

文章编号: 2095-4980(2024)03-0227-13

卫星通信干扰信号识别技术研究现状及展望

陈 凤¹, 李 聪², 朱立东¹, 吴 琦¹, 乐秀权³, 戴志坚³(1.电子科技大学 通信抗干扰全国重点实验室, 四川 成都 611731; 2.中国空间技术研究院 通信与导航卫星总体部, 北京 100094;
3.电子科技大学(深圳)高等研究院, 广东 深圳 518110)

摘 要: 随着通信技术的发展, 卫星通信系统面临着日益严重的干扰问题以及干扰识别技术的挑战。针对这一现状, 介绍了常见的卫星干扰信号样式及卫星干扰信号的发展趋势, 分别从基于特征提取的干扰识别方法、传统机器学习方法以及深度学习方法 3 个方面介绍了卫星干扰信号分类识别技术的研究现状, 分析了其各自的优势与不足。最后对未来卫星干扰信号分类识别技术进行了展望。

关键词: 卫星通信; 干扰样式; 干扰识别; 深度学习

中图分类号: TN927

文献标志码: A

doi: 10.11805/TKYDA2023316

Overview of satellite communication interference signal recognition technology

CHEN Feng¹, LI Cong², ZHU Lidong¹, WU Qi¹, YUE Xiuquan³, DAI Zhijian³

(1.National Key Laboratory of Wireless Communication, University of Electronic Science and Technology of China, Chengdu Sichuan 611731, China; 2.Institute of Telecommunication and Navigation Satellites, China Academy of Space Technology, Beijing 100094, China; 3.Shenzhen Institute for Advanced Study, University of Electronic Science and Technology of China, Shenzhen Guangdong 518110, China)

Abstract: Satellite communication, as an important means of communication, plays a key role in modern society. However, with the development of communication technology, satellite communication system is also facing the increasingly serious interference problem and the challenge of interference recognition technology. In view of this situation, this paper first introduces the common patterns of satellite interference signals, and summarizes the development trends of satellite interference signals. Secondly, the research status of satellite interference signal classification and recognition technology is introduced from three aspects: feature extraction based interference recognition method, traditional machine learning method and deep learning method, and their respective advantages and disadvantages are analyzed. Finally, the future classification and recognition technology of satellite interference signal is prospected.

Keywords: satellite communication; interference style; interference recognition; deep learning

卫星通信作为现代通信领域的关键组成部分, 为人们提供了广域覆盖、高质量的通信服务, 广泛用于国防、商业通信、紧急救援和全球导航等领域。随着通信环境日益复杂, 卫星通信系统常遭受各种干扰信号的威胁, 导致通信中断、质量下降以及安全风险。为应对这一挑战, 基于干扰感知与认知技术的卫星通信抗干扰研究逐渐崭露头角^[1]。对卫星干扰信号进行分类识别是干扰感知与认知过程中的关键环节, 全面了解干扰信号的类型是进行干扰识别的基石; 分析总结当前干扰信号的研究现状和发展趋势, 才能在进行抗干扰研究中有的放矢。传统的干扰识别方法主要依赖于基于特征提取的信号识别方法和传统的机器学习方法。随着深度学习技术的快速发展, 特别是卷积神经网络(Convolutional Neural Network, CNN)的广泛应用, 其能自动学习复杂的信号特征, 提高干扰识别的准确性和效率, 使干扰识别的研究取得了显著进展。未来, 随着卫星通信系统的不断发展和干扰威胁的不断演化, 高效可靠的干扰识别技术将继续成为研究和工程领域的重要课题。深度学习等新兴技术的应用将有望进一步提高卫星通信系统的鲁棒性和安全性, 确保其在日益复杂的通信环境中能够持续可靠地运行。

收稿日期: 2023-10-10; 修回日期: 2024-01-08

基金项目: 国家自然科学基金资助项目(62371098); 基础加强资助项目(2020-JCJQ-ZD-119)

本文在综述干扰信号类型的基础上, 主要探讨卫星干扰信号类别和干扰识别相关技术的研究现状, 特别关注干扰感知与认知对卫星通信系统的重要性, 全面了解卫星通信干扰问题以及相关技术的研究进展, 并对未来的发展进行展望。

1 卫星干扰信号

卫星通信系统由于其信道的开放性特征, 在通信过程中易遭受自由空间中不同干扰的影响。了解干扰信号的类型是卫星通信系统进行感知并做出正确决策的基础。根据干扰来源, 可将干扰类型主要分为自然干扰、人为干扰^[2], 人为干扰又可进行更精细的划分。卫星干扰来源大致分类如图 1 所示, 本文主要对人为恶意干扰进行综述, 包括传统压制式干扰、灵巧干扰以及目前研究正热的智能干扰。

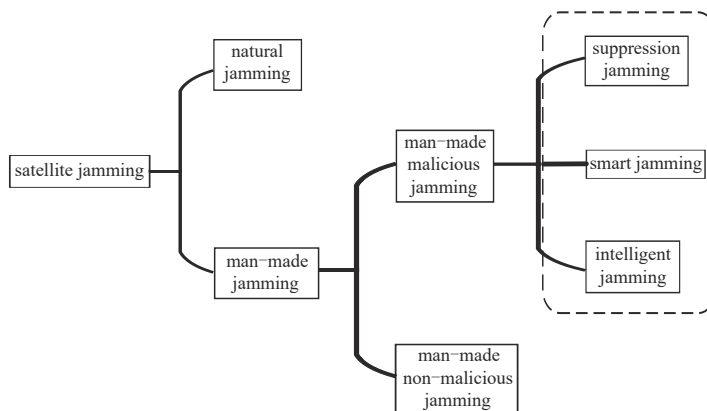


Fig.1 Classification of satellite interference sources

图 1 卫星干扰来源分类

1.1 传统压制式干扰

传统压制式干扰是通过高功率的信号对目标信号进行压制的一种干扰类型。不同压制式干扰占用的频率带宽不同, 受到压制干扰影响的频率带宽无法传输目标信号。常见的压制式干扰主要包含以下几种类别:

1) 音调干扰^[3]: 最简单、最基础的干扰波形, 从时域上看, 是一个简单的正弦波或多个正弦波的叠加; 从频域上看, 是功率集中在一个或多个频率上的干扰信号。因此音调干扰的干扰带宽较窄, 对无需实施干扰的频率带宽影响最小。音调干扰的表达式为:

$$J(t) = \sum_{i=1}^N \sqrt{2P} \cos(2\pi f_i t + \theta_i) \quad (1)$$

式中: P 为音调的平均功率; N 为音调个数 ($N \geq 1$); f_i 为音调的频率; θ_i 为相位。当 $i=1$ 时, $J(t)$ 为单音干扰; 当 $i \geq 1$ 时, $J(t)$ 为多音干扰。

2) 阻塞干扰^[4]: 对一个大范围的频带进行无缝隙的功率压制, 具有足够的功率, 可以降低敌方接收机的信噪比 (Signal-to-Noise Ratio, SNR)。随着干扰频率范围增大, 干扰输出功率会成比例减小, 干扰效率降低。阻塞干扰可分为宽带噪声阻塞干扰 (Broad-Band Noise Jamming, BBNJ) 和部分频带噪声阻塞干扰 (Partial Band Noise Jamming, PBNJ)。其通用表达式为:

$$J(t) = U_n(t) \exp[j(2\pi f_j t + \theta_j)] \quad (2)$$

式中: $U_n(t)$ 为低通滤波后的基带噪声信号; f_j 为干扰中心频率; θ_j 为初始相位, 并服从 0 到 2π 的均匀分布 (U), 可以表示为 $\theta_j \in U[0, 2\pi)$ 。

3) 脉冲干扰 (Pulse Jamming, PJ)^[5]: 主要是指由连续理想矩形脉冲组成的干扰信号, 通常表现为瞬间突发的高能量脉冲信号, 能对通信系统造成严重影响。这种干扰通常是突发的、短暂的, 但能量密度很高, 足以损坏或干扰通信信号。其表达式为:

$$J(t) = m(t) \times U_{T,\tau}(t) \quad (3)$$

式中: $m(t)$ 为调制信号; T 为脉冲重复周期; τ 为脉冲宽度, 一个脉冲周期内干扰的有效压制时间为 τ/T ; $U_{T,\tau}(t)$ 为周期脉冲信号:

$$U_{T,\tau}(t) = \begin{cases} 1, & kT \leq t \leq kT + \tau, \quad k \in \mathbf{Z} \\ 0, & \text{others} \end{cases} \quad (4)$$

