# 对抗智能干扰的主动防御技术

冯智斌[1]，徐煜华[1]，杜智勇[2]，刘鑫[3]，李文[1]，韩昊[1]，张晓博[1]
（1. 陆军工程大学通信与工程学院，江苏 南京 210014；2. 国防科技大学信息通信学院，湖北 武汉 430010；
3. 桂林理工大学信息科学与工程学院，广西 桂林 541006）

**摘 要**：在复杂电磁对抗环境下，干扰的智能化发展给无线通信造成了严重威胁，而传统抗干扰方法往往都是被动地调整工作模式或参数，在面对智能干扰时处于劣势甚至被压制。针对此问题，提出了干扰主动防御技术体系架构，旨在通过主动调整己方的通信行为，扰乱干扰的学习过程并降低干扰效能。为了渐进达到“理解对手”“克制对手”“战胜对手”的目的，在博弈论和对抗机器学习理论方法指导下，围绕干扰反向推理、算法脆弱性分析和对抗策略设计、抗干扰策略自主优化和在线决策 3 个方面对关键技术展开论述。最后，结合 2 个具体案例，验证了所提技术架构的可行性和有效性。

**关键词**：智能抗干扰；主动防御；对抗机器学习；博弈论；智能干扰
**中图分类号**：TN975
**文献标志码**：A
**DOI:** 10.11959/j.issn.1000−436x.2022198

# Active defense technology against intelligent jammer

FENG Zhibin[1], XU Yuhua[1], DU Zhiyong[2], LIU Xin[3], LI Wen[1], HAN Hao[1], ZHANG Xiaobo[1]
1. College of Communications Engineering, Army Engineering University, Nanjing 210014, China
2. College of Information and Communication, National University of Defense Technology, Wuhan 430010, China
3. College of Information and Engineering, Guilin University of Technology, Guilin 541006, China

**Abstract:** In the complex electromagnetic countermeasure environment, the intelligent development of jammer has caused a serious threat to wireless communication, while the traditional anti-jamming methods often passively adjusted the working mode or parameters, which will be at a disadvantage or even suppressed in the face of intelligent jammer. To solve this problem, a technical framework of active defense against jammer was proposed, aiming to disrupt the learning process of the intelligent jammer and reduce the jamming efficacy. In order to gradually achieve the goals of “understanding opponent” “controlling opponent” and “defeating opponent”, under the guidance of game theory and adversarial machine learning, the key technologies were discussed from three aspects: backward reasoning of jammer, algorithm vulnerability analysis and confrontational strategy design, independent optimization and online decision-making of anti-jamming strategy. Finally, combined with two specific cases, the feasibility and effectiveness of the proposed technical framework were verified.

**Keywords:** intelligent anti-jamming, active defense, adversarial machine learning, game theory, intelligent jammer

## 0 引言

无线通信的开放和共享在给通信用户带来易于访问和接入等便利的同时，也使通信网络暴露于无线环境中且相比于有线网络更易受到干扰攻击。干扰攻击作为无线通信安全的重要威胁，主要通过辐射电磁信号影响和破坏用户的信号接收过程[1]，使通信性能严重下降。尤其在融入人工智能和通信对抗技术后，智能干扰设备具备感知、学习和决策能力，给无线通信抗干扰技术的发展带来了前所未

**收稿日期**：2022−06−13；**修回日期**：2022−09−25
**通信作者**：徐煜华，xuyuhua@aeu.edu.cn
**基金项目**：国家自然科学基金资助项目（No.62071488, No.61961010）
**Foundation Item:** The National Natural Science Foundation of China (No.62071488, No.61961010)

有的挑战[2-4]。因此，为了保证无线通信的安全性、可靠性和稳定性，本文对复杂电磁环境条件下的智能抗干扰技术展开研究。

近年来，众多研究者开展了智能抗干扰方面的相关研究，主要针对地面[5-7]、无人机[8-9]、卫星[10-11]、水下[12-13]等不同通信场景下的抗干扰问题，聚焦功率域[5-6]、频率域[7]、空间域[14-15]、编码域[16-17]、链路域[18-19]等维域，以能够应对干扰攻击或降低干扰的影响为目的，在“抗避消隐”[20]理念的指导下，通过跳时跳频、功率调整、波束成形、编码设计、链路优化等手段，利用机器学习、凸优化、博弈论等理论方法[21]，不断调整优化通信策略，在具体问题中取得了较好的抗干扰效果。

然而现有工作主要存在以下两点不足：1) 现有抗干扰研究通常将干扰视为一种动态的环境或客观存在且无法改变的对手，单方面地聚焦于如何对抗干扰攻击而忽略了双方之间的内在联系；2) 现有工作往往都是在干扰环境下被动调整工作模式或参数，随着干扰智能性的增强以及对抗双方之间算法能力差距的减小，通信方将处于劣势甚至被压制。

为此，本文转变传统的被动抗干扰思路，针对动态干扰及智能干扰，提出了一种通用的干扰主动防御架构，如图 1 所示。智能干扰具有环境认知、智能决策和干扰实施 3 个步骤。传统的抗干扰工作所采用的抗避消隐等手段都是针对已经实际产生的干扰行为，通过己方的被动适应来对抗干扰或降低干扰的影响。而主动防御的核心在于深入分析智能干扰的运行机理，自主挖掘干扰智能算法的固有局限性和脆弱性，前移抗干扰阵地，在干扰生效之前实施对抗策略，主动调整己方的通信行为来扰乱干扰方的学习过程，令干扰方做出错误决策，以降低干扰效能甚至使其完全失效，最终实现主动抗干扰的目的。

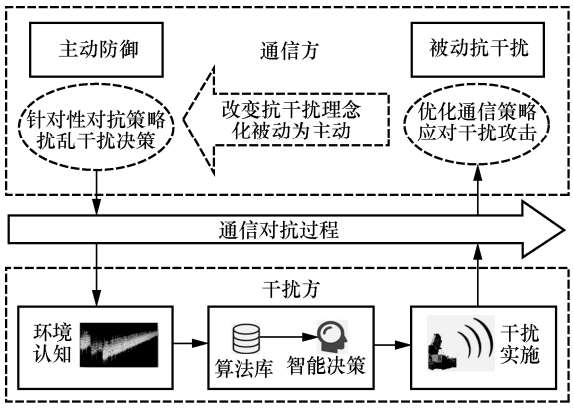



图 1　干扰主动防御架构

## 1　研究进展与挑战

本节对现有关于智能抗干扰方面的研究进行阐述和总结，并就未来智能抗干扰技术的发展梳理了可能会面临的挑战。

### 1.1　现有研究工作

传统的无线抗干扰技术主要包含三类：一是干扰躲避的方法，即将待传信号变换到与干扰信号不同维度的信号空间来躲避干扰，包括跳频扩频、跳时扩频、直接序列扩频等[22-25]；二是干扰消除的方法，即通过信号处理尽可能地消除接收信号中混杂的干扰信号，包括自适应滤波、盲源分离等[26-27]；三是干扰硬抗的方法，即通过调整传输功率来提高接收端的信号强度[28-29]。然而随着干扰的硬件设备能力和智能决策能力的增强，传统的抗干扰技术愈发难以保证无线通信的可靠传输。在此背景下，认知无线电和人工智能技术[30]在无线通信领域的应用与发展，显著提高了通信系统的抗干扰能力。此外，正如文献[30]所指出，智能抗干扰技术是一个庞大的技术体系结构，包括干扰认知、抗干扰波形重构、可靠信令传输、抗干扰智能决策等多个方面。下面主要就频谱域下的智能抗干扰方面的工作进行总结。

随着机器学习技术在无线通信领域的广泛应用，以强化学习为代表的方法被广泛应用于抗干扰工作中。现有频谱域下的抗干扰工作[31-33]以面向梳状、扫频、规律性阻塞、组合等常规干扰模式为主，采用 Q 学习等强化学习方法学习干扰变化规律，优化通信方的频率、功率和波束等策略，达到抗干扰的效果。然而，传统的强化学习方法主要应用于状态空间和策略空间较小的问题研究，状态空间和策略空间的提升会导致决策收敛速度降低甚至无法收敛，难以满足实时决策要求。为此，基于深度强化学习的抗干扰方法[34-36]成为了近年的研究热点，它同时结合了深度学习的特征提取能力和强化学习的决策能力，能够有效解决维数灾难这一难题，并广泛应用于通信对抗、无线资源分配等领域。然而，基于强化学习的抗干扰方法所面临的最大局限是当通信用户的环境状态不能满足马尔可夫特性时，相关方法不仅缺乏理论依据，甚至可能无法收敛。

