doi:10.19306/j.cnki.2095-8110.2023.04.005

基于 VBGMM-DCNN 的列车卫星定位欺骗干扰检测方法

王思琦[1]，刘 江[1,2,3]，蔡伯根[1,3,4]，赵 阳[5]

（1. 北京交通大学电子信息工程学院，北京 100044；
2. 北京交通大学智慧高铁系统前沿科学中心，北京 100044；
3. 北京市轨道交通电磁兼容与卫星导航工程技术研究中心，北京 100044；
4. 北京交通大学计算机与信息技术学院，北京 100044；
5. 中国铁道科学研究院集团有限公司通信信号研究所，北京 100081）

摘 要：面向基于全球导航卫星系统的铁路列车定位实施欺骗干扰的主动检测，在卫星定位解算层次，运用深度学习建模学习方法的优势，提出一种基于变分贝叶斯高斯混合模型－深度卷积神经网络（variational Bayesian Gaussian mixture model-deep convolutional neural network，VB-GMM-DCNN）的列车卫星定位欺骗干扰检测方法。该方法首先提取能够充分体现欺骗干扰对定位解算过程作用影响的卫星观测特征参数，构建干扰检测特征矢量；然后，采用 VBGMM 模型拟合经过预处理的特征向量的概率分布，得到二维概率密度图；最后，将概率密度图用于 DCNN 模型实施欺骗干扰的检测决策。结合现场实验所得运行场景数据，利用实验室搭建的欺骗干扰测试环境实施了干扰注入测试与检验，结果表明，欺骗干扰检测性能随着 DCNN 网络深度的增加而提升，相对于常规有监督决策方法 F1 值最高提升 44.68%。基于 VBGMM-DCNN 的欺骗干扰检测能够适应测试验证中运用的列车运行特征及定位观测条件，所达到的检测性能优于对比算法。

关键词：全球导航卫星系统；列车定位；欺骗攻击检测；变分贝叶斯高斯混合模型；深度卷积神经网络
中图分类号：U284 **文献标志码**：A **文章编号**：2095-8110(2023)04-0058-11

Spoofing detection method for satellite-based train positioning based on VBGMM-DCNN

WANG Siqi[1], LIU Jiang[1,2,3], CAI Baigen[1,3,4], ZHAO Yang[5]

1. School of Electronic and Information Engineering, Beijing Jiaotong University, Beijing 100044, China;
2. Frontiers Science Center for Smart High-speed Railway System, Beijing Jiaotong University, Beijing 100044, China;
3. Beijing Engineering Research Center of EMC and GNSS Technology for Rail Transportation, Beijing 100044, China;
4. School of Computer and Information Technology, Beijing Jiaotong University, Beijing 100044, China;
5. Signal & Communication Research Institute, China Academy of Railway Sciences Corporation Limited, Beijing 100081, China)

Abstract: Aiming at the active detection of spoofing in railway train positioning based on global navigation satellite system (GNSS), a spoofing detection method for satellite-based train positio-

收稿日期：2023-06-08；**修订日期**：2023-06-29
基金项目：国家自然科学基金(T2222015)；国家自然科学基金委员会-中国国家铁路集团有限公司铁路基础研究联合基金(U2268206)；北京市自然科学基金(4232031)
作者简介：王思琦(1997-)，女，博士研究生，主要从事卫星导航定位、导航抗干扰及轨道交通运行控制等方面的研究。
通信作者：刘江(1985-)，男，教授，博士，主要从事卫星导航定位、智能交通系统及轨道交通运行控制等方面的研究。

ning based on variational Bayesian Gaussian mixture model-deep convolutional neural network (VBGMM-DCNN) is proposed by taking the advantages of deep learning (DL) at the GNSS navigation calculation stage. Firstly, feature parameters of satellite observation that can fully represent the spoofing effect on the positioning calculation process are extracted to construct the feature vector. Then, the VBGMM model is used to fit the probability distribution of the preprocessed feature vector and the two-dimensional probability density map is obtained. Finally, the probability density map is used in DCNN model for identifying the spoofing detection decision result. With the operation scene data obtained from the field experiment, the spoofing injection test and verification are carried out with a specific spoofing test environment built in the laboratory. The results illustrate that the enhanced spoofing detection performance could be achieved with an increasing DCNN network depth. The value of F1 increases by 44.68 % compared with the conventional supervised decision method. The spoofing detection based on VBGMM-DCNN can adapt to the train operation characteristics and positioning observation conditions used in the test verification, and the detection performance is better than the comparison algorithm.

Key words: Global navigation satellite system (GNSS); Train positioning; Spoofing detection; Variational Bayesian Gaussian mixture model (VBGMM); Deep convolutional neural network (DCNN)

0　引言

基于全球导航卫星系统(global navigation satellite system, GNSS)的列车定位不仅可以提高列车运行控制系统车载设备的高度自主性、灵活性,还可以大幅简化轨旁设备,降低维护成本,提高经济效益[1-3]。然而,考虑到 GNSS 固有的脆弱性以及庞大铁路网内复杂多变的运行环境,卫星定位在铁路关键装备及服务中的实际运用仍存在一定的潜在威胁[4-5],其中,信号干扰会为列车卫星定位带来信息安全层面的风险。蓄意欺骗攻击作为一种典型的干扰形式,旨在诱骗车载卫星定位终端解算出错误的位置和时间信息,会对列车定位信息用于监测、控制等决策带来直接危害。为此,考虑到列车运行控制系统对列车定位的特定安全需求,亟需引入针对卫星定位欺骗攻击的主动防御机制,强化列车卫星的自主防护能力,在实施防护的过程中,如何有效检测欺骗干扰攻击的存在,是实施防御的前提。

目前,卫星定位欺骗检测与防护技术的研究相对成熟。根据在用户接收机信号处理中检测欺骗攻击的位置不同,可将欺骗攻击检测手段分为:1)射频前端方案,根据欺骗攻击信号来向单一、信号功率普遍高于真实信号的特点,采用多天线阵列[6]、信号到达角[7]、自适应增益控制器输出功率[8]等方法,可以实现对不同欺骗攻击的较高检测成功率;2)基带信号处理端方案,通过检测捕获阶段二维时频搜索峰值或跟踪环路的自相关函数畸变,判定是否受到欺骗攻击,如捕获峰值多峰检测[9]、基于信号质量检测(signal quality monitoring, SQM)的相关峰失真检测[10]、码和载波相位联合一致性检测[11]等;3)定位解算端方案,利用辅助传感器冗余信息[12]或接收机自主完好性监测(receiver autonomous integrity monitoring, RAIM)机制[13]对特定特征参数进行一致性检测。近年来,机器学习、深度学习以及深度强化学习等人工智能领域前沿技术的引入,为卫星定位欺骗检测提供了新的思路[14-16]。然而,现有方法尚缺乏适用于列车卫星定位场景的专用设计,不断涌现的新型学习建模方法也为列车定位应用提供了有效途径。为此,本文针对列车定位解算端的欺骗检测问题,提出了基于变分贝叶斯高斯混合模型-深度卷积神经网络(variational Bayesian Gaussian mixture model-deep convolutional neural network, VBGMM-DCNN)的检测方法,主要的创新工作包括:

1)考虑轨迹欺骗、时间欺骗和伪距欺骗攻击对定位观测的显著影响,设计了基于卫星量测偏差的欺骗检测方案,根据其在欺骗攻击前后的不同分布特性实施检测;