4) 调频干扰^[6]: 是指通过调制信号对干扰信号的载波频率进行调制产生的干扰信号。由于干扰信号的载波频率会随调制信号而变化, 而调制信号本身为时变函数, 因此调频干扰是一类非平稳信号。其一般数学表达式为:

$$J(t) = \sqrt{2P_j} \cos \left[2\pi f_j t + 2\pi K_{FM} \int m(t) dt + \theta_j \right] \quad (5)$$

式中: P_j 为平均功率; $m(t)$ 为调制信号, 用以控制干扰信号的载波频率; K_{FM} 为调频比例系数; θ_j 为干扰信号初始相位, $\theta_j \in U[0, 2\pi)$ 。

调频信号根据频率的变化规律可分为正弦调频(Sinusoid Frequency Modulation, SFM)干扰、噪声调频(Noise Frequency Modulation, NFM)干扰、线性调频(Linear Frequency Modulation, LFM)干扰等。

5) 复合干扰：单一的压制式干扰具有处理难度低，易于实现等优点。当干扰作用于适当的通信频段，能较好地干扰正常通信。当今复杂的电磁环境中，干扰信号已不再仅限于单一形式，往往以多种干扰信号同时存在的方式出现。因此，考虑复合干扰信号的情况变得十分必要。文献[7]建立了复合干扰数学模型，并对其进行仿真，得到了不同复合干扰信号的波形，对比分析了复合干扰信号相对单一干扰信号的特点。除了波形上的区别，文献[8]还从干扰识别和消除的角度分析了复合干扰信号相对于单一干扰信号具备的特点，如更高的复杂性、更难检测、更高的干扰级别和处理复杂性等。

1.2 灵巧干扰

压制式干扰的本质是大功率压制，干扰功率越大，压制效果越好，但过大的干扰功率对干扰发射方是极大的挑战；同时，随着干扰抑制技术研究的深入，针对传统压制式干扰的抗干扰技术研究趋于成熟，干扰信号的研究转向高效、灵活的干扰。因此，灵巧干扰的概念应运而生。灵巧干扰最早应用在雷达通信中，因其在雷达通信中取得了较好的干扰效果，因此也被引入到数字通信中^[2]。目前，通信过程中的灵巧干扰主要思想是对通信特定过程(如同步信号、训练序列等)实施针对性的干扰或对目标接收机实施欺骗行为。常规干扰是对信号的时域、频域、空域实施干扰，而对特定通信过程实施干扰的灵巧干扰可视为引入了新一维干扰空间(过程空间)，是对常规干扰的扩展。通信过程中的欺骗干扰也可视为一种灵巧干扰，其巧妙地运用了目标信号的特点，对目标接收机实施欺骗行为，干扰方式高效灵活。灵巧干扰结构框图如图2所示：首先对侦收信号的特征参数进行分析，再根据信号特征设计不同的干扰样式，生成干扰信号并发送。

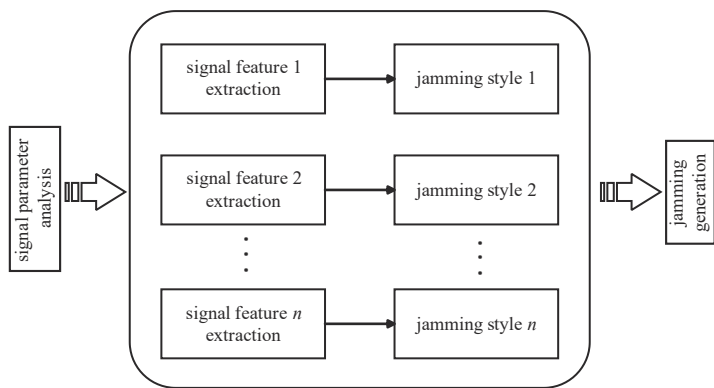


Fig.2 Overall design of smart jamming

图2 灵巧干扰总设计方案

文献[9]中认为灵巧干扰是在对通信信号侦察处理的基础上，生成精准压制式干扰，集中功率于通信链路的薄弱环节，给通信方致命一击，或是生成具有欺骗性的干扰信号，使通信方截获欺骗干扰，获得错误信息。此外，当存在多个干扰机时，各个干扰机之间采取合适的功率分配策略也是灵巧干扰的一种方式^[10]。干扰机的正确选择也是实施灵巧干扰的重要手段，文献[11]基于网络预测模型提出一种干扰策略，能在多个干扰机之间，选择最佳的干扰机位置。本文主要综述精准压制式干扰和欺骗干扰。

1) 精准压制式干扰。精准压制式干扰更注重通信的过程特性，如导频信号、同步信号、训练序列等过程。针对它们进行干扰，能起到事半功倍的效果。

a) 针对导频信号的干扰。文献[12]着重强调了正交频分复用(Orthogonal Frequency Division Multiplexing, OFDM)信号信道估计的重要性，利用灵巧干扰的思想有针对性地破坏导频信道估计环节，并通过实验证明针对导频信号的灵巧干扰比常规干扰的干扰效果更好。文献[13]着眼于“抵消”目标接收机的导频信号，在对敌我信道信息进行充分分析的基础上，通过构造灵巧干扰使目标接收机无法进行导频信道估计。不同于以上两种方法，文献[14]从导频信号本身出发，通过对获得的导频信号进行变换，使目标接收机获得错误的导频信息。

b) 针对同步信号的干扰。文献[9]认为，在帧同步序列识别和信道传输时延计算的基础上，通过实施针对同步字段的精准压制式干扰，可实现对下一个时隙的同步字段的精准压制式干扰。对于时间同步信号，文献[15]分别从接收机相关峰和训练序列的干扰入手，提出2种精准干扰方案。在接收机以同步信号的相关峰为同步依据的条件下，干扰方通过生成强相关的伪训练序列，在目标接收机处制造伪相关峰，使接收机无法正确同步。第2种方案与文献[13]中的方法有异曲同工之处，即“抵消”训练序列，使训练序列在接收端出现置零的效果，从而无法实现同步。对于OFDM系统的时频同步过程，文献[16]深入研究了窄带噪声干扰对训练序列的影响，并特别关注克服这种窄带干扰的训练序列的生成问题。

2) 欺骗干扰：欺骗干扰^[4]是指干扰方产生或转发与目标卫星信号高度相似的干扰信号，导致目标接收机无法正确分辨敌我信号，并将略微具有功率等优势欺骗信号捕获，获得错误信息的干扰技术。由其产生方式可知，

欺骗干扰相较于其他类型的干扰,具有更好的隐蔽性、抗侦测性以及更高的干扰效率^[17]。

按照干扰信号的生成方式可将欺骗干扰分为转发式欺骗干扰和生成式欺骗干扰。转发式欺骗干扰的实施方式为:对截获到的目标卫星信号附加传播时延,并进行适当的功率放大,然后再进行干扰发送^[18]。信号附加传播时延,使欺骗干扰类似于目标卫星信号的多径信号;信号进行适当功率放大,使目标接收机更容易捕获到干扰信号。生成式欺骗干扰是根据截获到的目标卫星信号的基本特征(包括码结构、调制方式等),产生与目标卫星信号强相关的伪随机码,调制与真实卫星信号相似的欺骗干扰^[19]。对比以上两类欺骗干扰信号可知,转发式欺骗干扰产生方式简单,但应用范围有限;产生式欺骗干扰生成难度较大,但灵活性更高。

文献[20]从欺骗干扰的实施设备出发,详细分析了不同欺骗设备产生干扰信号的特点和区别。目前主要的欺骗设备有:信号模拟器、信号转发器、单天线 receiver/spoofers、多通道信号转发器、多天线 receiver/spoofers。不同产生方式的欺骗干扰特点见表 1。

表 1 不同产生方式的欺骗干扰特点^[20]