除了机器学习方法在智能抗干扰领域大放异彩外，考虑通信对抗双方的非合作关系，博弈论[37]也可

以很好地分析多个相互影响的个体间的行为决策及均衡问题。早期，零和博弈[38]和非零和博弈[39]被用来建模用户和干扰之间的对抗关系，双方各自以最大化自身效用为目标，找到均衡解下的对抗策略。进一步，考虑通信方和干扰方之间的分层行为特性，Stackelberg 博弈被大量工作用来建模两者之间的主从关系，在 Stackelberg 博弈框架下，利用凸优化、强化学习等方法，在干扰环境下优化功率或信道策略，最大化通信方传输效用[40-43]。虽然博弈论能够从理论层面较好地刻画通信对抗双方的对抗决策关系，并指导设计相关均衡策略的求解算法，但往往假设用户和干扰都知道对方的决策效用模型，过于依赖先验信息或严苛的前提假设，在实际应用中仍然具有很大的局限性。

综上所述，现有智能抗干扰工作在算法层面和理论层面均得到了良好的发展，相关工作在特定干扰环境下均实现了理想的抗干扰效果，但仍然存在很多可以改进完善的地方。除了上述基于机器学习或博弈论的抗干扰方法的局限性之外，本文进一步总结了现有智能抗干扰工作的 2 个共性问题。

1) 现有的抗干扰理念通常都是被动反应式的

目前比较常见的抗干扰思路是在时间、频率、空间等维域躲避干扰，或者通过增加功率、降低解调门限等手段尽可能弱化干扰带来的影响，本质上都属于被动反应式抗干扰手段。这些手段虽然也能达到一定的效果，但忽略了通信方与干扰方之间的内在联系，即干扰本身也会受通信行为影响。对通信方而言，与其始终受制于干扰，不如化被动为主动，主动出击才能始终在对抗过程中保持优势。

2) 现有工作考虑的干扰对手往往都是弱智能的

现有抗干扰研究中考虑的干扰模式往往不能算作真正意义上的智能干扰，可以涵盖为以下两类：①具备感知和自适应决策能力（如以某种固定的模式或规律调整干扰功率、信道等参数）的干扰；②虽然也有部分工作将基于强化学习的干扰作为对手，同时考虑通信方能够使用深度强化学习方法，拥有更高的状态和策略空间，以更强的算法取胜，该类工作没有把对抗双方放在一个对等的位置上考虑，本质上仍假设通信方相较于干扰方是更加智能的。

### 1.2 主要挑战

基于上述对现有工作的总结，针对未来的智能抗干扰技术，本文从对抗背景、抗干扰需求和信息约束 3 个方面，梳理出以下 3 个核心挑战，并提出对应的解决思路。

1) 智能化干扰提升了对抗强度和难度

近年来，有关干扰效能评估的研究在一定程度上突破了干扰效果反馈困难的限制，有力推动了智能干扰技术的发展。基于决策智能水平差异将干扰划分为动态适变干扰和预测学习干扰，其中，前者智能性较弱，主要包括复合干扰、跟踪干扰和欺骗干扰等；后者智能性较强，能够基于实时的频谱态势，采用深度学习、强化学习等人工智能算法，通过感知–学习–决策–评估等手段，预测通信行为并确定干扰策略。可以预见，干扰方的智能化发展将加剧通信方所面临的对抗强度和难度。当对抗双方都具备认知和智能决策能力时，对抗过程将呈现出动态多阶段、复杂演变等特性。为梳理智能通信对抗的数学机理，需要在交错争夺条件下构建对抗博弈模型，设计科学的对抗性效用函数，指导对抗策略的求解。

2) 研究自主优化的针对性抗干扰手段迫在眉睫

在复杂未知的通信对抗环境下，干扰模式或策略会随着通信策略的变化而动态切换，且不同干扰模式的决策机理各不相同，导致现有很多特定场景、特定干扰条件下的抗干扰方法已无法满足可靠通信需求，几乎不存在一种通用性的抗干扰策略。因此，为保证通信方抗干扰策略的长期有效性，研究能够自主优化的针对性抗干扰手段迫在眉睫。首先，非合作对抗条件下的干扰实时认知是实现智能抗干扰的前提；其次，针对不同干扰类型，需要分析其决策机理并挖掘固有局限性，通过“弱点剖析、对手模拟、虚拟训练”等方式，快速设计出高效的针对性对抗策略，并随着干扰对手的变化进行快速适配与自主优化调整，保证通信方在长期对抗中的决策优势。

3) 非合作对抗场景下存在多元信息约束

由于通信对抗双方之间天然的非合作关系，通信方将面临来自环境、干扰对手甚至己方的诸多信息约束。一是对频谱环境信息的稀缺，受限于设备感知能力不足等问题，通信方通常需要花费大量的时间来获得充足的频谱态势信息，在短时学习训练过程中将面临数据小样本的挑战；二是对干扰对手信息的未知，在缺乏关于干扰方先验信息的条件下，难以准确地识别出干扰模式甚至推理出其背后的智能学习算法类型；三是己方用户间信息交互困难，随着网络规模的扩大，如果缺乏有效的协调和

交互机制，将导致系统多用户之间决策冲突加剧、网络内部互扰严重。面对诸多信息约束，同样需要设计针对性的方法来增强频谱环境、干扰对手等数据信息或降低信息约束带来的影响，保证抗干扰策略的有效性。

## 2　干扰主动防御技术

针对现有工作的不足和当前面临的主要挑战，受反智能化作战研究[44]的启发，本节提出了一种面向智能干扰的干扰主动防御技术体系架构，如图 2 所示。针对具备感知–学习–决策–评估能力的智能干扰，深入分析其背后的运行机理，综合运用博弈论[37]、机器学习[45]和对抗机器学习[46]等理论和技术方法，突破干扰反向推理、算法脆弱性分析和对抗策略设计、抗干扰策略的自主优化与在线决策等关键技术，通过挖掘干扰规律、伪造虚假目标主动诱骗、打乱己方通信特征和自主生成对抗策略等方式，针对性设计能够降低干扰认知效率和决策准确性的抗干扰策略，以影响干扰的学习过程并降低干扰效能，实现主动抗干扰。

干扰主动防御的核心在于在博弈论和对抗机器学习的理论与技术框架指导下，化被动为主动，通信方主动出击来达到扰乱智能干扰的目的。其中，博弈论用来建模双方之间的博弈对抗机理，抗干扰本质是为了同时减少内部自扰和外部干扰的多主体自主决策，因此在进行主动防御策略设计及决策过程中，博弈论可以提供全局视角的分析工具，通过对通信对抗过程和预期效果的建模分析，进一步优化抗干扰策略和行动。而对抗机器学习用来指导设计面向智能干扰的抗干扰技术，它来源于机器学习与计算机安全的交叉领域，旨在攻击机器学习的脆弱性，阻碍其正常运行。

下面主要从干扰反向推理、脆弱性分析和对抗策略设计、抗干扰策略自主优化和在线决策 3 个方面，对所提干扰主动防御技术体系架构进行详细的论述。

### 2.1　干扰反向推理

识别出干扰模式甚至智能算法类型是进行主动防御的首要前提。由于无法直接获得先验信息，通信方需要从干扰与外部环境的相互作用过程进行学习分析和反向推理。然而在实际通信对抗过程中，受限于设备感知能力和反应时间，通信方面临频谱态势感知不完全、样本数量少等技术挑战，因此如何实现小样本条件下的干扰模式识别和智能算法反向推理是这一环节的核心内容。

#### 2.1.1　频谱态势生成

针对可用频谱态势样本信息较少的问题，可使用生成对抗网络[47]或孪生神经网络[48]实现频谱态势生成与获取。以生成对抗网络为例，利用对抗机制和神经网络快速拟合数据的优势，基于感知获取得到的小样本频谱态势数据，经过在线学习和训练，不断调整网络结构和参数，提高生成器的数据拟合能力，准确地生成大量有效数据，从而解决频谱态势数据小样本的挑战。

#### 2.1.2　干扰模式识别

干扰模式识别一直都是信号识别领域的一个主要研究方向，这里给出了基于神经网络和基于相关性分析的 2 种识别思路。现有基于卷积神经网络的干扰信号识别方法[49-50]已经取得了很好的效果，在神经网络的基础上可以进一步结合小波变换、支