2)提出了完整的基于 VBGMM-DCNN 模型的

列车卫星定位欺骗干扰检测方法，使用 VBGMM 模型拟合特征参数的概率密度分布，DCNN 模型通过提取分布特征来决策系统是否受到欺骗攻击；

3）针对同一欺骗攻击下不同卫星对欺骗攻击响应的差异，所提算法适应每颗卫星响应的差异性，并对单颗卫星是否受到欺骗攻击做出决策。

1 欺骗攻击下列车卫星定位性能影响分析

导致卫星定位脆弱性的原因包括自然环境、无意人为干扰和蓄意攻击等，其中，蓄意攻击往往主观上以卫星定位性能下降或定位失效为目的，其可操作性使卫星定位面临严重威胁。蓄意攻击主要包括压制和欺骗两类。压制攻击通过传输大功率干扰信号使接收机失去对卫星信号的锁定，导致接收机无法定位；欺骗攻击使目标接收机被迫跟踪与合法卫星信号具有相似结构的欺骗信号，从而产生错误的位置或时间信息，故而在不损害定位连续性的情况下更具误导性。对列车卫星定位系统实施欺骗攻击，欺骗者需要采取一定的技术手段跟踪列车的实时运行状态，据此产生调制了错误测量信息的伪信号；或转发真实卫星信号，通过增加信号传输延时，使列车卫星定位接收机解算错误定位信息。列车运行过程中，若受到生成式/转发式欺骗攻击，均会导致列车解算出带有显著偏移的错误位置信息，如图 1 所示。欺骗攻击可能引发定位失准，若在列车控制系统处理逻辑未采用针对性防护措施，则可能直接影响列车控制功能的正常执行，甚至可能对行车安全造成影响。

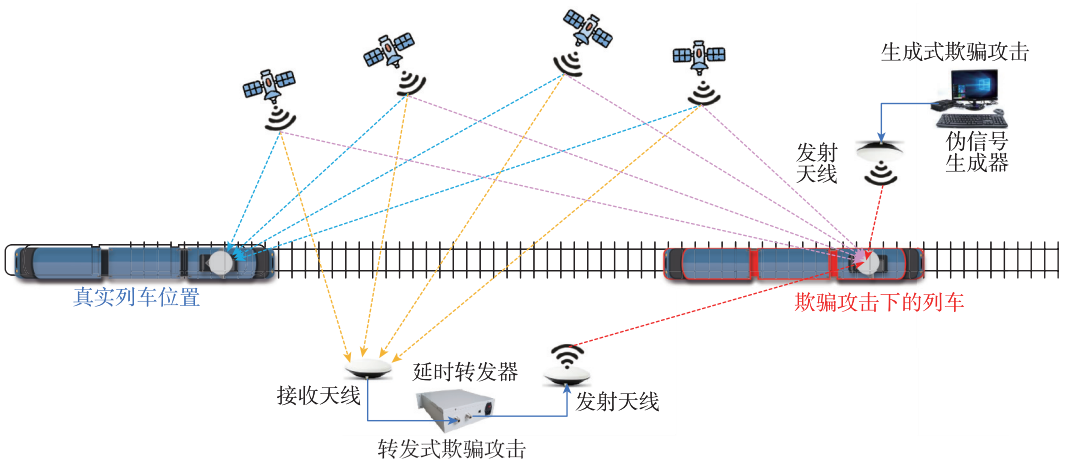

图 1 欺骗攻击下列车卫星定位影响示意图

Fig. 1 Schematic diagram of influence of satellite-based train positioning under spoofing attack

卫星定位通过测量信号从卫星到接收机天线端的传播时间，得到各可视卫星伪距、多普勒频移等观测量，结合卫星星历/历书，通过状态估计解算空间位置、速度。欺骗信号与真实信号存在相对码相位时延和多普勒频率偏移，故而，欺骗攻击最终将在伪距、伪距率、时钟偏差等观测信息中体现为一定偏差[17-18]。以伪距、伪距率和载波相位为例，受欺骗攻击作用下的观测方程为

$$\rho^{\mathrm{Sp}}=\rho^{\mathrm{Au}}+\delta\rho^{\mathrm{Sp}}=r_{\mathrm{u}}^{\mathrm{s}}+\mathrm{c}\times(\delta t^{\mathrm{u}}-\delta t^{\mathrm{s}})+I+T+\varepsilon_{\rho}+\delta\rho^{\mathrm{Sp}} \tag{1}$$

$$\dot{\rho}^{\mathrm{Sp}}=\dot{\rho}^{\mathrm{Au}}+\delta\dot{\rho}^{\mathrm{Sp}}=\dot{r}_{\mathrm{u}}^{\mathrm{s}}+\mathrm{c}\times(\delta\dot{t}^{\mathrm{u}}-\delta\dot{t}^{\mathrm{s}})+\dot{I}+\dot{T}+\varepsilon_{\dot{\rho}}+\delta\dot{\rho}^{\mathrm{Sp}} \tag{2}$$

$$\lambda\phi^{\mathrm{Sp}}=\lambda\phi^{\mathrm{Au}}+\lambda\delta\phi^{\mathrm{Sp}}=r_{\mathrm{u}}^{\mathrm{s}}+\mathrm{c}\times(\delta t^{\mathrm{u}}-\delta t^{\mathrm{s}})-I+T+\lambda N_{\phi}+\varepsilon_{\phi}+\lambda\delta\phi^{\mathrm{Sp}} \tag{3}$$

其中，ρ^{Sp}，$\dot{\rho}^{\mathrm{Sp}}$ 和 ϕ^{Sp} 分别为在欺骗攻击下接收机测量的卫星伪距、伪距率（由多普勒频移计算得到）和载波相位；λ 为信号波长；ρ^{Au}，$\dot{\rho}^{\mathrm{Au}}$ 和 ϕ^{Au} 分别为卫星真实伪距、伪距率和载波相位；$\delta\rho^{\mathrm{Sp}}$，$\delta\dot{\rho}^{\mathrm{Sp}}$ 和 $\delta\phi^{\mathrm{Sp}}$ 为欺骗攻击引起的伪距偏差、伪距率偏差和载波相位偏差；$r_{\mathrm{u}}^{\mathrm{s}}$ 为卫星与接收机之间的几何距离；$\dot{r}_{\mathrm{u}}^{\mathrm{s}}$ 为测距率；c 为光速；δt^{u} 和 $\delta\dot{t}^{\mathrm{u}}$ 分别为接收机钟差和钟漂；δt^{s} 和 $\delta\dot{t}^{\mathrm{s}}$ 分别为卫星钟差和钟漂；I 和 T 分别为电离层和对流层引起的等效伪距误差；$\dot{I}$ 和 $\dot{T}$ 为对应的延时变化率，其值一般很小；N_{ϕ} 为整周模糊度；ε_{ρ}，$\varepsilon_{\dot{\rho}}$ 和 ε_{ϕ} 为未建模的测量噪声。联立至少 4 颗卫星观测方程，采用最小二乘算法对式（1）和式（2）构成的方程组进行估计解算

$$\Delta\dot{\boldsymbol{X}}^{\mathrm{Sp}}=(\boldsymbol{H}^{\mathrm{T}}\boldsymbol{H})^{-1}\boldsymbol{H}^{\mathrm{T}}(\boldsymbol{Z}^{\mathrm{Au}}+\delta\boldsymbol{Z}^{\mathrm{Sp}})$$

$$=(\boldsymbol{H}^{\mathrm{T}}\boldsymbol{H})^{-1}\boldsymbol{H}^{\mathrm{T}}\boldsymbol{Z}^{\mathrm{Au}}+(\boldsymbol{H}^{\mathrm{T}}\boldsymbol{H})^{-1}\boldsymbol{H}^{\mathrm{T}}\delta\boldsymbol{Z}^{\mathrm{Sp}}$$
$$=\Delta\dot{\boldsymbol{X}}^{\mathrm{Au}}+\delta\boldsymbol{X}^{\mathrm{Sp}} \tag{4}$$