Table 1 Characteristics of deception interference in different production modes^[20]

	signal simulation deception mode	signal transmitting spoofing mode	single antenna receiver/ spoofers spoofing mode	multichannel transmitting spoofing mode	multi-antenna receiver/ spoofers spoofing mode
hardware platform	signal simulator	regular transponder	single receiver/spoofers	multichannel transponder	multiple synchronous receiver/spoofers
signal generation	generative	transmitting	generative	transmitting	generative
implementation complexity	low	low	high	medium	very high
deception threat	high	low	high	high	high
attack requirements for tracking state receiver	start with suppression jamming	start with suppression jamming	get the target's real-time location	get the target's real-time location;start with suppression jamming	get the target's real-time location
difficulty of detection	low	low	high	medium	high

a) 信号模拟欺骗模式:由信号模拟器产生欺骗信号的优点是模拟效果较好,干扰生成方式简单;缺点是模拟器商业成本较高,低成本的模拟器还未得到广泛应用。

b) 信号转发欺骗模式:采用信号转发器生成欺骗干扰的优点是干扰生成方式简单,信号转发器应用广泛,并且转发器可以转发军用信号,对军用接收机造成欺骗;缺点是转发生成的信号与目标信号的多径信号相似,转发信号容易被目标接收机检测到。

c) 单天线 receiver/spoofers 欺骗模式:receiver/spoofers 设备不仅可以对目标信号进行捕获分析,而且可以产生欺骗干扰对接收机进行欺骗攻击。receiver/spoofers 设备严格把控干扰机和目标接收机之间的距离,确保能进行码相位同步,然后控制干扰功率略高于真实信号,使欺骗信号被接收机捕获。

d) 多通道转发欺骗模式:多通道转发器与单通道转发器的区别是可以通过多个通道对目标信号附加不同的传播时延。和单天线 receiver/spoofers 欺骗模式一样,多通道转发器可以获得目标接收机的实时位置。

e) 多天线 receiver/spoofers 欺骗模式:具有多个同步 receiver/spoofers 设备的欺骗攻击模式,称为多天线 receiver/spoofers 欺骗模式,主要针对的是多天线接收机的欺骗^[20]。通过多个 receiver/spoofers 设备或欺骗单元的组合,可以使每个欺骗单元欺骗接收机的一根天线,完成对多天线接收机的有效欺骗。

综上所述,灵巧干扰(精准压制式干扰和欺骗干扰)相对于传统压制式干扰,具有干扰功率较小、干扰效率较高、灵活性较好和干扰样式丰富等优点,但缺点是产生方式复杂。因此在通信对抗系统中选择干扰信号时,应根据具体需求合理选择干扰信号。

1.3 智能干扰

随着通信干扰与抗干扰技术的发展,通信干扰方可能配备了认知无线电技术,能实时感知无线电频谱,快速表征和分析环境,确定最佳攻击策略。干扰技术逐渐趋于智能化,越来越多的算法和理论被用于通信对抗环境中以寻求最佳干扰策略,如博弈论、粒子群算法、遗传算法等。通过算法改变通信参数,进而改变干扰样式,使干扰具有一定的智能性,但智能干扰实施的重要前提是需获取信道以及目标信号的先验信息。因先验信息的获取困难,因此智能干扰的研究受到限制,目前仍处于发展阶段。智能干扰的模型框架见图 3。

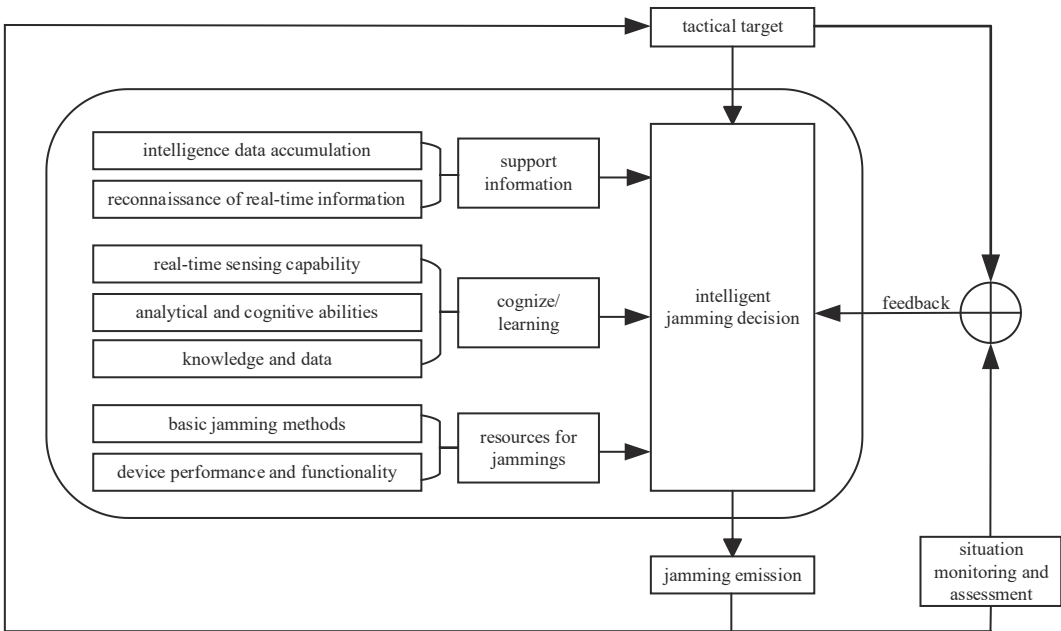


Fig.3 Framework of intelligent jamming
图3 智能干扰框架

面对未知、复杂环境问题时，强化学习(Reinforcement Learning, RL)具有鲁棒性强、实时交互等特点。在RL的交互过程中，利用所执行的行动是好是坏的反馈改进其策略，使回报最大化或成本最小化。将RL这种能力用于通信系统中，能够明智地管理卫星通信系统资源并自主减轻干扰攻击，而无需事先进行干扰类型分类^[21]。目前，已有部分研究将RL用于智能干扰。

智能干扰的目的是根据对抗环境实现最佳干扰决策。干扰方在构造干扰信号时，不仅需要准确选择干扰样式，还需确定干扰信号的功率、脉冲率等干扰参数，从而实现最佳干扰。其中脉冲率定义为干扰时间与通信信号持续时间的比值^[22]。文献[22]采用基于强化学习的干扰多臂赌博机(Jamming Bandit, JB)算法对功率、脉冲率等连续参数进行离散处理，并从干扰参数集{功率、干扰样式、脉冲率}中动态地选择干扰参数组，经过一段时间的交互学习后，完成最佳干扰决策^[23]。在军事领域为了更好地应用干扰优化方法，对基于RL的智能干扰决策进行奖励机制改变。文献[24]通过在决策问题中引入贪婪算法，设计新的基于功率和持续时间变化的奖赏标准，快速得到干扰样式、功率和脉冲间隔^[25]等干扰参数，并完成最佳干扰决策。为了避免贪婪算法中的随机选择方法，引入正强化学习思想用于干扰动作的选择^[23,26]。此外，RL的良好特性也被众多学者用于卫星通信抗干扰中。文献[27]提出一种新颖的智能反应式卫星通信干扰方法，该方法可有效对抗基于RL的卫星通信抗干扰策略，但依旧存在几何条件的限制。

综合以上分析，通信干扰的发展从传统的压制式干扰演变到更复杂的灵巧干扰和最终的智能干扰。最初，通信干扰主要关注大功率压制干扰，采用简单的频率干扰或噪声等方法阻碍通信。随着技术的进步，干扰者开始采用更高效的灵巧干扰策略，包括精准压制干扰，及欺骗干扰，旨在有针对性地干扰特定目标系统，或试图欺骗目标系统。干扰信号最新的研究热点是智能干扰，这一阶段涵盖了高级的干扰技术和算法，依赖深度学习、感知和自适应等方法，根据目标系统的行为动态选择和调整干扰策略。这一演进代表了通信干扰从简单到复杂、从静态到动态的发展趋势，对通信安全提出了更大的挑战。表2为以上几种类型干扰信号各自的优缺点，图4为卫星通信干扰信号的发展历程示意图。

表2 不同类型干扰的特点
Table 2 Characteristics of different types of interference

	conventional suppression jamming	smart jamming	intelligent jamming
complexity	low	high	very high
accuracy of jamming	limited, usually extensive	more accurate and targeted	more accurate and adaptive
prior information required	low	high	high
flexibility	low	high	very high
difficulty of confrontation	easy	difficult	very difficult
difficulty of detection	low	low	high

2 干扰识别技术

随着电磁环境的复杂化,干扰信号的种类越来越多,卫星通信系统面临更大的威胁。在进行干扰感知的过程中,为更好地对抗通信过程中受到的干扰,需对检测到的干扰信号进行分类和识别,以便后续有针对性地分离和消除干扰。卫星通信干扰信号识别系统结构见图 5。根据文献[28],干扰信号的识别通常先进行信号特征提取,在此基础上完成信号识别与分类。目前对信号特征提取的研究相对成熟,对信号识别分类的研究仍处于发展阶段。随着深度学习方法的引入,研究者已经开始探索更高效的方式来进行干扰信号识别,这已成为一个备受关注的热点领域。随着干扰识别技术的发展,目前主要的干扰识别方法可分为:基于特征提取的信号处理方法、传统机器学习方法和深度学习