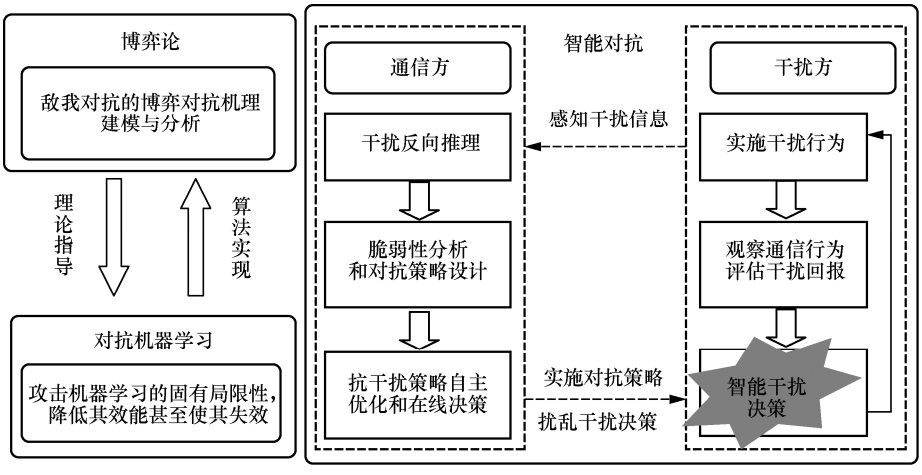



图 2　干扰主动防御技术体系架构

持向量机等方法，提高分类的准确性。然而现有大部分工作假设待识别干扰模式集与训练阶段的模式集完全相同。但实际对抗场景中干扰模式未知多样，需要识别的模式往往超出了训练阶段的模式范围，导致现有的识别方法难以达到满意的效果。在此背景下，基于零样本学习[51-52]的干扰模式识别是一种可行的思路，针对开集识别的挑战，该方法基于有限类别的标签数据，学习已知模式的潜在特征表示，保证最小化类内距离的同时最大化类间距离；并设计基于特征距离的分类准则，从而达到在特征空间内同时识别已知和未知干扰模式的目的。

另一种思路是针对不同干扰模式在时域、频域、编码域等维域上的相关性[53]差异对干扰模式进行识别。利用深度学习等方法提取一段时间内干扰的频率、信号等特征，通过对不同特征下通信与干扰行为之间的相关性进行度量划分，识别对应的干扰模式。例如，弱相关状态对应复合干扰，由于复合干扰遵循固定的模式或规律，因此与通信策略无直接关系。强相关状态可进一步划分为信号相关和时频相关，其中，信号相关对应转发干扰，因为干扰将收集到的通信信号进行加工再转发的方式使接收端重复接收信号。时频相关状态对应跟踪干扰和智能干扰，其中，跟踪干扰的反应通常具有一定的滞后性，而智能干扰能够通过“预测+学习”主动实现与通信信号的同步跳变。

#### 2.1.3 智能算法反向推理

针对智能干扰，通信方期望能够基于真实的通信态势和所做假设来解释干扰随通信行为变化的现象，并推理出其背后的决策算法，这是一个开放性且颇具难度的问题。一种比较直观但存在局限的可能方法是针对几种典型算法（如强化学习、深度学习等）的运行原理，以特定的通信模式（如扫频通信等）来试探干扰，通过故意添加扰动（如改变扫频的序列、速率或带宽），获取干扰行为并分析其反应变化快慢、干扰效果好坏等，以实现对干扰智能决策算法的有效推理。

从更高层面上对该问题进行探讨，可以借鉴由机器学习领域专家周志华教授[54]提出的反绎学习（也被称为溯因学习），即在一个统一的框架下将机器学习和逻辑推理以“相对均衡”的方式结合起来，更充分地发挥各自的优势，也给智能算法反向推理提供了一个可行的思路。通信方基于其掌握的有限的关于智能干扰算法的知识，通过主动改变通信方的部分行为来观察干扰行为的变化，然后从信息不完备的角度出发，挖掘通信变化与干扰行为之间的潜在联系，做出推理与假设，并根据已有知识来寻找一个最可能的解释，最终反向推理出智能算法类型。

### 2.2 脆弱性分析和对抗策略设计

脆弱性分析和对抗策略设计是干扰主动防御的关键环节，其核心在于基于识别或推理得到的干扰类型及算法，深入分析不同干扰类型及其运行规律中潜在的弱点，从频率、功率、编码等多个维度出发，综合运用隐蔽、欺骗、对抗和利用等多种手段，设计针对性的能够扰乱干扰算法执行条件或显著降低算法运行效率的对抗策略，从而构建能够应对不同干扰的抗干扰策略库。

需要注意的是，根据 1.2 节中对智能化干扰威胁的介绍，本文主要基于决策智能水平差异划分并考虑了 2 种干扰类型：动态适变干扰（复合、跟踪和欺骗干扰，智能水平较弱）和预测学习干扰（基于深度学习、强化学习和迁移学习的干扰，智能水平较强）。本节具体针对不同干扰类型，设计针对性对抗策略。

#### 2.2.1 对抗动态适变干扰的主动防御技术

面向智能水平较弱的动态适变干扰，针对复合干扰决策规律相对固定、跟踪干扰被动跟随己方通信跳变、欺骗干扰硬件容差无法篡改的弱点，设计针对性抗干扰手段，实现对抗动态适变干扰的主动防御技术，如图 3 所示。

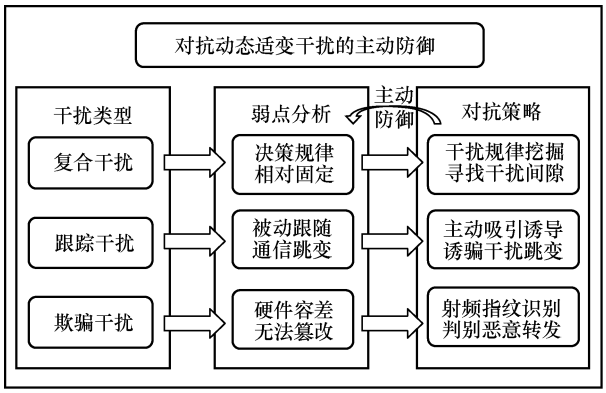



图 3 对抗动态适变干扰的主动防御技术

1) 基于干扰规律挖掘的抗复合干扰

复合干扰由梳状干扰、扫频干扰、规律性阻塞干扰等动态组合而成[7]，能够动态自主地切换干扰模式，其脆弱性体现在干扰模式具有较强规律性，易被智能学习算法挖掘利用。针对复合干扰决策规

律相对固定的弱点，本节提出基于干扰规律挖掘的抗复合干扰方法。利用深度强化学习算法，通过感知、生成、预测和动态频谱接入决策一体化设计，挖掘干扰间隙进行通信，实现主动避扰。该方法融合了复杂环境下深度学习特征提取能力强和动态环境中强化学习在线决策的优点，可克服环境及动作状态空间巨大的挑战，输入当前频谱状态信息，即可直接输出下一时刻的最优通信频率，实现抗干扰可靠通信。

2) 基于主动吸引诱导的抗跟踪干扰

跟踪干扰通过侦察感知通信信号的改变而调整干扰频率以实现对通信信号的实时跟踪和攻击[55]。面对跟踪干扰，在通信设备硬件频谱捷变能力无优势的情况下，通信效能将大幅降低甚至被压制。然而，跟踪干扰只能被动跟随用户进行频谱切换，且具有明显的攻击偏好（如偏向于攻击高功率通信信道、控制信道或关键节点）。针对该弱点，本节提出基于主动吸引诱导的抗跟踪干扰方法，部分用户牺牲自身通信效能，通过发送高功率信号主动吸引干扰攻击，为其余用户留出空闲信道并伺机传输。此外，在该方法执行过程中，选出哪些用户吸引干扰攻击、哪些用户能够通信，还需要相应的公平性机制或补偿机制设计，以保证系统的正常运行。

3) 基于射频指纹识别的抗欺骗干扰

转发式欺骗干扰对感知接收到的通信信号进行加工后转发，或者直接发射仿制合成的通信信号，以诱骗合法接收端持续接收非法信号，降低通信质量[55]。然而转发干扰发射机与用户发射机硬件容差会引起调制误差（如 I/Q 偏移、频偏、幅度误差等），且这些误差特征难以被篡改。针对该弱点，考虑将硬件容差引起的调制误差作为射频指纹，本节提出基于射频指纹识别的抗转发干扰方法。考虑发射机的硬件容差在 I/Q 数据上表现为幅度和相位的偏移，利用发射机独特的 I/Q 数据分布建立发射机射频指纹[56]。通过生成对抗网络的对抗性学习，判别器学习到可信发射机特有的 I/Q 数据分布特性，掌握可信发射机的射频指纹。当接收到未知的 I/Q 数据时，判别器判断其是否来自合法发射机，从而实现对无线发射机的身份识别和接入认证，在接收端区分合法信号和恶意转发信号。

