进行训练，实现对无人机GPS欺骗攻击的协同检测。联邦学习是一种分布式的机器学习范式，它通过多个客户端在本地通过自身的数据集对模型进行训练来更新参数信息，并由中央服务器对更新的参数进行聚合来更新全局模型，实现对模型的多方协同训练[24]。针对联邦学习过程中中央服务器的聚合计算，目前的研究工作已经提出了许多不同的聚合算法。本文将基站作为联邦学习的训练客户端，采用联邦平均算法[25]对基站上传的模型更新参数进行聚合，以下介绍其基本流程。

假设要训练的全局模型参数的初始值为ω_0，参与训练的基站个数为n，用于训练的无人机正常运行数据的批样本大小为B，模型本地训练次数为E，全局聚合轮数为r，局部模型学习率为η，各基站的本地训练样本数为m_k。训练开始时，中央服务器首先初始化全局模型参数ω_0，并将其传输给所有参与模型训练的基站；所有基站在收到初始模型参数后，在本地开始全局模型的训练，对于第t轮全局聚合过程，$t=1,2,\cdots,r$，模型参数聚合的基本步骤如下：

1）中央服务器向所有基站发送上一轮聚合得到的全局模型参数ω_t。

2）对任意基站k，$k=1,2,\cdots,n$，将其本地训练数据集按照批样本大小B分为若干个批次，将所有批次构成的集合表示为B_k。

3）基站根据训练批次集合B_k进行本地迭代训练，在每次迭代训练j，$j=1,2,\cdots,E$中，对于任意批次$b\in B_k$，更新局部模型参数

$$\omega_{t+1}^k\leftarrow\omega_t^k-\eta\nabla F_k(\omega;\ b) \tag{13}$$

其中，ω_t^k表示基站k在第t轮全局训练中的局部模型参数，$\nabla F_k(\omega;\ b)$为基站本地训练集的第b个批次经过本地迭代训练后更新的梯度；本地训练完成后，基站将更新好的局部参数ω_{t+1}^k上传中央服务器。

4）在收到所有基站上传的局部模型更新参数后，中央服务器聚合所有参数，并将其传输回所有基站

$$\omega_{t+1}=\sum_{k=1}^{M}\frac{m_k}{m}\omega_{t+1}^k \tag{14}$$

其中，$\frac{m_k}{m}$表示第t轮全局聚合过程中基站k的本地训练样本占所有基站的总训练样本的比例。

在联邦学习训练过程中，重复上述参数聚合步骤直到达到设定的全局聚合轮数。在达到设定的全局聚合轮数后，各基站根据最终聚合的收缩自编码器来计算自身的局部异常检测阈值，之后，中央服务器再根据各基站计算得到的局部异常检测阈值确定全局异常检测阈值，来用于受GPS欺骗攻击的无人机异常运行数据的检测。对于基站的局部异常检测阈值，本文参考文献[26]提出的计算方法。该方法根据基站所有本地训练数据样本输入收缩自编码器得到的重建损失的均值和标准误差来计算阈值，其表述如下：

$$\mathrm{th}_{\mathrm{local}}=\bar{L}_i+\frac{\alpha}{\sqrt{s}}\sigma(L_i) \tag{15}$$

