doi:10.11887/j.cn.202305001 http://journal.nudt.edu.cn

认知电子战综述*

黄知涛[1,2],王 翔[1],赵雨睿[1]
(1. 国防科技大学 电子科学学院,湖南 长沙 410073;2. 国防科技大学 电子对抗学院,安徽 合肥 230037)

摘 要:认知电子战通常被定义为以具备认知性能的电子战装备为基础,注重自主交互式的电磁环境学习能力与动态智能化的对抗任务处理能力的电子战形态。自其被首次提出以来,以其感知准、推理强、决策快的优势备受国内外研究学者广泛关注。随着人工智能新理念、新技术、新应用的不断涌现,认知电子战步入崭新的发展阶段。为捕捉其未来发展方向,从人工智能角度出发,总结并丰富了认知电子战概念内涵,梳理认知电子战的发展脉络及外国典型项目,搭建认知电子战系统框架及架构,从感知、判断、决策等方面对认知电子战关键技术进行了全面系统综述,并总结了认知电子战面临的挑战和发展趋势。

关键词:认知电子战;电子战;人工智能
中图分类号:TN97 **文献标志码**:A **开放科学(资源服务)标识码(OSID)**:
文章编号:1001-2486(2023)05-001-11

Overview of cognitive electronic warfare

HUANG Zhitao[1,2], *WANG Xiang*[1], *ZHAO Yurui*[1]
(1. College of Electronic Science and Technology, National University of Defense Technology, Changsha 410073, China;
2. College of Electronic Engineering, National University of Defense Technology, Hefei 230037, China)

Abstract: Cognitive electronic warfare is usually defined as a form of electronic warfare that is based on electronic warfare equipment with cognitive performance and focuses on autonomous interactive electromagnetic environment learning capability and dynamic intelligent confrontation task processing capability. Since it was first proposed, it has attracted extensive attention from researchers and scholars at home and abroad for its advantages of accurate perception, strong reasoning and fast decision-making. With the continuous emergence of new concepts, technologies and applications of artificial intelligence, cognitive electronic warfare has stepped into a brand new stage of development. In order to capture its future development direction, the connotation of the concept of cognitive electronic warfare was summarized and enriched from the perspective of artificial intelligence, the development of cognitive electronic warfare and typical foreign projects were sorted out, the framework and architecture of cognitive electronic warfare system was built, a comprehensive and systematic review of the key technologies of cognitive electronic warfare was conducted from the aspects of perception, judgment, decision-making, etc., and the challenges and development trends of cognitive electronic warfare were summarized.

Keywords: cognitive electronic warfare; electronic warfare; artificial intelligence

电子战是争夺制电磁权的关键,其旨在利用电磁能、定向能等实现对电磁频谱的控制,包括掌握、攻击敌方电子信息系统和电子系统等,以及保护己方电子信息系统和电子系统等[1]。电子战的发展经历了三个演变过程,即传统电子战、自适应电子战以及认知电子战。传统电子战是指采用预置的干扰方式破坏敌方雷达、通信等电子信息系统的正常工作;自适应电子战则是融合自适应技术,使电子战系统具备适应电磁环境变化的能力;而认知电子战则代表了电子战演变的最新形态,具备推理、学习等认知能力,能够对未知的目标和环境进行分析并自主做出有效的对抗决策。

催生电子战形态改变的关键因素是人工智能技术的蓬勃发展。在20世纪70年代时期,电子战系统高度依赖以特征工程为主导的专家系统。进入21世纪以来,数据规模和算力的急剧增加促使以深度学习等为代表的人工智能学习模型不断涌现,电子战系统中的关键算法从特征工程走向机器学习。自今年以来,以生成式大语言模型为代表的新一代人工智能技术突起,为认知电子战

* **收稿日期**:2023-06-30
基金项目:国家自然科学基金面上资助项目(62271494)
作者简介:黄知涛(1976—),男,湖北荆州人,教授,博士,博士生导师,E-mail:huangzhitao@nudt.edu.cn;
王翔(通信作者),男,福建福州人,副教授,博士,硕士生导师,E-mail:christopherwx@163.com

的发展提供了进一步的机遇。

美国最先意识到人工智能技术给电子战发展带来的机遇。从2008年起,美军以提高电子战装备认知能力为核心,陆续启动和开展了多个认知电子战项目的研究[2]。中国从2013年开始跟踪研究认知电子战技术,主要团队包括中国电子科技集团公司第三十六研究所的杨小牛院士团队[3]、军事科学院的王沙飞院士团队[4]等。

随着人工智能技术的快速发展,学术界对认知这一概念已经迈进了崭新的阶段。因此,重新梳理认知电子战的发展脉络,剖析其核心技术原理,进一步捕捉其发展趋势就显得尤为重要。