### 2.2.2 对抗预测学习干扰的主动防御技术

面向智能水平较强的预测学习干扰，剖析不同学习算法决策机理的弱点，考虑深度学习干扰的神经网络具有高度非线性特征、强化学习干扰的状态−动作−回报学习机理固定、迁移学习干扰对算法源域与目标域的共性要求高等局限性，在对抗机器学习的理论与技术指导下，从不同算法的脆弱环节入手，设计针对性抗干扰手段，实现对抗预测学习干扰的主动防御技术，如图 4 所示。

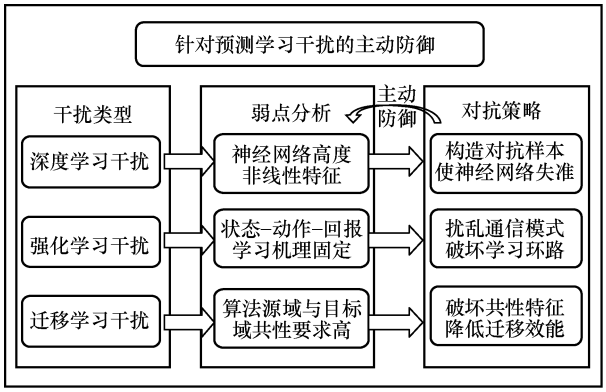



图 4　对抗预测学习干扰的主动防御技术

1) 基于对抗样本构造的抗深度学习干扰

面向基于深度学习的干扰[57]，考虑深度神经网络的高度非线性特征和监督学习模型中的不充分正则化特征容易导致学习过程出现过拟合的问题。针对深度学习识别算法易受微小扰动而失效的弱点，本节提出了基于对抗样本构造的抗深度学习干扰方法。通过在通信信号上添加微小扰动，使深度神经网络将对抗样本判别为错误分类结果，在尽可能降低对己方通信性能影响的同时，降低智能干扰系统的感知和识别能力。具体而言，可以使用快速梯度法或梯度迭代法构建通用对抗扰动样本，在最小化对抗样本与真实样本之间范数距离的同时最大化神经网络针对对抗样本的误分辨率；最后基于己方构建的干扰神经网络根据对抗样本的判别结果和能够使其产生误判的反馈结果调整己方构建干扰的网络结构和参数，使其能够以较大概率欺骗具有不同体系结构的深度学习模型；最后生成混有扰动的通信对抗样本信号，使智能干扰在识别通信方信号特征（频点、调制方式、波形等）时产生误识别，从而破坏干扰的认知决策能力。

2) 基于学习环路破坏的抗强化学习干扰

采用强化学习的智能干扰[58]无须对通信模式进行估计与预测，可实现对通信方感知、学习、干扰的一体化设计，常规通信抗干扰方法难以与其对

抗。强化学习环包括状态、动作和收益评估 3 个环节，任何一个环节出错都将导致强化学习方法失效。因此，从干扰的状态感知和回报获取环节入手，本节提出了基于学习环路破坏的抗强化学习干扰方法。具体包括以下 2 个方面。

① 针对干扰方观测的扰动，强化学习干扰为了获得最优干扰策略，需要通过试探的方式来积累经验、学习通信规律。为此，可设计无规律联系的通信变化模式，其核心在于破坏通信行为之间的马尔可夫特性，使干扰系统一直处于学习阶段，降低其干扰效能。

② 针对干扰方收益的欺骗，智能干扰通过观察实施干扰前后通信方的动作变化（如切换频率、变化波形等）来评估干扰收益，即将干扰效能建模为通信行为观察状态的函数。针对这一特性，本节提出了攻击干扰效能评估函数的方法，例如，通信方未被干扰时依概率切换通信模式、被干扰时依概率不切换通信模式，使干扰收益评估出错，从而破坏强化学习的环路。

3) 基于共性特征扰乱的抗迁移学习干扰

迁移学习干扰能够在通信环境动态变化、通信数据不足的情况下，通过模型、算法和样本等信息迁移，实现新环境下的快速有效干扰，成为未来通信方的重要对手。然而，迁移学习的有效性主要取决于源域和目标域之间存在共性特征这一必要条件。因此，针对模型迁移、特征迁移等常见的迁移学习方法，本节提出了基于共性特征扰乱的抗迁移学习干扰方法。通过添加欺骗信号或人工噪声等方式扰乱目标域的数据信息，主动破坏不同通信场景之间的共性特征，从而破坏干扰算法的可迁移性，使干扰机的迁移学习算法失效甚至产生负向迁移效果，令其无法适应新的通信对抗环境。

### 2.3 抗干扰策略自主优化和在线决策

在实际智能通信对抗过程中，双方都不会固定地使用某种模式或策略，两者理应都具备动态调整能力，即能够根据对方的行为以及环境和即时回报的变化调整策略（这里的调整策略指的是更加宏观的调整，如干扰方切换干扰模式，或者通信方切换针对性抗干扰策略）。因此，即使某种抗干扰策略在短期内有效对抗干扰，干扰可通过实时效果评估重新调整干扰类型或优化干扰算法，如果己方通信系统缺乏自主在线学习能力，将难以获得长期稳定的抗干扰效果。

综上，理想情况应该是双方始终处于博弈对抗的均衡状态。根据不同的场景和阶段，即使在面对具备感知、学习和智能决策能力的干扰系统时，通信方也能够根据干扰算法类别和抗干扰通信效果反馈，自主在线进行抗干扰策略的选择和调整，在动态多阶段的对抗过程中始终占据优势，实现可靠通信。

为了实现上述目的，考虑多阶段抗干扰过程中对抗双方的动态演化和复杂特性，本节提出抗干扰策略自主优化和在线决策过程，如图 5 所示。首先，构建干扰主动防御策略库，主要包括干扰规律挖掘、主动吸引诱导、射频指纹识别、对抗样本构造、学习环路破坏以及共性特征破坏等针对性策略，以此为基础组成混合策略集。然后，根据当前干扰推理结果和抗干扰效果，不断优化抗干扰策略决策，在智能通信对抗的过程中学习获得与当前的干扰模式最匹配的抗干扰策略（如干扰规律挖掘等）。进一步，在当前抗干扰策略指导下，动态调整抗干扰动作（如优化通信频率、功率等），最终达到最佳的抗干扰效果。

综上，所提干扰主动防御架构主要包括 3 个部

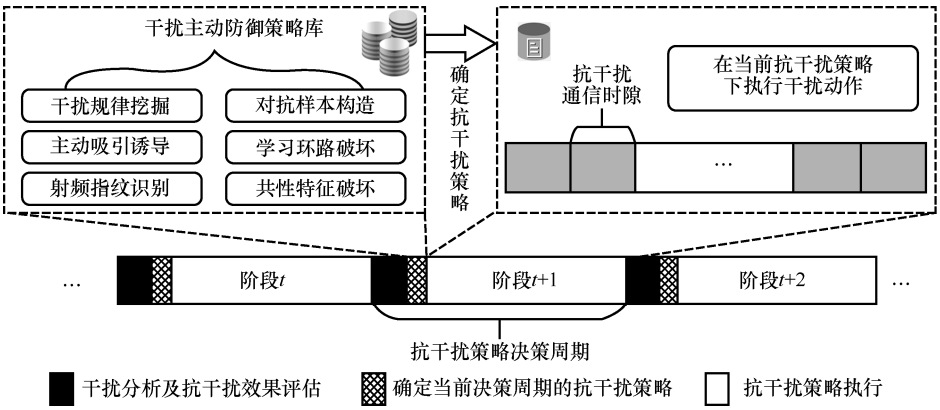



图 5 抗干扰策略自主优化和在线决策过程

分，其中，干扰反向推理表示对干扰的认知过程，是首要前提；脆弱性分析和对抗策略设计表示在面对不同干扰对手时形成不同的对抗策略，是核心要素；抗干扰策略的自主优化和在线决策表示在整个对抗过程中的决策优化过程，是关键环节。这 3 个部分顺序相接，形成闭环。相关技术如深度强化学习、对抗机器学习等都已经具有比较完备的理论基础。在体系架构的硬件实现方面，一方面可以设计低复杂度的算法，尽量设置在常规多核 CPU 运算速度的 $10^{10}$ 量级或 GPU 运算速度的 $10^{12}$ 量级以下；另一方面，随着近年来基于软件无线电平台的通信系统构建技术日益成熟，其频率、功率和调制编码的动态可重构能力在硬件实现上提供了很好的保障能力，其难点主要在于算法与平台适配，即如何实现仿真算法到硬件平台的适配与迁移，需要深入设计和研究。但整体而言，所提技术体系架构在理论算法层面是可行且有效的，且具有良好的工程可实现性。