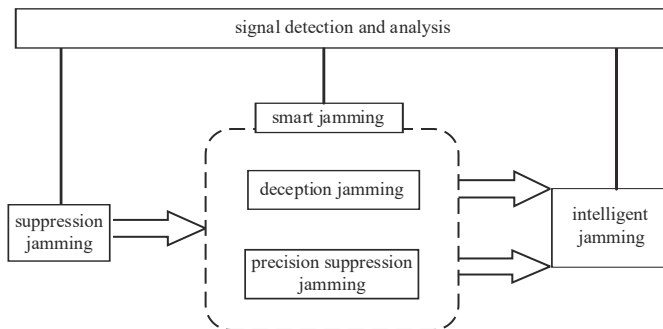


Fig.4 Development of satellite communication interference signals
图4 卫星通信干扰信号的发展历程

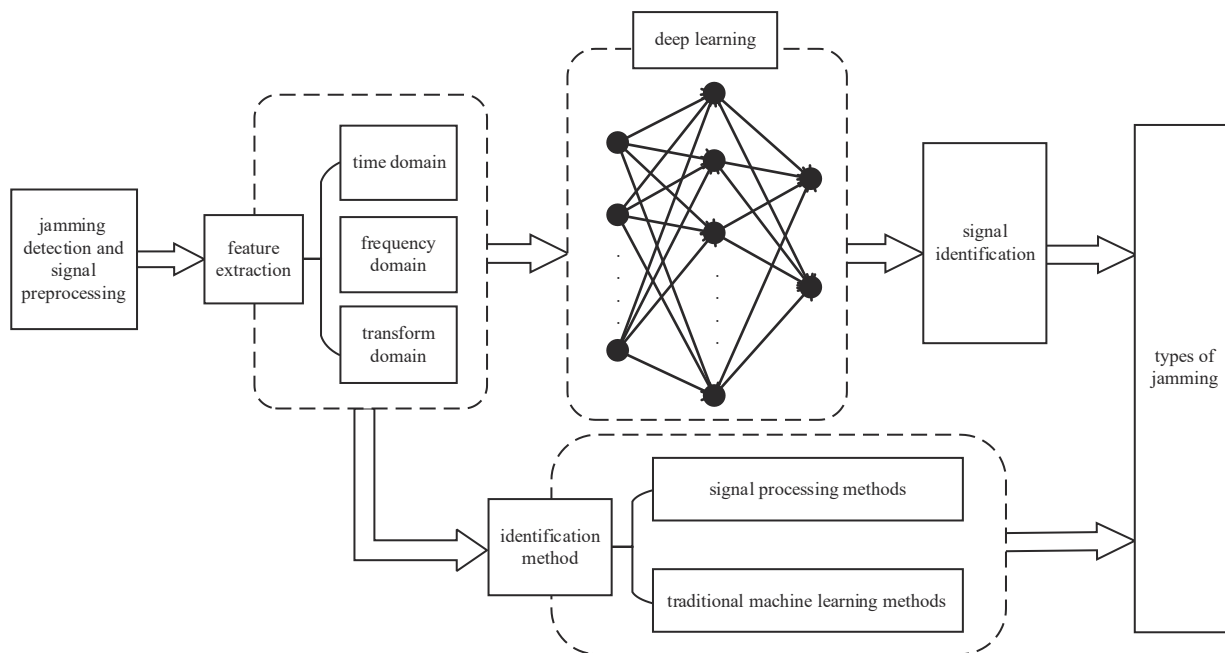


Fig.5 Diagram of satellite interference signal recognition system
图5 卫星干扰信号识别系统结构框图

2.1 用于干扰识别的信号处理方法

信号处理方法主要通过对接收信号进行数学和算法分析,获取信号的时域、频域和时频域等特征,包括波形、频谱、自相关性等,借此识别和区分干扰信号。在进行干扰信号识别的过程中,最常见的特征有:

1) 单频能量聚集度。表示信号在频域的能量聚集,主要用于区分单音干扰。首先对功率归一化后的干扰信号做快速傅里叶变换(Fast Fourier Transform, FFT),得其频谱幅值 $F(i)$, $i = 1, 2, \dots, N$, 找出最大频谱值对应的索引 m 。单频能量聚集度的定义表达见式(6), k 为一个很小的整数,通常取 1。

$$C = \frac{\sum_{i=m-k}^{m+k} F^2(i)}{\sum_{i=1}^N F^2(i)} \quad (6)$$

2) 平均频谱平坦系数。表示信号幅度在功率谱域中的变化程度,是原始功率谱与加窗平滑后的信号功率谱之差的标准差。对归一化后的干扰信号做 FFT 变换,得其频谱幅值 $F(n)$, $n = 1, 2, \dots, N$, 取平方得其功率谱 $P(n)$, 然后对 $P(n)$ 进行均值归一化:

$$P_u(n) = P(n) / \overline{P(n)} \quad (9)$$

式中 $\overline{P(n)}$ 为 $P(n)$ 的均值。对 $P(n)$ 中的冲激部分进行提取，有：

$$P_p(n) = P_u(n) - \frac{1}{2L+1} \sum_{i=-L}^L P_u(n-i) \quad (8)$$

式中：等式减数项为 $P_u(n)$ 经过滑动平均后的归一化平滑功率谱； L 为滑动平均窗口的长度，取 $L=0.03N$ ，得到平均频谱平坦系数为：

$$F_c = \sqrt{\frac{1}{N} \sum_{n=1}^N [P_p(n) - \overline{P_p(n)}]^2} \quad (9)$$

3) 频域矩偏度和频域矩峰度。频域矩偏度系数表示相对于频域正态分布的幅值偏移程度；频域矩峰度系数表示信号频谱的幅值陡度。两者的表达式为：

$$b_k = \frac{E(F(n) - \mu)^k}{\sigma^k} \quad (10)$$

式中： $F(n)$ 为信号频谱的幅度； μ 为 $F(n)$ 的均值； σ 为 $F(n)$ 的标准差。当 $k=3$ 时，式(10)表示频域矩偏度；当 $k=4$ 时，式(10)表示频域矩峰度。

4) 分数傅里叶域能量聚集度。表示信号在 p 阶分数傅里叶变换(Fractional Fourier Transform, FRFT)域中的能量聚集度，根据最大能量聚集度对应的 FRFT 域选择 p ，如 LFM 干扰信号， $p=2$ 。部分干扰信号在时域和频域都难以区分，如 LFM 信号与宽带噪声干扰(Broad Band Noise Jammer, BBNJ)信号，将信号变换到时频域，能更清晰地看到其变化特点^[7]，并加以区分。 p 阶 FRFT 域中的能量聚集度的表达式为：

$$R_f = \frac{\sum_{e=m-r}^{m+r} |X(e)|^2}{|\overline{X(n)}|^2} \quad (12)$$

式中： $X(e)$ 表示分数傅里叶变换谱值； m 表示 $X(e)$ 最大值的索引； $|\overline{X(n)}|^2$ 的表达式为：

$$|\overline{X(n)}|^2 = \frac{1}{N-2r-1} \left[\sum_{n=1}^N |X(n)|^2 - \sum_{e=m-r}^{m+r} |X(e)|^2 \right] \quad (13)$$

式中 r 为一个很小的整数，通常取 1。

5) 频域参数。表示信号频域幅度的包络变化。不同的干扰信号幅度谱的变化不相同，因此包络的变化程度也各不相同，如单音干扰、多音干扰的频域包络变化较大，提取干扰信号的包络起伏度是必要的。其表达式为：

$$R_f = \sigma^2 / \mu^2 \quad (14)$$

6) 时域矩峰度系数。表示信号在时域上的幅值陡度。当时域矩峰度较大时，说明信号分布紧凑，呈现出明显的尖峰；当时域矩峰度较小时，说明信号分布较为平缓。其表达式为：

$$a_4 = \frac{E(|X - \mu|^4)}{\sigma^4} \quad (15)$$

式中 X 为信号的时域离散值。

此外，还可以对信号进行统计分析，通过信号的统计量，如均值、方差、高阶统计量^[29]等，判断其是否受到干扰，进而识别干扰信号。如，结合维格纳-威利分布(Wigner-Ville Distribution, WVD)提取非平稳干扰信号的特征^[30]，得到干扰信号的统计特征(一阶矩、二阶矩)和二维时频特征，进而对干扰信号进行识别。不少研究通过对信号进行变换，从变换域做进一步的分析。如，使用小波变换分解信号^[31]，提取各阶分量的能量比作为特征进行干扰识别；根据谱相关理论^[32-33]，对干扰进行循环谱分析，该方法具有良好的抑制噪声性能，对信号进行分类识别效果较好。还可以将多种方法进行结合，如结合高阶累积量^[33](High-Order Cumulative, HOC)和小波变换^[34]的方法。在利用高阶累积量提取特征之前，首先使用小波变换进行去噪，然后利用频域高阶累积量分析常见的干扰，提取各种干扰的特征参数，并结合简单的分层网络对信号进行分类和识别。

