基于相关域信息的支持向量机诱导式欺骗检测算法研究

刘文祥[1,2]，宋贻立[1,2]，叶小舟[1,2]，肖 伟[1,2]，李蓬蓬[1,2]
（1. 国防科技大学电子科学学院，长沙 410073；2. 导航与时空技术国家级重点实验室，长沙 410073）

摘 要：针对全球导航卫星系统易受欺骗攻击的问题，提出一种基于相关域信息的支持向量机检测算法。传统方法存在依赖先验信息、多径干扰易虚警及特征选择主观等局限；相关域信息的支持向量机通过分析信号跟踪过程，提取相关器的同相和正交支路输出，早迟码和即时码组合特征，并利用特征相关性及互信息分析优化特征组合，充分挖掘相关域信息。实验表明，在特征数量为6时该算法对欺骗与多径混合场景的检测正确率达95.61%，较传统支持向量机算法提升12%，各项指标均显著优于对比算法。在泛化能力评估中，相关域信息的支持向量机对未训练数据的准确率、精确率、召回率可达90%；经德州欺骗测试集验证，在场景2训练集和场景3迁移测试集上的准确率均大于98%。该方法有效提升了GNSS欺骗检测的精度与场景适应性，为复杂电磁环境下的鲁棒检测提供了新思路。

关键词：诱导式欺骗；多径干扰；基于相关域信息的支持向量机(CD-SVM)；泛化能力
中图分类号：V249.32+4 **文献标识码：**A **文章编号：**1000-1328(2025)06-1189-14
DOI：10.3873/j.issn.1000-1328.2025.06.014

Research on Support Vector Machine Induced Deception Detection Algorithm Based on Correlation Domain Information

LIU Wenxiang[1,2], SONG Yili[1,2], YE Xiaozhou[1,2], XIAO Wei[1,2], LI Pengpeng[1,2]
(1. College of Electronic Science and Technology, National University of Defense Technology, Changsha 410073, China;
2. Navigation and Space-Time Technology National Key Laboratory, Changsha 410073, China)

Abstract: Addressing the vulnerability of Global Navigation Satellite Systems (GNSS) to spoofing attacks, a Support Vector Machine (SVM) detection algorithm based on correlator-domain information is proposed. Limitations of conventional methods, such as reliance on a priori information, susceptibility to multipath-induced false alarms, and subjective feature selection, are noted. Utilizing correlator-domain information, the proposed SVM analyzes the signal tracking process. Key features are extracted, including the in-phase (I) and quadrature (Q) branch outputs of the correlator, and combined features derived from early, prompt, and late codes. Feature correlation and mutual information analysis are employed to optimize feature combinations, thereby fully exploiting the information within the correlator domain. Experimental results demonstrate that with 6 features, the proposed algorithm achieves a correct detection rate of 95.61% under combined spoofing and multipath scenarios, representing a 12% improvement over traditional SVM. All performance metrics are shown to be significantly superior to those of comparative algorithms. Regarding generalization capability, the correlator-domain SVM achieves accuracy, precision, and recall rates exceeding 90% for untrained data. Further validation using the Texas Spoofing Test Battery (TEXBAT) confirms detection accuracy greater than 98%, both when trained on Scenario 2 and tested on Scenario 3 via transfer learning. This method effectively enhances the accuracy and scenario adaptability of GNSS spoofing detection, providing a novel approach for robust detection in complex electromagnetic environments.

收稿日期：2024-12-27； 修回日期：2025-01-17
基金项目：国家自然科学基金(U20A20193)

Key words: Induced spoofing; Multipath interference; Correlation domain support vector machine (CD-SVM); Generalization ability

0 引 言

卫星导航技术已在全球范围内广泛应用,无论是民用设备还是军用设备,都依赖这一技术实现精准定位和导航。然而,随着技术的普及,针对卫星导航系统的欺骗攻击日益增多,其已成为亟需解决的重要问题[1-2]。在民用应急服务和关键军事行动中,确保导航信号的真实性和准确性对设备的有效性和操作的安全性至关重要。因此,研究和开发有效的卫星导航欺骗检测技术以应对不断演变的安全威胁非常必要,其可以确保导航系统的安全性和可靠性。

传统的卫星导航欺骗技术可以分为简单、中级和复杂3种类型[3]。简单欺骗通过发送类似真实信号的虚假信号来迷惑接收机;复杂欺骗则完全模拟真实导航信号,技术更为精湛。其中,中级欺骗中的诱导式欺骗因具备欺骗效果出色和易于实现的特点,成为研究热点[4-6]。该技术通过逐步调整信号的功率和码速率,使接收机偏离真实信号,最终锁定到欺骗信号上[7]。强大的隐蔽性和较高的成功率使其相比于复杂方法更具可操作性,同时也优于简单方法。因此,诱导式欺骗在军事和民用领域得到了广泛的应用[8-10]。其隐蔽性和有效性使其成为导航欺骗研究中的一个重要领域,并逐渐成为一种主流欺骗技术;其也因此成为欺骗检测研究的重要目标领域。

诱导式欺骗攻击主要通过缓慢偏移环路跟踪点来操控接收机,从而实现对环路的控制。为了应对这种攻击,许多学者在相关域构建了各种检测量来进行欺骗检测[11]。文献[12-14]提出了经典的Delta,Ratio和ELP等检测量,能够在诱导式欺骗进入接收机环路以后造成相关峰畸变,从而实现欺骗检测。文献[15-17]提出并使用的新型信号质量监测(Signal quality monitoring,SQM)检测量,在公开数据集上的欺骗检测性能相较于传统的Delta,Ratio和ELP检测量得到了大幅度提升。然而,因为诱导式欺骗对环路相关峰的畸变影响与多径干扰极为相似,这些传统检测量在多径环境下容易将多径干扰检测为欺骗,从而产生大量虚警[11,18]。

传统的相关域信号质量监测技术在欺骗检测中处理多径干扰时,仍面临高虚警率的问题。Tohidi等[19]通过引入小波变换,从相关峰中提取特征,并结合模糊分类器区分多径与欺骗信号。Zhu等[20]提出使用支持向量机(Support vector machine,SVM)算法结合多域信息直接进行欺骗检测,在德州欺骗测试集(Texas spoofing test battery,TEXBAT)等公开数据集上欺骗检测准确率、受试者工作特征曲线下的面积值(Area under curve,AUC)值指标相较于Delta算法分别提升30.82%和0.24,表现出优于传统SQM方法的性能。在此基础上,Chen等[21]评估了输入特征数量对SVM算法的影响,并增加了在橡树岭欺骗测试集(Oak Ridge spoofing and interference test battery, OAKBAT)上的测试。评估其在所有数据场景下的欺骗检测性能后可知,其在场景7下的性能最佳,欺骗检测准确率达到97.02%,AUC为0.99。

然而,已有研究的特征选择均为人工挑选,缺乏对特征贡献度和相关性的系统分析,且对模型的泛化能力评估不足。通过深入挖掘相关域的信息,分析特征相关性和特征贡献度,可完善特征选择过程。其次,欺骗数据集包含同步和异步两种欺骗,并且包含相同场景下的多径干扰数据。利用多径干扰在短时间内对相关峰的持续影响与诱导式欺骗对相关峰的动态影响这一时序差异,本文设计的欺骗检测算法能够抑制多径干扰在诱导式欺骗检测过程中造成的虚警。具体而言,我们使用SVM算法,结合传统ELP三点相关器输出的多个特征,通过特征相关性分析和互信息分析来自动选取最佳输入特征组合,从而学习相关峰畸变的时序规律以及多个特征之间的联合关系。此外,还在陌生数据上对训练得到的SVM模型进行了泛化能力评估,以验证其在不同数据集上的适用性和鲁棒性。

1 信号模型及现有检测方法

1.1 信号模型

在现代导航系统中,全球定位系统(Global positioning system, GPS)卫星通过L1和L2两个频段进行数据传输,其中L1频段是广泛应用于民用领域的信号。本研究聚焦于L1频段信号,并对此频段的信号模型进行深入探讨。接收机正常接收到的导航信

号可以表示为

$$S_{\mathrm{A}}(t)=\sum_{k=1}^{K_{\mathrm{A}}}\sqrt{p_{\mathrm{A}}^{k}(t)}\,D_{\mathrm{A}}^{k}(t-t_{\mathrm{A}}^{k})C_{\mathrm{r}}^{k}(t-\tau_{\mathrm{A}}^{k})\cdot\cos\left(2\pi\left(f_0+f_{\mathrm{d,A}}^{k}\right)t+\varphi_{\mathrm{A}}^{k}\right)\tag{1}$$