式中，L_i表示基站本地训练数据第i个样本的重建损失，s为本地训练数据的样本数，α为计算异常检测阈值的平衡系数，其用来调整所计算的阈值大小。

综上所述，本文提出的无人机GPS欺骗攻击协同检测算法主要分为初始化、全局训练、异常检测阈值计算和无人机GPS欺骗攻击检测四部分，表1描述了算法的主要流程。

表1 无人机GPS欺骗攻击协同检测算法流程

Tab. 1 UAV GPS spoofing attack collaborative detection algorithm process

无人机GPS欺骗攻击协同检测算法
初始化：中央服务器初始化全局模型参数 ω_0，并将其发送给所有基站。
全局训练：对于全局聚合轮数 $t=1$ 到 r，重复以下步骤： 1. 对于基站 $k=1$ 到 n，根据本地接收的无人机正常运行数据训练收缩自编码器，达到设定的本地训练次数 E 后，更新局部模型参数 $\omega_{t+1}^k \leftarrow \omega_t^k - \eta \nabla F_k(\omega; b)$，将更新后的参数 ω_{t+1}^k 上传中央服务器。 2. 中央服务器在收到所有基站上传的局部参数 ω_{t+1}^k 后，通过联邦平均算法聚合得到全局模型参数 $\omega_{t+1}=\sum_{k=1}^{M}\frac{m_k}{m}\omega_{t+1}^k$。 3. 中央服务器将本轮聚合得到的全局模型参数 ω_{t+1} 重新发送给各基站，用于下一轮的模型参数更新。
异常检测阈值计算： 1. 在完成模型参数聚合后，中央服务器将最终聚合得到的全局模型参数 ω_r 发送给所有基站，作为最终训练所得的收缩自编码器的模型参数。 2. 各基站将自身的本地训练数据输入训练得到的收缩自编码器中，计算局部异常检测阈值 $\mathrm{th}_{\mathrm{local}\,k}=\overline{L_i^k}+\frac{\alpha}{\sqrt{s_k}}\sigma(L_i^k)$，并将其上传中央服务器。 3. 中央服务器根据上传的局部异常检测阈值，计算全局异常检测阈值 $\mathrm{th}_{\mathrm{global}}=\overline{\mathrm{th}}_{\mathrm{local}\,k}+\alpha*\sigma(\mathrm{th}_{\mathrm{local}\,k})$。
无人机GPS欺骗攻击检测：基站将接收到的无人机运行数据输入训练好的收缩自编码器中，将得到的重建损失 $\mathrm{LOSS}_{\mathrm{SAE}}$ 与全局异常检测阈值 $\mathrm{th}_{\mathrm{global}}$ 比较，若 $\mathrm{LOSS}_{\mathrm{SAE}}>\mathrm{th}_{\mathrm{global}}$，则对应的无人机受GPS欺骗攻击。

4 仿真实验

为了验证提出的无人机GPS欺骗攻击协同检测方法的可行性，本文通过仿真实验实现了联邦学习对收缩自编码器的协同训练，并测试了协同训练的模型检测无人机GPS欺骗攻击的效果。本节首先说明了实验的相关设置，包括实验数据和实验参数的选取，之后对所得的实验结果进行了分析，证明了本文所提方法的优越性。

4.1 实验相关设置

（1）实验数据选取。本文采用UAV ATTACK数据集[27]作为异常检测模型的训练数据和测试数据。该数据集分别从正常运行的无人机飞行日志和受GPS攻击的无人机飞行日志中提取得到。数据集中的GPS攻击包括GPS欺骗攻击和GPS干扰。其中，GPS欺骗攻击通过HackRF软件定义无线电设备实现。该设备采用GPS-SDR-SIM工具对接收到的GPS信号进行高保真处理，之后再延时转发给无人机，从而误导无人机的GPS接收器计算得到错误的无人机运行状态，产生GPS欺骗攻击。数据集构建过程中使用的无人机型号为Holybro S500，该无人机搭载Pixhawk GPS接收器，通过Pixhawk 4飞行控制器运行。

在得到仿真实验所用的数据集后，根据该数据集选取用于收缩自编码器训练及异常检测的输入特征。由于所训练的收缩自编码器用于检测无人机GPS欺骗攻击。因此，应根据攻击对无人机所造成的影响来选择输入模型的特征。特征的选择应遵循通用性和稳定性两个原则[18]。其中，通用性指所选的特征应在异常检测模型中适用于所有类型的无人机。该原则旨在消除异常检测中由于部分特征只适用于特定类型的无人机，而导致检测模型泛化性下降的问题。在无人机飞行过程中，经常会出现某些特定特征无法记录的情况，这些特征会使输入特征向量中包含Null值。此外，某些特征对无人机的运行并不敏感，在无人机飞行过程中基本保持不变。将这些特征输入自编码器中并不会改善模型的性能，反而会因为维数的增加而增加训练时间。因此，稳定性原则旨在消除在无人机飞行过程中无法记录以及基本不变的特征，从而提升模型的检测性能。基于上述特征选择规则，本文用于收缩自编码训练和测试的数据集特征如表2所示，数据集的特征维度为16。

（2）数据预处理。在选取了本实验的特征数据后，还应对不同特征对应的数据样本进行一定的预处理，来将其转换为用于收缩自编码器训练的特征向量。本实验中，对数据样本进行的预处理包括归一化和时间戳池化两部分，以下分别对其进行描述：

1）归一化。归一化旨在统一不同特征对应的数据样本值的范围。由于不同特征数据的尺度大小不同，如果直接将其输入收缩自编码器中，会导致算法无法快速的进行梯度下降，从而难以达到全