对于复合干扰，采用常规的信号处理方法提取干扰信号特征，识别率较低。现有的研究通常通过快速独立分量分析^[35](Fast Independent Component Analysis, FICA)算法对干扰信号进行分离，再结合其他识别算法完成复合干扰信号的识别，识别率更高。随着干扰技术的发展，对干扰信号特征的研究逐渐趋于多样化。目前，国内外诸多文献对参数提取有丰富的研究，具体总结见表3。

表3 特征参数
Table3 Characteristic parameters

categories	features
time domain	high order cumulant characteristic factor ^[36]
frequency domain	normalized 3dB bandwidth ^[37] , Welch periodogram ^[38] , bispectrum analysis ^[39]
time–frequency domain	the short–time Fourier transform ^[40] , wavelet analysis ^[31] , time–frequency domain separability ^[41]
information domain	entropy feature ^[42–46] (hierarchy entropy, fuzzy entropy, sample entropy, mixing entropy)

干扰特征提取对后续干扰识别有举足轻重的作用，然而仅依赖于固定的特征参数来研究不同信号的特征已面临瓶颈，需从信号本身重新考虑合适的特征参数。

由以上分析可知，通过特征提取进行干扰信号识别的方法众多，但如何选择适合信号数据本身的特征成为研究瓶颈。文献[47]对不平衡数据和标记样本少的数据进行了特征选择的研究。借鉴引导聚集算法(Bootstrap aggregating, Bagging)，提出一种基于特征权重算法和聚类的不平衡数据特征选择方法^[48]，该方法在信号识别中具有良好的性能。也有相关研究从接收机的设计上考虑干扰信号的识别。文献[49]根据接收机受不同干扰信号影响产生的相关峰来判别干扰信号的类型。提取并分析受不同干扰信号影响的相关峰，然后通过机器学习方法对它们进行分类和识别。为降低机器学习网络的复杂性，只提取有限长度相关感兴趣的峰区域(Region Of Interest, ROI)作为网络输入。

2.2 传统机器学习方法

直接使用信号样本数据进行识别和分类会消耗大量的运算时间，容易导致识别算法不收敛，影响系统识别性能。为避免以上问题，基于特征提取的机器学习方法得到了充分研究，即在提取待识别信号特征参数的基础上，传统的机器学习方法利用分类算法或网络完成干扰信号的识别。

传统机器学习算法在干扰识别中发挥了重要作用，包括支持向量机(Support Vector Machine, SVM)、决策树(Decision Tree, DT)、传统神经网络、K-最近邻(K-Nearest Neighbor, K-NN)算法、随机森林(Random Forest, RF)、朴素贝叶斯分类器、逻辑回归、最大熵模型等。这些算法可用于构建模型，将干扰信号的特征视为样本数据，并利用分类算法和网络对其进行分类和识别。这些传统方法通常需要合适的特征工程和模型调优，对于特定的干扰信号类型和应用场景，可以提供有效的解决方案。目前国内外研究相对较多的主要为前3类算法。

1) 决策树。决策树首先从原始的混沌和无序样本数据点中找到一组用于数据内部分类的规则，通过递归的方式将规则方法表达为树形结构，从上到下进行判断，直到被分类为特定的叶节点类别。

使用决策树进行分类识别，通常结合信号的变换处理。如，结合 Welch 修正周期图法以及分数傅里叶变换提取特征，或采用高阶累积量、循环谱特征进行干扰特征提取，并通过决策树实现干扰识别^[30]。

随着干扰识别技术的发展，决策树用于干扰识别也存在不少缺点：a) 当树的深度较大时，容易过拟合训练数据；b) 对高维数据和复杂关系的建模能力有限；c) 树的结构可能不稳定，对输入数据的微小变化敏感，导致模型不稳定；d) 若生成的树过于复杂，难以解释和理解。

2) 支持向量机。支持向量机^[50]本质上是一个凸二次规划问题，也是一种有监督的学习算法。它的优势在于解决分类和回归等问题，强大的泛化能力使其在解决分类识别问题时备受青睐。目前，国内外已有大量的研究将信号处理方法与SVM模型相结合，用于干扰识别。随着研究深入，SVM模型在许多识别问题中表现出良好的性能。然而，鉴于模型本身学习的复杂度以及结合其他算法的实现难度，真正用于实际中的方法很少。据此，有不少学者从SVM模型的复杂度入手，研究如何降低算法的实现难度，使方法更具有研究意义和工程价值。上述两方面的主要研究内容见表4。

表4 基于SVM的干扰识别研究
Table4 Research on interference recognition based on SVM

research directions	research contents
classification and recognition method based on SVM model	recognition of complex jamming signals based on FICA and SVM ^[51]
	recognition of digital modulation based on HOC algorithm and SVM ^[52]
	modulation recognition based on wavelet analysis and SVM ^[53]
reduce the complexity of SVM model for classification recognition	incremental learning, incremental SVM ^[28,54] twin SVM ^[55]

3) BP神经网络^[7]。BP神经网络(Backpropagation Neural Network)是一种常用于模式识别和分类任务的人工神经网络，由输入层、隐藏层和输出层构成，通过前向传播和误差反向传播机制来训练网络，使其能够学习和适应复杂的数据模式，如干扰信号的特征。目前，基于特征提取的BP神经网络干扰识别技术已发展成熟，国内外也有很多相关研究。BP神经网络是最简单的人工神经网络，因此，面对复杂且庞大的数据，BP神经网络也存在

不少缺点：a) 网络结构的选择依赖经验；b) 需要大量标记数据用于训练；c) 容易过拟合复杂模型；d) 对初始权重敏感；e) 面对复杂数据，训练时间较长；f) 网络的性能高度依赖于数据的质量和特征工程，需要仔细的预处理和参数调整，可能需要投入较多的时间和计算资源。

2.3 深度学习方法

传统神经网络不仅需要人为提取干扰信号特征，而且需要大量训练样本，泛化能力较弱，给传统神经网络的实际应用带来了困难。近年来，随着深度学习的不断发展及其在图像和语音处理方面的突出表现，已经验证了深度学习具有极强的非线性映射和数据表达能力，激发了研究人员将深度学习用于通信抗干扰领域，提高系统的抗干扰能力。深度学习的目标是通过学习自动提取数据中的特征，以进行分类、回归、聚类任务。深度学习模型可以是前馈神经网络、循环神经网络或卷积神经网络(CNN)等。目前，卷积神经网络用于干扰信号识别的问题最具研究热度，该技术在这一领域也极具潜力和优势。

CNN将干扰特征提取和干扰分类识别两个步骤合二为一，避免了人工提取信号特征参数带来的问题。CNN结构见图6，其中卷积层、池化层实现干扰特征提取的功能，全连接层对提取到的干扰特征进行非线性映射，最终在输出层得到干扰类型的识别结果。针对CNN自动提取特征的研究目前主要集中在CNN的输入处理对象、CNN的网络结构、CNN自动提取特征的可视化、CNN与其他算法的结合等方面^[56]。

1) 输入处理对象：针对待识别的复基带干扰信号，文献[56]重点关注不同的输入对CNN识别率的影响。主要考虑两种不同的输入，一是提取信号I、Q两路的数据构成2个通道用作CNN的输入；二是在前一种方法的基础上增加信号幅度谱，形成3个通道用作网络的输入。采用深度学习模型GoogLeNet中Inception^[57](多个卷积和池化组成的模块)的改进结构来构建CNN，进行干扰识别。经实验验证，第二种方法的识别率高于第一种，原因是第二种方法用于识别的数据多出一维，因此CNN从数据中能提取到的特征更丰富，识别效果更好。

2) 网络结构：最基本的CNN结构中包含输入层、卷积层、池化层以及激活函数等，通过各个部分之间的合理组合以及参数设置，得到不同的CNN结构，经典的CNN结构见图6。随着对基于CNN的分类识别问题研究的不断深入，根据不同的识别问题，更多的CNN结构被提出，如，将GoogLeNet中的Inception^[57]、批归一化(Batch Normalization, BN)等加入CNN结构中，新的CNN结构更有利于识别ImageNet数据集。