式中：$S_{\mathrm{A}}(t)$表示真实导航信号；K_{A}表示可见星数量；$p_{\mathrm{A}}^{k}(t)$表示第k路卫星信号的能量；$D_{\mathrm{A}}^{k}(t)$表示第k路卫星信号的数据码；$C_{\mathrm{r}}^{k}(t)$表示第k路卫星信号的C/A码；φ_{A}^{k}表示载波的起始相位偏差；f_0和$f_{\mathrm{d,A}}^{k}$分别表示载波的中心频率和第k路卫星信号的多普勒偏移量。

欺骗信号的结构与真实卫星信号相似，然而各参数却有所不同。因此，欺骗信号可以用以下形式表示：

$$S_{\mathrm{S}}(t)=\sum_{k=1}^{K_{\mathrm{S}}}\sqrt{p_{\mathrm{S}}^{k}(t)}\,D_{\mathrm{S}}^{k}(t-t_{\mathrm{S}}^{k})C_{\mathrm{r}}^{k}(t-\tau_{\mathrm{S}}^{k})\cdot\cos\left(2\pi\left(f_0+f_{\mathrm{d,S}}^{k}\right)t+\varphi_{\mathrm{S}}^{k}\right)\tag{2}$$

式中：$S_{\mathrm{S}}(t)$表示欺骗信号；K_{S}表示该欺骗信号中的卫星数量；$p_{\mathrm{S}}^{k}(t)$表示第k路卫星欺骗信号的能量；τ_{S}^{k}表示第k路卫星欺骗信号的伪码偏移量；$f_{\mathrm{d,S}}^{k}$表示第k路卫星欺骗信号的多普勒偏移量。

多径干扰信号是指经反射后的导航信号，其在结构上与欺骗信号高度相似，这种特性导致其对环路的影响与诱导式欺骗非常相似。其表达式如下：

$$S_{\mathrm{M}}(t)=\sum_{k=1}^{N}\eta_i\sqrt{p_{\mathrm{A}}^{i}}\,D_{\mathrm{M}}^{i}\left(t-\tau_i(t)\right)C_{\mathrm{M}}^{i}\left(t-\tau_i(t)\right)\cdot\cos\left(2\pi\left(f_0+f_{\mathrm{d,M}}^{i}\right)t+\varphi_i(t)\right)\tag{3}$$

式中：N表示多径信号的总数量；η_i表示第i路多径信号的功率衰减；p_{A}^{i}表示第i路导航信号的真实信号能量；$\tau_i(t)$和$\varphi_i(t)$分别表示第i路导航信号相对真实信号的时延和相位。在本文的后续分析中，多径干扰方面，仅针对单星导航信号的多径效应进行研究。

在接收信号处理中，将剥离中频信号后剩余的载波与本地复制码进行相关运算，并通过T ms的相干积分，得到各路相关器的相干积分值I_{E}, I_{P}, I_{L}, Q_{E}, Q_{P}, Q_{L}。其中，即时相关器的相干积分值表达式为

$$I_{\mathrm{P}}=AD(n)R(\tau_{\mathrm{p}})\mathrm{sinc}(f_{\mathrm{e}}T_{\mathrm{coh}})\cos\phi_{\mathrm{e}}+\eta_{\mathrm{I}}\tag{4}$$

$$Q_{\mathrm{P}}=AD(n)R(\tau_{\mathrm{p}})\mathrm{sinc}(f_{\mathrm{e}}T_{\mathrm{coh}})\cos\phi_{\mathrm{e}}+\eta_{\mathrm{Q}}\tag{5}$$

式中：τ_{p}表示接收伪码与本地即时码之间的码相位差异；$R(\cdot)$表示伪码的自相关函数；$\mathrm{sin}\,c(x)=\dfrac{\sin(\pi x)}{\pi x}$；$f_{\mathrm{e}}$和$\phi_{\mathrm{e}}$分别为接收信号与本地即时码之间的频率和载波相位差异；T_{coh}表示相干积分时间间隔；A表示幅值；D表示数据电平，其值为±1。

以GPS L1频段信号的C/A码为例，有：

$$R(\tau_{\mathrm{p}})=\begin{cases}1-\left|\tau_{\mathrm{p}}\right|, & \left|\tau_{\mathrm{p}}\right|\leqslant 1\\ 0, & \left|\tau_{\mathrm{p}}\right|>1\end{cases}\tag{6}$$

式中：τ_{p}数值以码片数为单位。

1.2　现有检测方法

现有的诱导式欺骗检测方法主要分为两大类：第一大类是基于信号质量监测（SQM）的欺骗检测方法，第二大类是基于机器学习的欺骗检测算法。传统的SQM技术通过检测跟踪环路的相关峰形变执行欺骗检测。一般情况下，监测复相关域中失真的相关峰，是通过计算复相关函数多个样本的度量指标来完成的。

常用的经典指标包括：

Delta：

$$\Delta_{\tau}(t)=\frac{I_{\mathrm{E},\tau}(t)-I_{\mathrm{L},\tau}(t)}{2I_{\mathrm{P}}(t)}\tag{7}$$

Ratio：

$$T_{\tau}(t)=\frac{I_{\mathrm{E},\tau}(t)+I_{\mathrm{L},\tau}(t)}{2I_{\mathrm{P}}(t)}\tag{8}$$

ELP：

$$P_{\tau}(t)=\tan^{-1}\left(\frac{Q_{\mathrm{L},\tau}(t)}{I_{\mathrm{L},\tau}(t)}-\frac{Q_{\mathrm{E},\tau}(t)}{I_{\mathrm{E},\tau}(t)}\right)\tag{9}$$

其中，τ表示即时码与早迟码之间的相关器间距，$\tan^{-1}(\cdot)$表示反正切函数。

传统的相关域诱导式欺骗检测方法借鉴了多径检测的思路，但由于多径干扰和诱导式欺骗均会导致相关峰的畸变，其在实际检测过程中面临着严峻的挑战。首先，多径干扰一旦进入环路，其对检测量的影响与诱导式欺骗高度相似，这极易引发大量误报的情况。其次，传统的单指标或复合指标检测方法往往需要依赖大量的先验样本进行检测量统计；然而在真实的对抗环境中，获取充足的先验样本数据往往难以实现。现有的机器学习诱导式欺骗检测算法通过整合多域信息，在欺骗检测概率上取得了显著提升。然而，这些算法在特征选择上仍主要依赖人工挑选，未能充分挖掘相关域信息的潜力，且现有欺骗场景设置不够全面，大多局限于同步式欺骗场景。

为应对上述挑战，本文提出了一种基于联合相关域多特征的支持向量机（Correlation domain support vector machine，CD-SVM）分类方法。该方法通过特

征相关性分析和互信息计算自动甄选目标数量的特征组合，并通过对同步、异步及多径干扰数据集进行训练，深入学习多个特征间的联合关系及其时序演变。实验结果表明，此方法在欺骗检测效果方面表现出色，并能有效区分多径干扰与欺骗信号。此外，该模型还展现出一定的迁移能力，无需在各场景下重新训练，从而显著提升了其实用性和广泛适应性。

2 基于CD-SVM算法的诱导式欺骗与多径检测模型

在全球导航卫星系统（Global navigation satellite system，GNSS）欺骗与多径信号检测任务中，多元假设检验问题可被视为对多径干扰、欺骗信号及真实信号进行多元分类的挑战。SVM作为一种广泛应用于信号分类问题的监督式机器学习模型，凭借其强大的分类能力在这一领域得到了广泛应用[22]。基于此，将不同信号场景中的多种参数视为特征，并选择SVM作为算法模型，以期在复杂的信号环境中实现精准、可靠的分类识别。

2.1 CD-SVM欺骗检测处理流程与算法框架

CD-SVM算法的处理流程如图1所示，主要包括以下几个步骤：软件接收机信号处理，特征数据预处理以及SVM模型的训练测试与评估。

1）软件接收机处理：在GNSS欺骗和多径干扰场景下，读取信号源生成的信号，配置软件接收机各阶段的参数；运行信号捕获，信号跟踪和位置信息（position）、速度信息（velocity）和时间信息（time）解算功能；输出原始数据，包括ELP相关器的同相（In-phase，I）、正交（Quadrature，Q）支路输出，Ratio，Delta，ELP等检测指标。

2）多参数特征提取：分析欺骗和多径干扰信号对接收机相关域模块的影响，从原始输出信息中提取特征参数。通过对相关域信息的深入挖掘，构建联合多参数信息特征的模型输入，从而实现对相关域信息的完整体现。比如，可以利用SQM特征（DeltaAvg&Diff、Ratio-Avg&Diff、ELP-Avg&Diff）和原始I路（IP、IE&IL）、Q路特征（QP、QE&QL）组合作为SVM算法的输入特征向量。

3）数据预处理、SVM模型训练与测试：首先，通过特征相关性分析、数据标准化处理、特征与标签互信息计算对特征数据进行预处理。然后，随机选择部分数据作为训练集，其余数据用作测试集，利用训练集求解SVM模型参数，构建能够有效检测GNSS欺骗和多径干扰的分类器。随后，利用测试数据集对分类器进行分类和预测，评估模型的检测性能。最后，通过未训练样本测试模型的泛化能力，以确保其在实际应用中的可靠性和有效性。