其中，$\Delta\dot{\boldsymbol{X}}^{\mathrm{Sp}}$ 为欺骗攻击下定位时间间隔内列车三维位置、三维速度、接收机钟差、接收机钟漂变化量组成的状态矢量；$\Delta\dot{\boldsymbol{X}}^{\mathrm{Au}}$ 为无干扰状态矢量；$\delta\boldsymbol{X}^{\mathrm{Sp}}$ 代表欺骗攻击下状态矢量的相对变化量，$\boldsymbol{H}$ 为观测矩阵，$\boldsymbol{Z}^{\mathrm{Au}}$ 为校正后的伪距和伪距率组成的观测矢量，$\delta\boldsymbol{Z}^{\mathrm{Sp}}$ 为 $\delta\rho^{\mathrm{Sp}}$ 和 $\delta\dot{\rho}^{\mathrm{Sp}}$ 组成的偏差矢量。欺骗攻击对量测引起的偏差将通过式(4)影响最终的定位估计结果。

2　列车卫星定位欺骗干扰检测方案

考虑到欺骗干扰检测可以视为一种典型的二分类问题，且基于深度学习方法对解决二分类问题的潜在优势，本文提出了一种基于变分贝叶斯高斯混合模型－深度卷积神经网络(VBGMM-DCNN)的列车卫星定位欺骗干扰检测方案，其总体框架如图 2 所示。可以看到，该框架分为离线建模和在线检测两个部分，每个部分都包括基于 VBGMM 的卫星特征参数拟合和基于 DCNN 的卫星信号分类决策两个环节：在离线建模中，采集列车运行目标线路所有可见卫星的观测数据，建立列车卫星定位无干扰和欺骗干扰数据库，通过对数据的详细分析建立欺骗干扰检测模型，通过模型训练和验证，使模型满足预期性能；在在线检测中，车载卫星定位终端采集可见卫星观测数据，实时计算并更新可见卫星观测特征，并将每颗卫星的观测特征输入至该卫星对应的已经训练所得欺骗干扰检测模型，判定是否受到欺骗攻击。

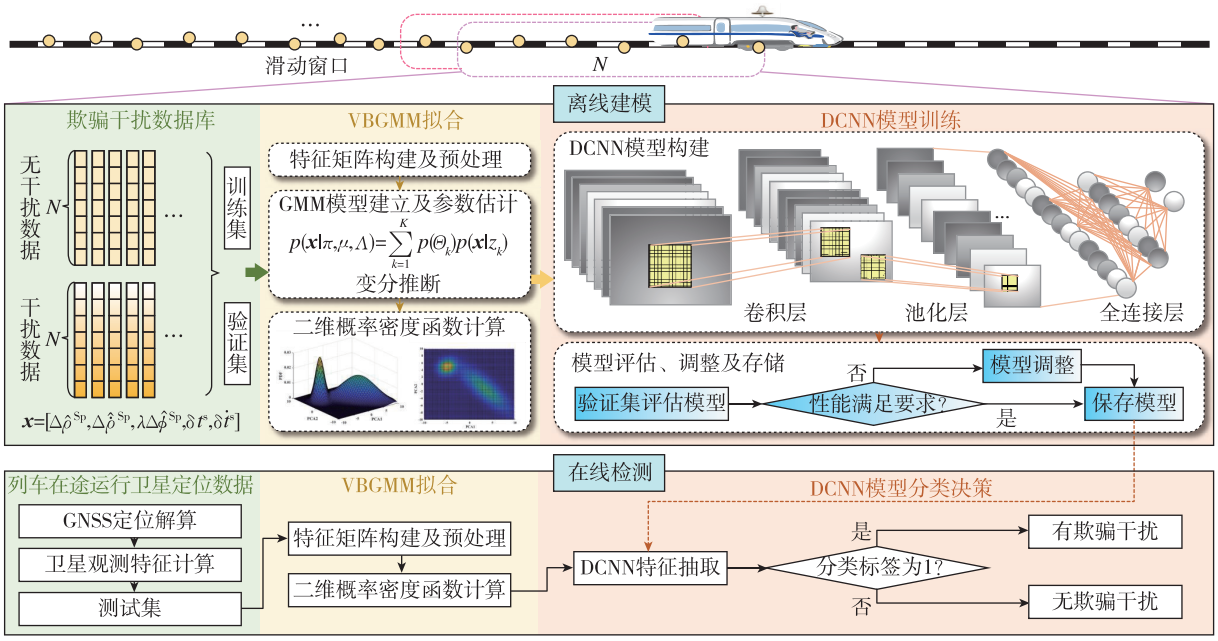

图 2　基于 VBGMM-DCNN 的列车卫星定位欺骗干扰检测方案框架

Fig. 2　Spoofing detection scheme framework for satellite-based train positioning based on VBGMM-DCNN

离线建模和在线检测的具体操作如下：

首先，设置滑动窗口，即取当前时刻及其前 $(N-1)$ 个定位周期列车卫星定位特征参数，包括每颗可见卫星的伪距残差、伪距率残差、载波相位残差、卫星钟差和卫星钟漂，针对每颗卫星观测通道构造一个特征参数矩阵(矩阵大小为 $N\times5$)；其次，将标准化的特征参数矩阵进行主成分分析(principal component analysis，PCA)特征降维至两维，输入 VBGMM 模型，通过参数初始化、变分推断和自适应调整高斯混合分量个数等操作求解各个高斯分量的参数，计算二维高斯混合概率密度函数，对其进行等间隔采样得到二维概率密度图；最后，采用灰度化处理，将概率密度图转为灰度图，并输入至 DCNN 模型中，模型进行有监督分类，以判断是否受到欺骗攻击。离线建模和在线检测的主要区别在于输入模型的数据不同，离线建模将列车卫星定位历史数据输入至模型中，进行模型的训练和调整；在线检测则将实时定位数据输入至已经训练的模型中，实时检测欺骗攻击。

3 基于 VBGMM-DCNN 的欺骗干扰检测方法

3.1 特征参数

本文选取卫星伪距残差、伪距率残差、载波相位残差、卫星时钟误差及卫星时钟漂移构建干扰检测特征量。

1)伪距残差 $\Delta\hat{\rho}^{\mathrm{Sp}}$:假设经过电离层延迟、对流层延迟和卫星钟差矫正后的伪距为 $\tilde{\rho}^{\mathrm{Sp}}$,解算后的列车位置为$(\hat{x}^{\mathrm{u}},\hat{y}^{\mathrm{u}},\hat{z}^{\mathrm{u}})$,接收机钟差为 $\delta\hat{t}^{\mathrm{u}}$,则伪距残差为

$$\Delta\hat{\rho}^{\mathrm{Sp}}=\tilde{\rho}^{\mathrm{Sp}}-\sqrt{(\hat{x}^{\mathrm{u}}-x^{\mathrm{s}})^2+(\hat{y}^{\mathrm{u}}-y^{\mathrm{s}})^2+(\hat{z}^{\mathrm{u}}-z^{\mathrm{s}})^2}-\mathrm{c}\times\delta\hat{t}^{\mathrm{u}} \quad (5)$$

式中,$(x^{\mathrm{s}},y^{\mathrm{s}},z^{\mathrm{s}})$ 为卫星三维空间坐标。

2)伪距率残差 $\Delta\hat{\dot{\rho}}^{\mathrm{Sp}}$:假设经过电离层延迟变化率、对流层延时变化率和卫星钟漂校正后的伪距率为 $\tilde{\dot{\rho}}^{\mathrm{Sp}}$,若由伪距率方程定位解算后的列车速度为 $\hat{\boldsymbol{v}}^{\mathrm{u}}$,接收机时钟频漂为 $\delta\hat{\dot{t}}^{\mathrm{u}}$,则伪距率残差为

$$\Delta\hat{\dot{\rho}}^{\mathrm{Sp}}=\tilde{\dot{\rho}}^{\mathrm{Sp}}-(\boldsymbol{v}^{\mathrm{s}}-\hat{\boldsymbol{v}}^{\mathrm{u}})\boldsymbol{u}_{\mathrm{u}}^{\mathrm{s}}-\mathrm{c}\times\delta\hat{\dot{t}}^{\mathrm{u}} \quad (6)$$