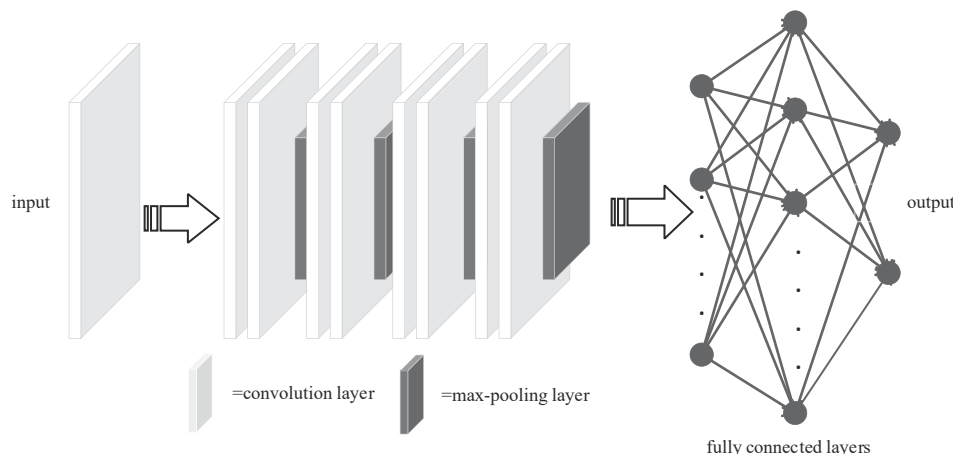


Fig 6 Diagram of CNN
图6 CNN结构图

3) 自动提取特征的可视化：文献[8,33]借助多维尺度分析(Multi-Dimensional Scale analysis, MDS)清楚地展现了经CNN自动提取的高维干扰特征参数的可分离性，并对特征进行降维处理。尽管干扰信号处于动态的干噪比(Jamming Noise Ratio, JNR)环境中，该方法自动提取的特征仍具有较好的聚合度。实验证明，CNN提取的特征具有良好的可分离性，非常适用于干扰信号的分类。

4) CNN与其他算法结合：从数据训练的角度考虑，结合其他算法研究如何减少CNN训练成本是一个重要的研究方向。迁移学习与CNN结合用于信号识别，克服了训练困难的问题。迁移学习是一种深度学习方法，其核心思想是将已在一个任务上学到的知识或模型用于不同但相关的任务中，提高目标任务的性能。迁移学习通过使用卷积神经网络的经典模型视觉集合群网络(Visual Geometry Group network 16, VGG16)在ImageNet数据集上进行预训练，将源领域(Source Domain)上学到的知识迁移到目标领域(Target Domain)上，从而减少在目标任务上的数据需求和模型训练成本，同时改善性能。文献[58]结合迁移学习和VGG16模型(在ImageNet数据集上进行了预训练)进行

特征提取,研究全球卫星导航系统(Global Navigation Satellite System, GNSS)干扰信号的分类问题。由于迁移学习的引入,该方法不仅能提高信号识别率,还避免了庞大的数据集需求。

从 CNN 模型的角度考虑,根据信号特点设计适合干扰识别的 CNN 网络是一个关键的研究内容。干扰信号的指纹谱(Fingerprint Spectrum, FPS)是干扰信号在频谱上的特定特征或模式,包括干扰信号的频率、幅度、持续时间、调制方式、时域特征和频域特征等,用于描述干扰信号的频率分布和性质。文献[59]结合干扰信号的时频分析以及功率随时间的变化情况,设计了一种深度学习模型 FPS-DNN(Fingerprint Spectrum-Deep Convolutional Neural Network),用于指纹图谱的识别。FPS-DNN 模型是传统 CNN 模型的拓展,结构更复杂,但具有更好的识别性能。尽管干扰识别方法已经智能化,但在 JNR 较低的情况下,大多数方法的识别效果仍较差。由于复数卷积神经网络能挖掘数据内部的潜在特征,并具有识别率高、噪声影响小等优点,将复数卷积神经网络^[60]用于干扰识别,能识别更大范围 JNR 的干扰信号,识别率高于传统的 CNN。

3 卫星干扰识别技术未来发展趋势

随着卫星通信技术的发展以及通信侦察分析能力的提高,通信干扰技术的重点研究对象不再是传统压制式干扰,而慢慢转变为更加高效、智能的干扰技术。有效对抗敌方的智能干扰,已成为卫星通信领域所面临的重大挑战,因此必须深入研究并不断提高应对方法。综合分析卫星干扰识别技术的研究现状,卫星干扰识别技术在以下几个方面具有发展潜力:

1) 多模态干扰识别:目前大多数研究都是基于单一干扰信号的识别,对复合干扰识别技术的研究还不够充分。复杂的干扰信号具有更复杂的特征信息,需要综合提取信号多种模态的信息,如时域、频域、时频域、空域等信息,进行数据融合、信号识别以及实时监测等工作。此外,在卫星通信系统中,充分利用多种数据源或传感器数据,实现多数据的融合,是提高识别系统鲁棒性和识别性能的重要途径之一。

2) 大数据和云边协同:随着通信数据的不断增长,卫星的数据处理能力受限。在卫星干扰信号识别中,大数据技术能够有效地处理这些大规模的信号数据集,从中提取有用的特征和趋势。云计算提供了高性能的计算资源和实时处理能力,而卫星服务器作为边缘服务器具有轻量级数据处理能力,二者结合构建云边协作的数据处理框架,能大量减少从卫星服务器到云服务器的带宽压力和响应时间。相比单独利用云服务器进行数据处理,节省了大量网络流量,使系统能够对干扰信号进行实时监测,快速分析数据,并迅速做出反应。

3) 频谱感知和认知无线技术:频谱感知技术通过监测和分析当前的频谱使用情况,确定可用的频谱范围和时段,有助于避免有用信号与干扰信号冲突,提高通信的可靠性和效率。认知无线技术允许设备智能地感知和适应周围的无线频谱环境,实时监测频谱使用情况,并自动选择最适合的频谱进行通信,减小受到干扰的概率。

4 结论

卫星通信作为未来各国主要竞争领域,其安全性的研究备受关注。本文全面探讨了卫星通信干扰类型及干扰信号识别技术的研究现状,通过对各种卫星通信干扰类型的分类和特点进行分析,强调了干扰信号的多样性和复杂性,并总结了卫星干扰信号的发展趋势。此外,本文还详细介绍了当前用于干扰信号识别的技术和方法,包括用于干扰处理的信号处理方法、传统机器学习方法以及备受瞩目的深度学习方法,强调了深度学习在这一领域中的潜力和优势。随着干扰技术的不断发展,卫星通信干扰识别技术将面临更多挑战和机遇。因此,未来的研究需要更多关注多模态干扰的识别、深度学习在干扰识别中的进一步应用以及大数据和云边协同技术在处理干扰数据方面的作用。卫星通信干扰识别技术是一个充满挑战,同时充满前景的领域,通过持续的研究和创新,有望更好地保护卫星通信免受各种干扰的影响,确保通信的可靠性和安全性。期待未来在这一领域取得更多重要的突破和进展,以应对不断发展的通信干扰挑战。

参考文献:

- [1] RODDY D. Satellite communications[M]. New York: McGraw-Hill Education, 2006.
- [2] POISEL R. Modern communications jamming principles and techniques[M]. Norwood: Artech House, 2011.
- [3] 逢天洋,李永贵,牛英滔,等. 通信电子干扰的分类与发展[J]. 通信技术, 2018, 51(10): 2271-2278. (PANG Tianyang, LI Yonggui, NIU Yingtao, et al. Classification and development of communication electronic jamming[J]. Communications Technology, 2018, 51(10): 2271-2278.) doi:10.3969/j.issn.1002-0802.2018.10.001.
- [4] MPITZIOPOULOS A, GAVALAS D, KONSTANTOPOULOS C, et al. A survey on jamming attacks and countermeasures in WSNs[J]. IEEE Communications Surveys & Tutorials, 2009, 11(4): 42-56. doi:10.1109/SURV.2009.090404.