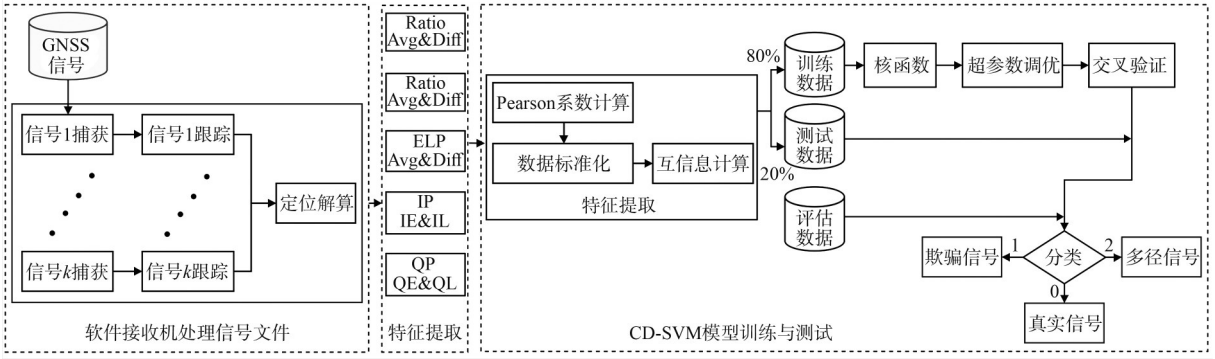

图1 基于相关域特征的SVM分类算法处理流程

Fig. 1 Workflow of SVM classification algorithm based on correlated domain features

2.2 相关峰测量与特征分析

模型输入特征为相关域ELP相关器I，Q支路输出的移动均值，Ratio，Delta和ELP的移动均值和移动差值12个特征，具体特征见表1。

通过对原始12个特征进行相关性分析以及特征对标签的贡献度来确定最终模型选用的输入特征。在特征贡献度排序的基础上，考虑不同特征之间的相关性以及其所含有的原始信息量作为不同特征数量下特征组合的选取原则。

首先采用Pearson系数对表1中原始的12个特征进行相关性分析，公式如下：

$$r_{xy}=\frac{\sum_{i=1}^{n}\left(x_i-\bar{x}\right)\left(y_i-\bar{y}\right)}{\sqrt{\sum_{i=1}^{n}\left(x_i-\bar{x}\right)^2\sum_{i=1}^{n}\left(y_i-\bar{y}\right)^2}} \tag{10}$$

表 1　原始特征参数

Table 1　Original feature parameters

序号	名称	缩写
1	Delta 检测量的移动平均（average，Avg）和移动差分（difference，Diff）	Delta-Avg Delta-Diff
2	Ratio 检测量的移动平均和移动差分	Ratio-Avg Ratio-Diff
3	ELP 检测量的移动平均和移动差分	ELP-Avg ELP-Diff
4	I 路相关器输出的移动平均	IE-Avg IL-Avg IP-Avg
5	Q 路相关器输出的移动平均	QE-Avg QL-Avg QP-Avg

式中：r_{xy} 表示 Pearson 相关系数，用于衡量变量 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 之间的线性相关性，即分析表 1 中 12 个特征之间的相关性。x_i 和 y_i 表示变量 $\boldsymbol{x}$ 和 $\boldsymbol{y}$ 的第 i 个观测值。$\bar{y}$ 变量 $\boldsymbol{y}$ 的平均值，即 $\bar{y}=\frac{1}{n}\sum_{i=1}^{n}y_i$。$\sum_{i=1}^{n}$ 表示从第 1 个观测值到第 n 个观测值的累加和。

在特征选择中，互信息用于衡量每个特征与目标变量（类别标签）之间的相关性。较高的互信息值表示特征与目标变量之间更强的关联性，因此这些特征更有助于分类任务。

计算公式如下：

$$I(\boldsymbol{X};\ \boldsymbol{Y})=\sum_{y\in Y}\sum_{x\in X}p(\boldsymbol{x},\boldsymbol{y})\lg\left(\frac{p(\boldsymbol{x},\boldsymbol{y})}{p(\boldsymbol{x})p(\boldsymbol{y})}\right)\tag{11}$$

式中：$\boldsymbol{X}$ 表示特征变量，即表 1 中的 12 个特征；$\boldsymbol{Y}$ 表示标签，即是否被欺骗以及是否含多径的分类结果；$p(\boldsymbol{x},\boldsymbol{y})$ 表示联合概率分布；$p(\boldsymbol{y})$ 表示 $\boldsymbol{Y}$ 的边缘概率分布。

2.3　SVM 分类处理

SVM 是一种基于统计学习理论的监督学习方法，广泛应用于分类和回归任务。SVM 的核心思想是通过寻找一个超平面，将不同类别的样本在高维特征空间中进行最大化间隔的划分。本节将详细介绍 SVM 的基本原理、输入数据和输出特征，以及核函数的作用。

考虑一个包含 m 个训练数据和 n 个测试数据的样本集合：

$$D=\left\{\left(\boldsymbol{x}_1,y_1\right),\cdots,\left(\boldsymbol{x}_i,y_i\right),\cdots,\left(\boldsymbol{x}_{m+n},y_{m+n}\right)\right\}\tag{12}$$

式中：$\boldsymbol{x}_i$ 表示混合信号经接收机处理后第 i 时刻相关域输出的 k 维特征向量，其中 $\boldsymbol{x}_i=\left[f_1(i),f_2(i),\cdots,f_k(i)\right]^{\mathrm{T}}$；$f_k(i)$ 在本实验中代表 12 个特征中被挑选的某一特征；$y_i\in\{0,\ 1,\ 2\}$ 代表输出结果，在本实验中代表检测的信号中是否含有欺骗或者多径信号。

具体来说，特征向量 $\boldsymbol{x}_i$ 是由接收到的混合信号经处理后得到的输入，输出 y_i 标记了当前时刻信号的类别。

SVM 的目标是找到一个最优的分离超平面 $\boldsymbol{w}^{\mathrm{T}}\boldsymbol{x}+b=0$，该超平面能够正确划分训练数据集并最大化几何间隔。如图 2 所示，其中绿色和橙色的点分别表示正类和负类，而红色边框的点表示支持向量。支持向量是距离超平面最近的样本点，决定了超平面的位置和方向：

$$\begin{cases}\min\limits_{\boldsymbol{w},b}\dfrac{1}{2}\|\boldsymbol{w}\|^2\\ \text{s. t. }\ y_i(\boldsymbol{w}^{\mathrm{T}}\boldsymbol{x}+b)\geqslant 1,\ \ i=1,2,\cdots,m\end{cases}\tag{13}$$

式中：$\boldsymbol{w}=\left[w_1,w_2,\cdots,w_d\right]^{\mathrm{T}}$ 是超平面的法向量，表示超平面的平均向量；b 是偏移量，表示超平面与原点之间的距离。

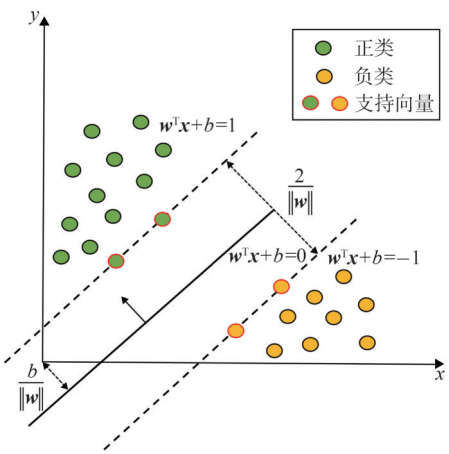

图 2　支持向量机工作原理

Fig. 2　Working principle of SVM

在实际应用中，特别是处理复杂的 GNSS 欺骗信号分类任务时，输入特征空间中的数据可能是非线性可分的。为了克服这一问题，SVM 通过核函数将原始特征空间映射到更高维的空间，在高维空间中寻找线性超平面。

核函数可以表示为

$$\begin{aligned}k(\boldsymbol{x}_i,\boldsymbol{x}_j)&=\left\langle\boldsymbol{\phi}\left(\boldsymbol{x}_i\right),\boldsymbol{\phi}\left(\boldsymbol{x}_j\right)\right\rangle\\&=\boldsymbol{\phi}^{\mathrm{T}}\left(\boldsymbol{x}_i\right)\cdot\boldsymbol{\phi}\left(\boldsymbol{x}_j\right)\end{aligned}\tag{14}$$