表 2　数据集特征

Tab. 2　Dataset features

特征名称	描述
局部位置(x,y,z)	无人机在以参考坐标(本研究中为经度138.3，纬度36.2)为原点建立的局部坐标系下的位置
局部速度(v_x,v_y,v_z)	无人机在局部坐标系下沿x,y,z轴的速度
局部加速度(a_x,a_y,a_z)	无人机在局部坐标系下沿x,y,z轴的加速度
CPU负载	无人机在运行过程中每一时段的CPU负载
横滚角(Roll)	无人机运行过程中每一时刻的横滚角
俯仰角(Pitch)	无人机运行过程中每一时刻的俯仰角
偏航角(Yaw)	无人机运行过程中每一时刻的偏航角
横滚角速度(Roll Speed)	无人机运行过程中每一时刻的横滚角速度
俯仰角速度(Pitch Speed)	无人机运行过程中每一时刻的俯仰角速度
偏航角速度(Yaw Speed)	无人机运行过程中每一时刻的偏航角速度

局最优解。因此，为了使得模型收敛到最优结果，应对选取的特征数据进行归一化。归一化采用Min-Max Scaling函数，其数学表达如下：

$$x_i^*=\frac{x_i-\min(x_i)}{\max(x_i)-\min(x_i)} \tag{16}$$

式中，x_i^*为归一化后的特征值。

2)时间戳池化。在各个特征对应的数据样本尺度统一后，还应保证输入异常检测模型的不同特征数据的一致性。由于输入模型的数据集应为一个固定大小的矩阵，因此在每一时间窗口内，数据集中各特征对应的样本数应相同。然而，在无人机的飞行日志中，由于不同特征数据的记录方式以及测量条件不同，在一个固定的时间窗内，不同特征提取出的样本数不同。针对单个时间窗内不同特征对应的数据样本长度不同的问题，采用时间戳池化进行解决。时间戳池化通过在固定的时间窗口内对每一特征随机选取单个数据点，以保证各特征在单个时间窗口内样本长度的一致。图4为对特征数据进行时间戳池化的示例。

从图中可知，特征A、B、C在单个时间窗口内分别对应6、9、3个样本点。通过采用时间戳池化，保

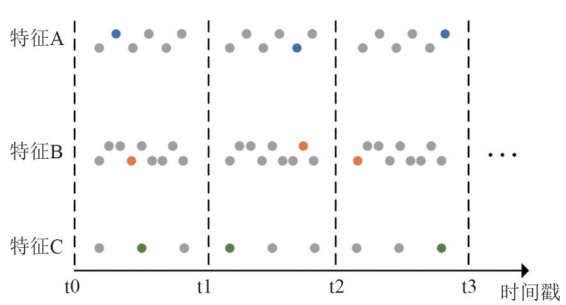


图4　时间戳池化

Fig. 4　Timestamp pooling

证了在每一时间窗口内，各特征对应的样本数量一致，从而将无人机飞行日志中的样本数据转化为固定大小的输入向量，以便于输入收缩自编码器进行训练。经过时间戳池化后，构建出用于异常检测模型训练的训练集以及检测模型性能的测试集。其中，训练集为无人机正常状态下的运行数据；测试集包含无人机正常运行数据和受GPS欺骗攻击的异常数据。

由于本文所研究的协同训练场景为横向联邦学习场景，即不同客户端用于进行本地训练的训练数据的特征空间相同，样本空间不同。因此，在采用联邦学习训练收缩自编码器之前，还应对构建的训练数据集进行数据划分，以分别对应不同客户端的本地训练数据。在本文的实验场景中，设置5个配备监测设备的基站作为联邦学习中的训练客户端。在数据划分过程中，将训练集按照时间戳横向划分为五份维度相同、样本数相同的本地数据集，对应五个客户端的本地训练数据。其中每个客户端对应的本地训练集的样本数为50。

(3)实验参数设置。本文通过python的Pytorch工具库实现联邦学习对收缩自编码器的协同训练，实验的相关参数如表3所示。

根据式(15)可知，在异常检测阈值的计算中，平衡系数α用于控制计算所得阈值的大小。由于阈值大小的改变会影响模型异常检测的性能，因此应选择合适的α用于异常检测阈值的计算。选择α的总体原则应使计算得到的阈值在能够覆盖正常数据样本输入模型所得重建损失的同时，尽可能准确地区分正常数据和异常数据。本文在实验中选取不同的平衡系数α来进行无人机GPS欺骗攻击检

表3 实验参数

Tab. 3 Experimental parameters

参数	值
全局聚合轮数	5
本地训练次数	100
客户端总数	5
学习率	0.001
本地批量样本大小	10
优化器	adam
权重衰减	1e-4
更新步长	4
损失权衡系数λ	1e-3