- [5] LI Xiangjun, CHEN Lei, LU Zukun, et al. Overview of jamming technology for satellite navigation[J]. *Machines*, 2023, 11(7):768. doi:10.3390/machines11070768.
- [6] MITCH R H, DOUGHERTY R C, PSIAKI M L, et al. Signal characteristics of civil GPS jammers[C]// *Proceedings of the 24th International Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS 2011)*. Portland, OR: ION, 2011: 1907–1919.
- [7] WANG Yunxuan, HUANG Yan, CHEN Zhanye, et al. Complicated interference identification via machine learning methods[C]// *2021 IEEE the 4th International Conference on Electronic Information and Communication Technology (ICEICT)*. Xi'an, China: IEEE, 2021: 400–405. doi:10.1109/ICEICT53123.2021.9531191.
- [8] WU Zhilu, ZHAO Yanlong, YIN Zhendong, et al. Jamming signals classification using convolutional neural network[C]// *2017 IEEE International Symposium on Signal Processing and Information Technology (ISSPIT)*. Bilbao, Spain: IEEE, 2017: 62–67. doi:10.1109/ISSPIT.2017.8388320.
- [9] 邵堃, 雷迎科. 对武器制导数据链灵巧干扰技术[J]. *弹箭与制导学报*, 2020, 40(3): 17–22. (SHAO Kun, LEI Yingke. Smart jamming technology for weapon guidance data link[J]. *Journal of Projectiles, Rockets, Missiles and Guidance*, 2020, 40(3): 17–22.) doi:10.15892/j.cnki.djzdx.2020.03.005.
- [10] WANG Jianqi, LEE S A. Cooperative jamming in MIMO ad-hoc networks[C]// *2009 Conference Record of the Forty-Third Asilomar Conference on Signals, Systems and Computers*. Pacific Grove, CA, USA: IEEE, 2009: 1719–1723. doi:10.1109/ACSSC.2009.5469718.
- [11] VILELA J P, PINTO P C, BARROS J. Jammer selection policies for secure wireless networks[C]// *2011 IEEE International Conference on Communications Workshops (ICC)*. Kyoto, Japan: IEEE, 2011: 1–6. doi:10.1109/iccw.2011.5963525.
- [12] 郭富强, 王呈贵, 于雨. 基于OFDM导频信道估计的灵巧干扰方法[J]. *电子信息对抗技术*, 2008, 23(3): 35–38. (GUO Fuqiang, WANG Chenggui, YU Yu. A jamming scheme based on pilot assisted channel estimation of OFDM[J]. *Electronic Information Warfare Technology*, 2008, 23(3): 35–38.) doi:10.3969/j.issn.1674–2230.2008.03.009.
- [13] SODAGARI S, CHARLES C T. Efficient jamming attacks on MIMO channels[C]// *2012 IEEE International Conference on Communications (ICC)*. Ottawa, ON, Canada: IEEE, 2012: 852–856. doi:10.1109/ICC.2012.6364173.
- [14] CHARLES C T. Efficient OFDM denial: pilot jamming and pilot nulling[C]// *2011 IEEE International Conference on Communications (ICC)*. Kyoto, Japan: IEEE, 2011: 1–5. doi:10.1109/icc.2011.5962467.
- [15] PAN T C C, CLANCY T C, MCGWIER R W. Jamming attacks against OFDM timing synchronization and signal acquisition[C]// *MILCOM 2012–2012 IEEE Military Communications Conference*. Orlando, FL, USA: IEEE, 2012: 1–7. doi:10.1109/MILCOM.2012.6415749.
- [16] COULSON A J. Narrowband interference in pilot symbol assisted OFDM systems[J]. *IEEE Transactions on Wireless Communications*, 2004, 3(6): 2277–2287. doi:10.1109/TWC.2004.837471.
- [17] 高扬骏, 李广云, 吕志伟. 卫星导航干扰技术的现状及展望[J]. *测绘与空间地理信息*, 2022, 45(6): 13–18. (GAO Yangjun, LI Guangyun, LYU Zhiwei. Current situation and prospect of satellite navigation interference technology[J]. *Geomatics & Spatial Information Technology*, 2022, 45(6): 13–18.) doi:10.3969/j.issn.1672–5867.2022.06.005.
- [18] 闫占杰, 吴德伟, 刘海波, 等. GPS转发欺骗式干扰时延分析[J]. *空军工程大学学报(自然科学版)*, 2013, 14(4): 67–70. (YAN Zhanjie, WU Dewei, LIU Haibo, et al. Analysis of time-delay in GPS repeater deception jamming[J]. *Journal of Air Force Engineering University (Natural Science Edition)*, 2013, 14(4): 67–70.) doi:10.3969/j.issn.1009–3516.2013.04.016.
- [19] JAFARNIA J A, BROUMANDAN A, NIELSEN J, et al. GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N_0 measurements[J]. *International Journal of Satellite Communications and Networking*, 2012, 30(4): 181–191. doi:10.1002/sat.1012.
- [20] 刘洋. 惯性/卫星组合导航欺骗检测关键技术研究[D]. 西安: 西北工业大学, 2019. (LIU Yang. INS/GNSS integrated navigation system spoofing detection techniques[D]. Xi'an, China: Northwestern Polytechnical University, 2019.) doi:10.27406/d.cnki.gxbgu.2019.000364.
- [21] SUTTON R S, BARTO A G. Reinforcement learning: an introduction[M]. Cambridge: MIT press, 2018.
- [22] AMURU S D, TEKIN C, DER-SCHAAR M V, et al. Jamming bandits—a novel learning method for optimal jamming[J]. *IEEE Transactions on Wireless Communications*, 2016, 15(4): 2792–2808. doi:10.1109/TWC.2015.2510643.
- [23] 颢孙少帅, 杨俊安, 刘辉, 等. 基于正强化学习和正交分解的干扰策略选择算法[J]. *系统工程与电子技术*, 2018, 40(3): 518–525. (ZHUANSUN Shaoshuai, YANG Jun'an, LIU Hui, et al. Jamming strategy learning based on positive reinforcement learning and orthogonal decomposition[J]. *Systems Engineering and Electronics*, 2018, 40(3): 518–525.) doi:10.3969/j.issn.1001–506X.2018.03.05.

- [24] ZHUANSUN Shaoshuai, YANG Jun'an, LIU Hui, et al. A novel jamming strategy-greedy bandit[C]// 2017 IEEE the 9th International Conference on Communication Software and Networks(ICCSN). Guangzhou, China: IEEE, 2017: 1142–1146. doi: 10.1109/ICCSN.2017.8230289.
- [25] AMURU S, MICHAEL BUEHRER R. Optimal jamming using delayed learning[C]// 2014 IEEE Military Communications Conference. Baltimore, MD, USA: IEEE, 2014: 1528–1533. doi: 10.1109/MILCOM.2014.252.
- [26] 颢孙少帅, 杨俊安, 刘辉, 等. 采用双层强化学习的干扰决策算法[J]. 西安交通大学学报, 2018, 52(2): 63–69. (ZHUANSUN Shaoshuai, YANG Jun'an, LIU Hui, et al. An algorithm for jamming decision using dual reinforcement learning[J]. Journal of Xi'an Jiaotong University, 2018, 52(2): 63–69.) doi: 10.7652/xjtub201802010.
- [27] ARIF S, HASHMI A J, KHAN W, et al. A smart reactive jamming approach to counter reinforcement learning-based antijamming strategies in GEO SATCOM scenario[J]. International Journal of Satellite Communications and Networking, 2022, 40(2): 96–119. doi: 10.1002/sat.1418.
- [28] YANG Ying, ZHU Lidong. An efficient way for satellite interference signal recognition via incremental learning[C]// 2019 International Symposium on Networks, Computers and Communications(ISNCC). Istanbul, Turkey: IEEE, 2019: 1–5.
- [29] 黄英, 雷菁. 卫星通信中调制识别算法研究[J]. 系统工程与电子技术, 2009, 31(6): 1303–1306. (HUANG Ying, LEI Jing. Research on recognition of modulation signals in satellite communication[J]. Systems Engineering and Electronics, 2009, 31(6): 1303–1306.) doi: 10.3321/j.issn:1001–506X.2009.06.009.
- [30] KURAL F, OZKAZANC Y. A method for detecting RGPO/VGPO jamming[C]// Proceedings of the IEEE the 12th Signal Processing and Communications Applications Conference. Kusadasi, Turkey: IEEE, 2004: 237–240.
- [31] 田晓, 唐斌. 基于归一化小波分解能量比的雷达有源欺骗干扰识别[J]. 数据采集与处理, 2013, 28(4): 416–420. (TIAN Xiao, TANG Bin. Active deception jamming recognition of radar based on normalized wavelet decomposition power ratio[J]. Journal of Data Acquisition & Processing, 2013, 28(4): 416–420.) doi: 10.3969/j.issn.1004–9037.2013.04.005.
- [32] ZHANG Ming, LIU Lutao, DIAO Ming. LPI radar waveform recognition based on time-frequency distribution[J]. Sensors, 2016, 16(10): 1682. doi: 10.3390/s16101682.
- [33] YU Hang, ZHANG Rui, DING Rui. Interference recognition based on machine learning for satellite communications[C]// Proceedings of the 2018 International Conference on Machine Learning Technologies. Jinan, China: Association for Computing Machinery, 2018: 18–23. doi: 10.1145/3231884.3231901.
- [34] HAO Wu, YONG Chen, TAO Liang, et al. An algorithm for jamming recognition based on inspecting spectrum of satellite communication[C]// 2010 International Conference on Microwave and Millimeter Wave Technology. Chengdu, China: IEEE, 2010: 1263–1266. doi: 10.1109/ICMMT.2010.5524967.
- [35] ZHOU Zhiyu, CHEN Hao, LIU Ningning. Automatic recognition of multiple interferences and signals in the same channel based on ICA[C]// 2009 IET International Radar Conference. Guilin, Guangxi, China: IET, 2009: 1–4. doi: 10.1049/cp.2009.0364.
- [36] 李建勋, 闫海, 吕强. 基于高阶累积量的欺骗式干扰识别方法[J]. 微计算机信息, 2009, 25(7): 233–235. (LI Jianxun, YAN Hai, LYU Qiang. Deceptive interference identification method based on high-order cumulants[J]. Microcomputer Information, 2009, 25(7): 233–235.)
- [37] 杨小明, 陶然. 直接序列扩频通信系统中干扰样式的自动识别[J]. 兵工学报, 2008, 29(9): 1078–1082. (YANG Xiaoming, TAO Ran. Automatic identification of interferences in direct sequence spread spectrum communication system[J]. Acta Armamentarii, 2008, 29(9): 1078–1082.) doi: 10.3321/j.issn:1000–1093.2008.09.012.
- [38] LU Ling, YANG Jie, WANG Hong, et al. The analysis and feature extraction of nonstationary random characteristics of radar jammer signal[C]// 2002 the 3rd International Symposium on Electromagnetic Compatibility. Beijing, China: IEEE, 2002: 660–663. doi: 10.1109/ELMAGC.2002.1177517.
- [39] CHEN Hua, ZEHNI M, ZHAO Zhizhen. A spectral method for stable bispectrum inversion with application to multireference alignment[J]. IEEE Signal Processing Letters, 2018, 25(7): 911–915. doi: 10.1109/LSP.2018.2831631.
- [40] DEMIRKIRAN I, SAMARASOORIYA V N S, VARSHNEY P K, et al. A knowledge-based interference rejection scheme for direct sequence spread-spectrum systems[C]// 1997 IEEE International Conference on Personal Wireless Communications(Cat. No. 97TH8338). Mumbai, India: IEEE, 1997: 120–124. doi: 10.1109/ICPWC.1997.655491.
- [41] 杨少奇, 田波, 李欣, 等. 基于时频图像特征提取的 LFM 雷达有源欺骗干扰识别[J]. 空军工程大学学报(自然科学版), 2016, 17(1): 56–59. (YANG Shaoqi, TIAN Bo, LI Xin, et al. A recognition method of LFM radar active deception jamming based on SPWVD figure[J]. Journal of Air Force Engineering University(Natural Science Edition), 2016, 17(1): 56–59.) doi: 10.3969/j.issn.1009–3516.2016.01.011.
- [42] XU Jie, YING Shuangshuang, LI Hui. GPS interference signal recognition based on machine learning[J]. Mobile Networks and