## 3　案例分析

本节结合研究团队前期的工作，分别就干扰模式识别[52]和基于主动诱导机制的抗跟踪干扰[59]2 个部分给出具体案例和分析。

### 3.1　基于零样本学习的干扰模式识别

现有干扰识别方面的研究大多基于闭集假设，即识别阶段的所有类别均在训练阶段已知且有对应的标签数据。然而在实际无线通信场景中，干扰识别问题更多的是开集问题，导致传统基于闭集的识别方法[49-50]性能严重下降。为此，本节研究了同时针对已知和未知模式的干扰识别问题。考虑一个无线通信干扰场景，未知干扰模式识别系统模型如图 6 所示。该场景包括一个用户、一个干扰机和一个感知设备，感知设备附带一个智能体。干扰机通过释放高功率的干扰信号破坏用户的通信。感知设备持续地感知频谱，并在智能体的辅助下基于感知结果识别干扰模式。

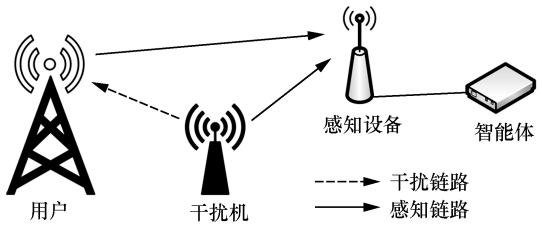



图 6　未知干扰模式识别系统模型

在 $t$ 时刻，感知设备感知到的频谱向量为 $\boldsymbol{o}_t=[p_{t,1},p_{t,2},\cdots,p_{t,N}]$，其中，$N=\dfrac{B}{\Delta f}$ 为频谱感知的采样点数，$B$ 为带宽，$\Delta f$ 为频谱感知的分辨率，$p_{t,1},p_{t,2},\cdots,p_{t,N}$ 分别表示 $t$ 时刻不同频率处的采样值。受文献[7]的启发，引入历史时刻感知到的频谱向量的序列即频谱瀑布图来刻画不同的干扰模式的多域特征，其数学表达式为 $\boldsymbol{O}_t=\left[\boldsymbol{o}_t,\boldsymbol{o}_{t-1},\cdots,\boldsymbol{o}_{t-L+1}\right]$，其中 $L$ 表示序列的长度。

针对未知干扰模式的零样本识别问题，设计了一种包含监督训练、无监督分类的零样本识别方法[52]，总体框架如图 7 所示。在监督训练阶段，利用已知干扰模式的频谱瀑布图样本训练编码器，训练目标是学习已知干扰模式数据在潜在特征空间内的特征表示；在无监督分类阶段，设计了一种基于欧氏特征距离的无监督分类准则，在特征空间内按照该准则同时对已知和未知的干扰模式进行分类，基于有限类别的标签数据，学习已知模式的潜在特征表示，在保证最小化类内距离的同时最大化类间距离，能够有效应对未知的干扰模式，获得较高的识别准确率。

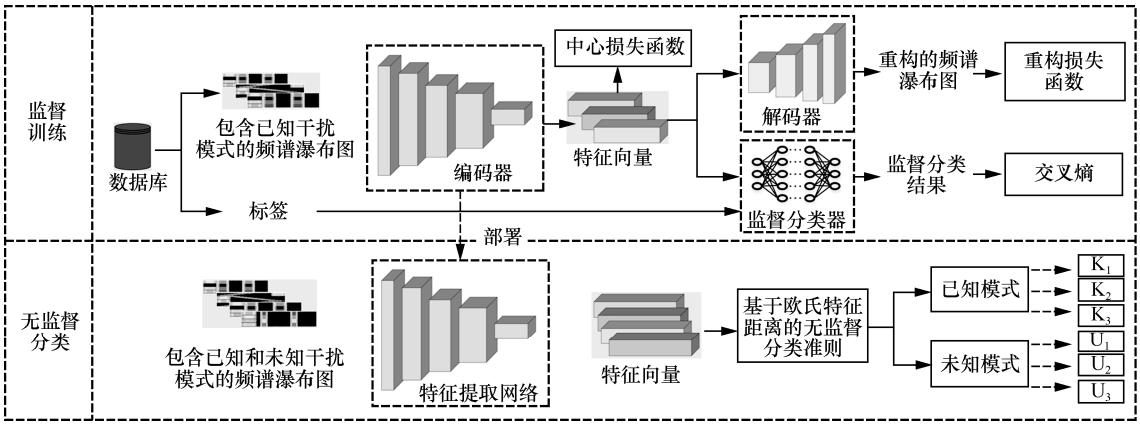



图 7　未知干扰模式零样本识别方法总体框架

在仿真过程中考虑 5 个非重叠信道，每个信道的带宽为 4 MHz。用户按照时隙基于感知结果选择空闲信道进行通信，感知和传输时隙的长度分别为 1 ms 和 4 ms，发射功率为 0 dBm。感知设备每 1 ms 进行一次全频段感知，感知的频率分辨率设置为 100 kHz。智能体利用当前和过去 40 ms 的感知结果来识别不同的干扰模式。考虑 3 种已知干扰模式（扫频速率为 1 GHz/s 的扫频干扰 $K_1$ 和双扫频干扰 $K_2$，干扰信号带宽为 4 MHz 的梳状干扰 $K_3$）和 3 种未知干扰模式（干扰信号带宽为 2 MHz 的梳状干扰 $U_1$，跟踪干扰 $U_2$，扫频速率为 4 GHz/s 的扫频干扰 $U_3$）。在监督训练阶段，训练数据集中仅包含 3 种已知干扰模式的样本；在测试阶段，测试集同时包含 3 种已知干扰模式和 3 种未知干扰模式的样本。编码器、解码器和监督分类器的学习率的初始值分别设置为 0.005、0.001 和 0.001，干扰模式特征中心的更新率初始值设置为 0.1。

首先，引入扰信比（JSR, jamming-to-signal ratio）来刻画干扰功率和背景信号功率的相对关系，JSR 的定义为 $\mathrm{JSR}=10\log\left(\frac{p_\mathrm{J}}{p_\mathrm{S}}\right)$，$p_\mathrm{J}$ 和 $p_\mathrm{S}$ 分别代表干扰和背景信号的功率。其次，图 8 给出了扰信比为 10 dB 时的混淆矩阵，用来判断对于已知和未知干扰模式的识别精度。对于已知的干扰模式 $K_1$～$K_3$，识别准确率可以达到 100%。对于未知的干扰模式 $U_1$～$U_3$，识别准确率略有下降，存在少量将 $U_2$ 识别为 $K_1$ 或将 $U_3$ 识别为 $K_1$ 的错误情况，但整体上仍然可以实现较好的识别效果。此外，识别准确率还和扰信比有关，当扰信比在–10~30 dB 之间并以 10 dB 的间隔变化时，随着扰信比的降低，整体的分类性能略有下降，这是因为扰信比的降低会提高对模式特征区分的难度。

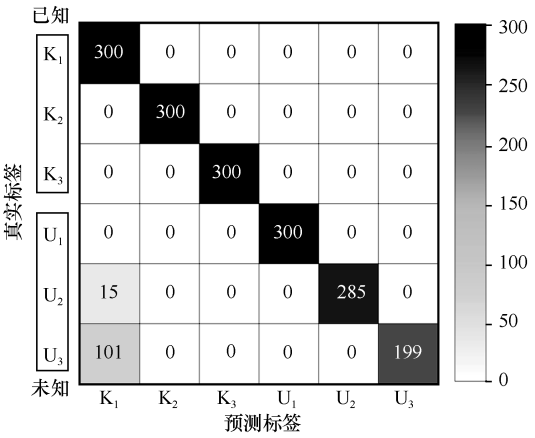



图 8　扰信比为 10 dB 时的混淆矩阵

### 3.2　基于主动诱导机制的抗跟踪干扰

现有功率域或频域方面的抗干扰工作往往通过功率调整硬抗[5-6]或跳频躲避[31-33]的方式实现抗干扰通信，但在面临具有高功率压制能力的跟踪干扰时，上述方法将不再适用。为此，针对强跟踪干扰环境下的抗干扰通信问题，本节提出了一种基于主动诱导机制的智能抗跟踪干扰方法[59]。考虑一个中继通信抗干扰网络中存在多个用户收发对、多个中继和一个移动的跟踪干扰机，如图 9 所示。每个用户都有唯一对应的目的接收端，其目的是在干扰环境中通过选择合适的中继将消息发送至合法接收端。干扰机具备信道感知能力和功率压制能力，按照一定的路径进行移动，在移动过程中选择其检测到能量信号最大的信道，并在该信道上释放噪声干扰攻击。