测。通过对实验结果进行比较，发现当平衡系数α取2时，模型的检测性能最好。

4.2 实验结果分析

本小节在上述实验设置的基础上，对仿真得到的实验结果进行分析。首先验证了采用联邦学习对收缩自编码器进行协同训练的效果。之后评估了本文所提方法的性能。

(1)训练效果验证。首先验证联邦学习训练所得的全局模型的收敛情况。在本实验中，为了防止过拟合，将训练集的20%划分为验证集，以验证模型的泛化性。由于训练收缩自编码器的目的是最小化输出向量与输入向量间的重建损失，从而通过神经网络的学习更好地重现输入特征数据。因此在联邦学习训练结束后，通过客户端在本地训练过程中损失函数的迭代结果来判断模型训练的收敛情况。在联邦学习的最后一轮全局聚合过程中，客户端在本地训练过程中损失函数的迭代结果如图5所示。

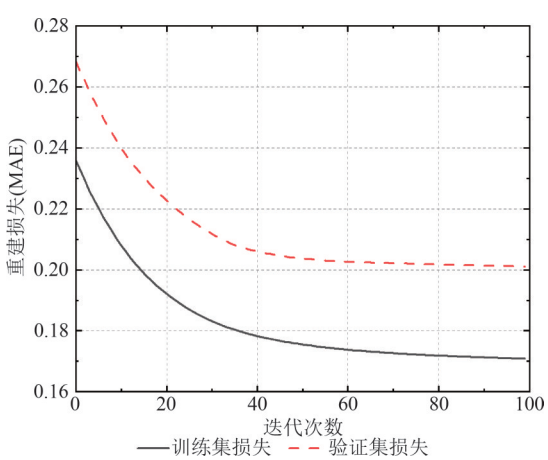


图5 模型训练收敛情况

Fig. 5 Model training convergence

从图中可以看出，在最后一轮全局训练过程中，客户端在本地训练100次后，训练集输入模型得到的重建损失基本收敛到一定范围内，证明模型取得了较好的训练结果。

(2)方法性能评估。为了评估本文所提方法的异常检测性能，本小节首先将自编码器异常检测模型与另外两种基准模型进行比较。选取的另外两种基准模型分别为逻辑回归和支持向量机，这两种模型都是典型的机器学习模型，可以用于无人机GPS欺骗攻击的检测[28]。其中，支持向量机选用高斯核函数，相关参数nu和gamma设为默认值。

为了评估三种模型在无人机受GPS欺骗攻击场景下的异常检测性能，实验中将准确率(Accuracy)、查准率(Precision)和召回率(Recall)作为异常检测性能的评估指标，其计算分别如下：

$$\text{Accuracy}=\frac{\text{TP}+\text{TN}}{\text{TP}+\text{FP}+\text{TN}+\text{FN}} \tag{17}$$

$$\text{Precision}=\frac{\text{TP}}{\text{TP}+\text{FP}} \tag{18}$$

$$\text{Recall}=\frac{\text{TP}}{\text{TP}+\text{FN}} \tag{19}$$

式中，TP、TN、FP、FN分别指通过模型检测后真阳性数据、真阴性数据、假阳性数据以及假阴性数据的数量。在本实验中，真阳性数据TP指检测为异常，实际也为异常的数据；真阴性数据TN为检测为正常，实际也为正常的数据；假阳性数据FP指检测为异常，实际为正常的数据；假阴性数据FN指检测为正常，实际为异常的数据。根据上式可知，在本实验中，准确率表示模型正确检测出的正常和异常样本数占总样本数的比例，它能够代表模型总的检测正确率；查准率表示模型正确检测出的异常样本占模型检测得到的总的异常样本数的比例，查准率越高，表示模型检测异常数据的准确度越高；召回率表示模型检测出的异常样本占实际异常样本数的比例，高的召回率能够减少模型对异常数据的漏检情况，但有可能提高错检率，即将正常数据检测为异常。综上所述，上述三种检测指标能够用来衡量异常检测模型的检测性能，检测指标越高，表示模型的检测性能越好。

实验中通过集中式学习方法对三种模型进行训练。为了保证性能比较的公平性，三种模型采用相同的数据集进行训练，并设置相同的训练迭代次数。在模型评估过程中，设置自编码器模型的平衡系数α为2，将包含无人机正常运行数据和异常数据(无人机受GPS欺骗攻击的运行数据)的测试集