式中：$\boldsymbol{\phi}(\boldsymbol{x}_i)$ 表示从原始特征空间 x_i 到高维特征空间

的映射函数;〈·〉表示内积运算。

常见的核函数有线性核、多项式核和高斯核。这3种核函数的表达式如表2所示,后续实验将对传统的多个核函数进行对比分析。

表2 SVM核函数

Table 2 SVM kernel functions

核函数名称	表达式
线性核(linear)	$k(\boldsymbol{x}_i,\boldsymbol{x}_j)=\boldsymbol{x}_i^{\mathrm{T}}\cdot\boldsymbol{x}_j$
多项式核(poly)	$k(\boldsymbol{x}_i,\boldsymbol{x}_j)=(\boldsymbol{x}_i^{\mathrm{T}}\cdot\boldsymbol{x}_j)^d$
高斯核(rbf)	$k(\boldsymbol{x}_i,\boldsymbol{x}_j)=\mathrm{e}^{-\frac{\left\|\boldsymbol{x}_i-\boldsymbol{x}_j\right\|^2}{2\sigma^2}}$
sigmoid核(sigmoid)	$k(\boldsymbol{x}_i,\boldsymbol{x}_j)=\tanh\left(\alpha\left(\boldsymbol{x}_i\cdot\boldsymbol{x}_j\right)+c\right)$

3 实验仿真与性能分析

3.1 信号源实验平台

本实验利用课题组自主开发的图形处理器(Graphics processing unit,GPU)信号源,实现了导航信号、欺骗信号和多径信号的生成。通过上位机对信号参数进行精确配置,系统能够完整地生成所需的信号数据文件。该实验平台旨在创建一个高度可控的环境,以模拟真实世界中可能遇到的各种导航信号干扰情况。利用开源软件接收机对信号进行处理[6],深入分析信号特性,并验证算法在处理复杂信号时的有效性,实验环境如图3所示。

尽管TEXBAT和OAKBAT数据集在导航欺骗信号处理领域具有显著价值,但在实验训练数据的选择上并未依赖这些公共数据集。根据是否已知目标信号的真实码相位,诱导式欺骗分为同步诱导式欺骗和异步诱导式欺骗。现有的公开欺骗数据集为同步诱导式欺骗场景,而本研究自建的欺骗数据集中,既包含同步诱导式欺骗也包含异步诱导式欺骗。

图3 实验环境

Fig. 3 Experimental environment

此外,仿真的数据集旨在提供一个更为全面的测试平台,确保算法在多种欺骗场景下均能表现出色。由于不依赖现有公开数据集,实验保持了更高的独立性和创新性,使得新的信号处理技术和算法可以不受限制地探索。

3.2 实验数据场景

本实验用户真实动态场景包括静态位置和动态运动两种。静态用户位置为地心地固坐标系(Earth-centered Earth-fixed,ECEF)下的(−2 836 275 m,3 333 782 m,4 623 813 m),动态用户从(−2 836 275 m,3 333 782 m,4 623 813 m)位置开始沿y轴以10 m/s的速度进行匀速直线运动。对于静态用户,设置−0.75 chips和−0.25 chips的起始伪码相位偏差,然后以0.1 chips/s和0.5 chips/s的码相位拉偏速度进行诱导式欺骗;对于动态用户,设置−10 chips的伪码相位偏移,然后以0.5 chips/s的码相位拉偏速度逐渐靠近真实目标,最后实施拉偏。多径干扰则通过在原始信号上对同一信号增加码相位时延和多普勒效应来模拟。

实验数据集场景参数配置见表3。训练集包括Spoofing1、Spoofing2、Multipath1和Multipath2,模型评估集为Spoofing3和Multipath3。其中Spoofing1是对动态用户实施欺骗,由于起始码相位大于相关器间距(1 chips),所以为异步诱导式欺骗数据集;Spoofing2和Spoofing3是对静态用户实施欺骗,并且起始码相位小于相关器间距,所以为同步诱导式欺骗数据集。Multipath1、Multipath2和Multipath3都是对静态用户实施多径干扰。

表3 实验场景

Table 3 Configuration of experimental scenarios

名称	数据说明	信号时长	欺骗/多径干扰切入时刻	真实信号载噪比	功率增益	起始伪码相位时延	多普勒	伪码相位拉偏速度
Spoofing1	训练测试数据集	100 s	30 s	45 dB·Hz	+3 dB	−10.0 chips	0 Hz	0.5 chips/s
Spoofing2	训练测试数据集	100 s	30 s	45 dB·Hz	+3 dB	−0.25 chips	0 Hz	0.1 chips/s, 0.5 chips/s
Spoofing3	评估数据集	100 s	30 s	45 dB·Hz	+3 dB	−0.75 chips	50 Hz	0.1 chips/s
Multipath1	训练测试数据集	100 s	30 s	45 dB·Hz	−1 ~ −5 dB	−0.5 chips	0 Hz	0 chips/s
Multipath2	训练测试数据集	100 s	30 s	45 dB·Hz	−1 ~ −5 dB	−1.0 chips	0 Hz	0 chips/s
Multipath3	评估数据集	100 s	30 s	45 dB·Hz	−1 ~ −5 dB	−1.25 chips	0 Hz	0 chips/s

对于本实验使用的场景数据集，表 3 详细列出了混合信号的持续时间、导航信号的载噪比、欺骗信号的切入时间、功率增益、起始伪码相位时延、伪码拉偏速度和多普勒频偏等参数。而对于多径干扰数据集，则提供了多径干扰的功率衰减、切入时刻、时延和多普勒频偏等信息。

训练和测试数据集中均包含多径干扰信号与导航信号的混合信号，以及欺骗信号与导航信号的混合信号。评估数据集与训练数据集存在一定的差异，这是为了在后续评估模型的迁移能力时提供参考依据。

3.3　特征处理结果

模型的输入特征包括对相关域 ELP 相关器的 I，Q 支路输出的移动均值，Ratio，Delta 以及 ELP 的移动均值和移动差值等共计 12 个特征。针对同一目标，Spoofing2 欺骗和 Multipath1 多径干扰对这些特征的影响如图 4 和图 5 所示。

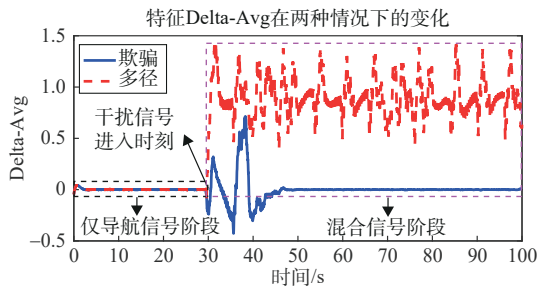

图 4　特征 Delta-Avg 在两种场景下的变化过程

Fig. 4　Variation process of feature Delta-Avg under two scenarios

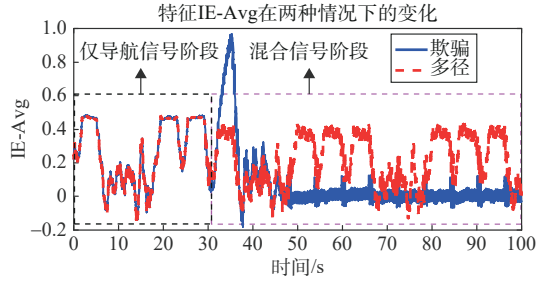

图 5　特征 IE-Avg 在两种场景下的变化过程

Fig. 5　Variation process of feature IE-Avg under two scenarios

图 4 展示了特征 Delta-Avg 在上述两种情况下的变化趋势，而图 5 则揭示了特征 IE-Avg 在两种情况下的变化规律。具体来看，在欺骗与多径干扰侵入前，检测量保持平稳；一旦欺骗或多径干扰介入，检测量会随即发生显著突变。尤其当欺骗介入后，检测量经历一段时间的动态变化后会再次趋于平稳；而多径干扰介入后，检测量则趋于稳定并维持在一个特定数值。

为确定模型最终选用的输入特征，本文首先对原始的 12 个特征进行细致的相关性分析，并通过特征对标签的贡献度评估了其重要性。采用 Pearson 系数对表 1 中列出的原始 12 个特征进行了相关性分析，进一步通过互信息法剖析特征对结果标签的实际贡献，详细分析结果如图 6 所示。从图 6 左侧的相关性分析部分可以直观地看到，Delta 与 Ratio 的移动均值检测量呈现出负相关性，而其差值则显示出正相关性，两者间的关联性尤为突出。然而，结合图 6 右侧的贡献度柱状图进行综合评估，发现尽管 Delta 和 Ratio 之间存在较强的负相关性，但这两个检测量对最终结果的贡献度依然相当高。进一步细察 I，Q 支路输出的特征可以看到，I 路与 Q 路信息之间具有高度正相关关系，而 I 路信息的贡献度明显高于 ELP 检测量及 Q 路检测量，这一结果与 I 路作为有效能量通道、Q 路作为噪声通道的物理学原理高度吻合。