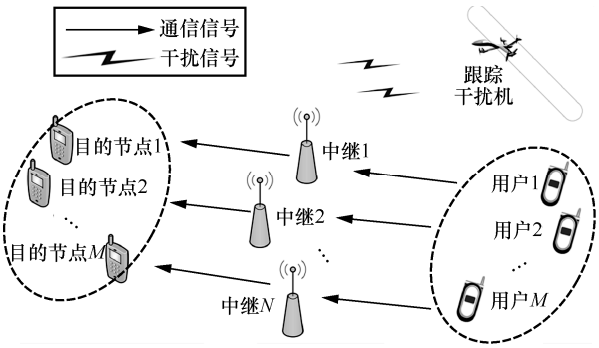



图 9　跟踪干扰环境下的中继通信抗干扰网络

中继采用放大转发的工作模式，则用户 $m$ 的发射端与其接收端之间的传输速率为 $C_m=\frac{B}{2L_{r_m}}\log\left(\frac{1+\mathrm{SINR}_{u_m,r_m}\mathrm{SINR}_{r_m,d_m}}{(1+\mathrm{SINR}_{u_m,r_m}+\mathrm{SINR}_{r_m,d_m})}\right)$，其中，$B$ 表示信道带宽，$L_{r_m}$ 表示和用户 $m$ 选择了相同中继的用户数量，$\mathrm{SINR}_{u_m,r_m}$ 表示中继 $r_m$ 接收来自用户 $m$ 信号的信干噪比，$\mathrm{SINR}_{r_m,d_m}$ 表示用户 $m$ 接收端的信干噪比。根据文献[60]，考虑用户 $m$ 的传输速率需求为 $C'_m$，则其传输满意度指标为 $\psi_m=\frac{1}{\left\{1+\exp\left[-\lambda_m(C_m-C'_m+\frac{\nu}{\lambda_m})\right]\right\}}$，其中 $\nu,\lambda_m$ 都是常数，用来表示系统对传输需求的要求程度。系统的优化目标为最大化所有用户的传输满意度 $\max\sum_{m=1}^{M}\psi_m$。

针对跟踪干扰被动跟随的特性，本节设计了一种基于双阶段中继选择的主动诱导机制。在没有中心控制的情况下，所有分布式用户在每个时隙共同选出一个中继主动释放伪通信信号来吸引干扰攻击，从而使用户能够通过其他中继与接收端进行通信。每个中继既可以转发用户通信信息，也可以主动发送伪通信信号吸引干扰机。

在双阶段中继选择过程中，首先，考虑干扰机始终处于周期性的移动状态，所以干扰机在移动过程中的干扰策略和用户、中继位置之间存在对应关系，因此将用户的诱导中继选择决策过程建模为马尔可夫决策过程，用户利用 Q 学习方法来探索学习干扰机在不同位置上的干扰规律，从而优化诱导中继选择策略。每个用户将各自的诱导中继选择结果发送给相应中继。需要注意的是，中继只有收到不少于一半用户数量的请求时才会认可该请求，并主动释放伪通信信号吸引干扰攻击，否则拒绝该请求。这样设计的目的是在分布式条件下达成诱导中继选择共识，且避免了过多中继都吸引干扰攻击而造成通信资源浪费。其次，所有用户利用随机自动学习机（SLA, stochastic learning automata）方法[61]进行分布式决策，在除诱导中继以外的集合中选择通信中继。

在仿真过程中，考虑设置用、中继和信道的数量都为 4，背景噪声密度为–174 dBm/Hz。所有用户的发射功率为 23 dBm，所有中继的发射功率为 30 dBm。每个信道的带宽为 1 MHz，用户的传输速率需求为 1 Mbit/s，路径衰落因子 $\varphi$=2，学习速率 $\alpha$=0.8，迭代步长 $b$=0.1。用户 1~用户 4 的发射端分别位于 (0.5 km, 4.5 km)、(0.5 km, 3.5 km)、(1 km, 4 km)、(1.5 km, 4 km)，接收端分别位于(4 km, 1.5 km)、(3.5 km, 0.5 km)、(3.5 km, 1 km)、(3.5 km, 1.5 km)；中继 1~中继 4 分别位于(1.5 km, 2.5 km)、(2km, 3km)、(2.5 km, 3.5 km)、(2.5 km, 3 km)。干扰机的起点和终点分别位于(3.5 km, 4 km)和(4 km, 3 km)，并以 10 m/s 的速度在两点之间往返移动。

图 10 分别给出了有无诱导机制下的用户传输满意度，并分析了当干扰机处于不同位置时的变化情况。从图 10(a)可以看出，在没有诱导机制的条件下，每次至少存在一个中继的转发信息被干扰机干扰，所以图 10(a)中存在用户 1 和用户 4 满意度为几乎 0 的情况。从图 10(b)中可以看出，诱导机制的存在能够保证所有用户的通信都不受干扰影响，显著提高了用户的平均满意度，并避免某一用户的满意度过低的情况，在跟踪干扰环境下实现了用户的可靠通信。

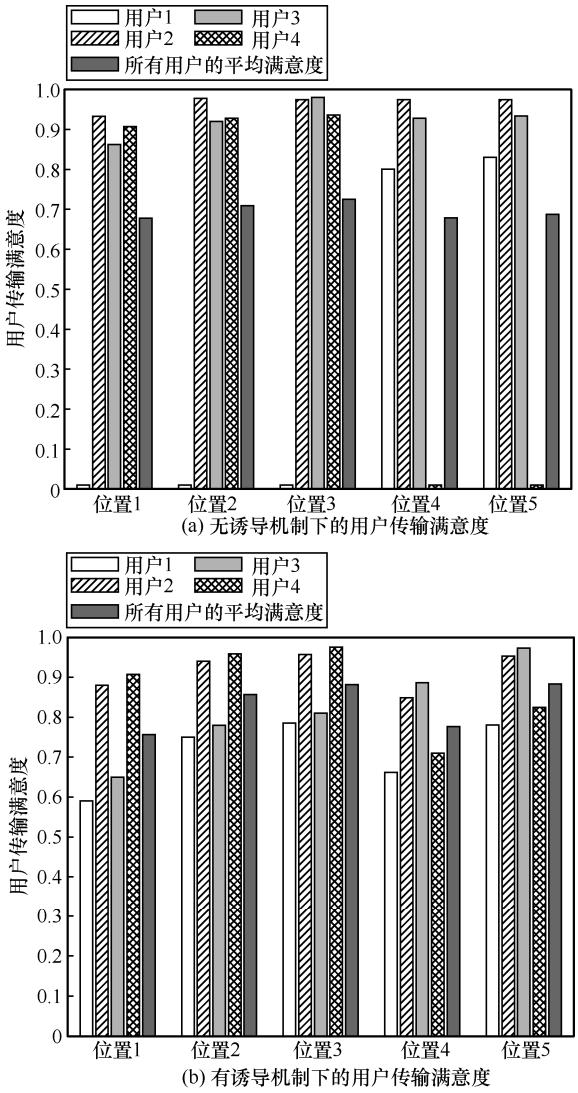



图 10　有无诱导机制下的用户传输满意度

上述案例对 2.1.2 节和 2.2.1 节中的部分关键技术进行了验证，但仍存在需要改进的地方。例如，3.1 节虽然研究了未知干扰模式识别问题，但假设的未知模式仍是和已知模式工作原理类似的常规干扰，可扩展性不强。总之，以现有工作为基础，将智能干扰作为对手，首先研究干扰反向推理技术来理解对手，其次研究对抗策略设计来克制对手，最后研究抗干扰策略自主优化和在线决策来战胜对手，是未来智能通信对抗的重要研究方向。

## 4　结束语

干扰的智能化发展给无线通信安全带来了巨

大威胁，关于智能抗干扰技术的研究变得尤为重要。本文突破传统被动抗干扰模式，提出对抗智能干扰的干扰主动防御技术，并简要说明了该技术的核心理念；其次，对现有智能抗干扰工作进行总结，并梳理出现有工作的共性问题及未来面临的挑战；再次，应对上述挑战，详细介绍了干扰主动防御技术体系架构，并分别从干扰反向推理、脆弱性分析和对抗策略设计、抗干扰策略自主优化和在线决策 3 个层面对关键技术进行详细阐述；然后，基于前期工作的 2 个具体案例，对部分关键技术进行论证和说明，表明所提干扰主动防御技术的理论指导意义；最后，对全文工作进行了总结。

## 参考文献：


[1] PELECHRINIS K, ILIOFOTOU M, KRISHNAMURTHY S V. Denial of service attacks in wireless networks: the case of jammers[J]. IEEE Communications Surveys & Tutorials, 2011, 13(2): 245-257.