式中,$\boldsymbol{v}^{\mathrm{s}}$ 为卫星速度;$\boldsymbol{u}_{\mathrm{u}}^{\mathrm{s}}$ 为卫星在接收机处的单位观测矢量。

3)载波相位残差 $\lambda\Delta\dot{\phi}^{\mathrm{Sp}}$:假设经过电离层延迟、对流层延迟和卫星钟差校正后的载波相位为 $\lambda\tilde{\dot{\phi}}^{\mathrm{Sp}}$,借助定位解算估计位置和接收机钟差,可计算载波相位残差为

$$\lambda\Delta\dot{\phi}^{\mathrm{Sp}}=\lambda\tilde{\dot{\phi}}^{\mathrm{Sp}}-\sqrt{(\hat{x}^{\mathrm{u}}-x^{\mathrm{s}})^2+(\hat{y}^{\mathrm{u}}-y^{\mathrm{s}})^2+(\hat{z}^{\mathrm{u}}-z^{\mathrm{s}})^2}-\mathrm{c}\times\delta\hat{\dot{t}}^{\mathrm{u}} \quad (7)$$

式中,载波相位残差 $\lambda\Delta\dot{\phi}^{\mathrm{Sp}}$ 是未知整周模糊度、欺骗攻击引起的偏差和未建模噪声等各部分效应的叠加。

4)卫星时钟误差:卫星时钟在观测时间为 t 时的卫星钟差 Δt^{s} 为

$$\Delta t^{\mathrm{s}}=a_{f0}+a_{f1}(t-t_{\mathrm{oc}})+a_{f2}(t-t_{\mathrm{oc}})^2 \quad (8)$$

式中,a_{f0},a_{f1},a_{f2} 以及参考时间 t_{oc} 均由卫星导航电文的第一数据块给出。

卫星时钟总的校正量还包括相对论效应的校正量 Δt_{r} 和群波延时校正量 T_{GD},即

$$\delta t^{\mathrm{s}}=\Delta t^{\mathrm{s}}+\Delta t_{\mathrm{r}}-T_{\mathrm{GD}} \quad (9)$$

5)卫星时钟漂移 $\delta\dot{t}^{\mathrm{s}}$:卫星钟差公式对时间求导,可得卫星时钟漂移

$$\delta\dot{t}^{\mathrm{s}}=a_{f1}+2a_{f2}(t-t_{\mathrm{oc}})+\Delta\dot{t}_{\mathrm{r}} \quad (10)$$

式中,$\Delta\dot{t}_{\mathrm{r}}$ 为相对论效应的校正量对时间的导数,一般群波延时校正量对时间的导数可认为等于零。

因此,针对每颗卫星可以构建特征矢量 $\boldsymbol{x}=[\Delta\hat{\rho}^{\mathrm{Sp}},\Delta\hat{\dot{\rho}}^{\mathrm{Sp}},\lambda\Delta\dot{\phi}^{\mathrm{Sp}},\delta t^{\mathrm{s}},\delta\dot{t}^{\mathrm{s}}]^{\mathrm{T}}$,由滑动窗口内的所有特征矢量可构成特征矩阵,用于实施建模和在线检测。

3.2 基于 VBGMM-DCNN 的建模检测方法

本文采用 PCA 降维方法将所构建的 5 维干扰检测特征矢量降至 2 维,减少冗余信息。假设每颗卫星干扰检测特征量构成的干扰检测特征矩阵为 $\boldsymbol{X}=[\boldsymbol{x}_1,\boldsymbol{x}_2,\cdots,\boldsymbol{x}_N]^{\mathrm{T}}$,$\boldsymbol{X}$ 为 $N\times5$ 的矩阵,设干扰检测特征量的均值为 $\overline{X}_k(k=1,2,\cdots,5)$,计算 $\boldsymbol{X}$ 的零均值化标准矩阵为

$$\dot{X}_{ik}=\frac{X_{ik}-\overline{X}_k}{\sqrt{\frac{1}{N-1}\sum_{i=1}^{N}(X_{ik}-\overline{X}_k)^2}} \quad (11)$$

则协方差矩阵为

$$\boldsymbol{D}=\frac{1}{N}\sum_{i=1}^{N}\dot{X}_{ik}(\dot{X}_{ik})^{\mathrm{T}} \quad (12)$$

计算协方差矩阵的特征值为 $\lambda_1,\lambda_2,\cdots,\lambda_5$,且 $\lambda_1>\lambda_2\cdots>\lambda_5$,取最大的 λ_1 和 λ_2 对应的特征矢量 $\boldsymbol{\beta}_1$ 和 $\boldsymbol{\beta}_2$,组成转换矩阵 $\boldsymbol{A}=[\boldsymbol{\beta}_1,\boldsymbol{\beta}_2]$,利用下式得到降维后的数据 $\boldsymbol{V}$。

$$\boldsymbol{V}=\boldsymbol{A}^{\mathrm{T}}\boldsymbol{X} \quad (13)$$

高斯混合模型(Gaussian mixture model,GMM)采用对多个高斯分量的线性组合来描述复杂数据的概率分布,广泛用于解决分类和密度估计问题。GMM 模型的概率密度函数可以表示为

$$p(\boldsymbol{v}\mid\pi,\mu,\boldsymbol{\Lambda})=\sum_{k=1}^{K}p(\Theta_k)p(\boldsymbol{v}\mid z_k)=\sum_{k=1}^{K}\pi_k\Phi(\boldsymbol{v}\mid\mu_k,\boldsymbol{\Lambda}_k) \quad (14)$$

其中,$\boldsymbol{v}$ 是使用 PCA 降维后的二维特征矢量;K 为高斯分量的总数;Θ_k 为第 k 个高斯分量的隐变量,均值为 μ_k;方差矩阵为 $\boldsymbol{\Lambda}_k$;$\pi_k(\pi_k\geqslant0$ 且 $\sum_k\pi_k=1)$ 是混合系数,表示高斯分量的权重;$\Phi(\boldsymbol{v}\mid\mu_k,\boldsymbol{\Lambda}_k)$ 为第 k 个高斯分量的概率密度函数。

本文使用变分推断(variational inference, VI)求解模型参数。将某一观测特征矢量 $\boldsymbol{v}^*$ 代入 VB-GMM 模型,预测其概率分布,结果为

$$p(\boldsymbol{v}^*\mid\boldsymbol{v})=\sum_{k=1}^{K}\iiint\pi_k\Phi(\boldsymbol{v}^*\mid\Theta^*,\mu_k,\boldsymbol{\Lambda}_k)\cdot q(\Theta^*\mid\pi)q(\pi,\mu_k,\boldsymbol{\Lambda}_k\mid\upsilon)\mathrm{d}\pi\mathrm{d}\mu_k\mathrm{d}\boldsymbol{\Lambda}_k \quad (15)$$

变分推断通过循环执行变分 E 步和变分 M 步来

更新均值、协方差矩阵和混合系数，直至算法收敛[19]，最终，得到混合学生 t 分布，即所求概率密度函数

$$p(\boldsymbol{v}^*\mid\boldsymbol{v})=\frac{1}{\hat{\alpha}}\sum_{k=1}^{K}\alpha_k St\left(\boldsymbol{v}^*\mid m_k,\frac{(\gamma_k+1-D)\beta_k}{1+\beta_k}W_k,\gamma_k+1-D\right)\tag{16}$$

式中，$St(*)$ 表示学生 t 分布，其均值矢量为 m_k；精度为 $\frac{(\gamma_k+1-D)\beta_k}{1+\beta_k}W_k$，自由度为 γ_k+1-D，当样本数充分时，式(16)趋向于高斯混合模型。在算法迭代过程中，可以通过自动剔除混合系数较小的高斯分量，达到自适应调节高斯分量个数的目的。对所求概率密度函数进行等间隔采样得到二维概率密度分布图 $\boldsymbol{S}_n$，从而可以将其输入至深度卷积神经网络进行特征提取。