首先，通过计算特征与标签之间的互信息以及特征之间的相关性来进行特征选择。这一过程确定了从 2 个到 6 个特征的最佳组合，并将这些组合如表 4 所示列出。随后，使用这些不同数量的特征组合进行模型的训练和测试。

其中 IP-Avg 特征虽然在贡献度上相较于 Delta-Diff 较低，但是由于 Delta-Diff 是 Delta-Avg 特征的一阶差分量，所以其在特征挑选优先级上低于 IP-Avg 特征。

3.4　CD-SVM 算法与传统 SQM 算法性能分析

3.4.1　传统算法的局限性分析

使用 SQM 技术进行欺骗干扰检测时，需要了解 SQM 指标的统计特征，以获得其概率密度函数，并根据设定的虚警概率确定判决门限。已有的研究显示，在高信噪比条件下，SQM 指标近似服从正态分布[23]。

本实验选用经移动平滑处理后的 Ratio 指标和 Delta 指标对欺骗与多径干扰进行检测[24]。设定虚警概率为 5%，由此得到欺骗检测门限。检测准确率定义为：每 100 ms 计算一次，超过检测门限的样本数与样本总数的比例。

使用传统 SQM 欺骗检测算法分别对表 3 中的第 1 组和第 4 组信号进行精准检测。第 1 组信号为初始伪码相位差距−0.25 chips，并以 0.1 chips/s 的拉

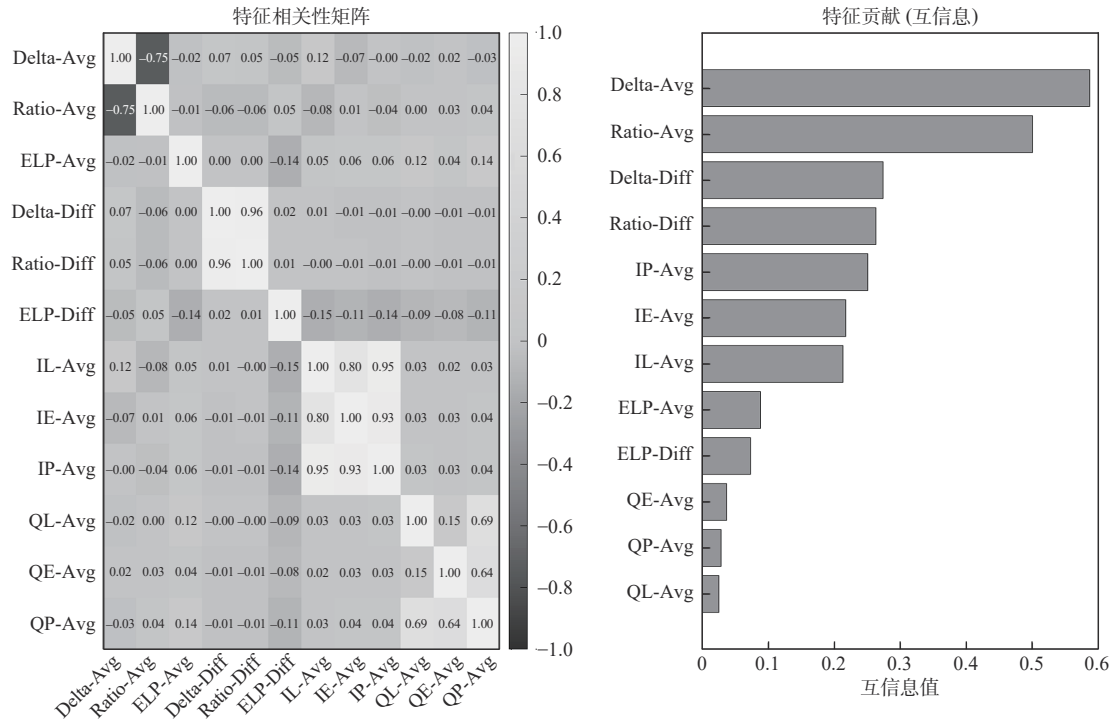

图6 特征相关性和对标签贡献度的分析结果

Fig. 6 Analysis results of feature correlation and contribution to labels

表4 CD-SVM特征选择结果

Table 4 Feature selection results of CD-SVM

组合数量	特征选择
2	Delta-Avg, Ratio-Avg
3	Delta-Avg, Ratio-Avg, IP-Avg
4	Delta-Avg, Ratio-Avg, Delta-Diff, IP-Avg
5	Delta-Avg, Ratio-Avg, Delta-Diff, IL-Avg, IP-Avg
6	Delta-Avg, Ratio-Avg, Delta-Diff, IL-Avg, IE-Avg, IP-Avg

偏速度实施的诱导式欺骗Spoofing1。Spoofing1混合信号的持续时间为100 s,其中前30 s为纯导航信号,第30 s之后的混合信号则由欺骗信号和导航信号共同构成。第2组信号则为伪码时延差距−0.5 chips的多径干扰Multipath1。Multipath1混合信号同样持续100 s,前30 s为纯导航信号,第30 s之后则混合了多径信号和导航信号。

Spoofing1欺骗场景中的Ratio和Delta检测量变化如图7和图8所示。观察这些图表可清晰发现:在欺骗信号尚未介入的纯导航信号阶段,检测量始终保持在检测门限以内;然而,一旦欺骗信号介入,检测量迅速攀升并超越检测门限。随着时间推移,当欺骗信号完全控制了环路后,检测量再次趋于平稳。

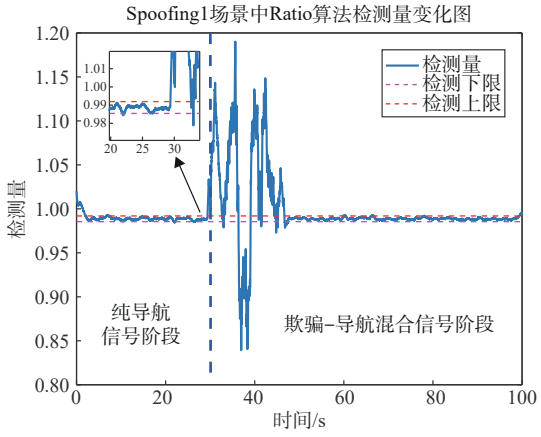

图7 Spoofing1欺骗场景Ratio检测量变化图

Fig. 7 Ratio detection change in Spoofing1 deception scenario

检测结果如图9所示。在大约30 s时,欺骗检测准确率由0%迅速跃升至100%,显示出算法在此阶段成功识别出欺骗信号,这与实际欺骗场景的设定情况完全吻合,证明了算法的优异性能。然而,在50 s左右,欺骗检测准确率却由100%迅速下降至0%,表明算法此时认为信号中已无欺骗,但实际情况却是欺骗信号持续存在,导致算法检测出现错误。出现这一现象的原因在于场景配置中,欺骗信号的介入时间为第30 s,从第30 s至第50 s,欺骗信号与导航信号在码环控制权上展开激烈争夺,导致

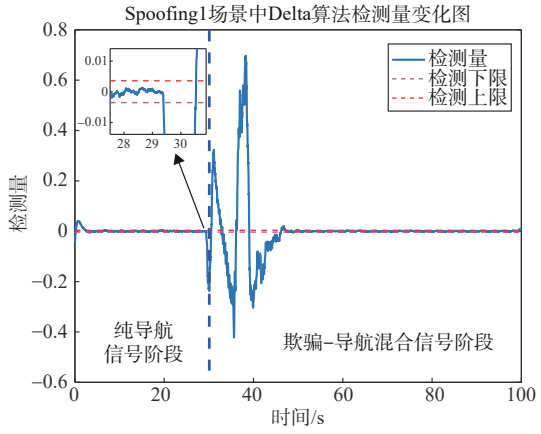

图 8　Spoofing1 欺骗场景 Delta 检测量变化图

Fig. 8　Delta detection change in Spoofing1 deception scenario

相关峰发生畸变。但在第 50 s 之后,欺骗信号已完全控制环路,相关峰的畸变消失,因此算法在 30 s 时检测准确率从 0% 迅速上升至 100%,但在欺骗信号彻底控制环路后,检测准确率却降到了 0%。

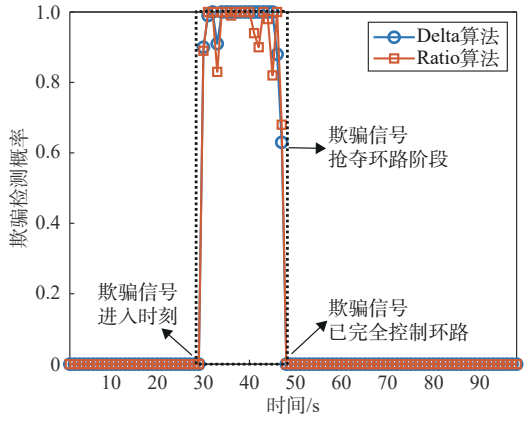

图 9　Spoofing1 传统诱导式欺骗检测结果

Fig. 9　Traditional guided deception detection results for Spoofing1

同理,使用传统 SQM 欺骗检测算法对表 3 中 Multipath1 多径干扰场景进行检测,检测量变化曲线如图 10 和图 11 所示。在多径干扰信号尚未介入的纯导航信号阶段,检测量始终保持在检测门限以内;当多径干扰进入以后,检测量迅速攀升并超越检测门限,并且持续存在。这会导致传统 SQM 欺骗检测算法在多径场景中出现大量虚警。