分别输入三种模型中，得到的比较结果如图6所示。根据图6可知，与其他两种基准模型相比，自编码器模型的异常检测效果最好。

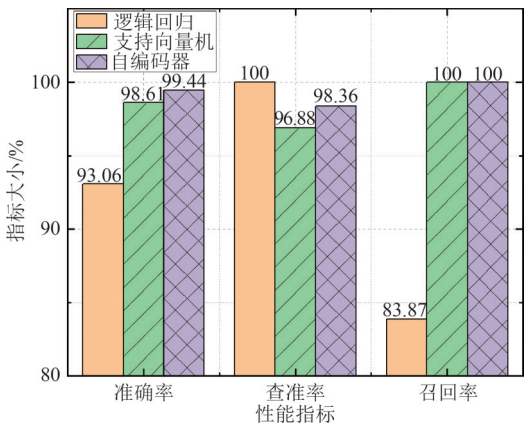


图6　三种模型的检测性能

Fig. 6　Detection performance of three models

此外，为了验证所提的基于收缩自编码器的无人机GPS欺骗攻击协同检测方法的优越性，本文通过仿真实验分别比较了所提方法与联邦学习自编码器方法、集中式学习自编码器方法的检测性能。在实验过程中，三种方法根据各自确定的异常检测阈值进行检测并计算相应的检测性能指标。在计算异常检测阈值时，由于选取的平衡系数α会影响模型的异常检测性能，为了得到最好的异常检测性能，本实验将α以0.5为间隔分别从1取到3，比较三种方法在不同平衡系数下的检测性能指标，如图7、图8、图9所示。

从图7、图8和图9可以看出，在平衡系数α取2时，本文所提的方法对应的准确率、查准率和召回率总体达到最高，分别为96.49%、96.03%和93.85%，与联邦学习自编码器的94.86%、95.23%和89.23%相比，分别提高了1.63%、0.8%和4.62%。此时收缩自编码器的异常检测性能最好，对应的异常检测阈值为0.218。