[2] 姚富强, 张余, 柳永祥. 电磁频谱安全与控制[J]. 指挥与控制学报, 2015, 1(3): 278-283.
YAO F Q, ZHANG Y, LIU Y X. Security and control for electromagnetic spectrum[J]. Journal of Command and Control, 2015, 1(3): 278-283.

[3] 王沙飞, 鲍雁飞, 李岩. 认知电子战体系结构与技术[J]. 中国科学: 信息科学, 2018, 48(12): 1603-1613, 1709.
WANG S F, BAO Y F, LI Y. The architecture and technology of cognitive electronic warfare[J]. Scientia Sinica (Informationis), 2018, 48(12): 1603-1613, 1709.

[4] 王金龙, 徐煜华, 陈瑾. 无线通信网络智能频谱协同与对抗[J]. 中国科学: 信息科学, 2020, 50(11): 1767-1780.
WANG J L, XU Y H, CHEN J. Intelligent spectrum collaboration and confrontation in wireless communication networks[J]. Scientia Sinica (Informationis), 2020, 50(11): 1767-1780.

[5] YANG D J, XUE G L, ZHANG J, et al. Coping with a smart jammer in wireless networks: a Stackelberg game approach[J]. IEEE Transactions on Wireless Communications, 2013, 12(8): 4038-4047.

[6] FENG Z B, REN G C, CHEN J, et al. Power control in relay-assisted anti-jamming systems: a Bayesian three-layer Stackelberg game approach[J]. IEEE Access, 2019, 7: 14623-14636.

[7] LIU X, XU Y H, JIA L L, et al. Anti-jamming communications using spectrum waterfall: a deep reinforcement learning approach[J]. IEEE Communications Letters, 2018, 22(5): 998-1001.

[8] XU Y F, REN G C, CHEN J, et al. A one-leader multi-follower Bayesian-Stackelberg game for anti-jamming transmission in UAV communication networks[J]. IEEE Access, 2018, 6: 21697-21709.

[9] GAO N, QIN Z J, JING X J, et al. Anti-intelligent UAV jamming strategy via deep Q-networks[J]. IEEE Transactions on Communications, 2020, 68(1): 569-581.

[10] 郭道省, 张邦宁, 甘仲民. 透明转发器卫星通信系统在干扰条件下的性能[J]. 通信学报, 2003, 24(2): 118-124.
GUO D X, ZHANG B N, GAN Z M. Performance of transparent transponder satcom system with interference[J]. Journal of China Institute of Communications, 2003, 24(2): 118-124.

[11] 韩晨, 刘爱军, 安康. 卫星互联网抗干扰策略研究展望[J]. 天地一体化信息网络, 2022, 3(1): 50-55.
HAN C, LIU A J, AN K. Research prospect of anti-jamming strategy for the satellite Internet[J]. Space-Integrated-Ground Information Networks, 2022, 3(1): 50-55.

[12] XIAO L, JIANG D H, WAN X Y, et al. Anti-jamming underwater transmission with mobility and learning[J]. IEEE Communications Letters, 2018, 22(3): 542-545.

[13] SU W, TAO J C, PEI Y H, et al. Reinforcement learning based efficient underwater image communication[J]. IEEE Communications Letters, 2021, 25(3): 883-886.

[14] YANG H L, XIONG Z H, ZHAO J, et al. Intelligent reflecting surface assisted anti-jamming communications: a fast reinforcement learning approach[J]. IEEE Transactions on Wireless Communications, 2021, 20(3): 1963-1974.

[15] HOU Z F, CHEN J, HUANG Y Z, et al. Joint trajectory and passive beamforming optimization in IRS-UAV enhanced anti-jamming communication networks[J]. China Communications, 2022, 19(5): 191-205.

[16] ZHANG L H, YE H L, ZHANG D W. Study on the key technology of image transmission mechanism based on channel coding ghost imaging[J]. IEEE Photonics Journal, 2018, 10(4): 1-13.

[17] BAI W L, ZOU X H, LI P X, et al. Photonic millimeter-wave joint radar communication system using spectrum-spreading phase-coding[J]. IEEE Transactions on Microwave Theory and Techniques, 2022, 70(3): 1552-1561.

[18] FENG Z B, REN G C, CHEN J, et al. An anti-jamming hierarchical optimization approach in relay communication system via Stackelberg game[J]. Applied Sciences, 2019, 9(16): 3348.

[19] YUAN H C, SONG F, CHU X J, et al. Joint relay and channel selection against mobile and smart jammer: a deep reinforcement learning approach[J]. IET Communications, 2021, 15(17): 2237-2251.

[20] JIA L L, XU Y H, SUN Y M, et al. Stackelberg game approaches for anti-jamming defence in wireless networks[J]. IEEE Wireless Communications, 2018, 25(6): 120-128.

[21] JIA L L, QI N, CHU F H, et al. Game-theoretic learning anti-jamming approaches in wireless networks[J]. IEEE Communications Magazine, 2022, 60(5): 60-66.

[22] 李少谦. 扩、跳频通信技术的发展和展望[J]. 电子科技大学学报, 1996(S3): 299-303.
LI S Q. The development and prospects of the spread spectrum and hopping frequenct communication[J]. Journal of University of Electronic Science and Technology of China, 1996(S3): 299-303.

[23] 姚富强. 军事通信抗干扰工程发展策略研究及建议[J]. 中国工程科学, 2005, 7(5): 24-29.
YAO F Q. Researches and suggestions on development strategy of military anti-jamming communication engineering[J]. Engineering Science, 2005, 7(5): 24-29.

[24] 朱毅超, 陆建勋. 动态频谱抗干扰系统在部分频带干扰下的性能[J]. 电子学报, 2011, 39(10): 2331-2337.
ZHU Y C, LU J X. Performance of dynamic spectrum anti-jamming systems under partial-band noise jamming[J]. Acta Electronica Sinica, 2011, 39(10): 2331-2337.

[25] LING Q, LI T T. Message-driven frequency hopping: design and analysis[J]. IEEE Transactions on Wireless Communications, 2009, 8(4): 1773-1782.

[26] 张贤达. 盲信号处理几个关键问题的研究[J]. 深圳大学学报, 2004, 21(3): 196-200.
ZHANG X D. Research on the key technologies of blind signal pro-

cessing[J]. Shenzhen University Journal, 2004, 21(3): 196-200.

[27] 王传丹, 张忠培, 李少谦. 变换域通信系统中干扰信号的逐次消除[J]. 电子与信息学报, 2008, 30(10): 2439-2441.
WANG C D, ZHANG Z P, LI S Q. Interferences mitigation one by one in transform domain communication system[J]. Journal of Electronics & Information Technology, 2008, 30(10): 2439-2441.

[28] GROVER K, LIM A, YANG Q. Jamming and anti-jamming techniques in wireless networks: a survey[J]. International Journal of Ad Hoc and Ubiquitous Computing, 2014, 17(4): 197.

[29] SUN W, AMIN M G. A self-coherence anti-jamming GPS receiver[J]. IEEE Transactions on Signal Processing, 2005, 53(10): 3910-3915.

[30] 李少谦, 程郁凡, 董彬虹, 等. 智能抗干扰通信技术研究[J]. 无线电通信技术, 2012, 38(1): 1-4.
LI S Q, CHENG Y F, DONG B H, et al. Research on intelligent anti-jam communication techniques[J]. Radio Communications Technology, 2012, 38(1): 1-4.

[31] YAO F Q, JIA L L, SUN Y M, et al. A hierarchical learning approach to anti-jamming channel selection strategies[J]. Wireless Networks, 2019, 25(1): 201-213.