- Applications, 2020,25(6):2336–2350. doi:10.1007/s11036-020-01608-1.
- [43] ZHU Keheng, SONG Xigeng, XUE Dongxin. A roller bearing fault diagnosis method based on hierarchical entropy and support vector machine with particle swarm optimization algorithm[J]. Measurement, 2014(47):669–675. .
- [44] CANOVAS J S, KUPKA J. On fuzzy entropy and topological entropy of fuzzy extensions of dynamical systems[J]. Fuzzy Sets and Systems, 2017(309):115–130. doi:10.1016/j.fss.2015.12.013.
- [45] MARWAHA P, SUNKARIA R K. Complexity quantification of cardiac variability time series using improved sample entropy(I-SampEn)[J]. Australasian Physical & Engineering Sciences in Medicine, 2016,39(3):755–763. doi:10.1007/s13246-016-0457-7.
- [46] XU Jie, YING Shuangshuang, LI Hui. GPS interference signal recognition based on machine learning[J]. Mobile Networks and Applications, 2020,25(6):2336–2350. doi:10.1007/s11036-020-01608-1.
- [47] DU Limin, XU Yang, ZHU Hua. Feature selection for multi-class imbalanced data sets based on genetic algorithm[J]. Annals of Data Science, 2015,2(3):293–300. doi:10.1007/s40745-015-0060-x.
- [48] 杜利敏. 面向不平衡数据的特征选择与半监督分类算法研究[D]. 成都:西南交通大学, 2017. (DU Limin. Feature selection and semi-supervised classification for imbalanced data[D]. Chengdu, China: Southwest Jiaotong University, 2017.)
- [49] YANG Bin, DONG Chunxiao, GAO Bo, et al. Research on GNSS interference recognition based on ROI of correlation peaks[J]. International Journal of Satellite Communications and Networking, 2022,40(5):330–342. doi:10.1002/sat.1444.
- [50] 李敏, 李时东, 黄欣. 基于改进SVM的通信干扰识别[J]. 现代电子技术, 2016,39(24):26–29. (LI Min, LI Shidong, HUANG Xin. Communication jamming recognition based on improved SVM[J]. Modern Electronics Technique, 2016,39(24):26–29.)
- [51] 吴昊, 张杭, 路威. 一种面向卫星频谱监测的复合式干扰自动识别算法[J]. 系统仿真学报, 2008,20(17):4681–4684. (WU Hao, ZHANG Hang, LU Wei. Algorithm for compound jamming auto-recognition based on inspecting spectrum of satellite communication[J]. Journal of System Simulation, 2008,20(17):4681–4684.)
- [52] WANG Lanxun, REN Yujing. Recognition of digital modulation signals based on high order cumulants and support vector machines[C]// 2009 ISECS International Colloquium on Computing, Communication, Control, and Management. Sanya, China: IEEE, 2009:271–274. doi:10.1109/CCCM.2009.5267733.
- [53] PARK C S, CHOI J H, NAH S P, et al. Automatic modulation recognition of digital signals using wavelet features and SVM[C]// 2008 the 10th International Conference on Advanced Communication Technology. Gangwon, Korea(South): IEEE, 2008:387–390.
- [54] GUO Yu, MENG Jin, LI Yaxing, et al. Incremental small sphere and large margin for online recognition of communication jamming[J]. Applied Intelligence, 2020,50(10):3429–3440. doi:10.1007/s10489-020-01717-0.
- [55] WEI Yi, OUYANG S R, LI Chao, et al. Hierarchical jamming recognition with spectrum fusion feature and twin-bound SVM for cognitive satellite communications[C]// 2023 IEEE Wireless Communications and Networking Conference(WCNC). Glasgow, United Kingdom: IEEE, 2023:1–6. doi:10.1109/WCNC55385.2023.10119124.
- [56] 徐国进. 典型通信干扰信号识别技术研究[D]. 成都:电子科技大学, 2018. (XU Guojin. Research on identification of typical communication jamming signals[D]. Chengdu, China: University of Electronic Science and Technology of China, 2018.)
- [57] SZEGEDY C, LIU Wei, JIA Yangqing, et al. Going deeper with convolutions[C]// 2015 IEEE Conference on Computer Vision and Pattern Recognition(CVPR). Boston, MA, USA: IEEE, 2015:1–9. doi:10.1109/CVPR.2015.7298594.
- [58] SWINNEY C J, WOODS J C. GNSS jamming classification via CNN, transfer learning & the novel concatenation of signal representations[C]// 2021 International Conference on Cyber Situational Awareness, Data Analytics and Assessment(CyberSA). Dublin, Ireland: IEEE, 2021:1–9. doi:10.1109/CyberSA52016.2021.9478250.
- [59] CHEN Xin, HE Di, YAN Xinyu, et al. GNSS interference type recognition with fingerprint spectrum DNN method[J]. IEEE Transactions on Aerospace and Electronic Systems, 2022,58(5):4745–4760. doi:10.1109/TAES.2022.3167985.
- [60] CHEN Yazhong, SHAN Jingmiao, ZHANG Chuanhao. Communication interference signal recognition based on complex number convolutional neural network[J]. Journal of Physics: Conference Series, 2023(2450):012083.

作者简介:

陈 凤(1999–), 女, 在读硕士研究生, 主要研究方向为电子信息. email:17738592993@163.com.

李 聪(1982–), 女, 博士, 高级工程师, 主要研究方向为卫星通信.

朱立东(1968–), 男, 博士, 教授, 博士生导师, 主要研究方向为卫星通信的传输与组网、星地网络融合等.

吴 琦(1998–), 男, 在读博士研究生, 主要研究方向为卫星通信智能抗干扰.

乐秀权(1971–), 男, MBA硕士, 高级工程师, 主要研究方向为卫星总体设计、卫星及应用.

戴志坚(1968–), 男, 硕士, 教授, 主要研究方向为集成电路测试技术与可测性设计.