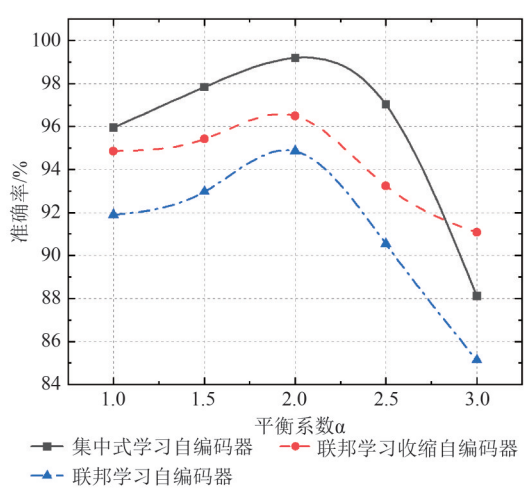


图7　三种方法在不同平衡系数α下的准确率

Fig. 7　Accuracy of three methods under different balance coefficient α

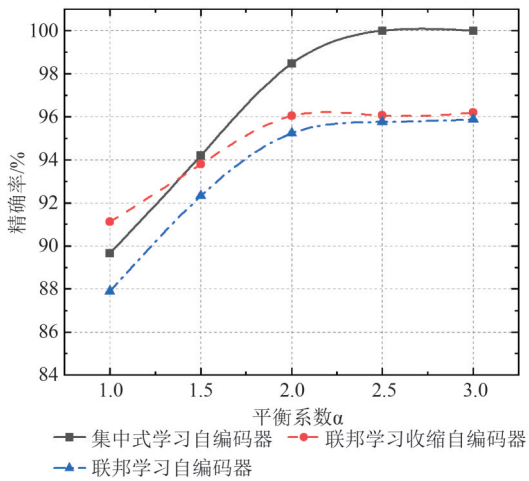


图8　三种方法在不同平衡系数α下的查准率

Fig. 8　Precision of three methods under different balance coefficient α

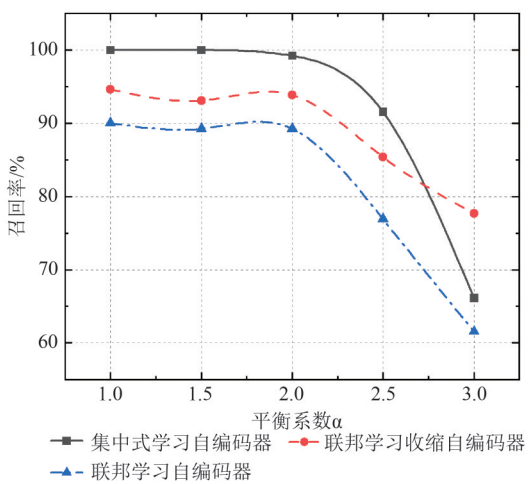


图9　三种方法在不同平衡系数α下的召回率

Fig. 9　Recall of three methods under different balance coefficient α

根据比较结果可知，在相同的测试集和实验参数下，对于不同的平衡系数α，采用本文提出的方法进行无人机GPS欺骗攻击检测得到的准确率、查准率和召回率均高于采用联邦学习自编码器方法得到的检测指标。证明了在协同检测方法中，收缩自编码器能够减少不同客户端本地训练数据间的分

布差异，提高训练所得模型的检测性能。在三种方法中，集中式学习自编码器在选取的大部分平衡系数α下表现出的异常检测性能最好。这是因为在集中式学习中，不同批样本之间的训练是串行的，模型是在前一个批样本已经训练好的基础上进行更新的；而在联邦学习中不同客户端的训练样本是并行训练的，每轮训练结束后通过聚合来更新模型，由于每个客户端都是在相对没有训练好的模型上进行训练，因此模型的训练效果相对集中式学习略有降低。但相应的，由于在联邦学习中，采用并行训练加快了模型的训练速度，与集中式学习方法相比，联邦学习方法应该具有更高的训练效率。本实验比较了三种方法在相同实验参数下模型的训练时间，结果如表4所示。

表4 训练效率比较

Tab. 4 Training efficiency comparison

检测方法	训练时间/s
联邦学习收缩自编码器	3.31
联邦学习自编码器	3.29
集中式学习自编码器	7.96

根据表4可知，在模型性能指标略微降低的情况下，采用联邦学习进行训练提高了异常检测模型的训练效率，证明了在训练数据集相同的情况下，本文所提的分布式检测方法与集中式学习方法相比能够减少模型的训练时间。

根据比较结果，分析不同的平衡系数α对三种方法检测性能的影响。由图7可知，随着平衡系数的增大，三种方法对应的准确率在α取2时达到最高，之后开始下降。从图中可知，与其他两种方法相比，本文所提的方法准确率的下降幅度最小。在α取3时，本文所提方法的准确率为91.08%，高于集中式学习自编码器的88.11%和联邦学习自编码器的85.14%。由图8可知，随着选取的平衡系数α的增加，三种方法对应的查准率逐渐升高。这是由于选取的α增大会导致实验中计算的异常检测阈值升高，高的异常检测阈值会保证覆盖更多正常数据样本的重建损失，从而降低模型将正常样本错误检测为异常样本的概率，此时模型检测异常样本的准确度升高，即查准率升高。然而，随着计算的异常检测阈值升高，其大小可能会高于部分异常样本的重建损失，导致模型的漏检率增高，造成召回率降低，如图9所示。根据图8和图9可知，本文所提方法的查准率和召回率最低为91.11%和76.69%，高于另外两种方法在最低情况下的查准率和召回率。综上所述，与其他两种方法相比，本文提出的联邦学习收缩自编码器受平衡系数α改变的影响最小，在异常检测阈值计算不合理的情况下仍然能够达到较好的检测结果，因此具有最好的检测性能。

5 结论

为了防止GPS欺骗攻击对无人机安全运行产生的影响，本文提出了一种无人机GPS欺骗攻击协同检测方法。通过联邦学习的训练方式，使多个监测设备通过本地接收的无人机运行数据协同训练异常检测模型，来检测受GPS欺骗攻击的无人机在运行过程中发送的异常数据。为了解决联邦学习训练过程中不同训练数据间分布差异过大造成模型训练效果降低的问题，本文将收缩自编码器作为联邦学习训练的异常检测模型。为了验证本文所提方法的性能，通过仿真实验将本文的方法与其他两种基准方法进行比较。实验结果表明，在联邦学习场景下，本文所提的收缩自编码器较原始的自编码器有着更好的异常检测性能。与采用集中式训练的模型相比，本文所提的协同训练方法能够提高模型的训练效率。此外，与另外两种基准方法相比，本文提出的方法受平衡系数改变的影响最小，在计算的异常检测阈值不准确的情况下仍然拥有较好的检测性能。实验证明本文提出的方法能够高效、精确地实现无人机GPS欺骗攻击的协同检测。