卷积神经网络(convolutional neural networks，CNN)是一种包含卷积操作的前馈神经网络，是深度学习的典型算法之一，被广泛应用于计算机视觉、自然语音处理等领域。基于深度卷积神经网络(deep convolutional neural networks，DCNN)的分类算法是一种有效的分类方式，通过多层卷积和池化操作提取学习大规模数据的复杂特征，提高分类准确度。DCNN 的核心是卷积层，由一组卷积核(也称为卷积滤波器)组成。卷积操作的本质是相关滤波，卷积核按照预设步长的滑动窗口在输入信号上移动，并与截取的相同大小的张量做点乘，添加偏置求和，不断重复上述过程直至遍历输入信号，最终得到一个特征图。一般在卷积层后紧跟池化层和激活函数，池化层对卷积层提取的特征图进行降维，改善过拟合现象，激活函数用于增加网络的非线性。在对 DCNN 模型进行训练时，采用交叉熵损失函数衡量预测的分类结果与真值的差距，通过反向传播更新网络参数。基于 KL 散度可推导交叉熵损失函数

$$\begin{aligned}L_{\mathrm{KL}}(P\mid Q)&=\int_{\Omega}p(x)\cdot\log_2\frac{p(x)}{q(x)}\cdot\mathrm{d}x\\&=\int_{\Omega}p(x)\cdot\log_2 p(x)\cdot\mathrm{d}x-\int_{\Omega}p(x)\cdot\log_2 q(x)\cdot\mathrm{d}x\\&=-\Upsilon(P)+\Upsilon(P,Q)\end{aligned}\tag{17}$$

其中，$p(x)$ 为样本真实的概率密度函数；$q(x)$ 为模型拟合的概率密度函数；Ω 为整个概率密度空间；$\Upsilon(P)$ 为样本真实分布 P 的信息熵；$\Upsilon(P,Q)$ 为样本真实分布与模型预测分布 Q 的交叉熵；KL 散度具有非负特性，使得最小化 KL 散度等价于最小化交叉熵。

基于上述思想的列车卫星定位欺骗干扰检测可视为一种有监督二分类问题，为引入深度卷积神经网络并发挥其建模描述能力的优势提供了契机。运用 DCNN 模型检测确认是否受到欺骗攻击，主要分为以下几个步骤：

Step 1：离线建模时，根据式(5)～(10)计算卫星观测特征矢量，采用 PCA 进行降维，得到 $\boldsymbol{v}$。

Step 2：采用 VBGMM 模型估计 $\boldsymbol{v}$ 的概率密度函数，进行二维等间隔采样，得到二维概率密度分布图 $\boldsymbol{S}_n$，关联相应的特征标签。

Step 3：将二维概率密度分布图 $\boldsymbol{S}_n$ 视为单通道图片信号，输入构建好的 DCNN 网络中，网络进行迭代训练，计算交叉熵损失函数，使用误差反向传播算法更新网络参数，多次迭代训练后得到优化的欺骗检测模型。

Step 4：列车运行中，调用 DCNN 网络对实时卫星观测特征的二维概率密度图进行二分类，若模型判决存在欺骗干扰，向列车定位应用端输出告警并实施欺骗防护；若模型判决未受到欺骗攻击，将卫星定位解算结果用于列车测速定位决策。

结合上述思路，本文提出的列车卫星定位欺骗干扰检测流程如图 3 所示。该方法可以监测每颗卫星的观测状态，若判定当前观测卫星受到欺骗攻击，可直接在列车测速定位决策处理中隔离该卫星定位通道，防止受到欺骗干扰的影响，或运用额外的欺骗攻击抑制手段恢复真实的导航卫星量测信息用于解算及定位决策处理，在保持卫星定位运用的条件下主动消除欺骗攻击的影响。本文所提方法的应用约束有：算法的欺骗检测性能与欺骗攻击的类型和强度有关；算法的检测性能与深度学习模型的深度有关；所提算法为数据驱动方式，需要大量的欺骗数据样本支持来进一步提升算法的优势。

4　验证与分析

4.1　数据采集

采用 2021 年 7 月在青藏铁路公司管辖内哈木线(哈尔盖-木里)现场采集的列车卫星定位数据对本文提出的欺骗干扰检测方法性能进行验证。在现场采集中，为满足使用真实现场数据构建基础测试场景的需求，需确保卫星定位可用且具有较优定位性能，选择较为开阔的线路区段，使用NovAtel SPAN-FSAS

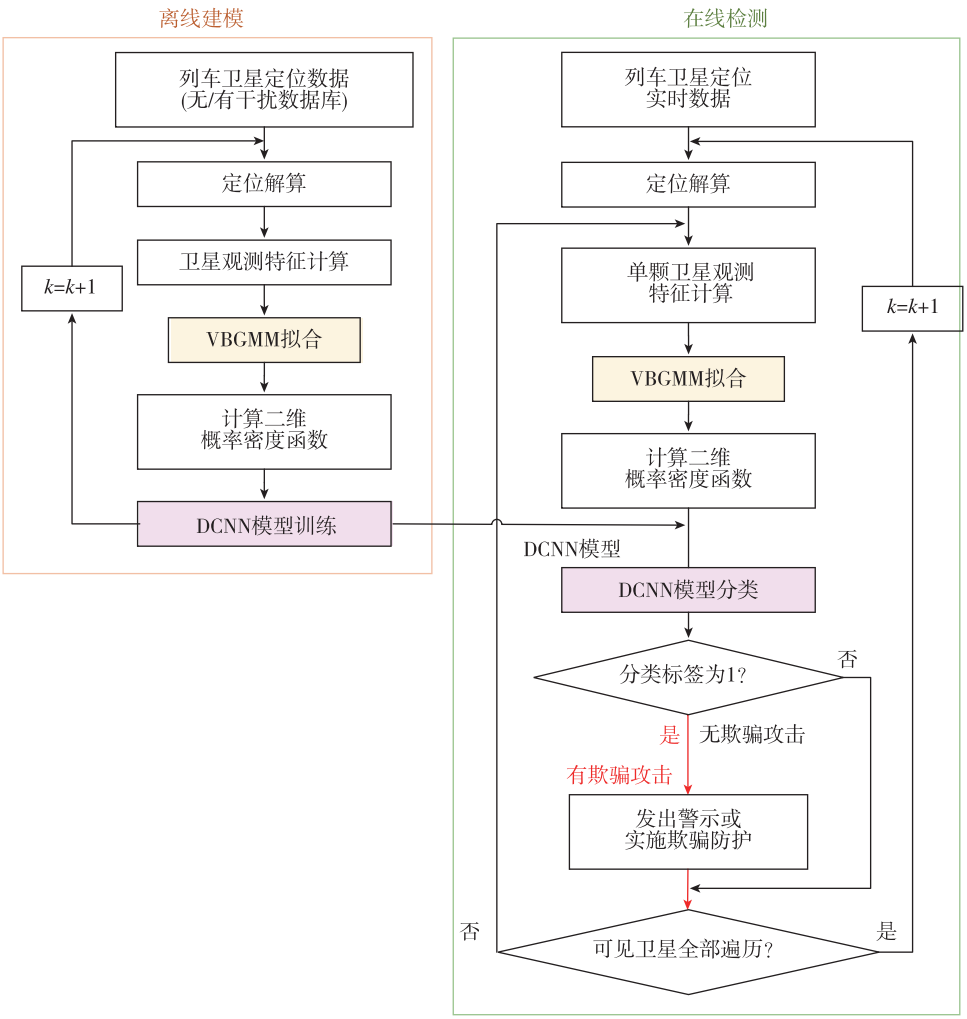

图 3　基于 VBGMM-DCNN 的列车卫星定位欺骗干扰检测流程

Fig. 3　Spoofing detection process for satellite-based train positioning based on VBGMM-DCNN