[32] PEI X F, WANG X M, RUAN L, et al. Joint power and channel selection for anti-jamming communications: a reinforcement learning approach[C]//Machine Learning and Intelligent Communications. Berlin: Springer, 2019: 551-562.

[33] KONG L J, XU Y H, ZHANG Y L, et al. A reinforcement learning approach for dynamic spectrum anti-jamming in fading environment[C]//Proceedings of 2018 IEEE 18th International Conference on Communication Technology. Piscataway: IEEE Press, 2018: 51-58.

[34] LI Y Y, XU Y H, XU Y T, et al. Dynamic spectrum anti-jamming in broadband communications: a hierarchical deep reinforcement learning approach[J]. IEEE Wireless Communications Letters, 2020, 9(10): 1616-1619.

[35] WANG X M, WANG J L, XU Y H, et al. Dynamic spectrum anti-jamming communications: challenges and opportunities[J]. IEEE Communications Magazine, 2020, 58(2): 79-85.

[36] LI W, CHEN J, LIU X, et al. Intelligent dynamic spectrum anti-jamming communications: a deep reinforcement learning perspective[J]. IEEE Wireless Communications, 2022: doi.org/10.1109/MWC.103.2100365.

[37] HAN Z, NIYATO D, SAAD W, et al. Game theory in wireless and communication networks[M]. Cambridge: Cambridge University Press, 2011.

[38] XIAO L, CHEN T H, LIU J L, et al. Anti-jamming transmission Stackelberg game with observation errors[J]. IEEE Communications Letters, 2015, 19(6): 949-952.

[39] ALTMAN E, AVRACHENKOV K, GARNAEV A. A jamming game in wireless networks with transmission cost[C]//Network Control and Optimization. Berlin: Springer, 2007: 1-12.

[40] JIA L L, YAO F Q, SUN Y M, et al. Bayesian Stackelberg game for anti-jamming transmission with incomplete information[J]. IEEE Communications Letters, 2016, 20(10): 1991-1994.

[41] JIA L L, XU Y H, SUN Y M, et al. A multi-domain anti-jamming defense scheme in heterogeneous wireless networks[J]. IEEE Access, 2018, 6: 40177-40188.

[42] ZHANG X B, WANG H, XU Y F, et al. Put others before itself: a multi-leader one-follower anti-jamming Stackelberg game against tracking jammer[J]. China Communications, 2021, 18(11): 168-181.

[43] FENG Z B, LUO Y J, CHEN X Q, et al. A MAB-based discrete power control approach in anti-jamming relay communication via three-layer stackelberg game[C]//Proceedings of 2020 IEEE 6th International Conference on Computer and Communications. Piscataway: IEEE Press, 2020: 267-272.

[44] 韦正现. 智能装备试验与测试的挑战与对策思考[J]. 测控技术, 2021, 40(2): 1-5, 12.
WEI Z X. Challenge and countermeasure of intelligent equipment experiment and test[J]. Measurement & Control Technology, 2021, 40(2): 1-5, 12.

[45] JORDAN M I, MITCHELL T M. Machine learning: trends, perspectives, and prospects[J]. Science, 2015, 349(6245): 255-260.

[46] HUANG L, JOSEPH A D, NELSON B, et al. Adversarial machine learning[C]//Proceedings of the 4th ACM Workshop on Security and Artificial Intelligence. New York: ACM Press, 2011: 43-57.

[47] CRESWELL A, WHITE T, DUMOULIN V, et al. Generative adversarial networks: an overview[J]. IEEE Signal Processing Magazine, 2018, 35(1): 53-65.

[48] KOCH G, ZEMEL R, SALAKHUTDINOV R. Siamese neural networks for one-shot image recognition[C]//Proceedings of the 32nd International Conference on Machine Learning. [S.l.]: JMLR, 2015: 1-8.

[49] SHAO G Q, CHEN Y S, WEI Y S. Convolutional neural network-based radar jamming signal classification with sufficient and limited samples[J]. IEEE Access, 2020, 8: 80588-80598.

[50] ZHU M T, LI Y J, PAN Z S, et al. Automatic modulation recognition of compound signals using a deep multi-label classifier: a case study with radar jamming signals[J]. Signal Processing, 2020, 169: 107393.

[51] BISWAS S, ANNADANI Y. Preserving semantic relations for zero-shot learning[C]//Proceedings of 2018 IEEE/CVF Conference on Computer Vision and Pattern Recognition. Piscataway: IEEE Press, 2018: 7603-7612.

[52] HAN H, LI W, FENG Z B, et al. Proceed from known to unknown: jamming pattern recognition under open-set setting[J]. IEEE Wireless Communications Letters, 2022, 11(4): 693-697.

[53] HARDOON D R, SZEDMAK S, SHAWE-TAYLOR J. Canonical correlation analysis: an overview with application to learning methods[J]. Neural Computation, 2004, 16(12): 2639-2664.

[54] ZHOU Z H. Abductive learning: towards bridging machine learning and logical reasoning[J]. Science China Information Sciences, 2019, 62(7): 1-3.

[55] 姚富强. 通信抗干扰工程与实践（2 版）[M]. 北京: 电子工业出版社, 2012.
YAO F. Communication anti-jamming engineering and practice[M]. 2nd ed. Beijing: Publishing House of Electronics Industry, 2012.

[56] URETEN O, SERINKEN N. Wireless security through RF fingerprinting[J]. Canadian Journal of Electrical and Computer Engineering, 2007, 32(1): 27-33.

[57] ERPEK T, SAGDUYU Y E, SHI Y. Deep learning for launching and mitigating wireless jamming attacks[J]. IEEE Transactions on Cognitive Communications and Networking, 2019, 5(1): 2-14.

[58] ZHANG S Y, TIAN H, CHEN X Q, et al. Design and implementation of reinforcement learning-based intelligent jamming system[J]. IET Communications, 2020, 14(18): 3231-3238.

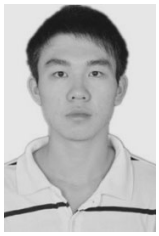
[59] 张晓博, 王海, 冯智斌, 等. 基于主动诱导机制的中继通信智能抗干扰方法[J]. 南京邮电大学学报(自然科学版), 2021, 41(5): 15-22.
ZHANG X B, WANG H, FENG Z B, et al. Intelligent anti-jamming relay communication method based on active induction mechanism[J]. Journal of Nanjing University of Posts and Telecommunications (Natural Science Edition), 2021, 41(5): 15-22.

[60] KUO W H, LIAO W. Utility-based radio resource allocation for QoS

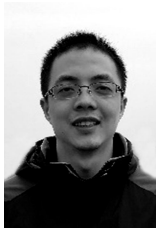
traffic in wireless networks[J]. IEEE Transactions on Wireless Communications, 2008, 7(7): 2714-2722.

[61] XU Y H, WANG J L, WU Q H, et al. Opportunistic spectrum access in unknown dynamic environment: a game-theoretic stochastic learning solution[J]. IEEE Transactions on Wireless Communications, 2012, 11(4): 1380-1391.

[作者简介]



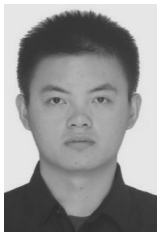
**冯智斌**（1995− ），男，河南平顶山人，陆军工程大学博士生，主要研究方向为智能抗干扰、博弈论和智能干扰。



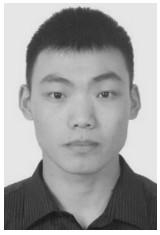
**徐煜华**（1983− ），男，贵州毕节人，博士，陆军工程大学教授、博士生导师，主要研究方向为认知无线电、智能频谱对抗、无人机集群通信和博弈论。

**杜智勇**（1986− ），男，湖北武汉人，博士，国防科技大学副教授，主要研究方向为无线通信中的智能决策、智能抗干扰和无人机通信。

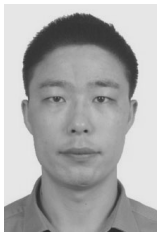
**刘鑫**（1983− ），男，江西上饶人，博士，桂林理工大学副教授、硕士生导师，主要研究方向为智能抗干扰、深度强化学习和软件无线电。



**李文**（1996− ），男，江西新余人，陆军工程大学博士生，主要研究方向为博弈论、机器学习和智能抗干扰。



**韩昊**（1996− ），男，山东临沂人，陆军工程大学博士生，主要研究方向为智能频谱对抗、博弈论和机器学习。



**张晓博**（1983− ），男，河南南阳人，博士，陆军工程大学讲师，主要研究方向为无线网络安全、智能抗干扰和博弈论。