3.4.2　CD-SVM 检测性能分析与对比

1)不同核函数下 CD-SVM 算法欺骗检测性能分析

使用 Delta-Avg、Ratio-Avg、Delta-Diff、IP-Avg 这 4 个特征对 CD-SVM 算法模型进行训练,使用不同的

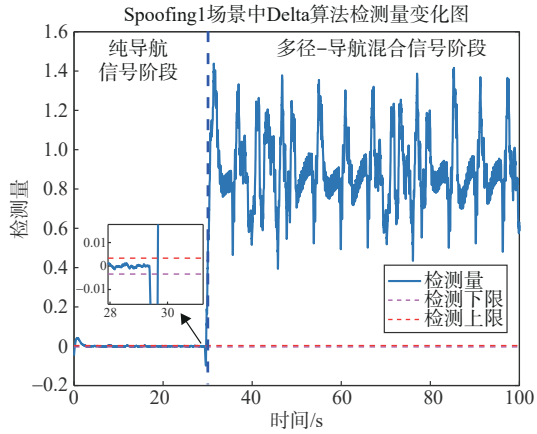

图 10　Multipath1 多径干扰场景 Delta 检测量变化图

Fig. 10　Delta detection change in Multipath1 multipath interference scenario

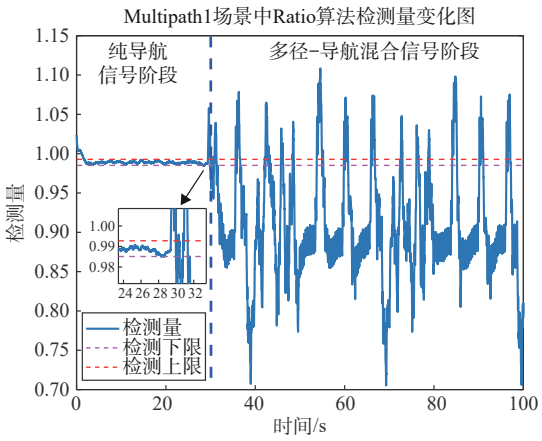

图 11　Multipath1 多径干扰场景 Ratio 检测量变化图

Fig. 11　Ratio detection change in Multipath1 multipath interference scenario

核函数测试模型性能,实验结果如表 5 所示。在 rbf 核函数下,准确率、精确率、召回率和 F1 分数[22]显著优于其他核函数模型的测试结果。

表 5　不同核函数下 CD-SVM 算法检测结果

Table 5　Detection results of CD-SVM algorithm under different kernel functions

核函数	准确率	精确率	召回率	F1 分数
linear	0. 894 2	0. 893 4	0. 894 2	0. 899 5
poly	0. 908 5	0. 908 5	0. 908 5	0. 905 7
rbf	0. 931 5	0. 932 5	0. 931 5	0. 931 0
sigmoid	0. 823 7	0. 811 2	0. 823 7	0. 815 1

2)CD-SVM 算法性能对比分析

在相同数据集下,将 CD-SVM 欺骗检测算法分别与传统 SVM 欺骗检测算法、传统 SQM 欺骗检测算

法进行检测性能的对比。传统SVM算法采用人工随机挑选特征[20-21]，传统SQM算法采用Phelts等[24]提出的移动平均检测量欺骗检测算法。

实验数据集选用了表3中的渐进欺骗拉偏场景（Spoofing1、Spoofing2）和多径场景（Multipath1、Multipath2）作为训练集，总共包含13条信号。每条信号的时长为100 s，以100 ms为一个数据点。在实验过程中，通过软件接收机对信号进行处理，并在跟踪环路输出的相关域特征中提取数据，这些特征的时间单位为ms。因此，每毫秒的信号会对应多个特征值。随后，我们对这些特征值进行了数据预处理和特征工程，最终生成了训练数据集。将数据集中无干扰信号时间段的信号标签置为0，有欺骗干扰时间段的信号标签置为1，有多径干扰时间段的信号标签置为2，随机选择80%的数据集进行训练，剩余20%的数据集用来测试。

对比CD-SVM算法和传统SVM算法的检测性能，通过使用ROC（Receiver operating characteristic curve）曲线和AUC数值来直观展示各算法的分类性能。ROC曲线是一种常用的性能评估工具，能够反映模型在不同阈值下真正率（True positive rate，TPR）和假正率（False positive rate，FPR）之间的关系[25]。模型的ROC曲线越接近左上角，表明模型在保持高TPR的同时，FPR很低，即模型性能越好。AUC是衡量分类模型性能的指标，值越接近1表示模型的分类能力越强。

本文提出的CD-SVM算法在不同特征数量下的ROC曲线如图12。图12中的3个子图分别是SVM算法对于纯净导航信号（Nav-only）、欺骗信号与导航信号混合（Nav+Spoof）和多径干扰和导航信号混合（Nav+Multipath）在不同特征数量下的ROC结果图。通过对ROC曲线分析，发现SVM算法的ROC曲线随着特征数的增加逐渐向左上角移动，特别是在多径干扰的分类任务中，曲线几乎达到最优。这表明SVM在高维特征组合下能够更精准地区分正负样本，且在多径干扰的识别中表现尤为优异。

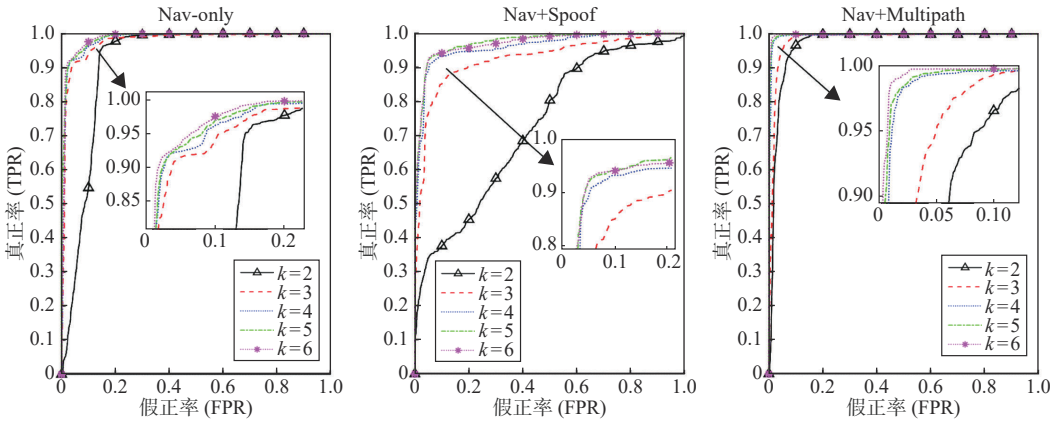

图12 CD-SVM算法在不同特征数量下的ROC曲线

Fig. 12 ROC curves of CD-SVM algorithm with different number of features

因此，在实际应用中，建议优先选择特征数为6的组合，以最大化SVM的分类性能，并对欺骗干扰的分类任务进行进一步的特征优化，以提升识别精度。

结合ROC曲线在表7中对应的AUC结果可知，SVM算法在特征数从2到6时的AUC值显示，随着特征数的增加，其在各分类任务下的AUC值整体呈上升趋势。特别是多径干扰（Nav+Multipath）的AUC值从0.963 9提升至0.997 1，表明SVM在高维特征组合下展现出极强的分类能力。这种现象在Nav-only和Nav+Spoof中同样显著，分别从0.947 9提升至0.993 9和从0.729 1提升至0.978 9。

图13为使用传统SVM欺骗检测算法时的ROC曲线。在已有的12个特征中随机挑选不同数量的特征组合，实验所选特征如表6所示。观察图13实验结果可知，相较于图12中CD-SVM的ROC曲线结果，CD-SVM算法的ROC曲线更加靠近左上角，性能更优。根据实验结果可知，随机挑选特征组合会导致ROC曲线性能不随特征数量增加而增加，增加人工遍历测试的复杂度。

从表7中的数据可以得出，CD-SVM在不同特征数量下的表现普遍优于传统SVM。具体来说，随着特征数量的增加，CD-SVM的准确率（accuracy）从0.881 3提升到0.956 1，显示出其强大的泛化能力。