高精度组合定位参考系统定位输出结果用于列车运行场景构建,在干扰测试中通过叠加特定类型欺骗信号模拟欺骗干扰攻击,实现信号级干扰仿真测试。图 4 显示了实验室内搭建的欺骗干扰测试环境。

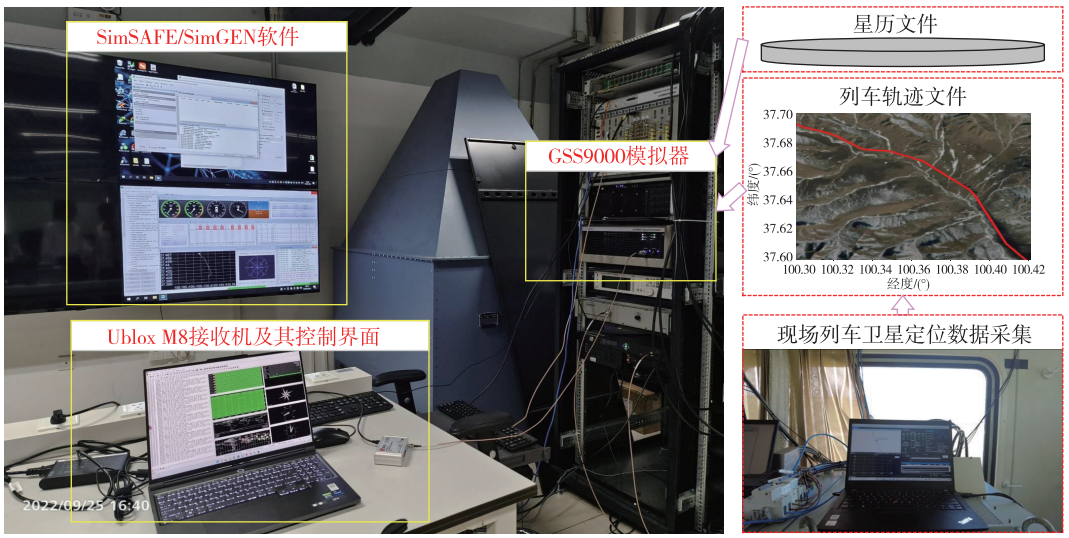

图 4　实验室搭建的欺骗干扰测试环境

Fig. 4　Spoofing test environment built in the laboratory

欺骗干扰测试环境由 Spirent GSS 9000 型导航卫星信号模拟器(含 SimSAFE 干扰套件)、受测接收机(Ublox M8)及相应控制软件组成。根据现场采集的列车运行数据,提取列车三维空间位置、速度信息制作列车轨迹文件,导入实测数据采集当天的星历,通过配置指令在不同的观测量注入欺骗场景事件。受测接收机通过射频天线接收模拟器产生的受干扰的卫星信号,并实施定位观测解算。

基于上述环境,实施了 4 种场景的测试检验,包括无干扰场景、轨迹欺骗场景、时间欺骗场景以及伪距欺骗场景。图 5 显示了每种场景模拟过程中 8 颗可持续跟踪卫星的天顶视图,实验设置真实卫星信号的强度为 −130 dBm,欺骗卫星信号的强度为 −125 dBm。无干扰场景:模拟器仅根据真实列车运行轨迹模拟真实卫星信号;轨迹欺骗场景:模拟器导入的欺骗轨迹相比于真实列车运行轨迹在 ECEF 坐标系下 X 轴添加了 30 m 偏差;时间欺骗场景:设置欺骗信号的时间参数为时钟偏移 af0=4×10^{-5} s、时钟漂移 af1=10^{-9} s/s、时钟漂移率 af2=10^{-15} s/s^2;伪距欺骗场景:模拟器根据真实列车运行轨迹模拟欺骗卫星信号,欺骗卫星伪距添加 50m 偏差。每种场景下列车运行时长 2 900 s,受测接收机采样频率设置为 10 Hz,4 种场景共记录时长 11 600 s,即 116 000 条卫星定位观测数据。滑动窗口长度设置为 10 s。在每一种场景下,针对每颗可视卫星可以构建 28 900 例样本(特征矩阵),欺骗场景的样本标签为“1”,表示欺骗样本,无干扰场景的样本标签为“0”,表示真实样本。每种场景每颗卫星的样本划分为训练集(50%)、验证集(30%)和测试集(20%),用于建模与检验。

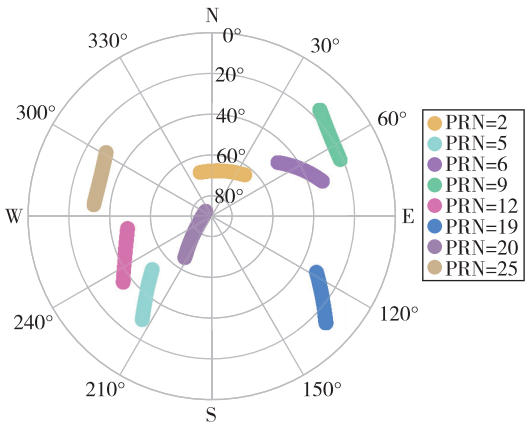

图 5　测试过程中可持续跟踪卫星的运行轨迹

Fig. 5　Trajectory of the satellites that can be continuously tracked during the test process

4.2　方法验证

为检验欺骗干扰检测算法的性能,首先,设置不同的 DCNN 网络模型,分析不同网络模型的适用性;其次,与常规有监督分类算法用于欺骗检测的性能进行对比分析,验证所提出 VBGMM-DCNN 建模检测策略的有效性。

本文选择 3 种 DCNN 网络模型用于模型对比,模型均由卷积层、批量归一化层、池化层、全连接层和激活函数混合构建,3 种模型深度逐渐增加,网络参数设置如下:

1) DCNN-1 模型:Conv(50, 11×11, 3);Bn();Relu();Mp(11×11, s=4);Fc(50);Relu();Fc(2);Softmax()。

2) DCNN-2 模型:Conv(50, 11×11, 2);Bn();Relu();Conv(100, 12×12, 2);Bn();Relu();Conv(50, 12×12, 2);Relu();Fc(50);Relu();Fc(2);Softmax()。

3) DCNN-3 模型:Conv(10, 3×3, 2);Bn();Relu();Mp(11×11);Conv(100, 11×11);Bn();Relu();Mp(11×11);Conv(50, 11×11);Bn();Relu();Conv(10, 4×4, 2);Bn();Relu();Fc(50);Relu();Fc(2);Softmax()。

其中,Conv (numFilters,filterSize,stride)表示卷积层,滤波器数量为 numFilters,滤波器大小为 filterSize,步长为 stride,默认步长为 1;Bn()表示批量归一化层;Relu()表示 Relu 激活函数;Mp(filterSize,stride)表示最大池化;Fc(outputSize)表示全连接层,输出 outputSize 个神经元;Softmax()表示 Softmax 激活函数。3 种模型迭代次数均设置为 50 次,学习率为 0.001,批量大小为 100,优化函数为 Adam()。

DCNN-1、DCNN-2 和 DCNN-3 模型的参数量分别为 96.3×10^3,1.4×10^6 和 742.7×10^3,在相同的硬件平台下,三种模型经过 50 轮训练耗时分别为 188.97 s,1 115.95 s 和 1 094.30 s。图 6 以 PRN2 号卫星通道数据为例显示了 DCNN-3 模型的训练过程。随着迭代次数的增加,模型在训练集和验证集的准确率逐渐增加超过 90%,模型损失逐渐减小至 0.1 附近。采用经典的分类算法评价指标,包括准确率、精准率、召回率和 F1 值,评价 3 种模型的性能。图 7、图 8 和图 9 分别统计了 3 种模型在训练集、验证集和测试集的评价指标结果,图中横坐标表示3种模型的4个评价指标,纵坐标表示不同