参考文献

[1] 张海艳，兰玉彬，文晟，等. 植保无人机旋翼风场模型与雾滴运动机理研究进展[J]. 农业工程学报，2020，36(22)：1-12.
ZHANG Haiyan，LAN Yubin，WEN Sheng，et al. Research progress in rotor airflow model of plant protection UAV and droplet motion mechanism[J]. Transactions of the Chinese Society of Agricultural Engineering，2020，36(22)：1-12.（in Chinese）

[2] 韩博文，姚佩阳，钟赟，等. 基于QABC-IFMADM算法的有人/无人机编队作战威胁评估[J]. 电子学报，2018，46(7)：1584-1592.
HAN Bowen，YAO Peiyang，ZHONG Yun，et al. Threat assessment of manned/unmanned aerial vehicle formation based on QABC-IFMADM algorithm[J]. Acta Electronica Sinica，2018，46(7)：1584-1592.（in Chinese）

[3] ZHOU Zhenyu, ZHANG Chuntian, XU Chen, et al. Energy-efficient industrial Internet of UAVs for power line inspection in smart grid[J]. IEEE Transactions on Industrial Informatics, 2018, 14(6): 2705-2714.

[4] KUNDID VASIĆ M, PAPIĆ V. Improving the model for person detection in aerial image sequences using the displacement vector: A search and rescue scenario[J]. Drones, 2022, 6(1): 19.

[5] 杨君一, 李博, 张钦宇. 基于物理层网络编码的无人机中继网络资源优化[J]. 通信学报, 2021, 42(9): 12-20.
YANG Junyi, LI Bo, ZHANG Qinyu. Resource optimization for UAV relay networks based on physical-layer network coding[J]. Journal on Communications, 2021, 42(9): 12-20. (in Chinese)

[6] 何道敬, 杜晓, 乔银荣, 等. 无人机信息安全研究综述[J]. 计算机学报, 2019, 42(5): 1076-1094.
HE Daojing, DU Xiao, QIAO Yinrong, et al. A survey on cyber security of unmanned aerial vehicles[J]. Chinese Journal of Computers, 2019, 42(5): 1076-1094. (in Chinese)

[7] 王璐, 张林杰, 吴仁彪. 功率监测与SQM融合的GNSS欺骗干扰检测[J]. 信号处理, 2023, 39(3): 505-515.
WANG Lu, ZHANG Linjie, WU Renbiao. GNSS spoofing detection based on power monitoring combined with SQM[J]. Journal of Signal Processing, 2023, 39(3): 505-515. (in Chinese)

[8] GUO Yan, WU Meiping, TANG Kanghua, et al. Covert spoofing algorithm of UAV based on GPS/INS-integrated navigation[J]. IEEE Transactions on Vehicular Technology, 2019, 68(7): 6557-6564.

[9] QU Yaohong, WU Jizhi, XIAO Bing, et al. A fault-tolerant cooperative positioning approach for multiple UAVs[J]. IEEE Access, 2017, 5: 15630-15640.

[10] PARDHASARADHI B, CENKERAMADDI L R. GPS spoofing detection and mitigation for drones using distributed radar tracking and fusion[J]. IEEE Sensors Journal, 2022, 22(11): 11122-11134.

[11] BASAN E, BASAN A, NEKRASOV A, et al. GPS-spoofing attack detection technology for UAVs based on kullback-leibler divergence[J]. Drones, 2021, 6(1): 8.

[12] HE Daojing, QIAO Yinrong, CHAN S, et al. Flight security and safety of drones in airborne fog computing systems[J]. IEEE Communications Magazine, 2018, 56(5): 66-71.

[13] AISSOU G, SLIMANE H O, BENOUADAH S, et al. Tree-based supervised machine learning models for detecting GPS spoofing attacks on UAS[C]//2021 IEEE 12th Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON). New York, NY, USA. IEEE, 2022: 649-653.

[14] DANG Yongchao, BENZAÏD C, YANG Bin, et al. Deep-ensemble-learning-based GPS spoofing detection for cellular-connected UAVs[J]. IEEE Internet of Things Journal, 2022, 9(24): 25068-25085.

[15] DANG Yongchao, KARAKOC A, NORSHAHIDA S, et al. 3D radio map-based GPS spoofing detection and mitigation for cellular-connected UAVs[J]. IEEE Transactions on Machine Learning in Communications and Networking, 2023, 1: 313-327.