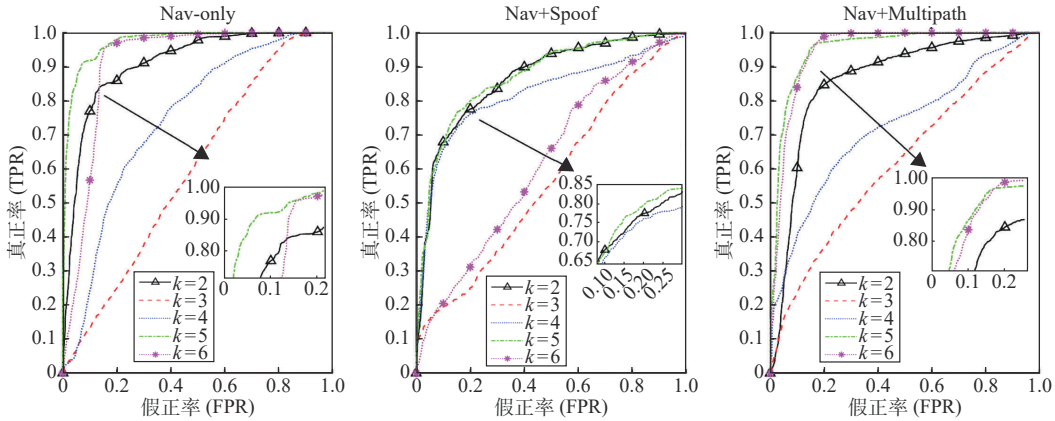

图 13　传统SVM算法在不同特征数量下的ROC曲线

Fig. 13　ROC curves of traditional SVM algorithm with different number of features

表6　SVM特征选择结果

Table 6　Feature selection results of SVM

组合数量	特征选择
2	Delta-Avg, ELP-Diff
3	ELP-Diff, QL-Avg, QP-Avg
4	ELP-Avg, QL-Avg, Delta-Diff, IP-Avg
5	Delta-Diff, Ratio-Avg, ELP-Diff, QL-Avg, IP-Avg
6	ELP-Avg, IE-Avg, Delta-Diff, Ratio-Avg, QE-Avg, QP-Avg

同样,CD-SVM在精度(Precision)、召回率(Recall)和F1分数(F1_score)方面也展现出显著的提升,尤其是在特征数量为6时,各项指标均达到最高值,分别为0.956 1、0.956 1和0.956 1,表明其在分类任务中的表现非常稳定且高效。

进一步观察AUC值,可以发现CD-SVM在不同特征数量下的表现同样优于传统SVM。随着特征数量的增加,CD-SVM的AUC值从2个特征时的0.947 9显著提升到6个特征时的0.997 1,显示出其对特征组合的高度适应性和强大的泛化能力。相比之下,传统SVM的AUC值在不同特征数量下波动较大,最高值为0.973 3(特征数量为4),但最低值仅为0.595 5(特征数量为2),表明其在特征选择和模型性能方面不如CD-SVM稳定和高效。

表7　混合场景下测试结果

Table 7　Test results under mixed scenarios

测试名称	准确率	精确率	召回率	F1分数	Nav-only-Auc	Nav+Spoof-Auc	Nav+Multipath-Auc
CD-SVM-features2	0.881 3	0.869 8	0.881 3	0.847 1	0.947 9	0.729 1	0.963 9
CD-SVM-features3	0.916 2	0.918 3	0.916 2	0.916 7	0.983 8	0.942 0	0.986 6
CD-SVM-features4	0.931 5	0.932 5	0.931 5	0.931 0	0.987 5	0.944 4	0.985 9
CD-SVM-features5	0.946 4	0.946 4	0.946 4	0.946 4	0.993 3	0.971 6	0.995 7
CD-SVM-features6	0.956 1	0.956 1	0.956 1	0.956 1	0.993 9	0.978 9	0.997 1
SVM-features2	0.772 5	0.772 7	0.772 5	0.772 6	0.910 0	0.715 2	0.860 4
SVM-features3	0.488 7	0.579 3	0.488 7	0.437 2	0.595 5	0.567 5	0.618 6
SVM-features4	0.620 3	0.627 2	0.620 3	0.619 1	0.744 8	0.821 4	0.722 3
SVM-features5	0.836 0	0.833 4	0.836 0	0.834 1	0.973 3	0.871 4	0.951 5
SVM-features6	0.787 3	0.729 7	0.787 3	0.723 0	0.908 7	0.620 2	0.946 5

值得注意的是,CD-SVM在特征数量为4和6时,所有指标(包括Nav-only-Auc和Nav+Spoof-Auc)均达到了较高水平,尤其是特征数量为6时,各项指标均表现出色,分别为0.993 9、0.978 9和0.997 1。这进一步验证了CD-SVM在复杂特征组合下的优越性能。虽然传统SVM在某些特征组合下也有较好的表现,但从整体上看,其在处理高维特征数据时的稳定性和准确性仍逊色于CD-SVM。

综上所述,CD-SVM在特征选择和模型训练方面具有明显优势,能够更好地利用不同数量的特征组合进行分类任务,从而显著提高模型的预测性能和鲁棒性。

使用传统信号质量测量(SQM)方法在动态目标异步欺骗数据集Spoofing1场景下进行欺骗检测,采

用传统的Ratio检测量，并将虚警概率设置为1%。实验结果如图14。观察这些结果可以发现，在处理只有欺骗与未欺骗的二元检测问题时，传统检测算法的AUC值为0.875 0；而根据表7的数据，CD-SVM的AUC值为0.978 9。这表明，即使在单一欺骗场景检测任务中，传统SQM算法的性能相较于CD-SVM算法仍然存在显著差距。

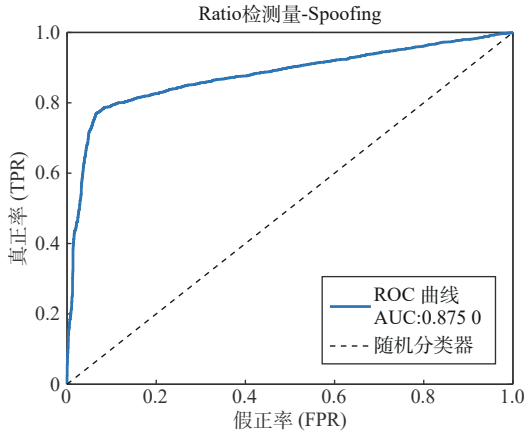

图14 传统SQM算法ROC曲线

Fig. 14 ROC curves of traditional SQM algorithm

这一结果进一步强调了CD-SVM算法在处理复杂欺骗检测任务中的优越性，特别是在考虑AUC值这一关键性能指标时，CD-SVM能够更准确地区分欺骗和未欺骗状态，显示出其高效且稳定的检测能力。

3.5 CD-SVM算法泛化能力评估

为了进一步评估训练得到的SVM模型性能，加载6个特征输入的CD-SVM模型，利用表3实验场景中的评估数据集进行了迁移测试[26]，实验结果如图15所示。左侧纵轴表示人工标注的真实标签，下侧横轴表示模型预测标签，对角线表示对3个检测目标的正确率，即无欺骗(Nav-only)、有欺骗(Nav+Spoof)、多径干扰(Nav+Multipath)3种情况下的检测准确率。

根据图15可知，SVM算法对于评估数据集中的Nav+Multipath的分类准确率达到99.0%，对于Nav-only和Nav+Spoof的分类准确率为93.7%和90.5%。

利用机器学习常见评价指标[27]对分类结果进行评估，其评估结果准确率、精确率、召回率、F1分数分别为0.904 3、0.910 6、0.904 3、0.893 9。

同样使用6个特征输入的CD-SVM模型对TEXBAT数据集进行测试，使用场景2[5]对CD-SVM模型进行训练，将训练好的模型用于对场景3的测试，具体结果如表8所示。

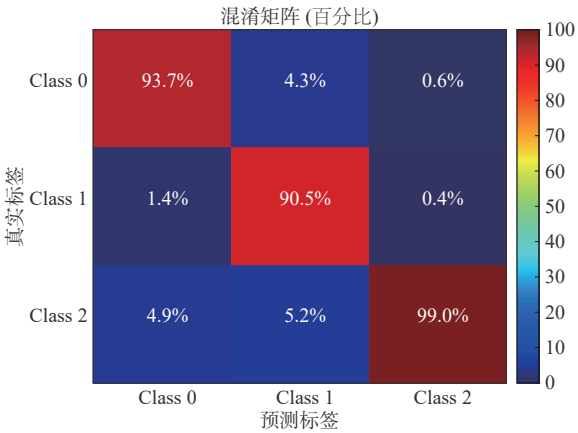

图15 评估数据集下SVM算法检测结果

Fig. 15 Detection results of SVM algorithm on the evaluation dataset

表8 TEXBAT数据集训练与迁移评估结果

Table 8 Training and transfer evaluation results on the TEXBAT dataset

场景	准确率	精确率	召回率	F1分数
场景2(训练)	0.996 57	0.996 59	0.996 57	0.996 57
场景3(迁移)	0.987 45	0.987 47	0.987 45	0.987 45