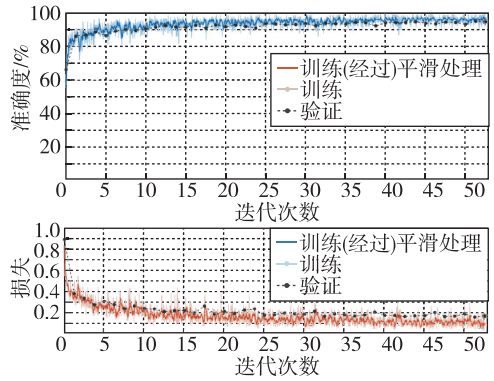

图 6 DCNN－3 模型的训练过程

Fig. 6 Training process of DCNN-3 model

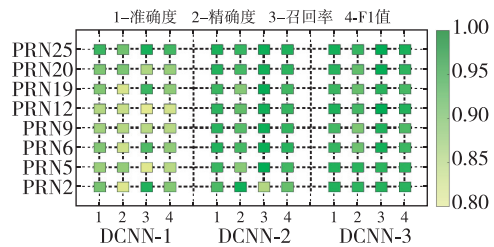

图 7 训练集评价指标统计

Fig. 7 Statistics of evaluation indexes of training set

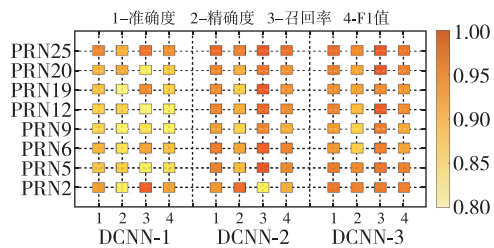

图 8 验证集评价指标统计

Fig. 8 Statistics of evaluation indexes of validation set

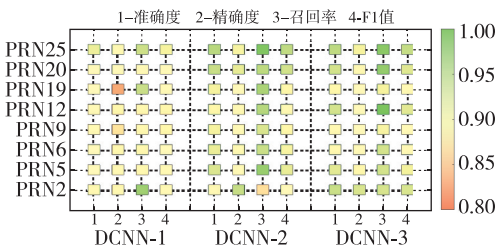

图 9 测试集评价指标统计

Fig. 9 Statistics of evaluation indexes of testing set

卫星通道，矩形颜色深浅量化表示了评价指标值的区别。总体来看，针对不同数据集，随着模型深度的增加，评价指标值越大，欺骗干扰检测性能越优，且不同卫星通道运用相同网络模型架构进行模型训练和检测，其检测性能存在差异，其原因在于随着卫星空间分布不同，不同卫星对同一欺骗攻击的响应程度不一致，具体体现在所选 5 维观测特征参数的变化存在差异，使得相同网络模型所得训练参数不一致，导致不同的检测效果。为了定量分析模型性能，对不同卫星观测的性能评价指标求算术平均(结果如表 1)，结果表明，DCNN 网络这一类方法能够有效实现对干扰特征的建模并支持干扰检测识别，在所采用的 3 种模型中，DCNN-3 模型在多个评价指标和多个数据集上能够获得总体更优性能，相对 DCNN-1、DCNN-2，模型深度的增加有助于提高欺骗干扰检测性能。

表 1 三种 DCNN 模型的欺骗检测性能评价指标统计

Tab. 1 Statistics of spoofing detection performance evaluation indexes of three DCNN models

类型	网络	准确率/%	精准率/%	召回率/%	F1 值/%
训练集	DCNN-1	90.90	88.92	91.22	89.64
	DCNN-2	95.90	93.82	97.07	95.34
	DCNN-3	**96.21**	**93.92**	**97.60**	**95.71**
验证集	DCNN-1	90.35	87.78	90.38	88.97
	DCNN-2	94.10	**91.46**	95.53	93.36
	DCNN-3	**94.47**	91.07	**96.04**	**93.80**
测试集	DCNN-1	90.22	87.15	91.14	89.02
	DCNN-2	94.49	92.16	95.46	93.68
	DCNN-3	**94.63**	91.75	**96.31**	**93.96**

本文选择伪距欺骗场景来验证 DCNN-3 模型对不同程度欺骗攻击的检测性能。设置 11 种伪距欺骗场景，欺骗卫星添加 20～200 m 伪距偏差。表 2 列出了在测试集上不同观测卫星的性能评价指标的算术平均值。整体来看，随着欺骗信号伪距偏差

表 2 不同伪距欺骗程度下 DCNN-3 模型的检测性能评价指标统计

Tab. 2 Statistics of detection performance evaluation indexes of DCNN-3 model under different pseudo-range spoofing

伪距偏差/m	准确率/%	精准率/%	召回率/%	F1 值/%
20	89.36	91.54	93.08	92.31
30	90.56	91.86	94.44	93.07
40	93.66	95.33	95.21	95.27
50	93.47	93.96	96.52	95.22
60	95.50	95.64	97.64	96.63
70	97.71	98.10	99.23	97.90
80	98.09	98.28	99.52	98.90
90	99.46	99.36	100.00	99.68
100	99.89	99.87	100.00	99.93
150	100.00	100.00	100.00	100.00
200	100.00	100.00	100.00	100.00

的增加，四个检测性能评价指标出现增加趋势，当伪距偏差达到 90 m 时，各个检测性能评价指标已接近 100%。因此，随着欺骗程度的增加，所提模型的检测性能具有一定的提升。

本文选择了 3 种经典的有监督分类算法作为参照来进一步对比分析所提算法的检测性能，包括决策树(DT)、支持向量机(SVM)、包含单隐藏层的感知机(MLP)，使用文本选择的 5 维卫星定位观测特征参数组成的特征矢量进行模型训练和测试。图 10 显示了包括本文所用策略(DCNN 网络配置为 DCNN-3)在内的 4 种方法的测试集性能统计结果。图中，纵坐标显示了不同卫星通道 4 种评价指标的算术平均值，并根据标准差添加了误差线。具体来看，本文所提出的方法的准确度相比于对比方法分别提升了 0.88%(DT)，2.32%(SVM)和 17.36%(MLP)；精确度相比于 SVM 算法提升了 2.50%，相比于 DT 和 MLP 算法分别降低了 0.21%、5.36%；召回率相比于对比方法分别提升了 4.88%(DT)，5.32%(SVM)和 92.96%(MLP)；F1 值分别提升了 2.25%(DT)，4.17%(SVM)和 44.68%(MLP)。总体来看，测试验证中所设置的欺骗干扰场景所致卫星观测特征与无干扰条件相比存在较明显异化，所选用的 3 种参照方法能够达到一定的欺骗干扰检测性能，本文所提出的方法充分发挥了 VBGMM-DCNN 策略的优势，达到了量化更优且更为稳定的检测性能，对于确保列车定位的欺骗干扰检测能力并驱动主动防护具有积极意义。

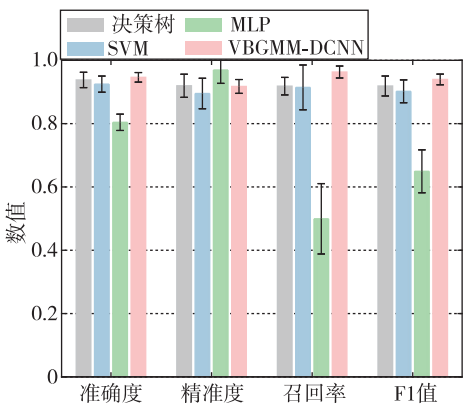

图 10　对比算法的评价指标统计

Fig. 10　Statistics of comparison algorithm evaluation index

综上所述，本文所提出欺骗干扰检测方法针对不同的深度卷积网络模型配置策略、不同空间分布下的卫星定位观测通道，其欺骗干扰检测性能存在差异，随着网络模型深度的增加，检测性能能够得到提升；分别在所建立的欺骗干扰数据集上实施本文方法和典型有监督分类算法，对比验证了所选用的卫星观测特征参数集的合理性和可用性，进一步验证了本文提出整体方案的检测性能和应用潜力。