[16] PANICE G, LUONGO S, GIGANTE G, et al. A SVM-based detection approach for GPS spoofing attacks to UAV[C]//2017 23rd International Conference on Automation and Computing (ICAC). Huddersfield, UK. IEEE, 2017: 1-11.

[17] WANG Shenqing, WANG Jiang, SU Chunhua, et al. Intelligent detection algorithm against UAVs' GPS spoofing attack[C]//2020 IEEE 26th International Conference on Parallel and Distributed Systems (ICPADS). Hong Kong, China. IEEE, 2021: 382-389.

[18] PARK K H, PARK E, KIM H K. Unsupervised fault detection on unmanned aerial vehicles: Encoding and thresholding approach[J]. Sensors, 2021, 21(6): 2208.

[19] VU T A, TRAN T P, VU L, et al. Shrink autoencoder for federated learning-based IoT anomaly detection[C]//2022 9th NAFOSTED Conference on Information and Computer Science (NICS). Ho Chi Minh City, Vietnam. IEEE, 2023: 383-388.

[20] YU Jianbo, ZHOU Xingkang. One-dimensional residual convolutional autoencoder based feature learning for gearbox fault diagnosis[J]. IEEE Transactions on Industrial Informatics, 2020, 16(10): 6347-6358.

[21] BALDI P. Autoencoders, unsupervised learning, and deep architectures[C]//Proceedings of ICML workshop on unsupervised and transfer learning. JMLR Workshop and Conference Proceedings, 2012: 37-49.

[22] CHEN Zhaomin, YEO C K, LEE B S, et al. Autoencoder-based network anomaly detection[C]//2018 Wireless Telecommunications Symposium (WTS). Phoenix, AZ, USA. IEEE, 2018: 1-5.

[23] CAO V L, NICOLAU M, MCDERMOTT J. Learning neural representations for network anomaly detection[J]. IEEE Transactions on Cybernetics, 2019, 49(8):

3074-3087.
[24] SMITH V, CHIANG C K, SANJABI M, et al. Federated multi-task learning[C]//31st Conference on Neural Information Processing Systems (NIPS 2017). Long Beach, CA, USA: Advances in Neural Information Processing Systems, 2017: 4424-4434.
[25] MCMAHAN B, MOORE E, RAMAGE D, et al. Communication-efficient learning of deep networks from decentralized data[C]//Proceedings of the 20th International Conference on Artificial Intelligence and Statistics. Fort Lauderdale, Florida, USA: PMLR, 2017: 1273-1282.
[26] ZHANG Tuo, HE Chaoyang, MA Tianhao, et al. Federated learning for Internet of Things[C]//Proceedings of the 19th ACM Conference on Embedded Networked Sensor Systems. Coimbra, Portugal. New York, NY, USA: ACM, 2021: 413-419.
[27] WHELAN J, SANGARAPILLAI T, MINAWI O, et al. Novelty-based intrusion detection of sensor attacks on unmanned aerial vehicles[C]//Proceedings of the 16th ACM Symposium on QoS and Security for Wireless and Mobile Networks. Alicante Spain. ACM, 2020: 23-28.
[28] SHAFIQUE A, MEHMOOD A, ELHADEF M. Detecting signal spoofing attack in UAVs using machine learning models[J]. IEEE Access, 2021, 9: 93803-93815.

作者简介

佘丁辰 男，2000 年生，陕西西安人。南京航空航天大学在读硕士生，主要研究方向为无人机异常行为协同检测方法。
E-mail：sz2204829@nuaa.edu.cn

王 威 男，1990 年生，山东单县人。南京航空航天大学研究员，博士，主要研究方向为无线通信、空天地一体化网络、低空智联网。
E-mail：wei_wang@nuaa.edu.cn

王加琪 男，2001 年生，江苏苏州人。南京航空航天大学在读硕士生，主要研究方向为低空无人机监管技术。
E-mail：nuaawjq@nuaa.edu.cn

晋本周 男，1984 年生，河南商丘人。南京航空航天大学教授，博士，主要研究方向为雷达信号处理、雷达抗干扰。
E-mail：jinbz@nuaa.edu.cn

刘敬颐 男，1981 年生，江苏宿迁人。江苏省电信有限公司，主要研究方向为低空无人机精准协同规划技术。
E-mail：15301588200@189.cn

吴启晖 男，1970 年生，安徽歙县人。南京航空航天大学电子信息工程学院教授，主要研究方向为认知信息论、电磁空间频谱智能管控、天地一体化信息网络和无人机集群智能通信。
E-mail：wuqihui@nuaa.edu.cn

（责任编辑：边熙淳）