可以发现在场景2的训练场景中，使用6特征CD-SVM模型进行训练和测试，准确率、精确率等各项检测指标均达到99%以上，在评估测试集场景3上的各项检测指标也均为98%以上。

以上结果证明本实验提出的CD-SVM模型不仅在多径场景下对诱导式欺骗检测性能较好，还具有一定的迁移能力。

4 结 论

本文针对诱导式欺骗的检测难题以及在多径环境下欺骗检测的虚警概率较高问题，通过分析多径和欺骗干扰对接收机环路相关峰的不同时序影响，提出了一种基于SVM算法的相关域多参数联合欺骗检测方法。该方法通过分析信号跟踪过程，提取了ELP相关器的I，Q支路输出、Ratio等特征，并利用特征相关性分析和互信息分析选择输入特征，构建了CD-SVM模型。实验结果表明，CD-SVM算法在分类任务中显著优于传统SVM和SQM算法。

具体来说，随着特征数量的增加，CD-SVM的准确率从88.13%提升至95.61%，特别是在特征数量为6时，相比传统SVM算法的最佳检测结果提升了

12%,展现出其强大的泛化能力和稳定性。在精度、召回率和F1分数方面,CD-SVM也表现出色,尤其在特征数量为6时各项指标均达到最高值。在AUC指标方面,CD-SVM同样优于传统SVM和SQM欺骗检测算法,特别是在三分类任务中表现更为稳定和高效。

综上所述,CD-SVM在本研究涉及的分类任务中展现了最高的准确性和稳定性。此外,模型的泛化能力较好,使用6输入特征CD-SVM模型,其在未训练数据集上的检测准确率、精确率和召回率分别为90.43%,91.06%和90.43%。对于公开数据集TEXBAT场景2进行训练,其各项检测指标达到99%以上,在未训练的场景3中进行迁移测试,各项指标也达98%以上。该方法为优化GNSS欺骗检测提供了有效的手段,未来的工作将聚焦于进一步提升其在复杂电磁环境下的鲁棒性和可靠性。

参 考 文 献

[1] 边少锋, 胡彦逢, 纪兵. GNSS欺骗防护技术国内外研究现状及展望[J]. 中国科学: 信息科学, 2017, 47(3): 275-287.
BIAN Shaofeng, HU Yanfeng, JI Bing. Research status and prospect of GNSS anti-spoofing technology[J]. Scientia Sinica (Informationis), 2017, 47(3): 275-287.

[2] JAFARNIA-JAHROMI A, BROUMANDAN A, NIELSEN J, et al. GPS vulnerability to spoofing threats and a review of antispoofing techniques[J]. International Journal of Navigation and Observation, 2012, 2012(1): 127072.

[3] MENG L X, YANG L, YANG W, et al. A survey of GNSS spoofing and anti-spoofing technology[J]. Remote Sensing, 2022, 14(19): 4826.

[4] ALBRIGHT A, POWERS S, BONIOR J, et al. A tool for furthering GNSS security research: The oak ridge spoofing and interference test battery (OAKBAT)[C]. The 33rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS+2020), Virtual Event, September 21-25, 2020.

[5] HUMPHREYS T, BHATTI J, SHEPARD D, et al. The Texas spoofing test battery: Toward a standard for evaluating GPS signal authentication techniques[C]. The 25th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2012), Nashville, USA, September 17-21, 2012.

[6] ISLAM S, BHUIYAN M Z H, LIAQUAT M, et al. An open GNSS spoofing data repository: Characterization and impact analysis with FGI-GSRx open-source software-defined receiver [J]. GPS Solutions, 2024, 28(4): 176.

[7] HUMPHREYS T E, LEDVINA B M, PSIAKI M L, et al. Assessing the spoofing threat: Development of a portable GPS civilian spoofer[C]. The 21st International Technical Meeting of the Satellite Division of the Institute of Navigation, Savannah, USA, September 16-19, 2008.

[8] BHATTI J, HUMPHREYS T E. Hostile control of ships via false GPS signals: Demonstration and detection[J]. Navigation, 2017, 64(1): 51-66.

[9] GAO Y J, LI G Y. Three time spoofing algorithms for GNSS timing receivers and performance evaluation[J]. GPS Solutions, 2022, 26(3): 87.

[10] BORHANI-DARIAN P, LI H Q, WU P, et al. Detecting GNSS spoofing using deep learning[J]. EURASIP Journal on Advances in Signal Processing, 2024, 2024(1): 14.

[11] WESSON K D, SHEPARD D P, BHATTI J A, et al. An evaluation of the vestigial signal defense for civil GPS anti-spoofing[C]. The 24th International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2011), Portland, USA, September 20-23, 2011.

[12] MUBARAK O M, DEMPSTER A G. Performance comparison of ELP and DELP for multipath detection[C]. The 22nd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2009), Savannah, USA, September 22-25, 2009.

[13] Phelts R E. Multicorrelator techniques for robust mitigation of threats to GPS signal quality[D]. Stanford: Stanford University, 2001.

[14] MUBARAK O M, DEMPSTER A G. Analysis of early late phase in single-and dual-frequency GPS receivers for multipath detection [J]. GPS Solutions, 2010, 14(4): 381-388.

[15] WANG Y W, KOU Y H, ZHAO Y, et al. Detection of synchronous spoofing on a GNSS receiver using weighed double ratio metrics[J]. GPS Solutions, 2022, 26(3): 91.

[16] 王文益, 侯迎龙, 史文浩. 基于SQM相关性的GNSS诱导式欺骗检测[J]. 信号处理, 2024, 40(9): 1748-1760.
WANG Wenyi, HOU Yinglong, SHI Wenhao. GNSS-induced spoofing detection based on SQM correlation[J]. Journal of Signal Processing, 2024, 40(9): 1748-1760.

[17] ZHOU W L, LV Z W, WU W B, et al. Anti-spoofing technique based on vector tracking loop[J]. IEEE Transactions on Instrumentation and Measurement, 2023, 72: 8504516.

[18] WESSON K D, GROSS J N, HUMPHREYS T E, et al. GNSS signal authentication via power and distortion monitoring[J]. IEEE Transactions on Aerospace and Electronic Systems, 2018, 54(2): 739-754.

[19] TOHIDI S, MOSAVI M R. GNSS spoofing detection using a fuzzy classifier based on time-frequency analysis of the autocorrelation function[J]. GPS Solutions, 2024, 28(3): 146.

[20] ZHU X F, HUA T, YANG F, et al. Global positioning system spoofing detection based on Support Vector Machines[J]. IET Radar, Sonar & Navigation, 2022, 16(2): 224-237.

[21] CHEN Z K, LI J Z, LI J, et al. GNSS multiparameter spoofing detection method based on support vector machine[J]. IEEE

Sensors Journal, 2022, 22(18): 17864-17874.

[22] DE OLIVEIRA NOGUEIRA T, PALACIO G B A, BRAGA F D, et al. Imbalance classification in a scaled-down wind turbine using radial basis function kernel and support vector machines [J]. Energy, 2022, 238: 122064.

[23] PIRSIAVASH A, BROUMANDAN A, LACHAPELLE G. Characterization of signal quality monitoring techniques for multipath detection in GNSS applications[J]. Sensors, 2017, 17(7): 1579.

[24] SUN C, CHEONG J W, DEMPSTER A G, et al. Moving variance-based signal quality monitoring method for spoofing detection [J]. GPS Solutions, 2018, 22(3): 83.

[25] 李欣怡, 陈昭岳, 徐明, 等. 基于机器学习的卫星轨道预测混合模型研究[J]. 宇航学报, 2024, 45(11): 1766-1774.
LI Xinyi, CHEN Zhaoyue, XU Ming, et al. Research on hybrid model of satellite orbit prediction based on machine learning[J]. Journal of Astronautics, 2024, 45(11): 1766-1774.

[26] DOUGLASS M J J. Book review: Hands-on machine learning with scikit-learn, keras, and tensorflow, 2nd edition by aurélien géron[J]. Physical and Engineering Sciences in Medicine, 2020, 43(3): 1135-1136.

[27] POWERS D M W. Evaluation: From precision, recall and F-measure to ROC, informedness, markedness and correlation[EB/OL]. (2020-10-11)[2024-12-27]. https://arxiv.org/abs/2010.16061.

作者简介:

刘文祥(1981-),男,博士,优聘研究员,主要从事北斗系统建设与军事应用等方面的研究。

通信地址:国防科技大学电子科学学院(410073)

电话:13807485196

E-mail: liuwenxiang08@nudt.edu.cn

宋贻立(2000-),男,博士生,主要从事导航对抗技术等方面的研究。本文通信作者。

通信地址:国防科技大学电子科学学院(410073)

电话:18307410059

E-mail: songyili@nudt.edu.cn