5　结论

针对列车卫星定位的欺骗干扰检测防护需求，面向卫星定位解算域，提出一种基于 VBGMM-DCNN 的欺骗干扰检测方法，该方法采用 VBGMM 模型拟合卫星定位观测特征矢量的概率密度函数，等间隔采样得到二维概率密度图，并将其输入至 DCNN 模型中进行二分类判决。论文结合欺骗干扰测试环境实施了测试验证，结论如下：

(1)构建了无干扰、伪距欺骗、轨迹欺骗和时间欺骗 4 类欺骗干扰模式的样本数据集，对不同的 DCNN 网络模型进行了测试，结果显示，不同卫星通道对同一欺骗攻击的响应有所区别，导致相同 DCNN 模型的欺骗干扰检测性能存在差异；整体而言，随着 DCNN 网络模型深度的增加，欺骗干扰检测性能能够得到提升。

(2)将所提出的方法与典型有监督分类算法进行对比，结果显示，本文所选用的卫星定位观测特征参数集能够充分体现欺骗干扰对定位解算的影响。综合各类性能指标来看，VBGMM-DCNN 建模检测策略的引入能够达到更优的整体性能。

(3)基于 VBGMM-DCNN 的欺骗干扰检测能够适应测试验证中运用的列车运行特征及定位观测条件，所达到的检测性能较高，且针对每颗可视卫星建立独立的神经网络模型，如果检测出卫星受到欺骗攻击，可以通过简单的排除该卫星通道，使其不参与最终卫星定位解算，从而简单地实现欺骗干扰的防护。

参考文献

[1] 蔡煊，陶汉卿，侯宇婷，等．北斗卫星导航系统在列车定位中的应用研究与发展[J]．铁道科学与工程学报，2022，19(8)：2417-2427.
CAI Xuan，TAO Hanqing，HOU Yuting，et al. Application research and development of Beidou navigation satellite system in train positioning[J]. Journal of Railway Science and Engineering，2022，19(8)：2417-2427(in Chinese).

[2] AMATETTI C，POLONELLI T，MASINA E，et al. Towards the future generation of railway localization and signaling exploiting sub-meter RTK GNSS

[C]// 2022 IEEE Sensors Applications Symposium (SAS), Sundsvall, Sweden, 2022: 1-6.

[3] NEDELIAKOVÁ E, HRANICKÝ M P, Č ECHOVIČ L. Possibilities of implementing satellite navigation elements in the field of railway transport[J]. Transportation Research Procedia, 2019, 40: 1504-1509.

[4] STALLO C, SALVATORI P, COLUCCIA A, et al. GNSS Anti-jam RF-to-RF on board unit for ERTMS train control[C]// Proceedings of the 2020 International Technical Meeting of the Institute of Navigation, San Diego, California, January 2020: 1045-1058.

[5] SPINSANTE S, COSIMO S. Issues on uncertainty to trainpositioning in hybridized-GNSS approaches[C]// 2019 IEEE 5th International Workshop on Metrology for AeroSpace (MetroAeroSpace), 2019: 387-392.

[6] 耿正霖,李峥嵘,聂俊伟,等. GNSS 阵列接收机信号解扩前的欺骗干扰检测算法[J]. 国防科技大学学报,2018,40(2):91-96.
GENG Zhenglin, LI Zhengrong, NIE Junwei, et al. Spoofing detection technique before despreading for GNSS antenna-array receivers[J]. Journal of National University of Defense Technology, 2018, 40(2): 91-96(in Chinese).

[7] LO S, CHEN Y H, JAIN H, et al. Robust GNSS spoof detection using direction of arrival: methods and practice [C]//Proceedings of the 31st International Technical Meeting of The Satellite Division of the Institute of Navigation (ION GNSS+ 2018), 2018: 2891-2906.

[8] LO S, ROTHMAIER F, MIRALLES D, et al. Developing a practical GNSS spoofing detection thresholds for receiver power monitoring[C]// Proceedings of the 34th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS+ 2021), St. Louis, Missouri, 2021: 803-815.

[9] 王文益,王沛菡. 基于捕获结果的 GNSS 欺骗式干扰检测[J]. 信号处理,2021,37(8): 1460-1469.
WANG Wenyi, WANG Peihan. GNSS spoofing interference detection based on acquisition results[J]. Journal of Signal Processing, 2021, 37(8): 1460-1469(in Chinese).

[10] JIE H, LETIZIA L, BEATRICE M, et al. GNSS spoofing detection: theoretical analysis and performance of the ratio test metric in open sky[J]. ICT Express, 2016, 2(1): 37-40.

[11] YUAN D, LI H, WANG F, et al. A GNSS acquisition method with the capability of spoofing detection and mitigation[J]. Chinese Journal of Electronics, 2018, 27(1): 213-222.

[12] GU N, XING F, YOU Z. GNSS Spoofing detection based on coupled visual/inertial/GNSS navigation system [J]. Sensors. 2021; 21(20): 1-22.

[13] 武智佳,吴文启,刘科,等. 基于 INS/GNSS 紧耦合组合的逐步诱导式欺骗检测算法研究[J]. 导航定位与授时,2019,6(1):7-13.
WU Zhijia, WU Wenqi, LIU Ke, et al. Research on algorithm of gradually induced spoofing detection based on tightly coupled INS/GNSS integration[J]. Navigation Positioning and Timing, 2019, 6(1): 7-13 (in Chinese).

[14] LI J, ZHUX, OUYANG M, et al. GNSS spoofing jamming detection based on generative adversarial network [J]. IEEE Sensors Journal, 2021, 21(20): 22823-22832.

[15] 周彦,王山亮,杨威,等. 基于 PSO-ELM 的卫星导航欺骗式干扰检测[J]. 导航定位与授时, 2022,9(5): 153-161.
ZHOU Yan, WANG Shanliang, YANG Wei, et al. Deceptive jamming detection of satellite navigation based on PSO-ELM[J]. Navigation Positioning and Timing, 2022, 9(5): 153-161(in Chinese).

[16] SHAFIEE E, MOSAVI M, MOAZEDI M. Detection of spoofing attack using machine learning based on multi-layer neural network in single-frequency GPS receivers[J]. The Journal of Navigation, 2018, 71(1): 169-188.

[17] LIU Y, LI S, FU Q, et al. Impact assessment of GNSS spoofing attacks on INS/GNSS integrated navigation system[J]. Sensors, 2018: 18(5), 1433.

[18] 张超,吕志伟,张伦东,等. 基于新息速率抗差估计的 INS/GNSS 组合导航系统欺骗检测算法[J]. 中国惯性技术学报,2021,29(3):328-333.
ZHANG Chao, LYU Zhiwei, ZHANG Lundong, et al. A spoofing detection algorithm for INS/GNSS integrated navigation system based on innovation rate and robust estimation[J]. Journal of Chinese Inertial Technology,2021,29(3):328-333(in Chinese).

[19] 戴卿,隋立芬,田源,等. 变分优化的高斯混合滤波及其在导航中的应用[J]. 武汉大学学报(信息科学版),2019,44(5):699-705.
DAI Qing, SUI Lifen, TIAN Yuan, et al. Gaussian mixture filter based on variational Bayesian learning optimization and its application to integrated navigation[J]. Geomatics and Information Science of Wuhan University, 2019, 44(5): 699-705(in Chinese).

(编辑:孟彬)