本文结合人工智能领域的最新研究进展,对认知电子战系统从概念内涵、典型项目、系统架构、关键技术与未来挑战五个方面进行全面总结及深入分析,进而为领域研究垫下基石。

1 认知电子战概念

传统电子战系统主要基于人工经验知识,缺乏足够的自学习能力,长期面临着“新型电磁目标”“未知目标难以识别”“难以生成干扰措施”“对抗效果难以评估”等问题。新一代雷达、通信等电子信息系统正在向智能化方向发展,急需电子战系统提升智能化水平,实现“以智对智”。认知电子战正是在这个背景下应运而生,其具备对电磁环境和辐射源目标深层次的“认知”能力,能够在极短的时间内自主地生成最佳对抗策略,通过实时在线评估对抗效果不断优化对抗策略[5]。

1.1 定义与内涵

目前,国内外对认知电子战尚未有统一的定义,研究人员先后给出过不同定义,总结如表1所示。虽然不同研究人员对认知电子战定义的侧重不同,但是核心都在强调对环境和目标的自主认知和理解,从而持续实现对目标辐射源的高效干扰策略生成与优化。然而,对目标辐射源究竟要认知什么、理解什么,才能有助于高效对抗,这方面国内外公开文献都没有深入研究。

虽然不同研究人员对认知电子战的定义侧重不同,但是核心都在强调对环境和目标的自主认知和理解,从而持续实现对目标辐射源的高效干扰策略生成与优化。但是已有定义并未充分考虑目标不同特性给认知以及策略优化带来的差异性。综合已有研究成果,并结合人工智能的新发展,本文结合不同目标变化特性详细阐述不同等级的认知电子战。

表1 国内外认知电子战定义总结

Tab. 1 Summary of the definition of cognitive electronic warfare at home and abroad

年份 文献	定义
2010 [6]	认知电子战的过程是一个“感知—学习—自适应对抗—感知”的不断循环过程,同时也是将先验知识和经验进行运用和更新的智能化过程,也是通过组网与其他领域和系统进行信息共享并自适应地做出决策的分布式协同工作过程
2014 [7]	认知电子战是一种在软件无线电技术基础上实现的智能化、网络化(知识共享)、多功能电子战理念,除可以对抗传统电子信息系统以外,还可以对抗新兴的认知电子信息系统(认知无线电台、认知网络、认知雷达等)。其核心技术包括软件无线电技术、机器学习技术、行为建模技术等
2016 [8]	认知电子战技术,有望使电子战在威胁系统面前领先一步,这些系统在更宽的带宽上运行,并具有比上一代威胁好得多的射频敏捷性
2018 [4]	认知电子战是以具备认知性能的电子战装备为基础,注重自主交互式的电磁环境学习能力与动态智能化的对抗任务处理能力的电子战作战行动,是电子战从“人工认知”向机器“自动认知”升级
2021 [5]	认知电子战将人工智能与电子战技术相结合,目的是提高电子战系统对复杂环境下先进电磁目标的精准感知能力和敏捷对抗能力
2022 [9]	认知电子战技术旨在改进电子战系统的工作模式,发展具有认知能力的自适应电子战技术。目前以提高电子战系统智能化水平为核心,具备自主感知、实时反应、精准对抗以及在线评估能力的认知电子战技术已成为电子战领域的重要发展方向
2023 [10]	认知电子战系统可以学习和适应不断变化的环境和敌人战术。这些系统可以使用人工智能来分析来自电子传感器和其他来源的数据,以检测、跟踪和分类电子信号,并预测敌方电子战系统的行为

从目标变化程度的角度出发,认知电子战可以分为三个层次:一是当辐射源目标信号参数以及工作模式不变或者缓慢变化时,认知电子战核心是如何基于尽可能少的侦测数据做出高效决策;二是当辐射源目标信号采用事先设定的规则实现变化时,认知电子战的核心是基于历史侦测

数据实现对目标辐射源工作规则的认知,并基于认知结果实现干扰策略生成与预测;三是当辐射源目标是智能化目标,即其参数或工作模式能够自主随环境动态变化时,认知电子战的核心是如何基于历史侦测数据和实时侦测数据完成对目标智能学习模型的在线认知,实现“以智对智”,并形成智能对抗决策模型对目标智能规划模型的“先发制人”优势。

可见,认知电子战最大的优势是实现对未知目标的认知与对抗。从目标未知属性的角度出发,认知又可以进一步细分为两个部分:一是当目标采用未知波形时,认知电子战需要实现对波形的认知以及最佳干扰波形的生成;二是当目标采用未知工作模式时,认知电子战需要实现对目标工作模式规律的认知以及针对该模式最佳干扰策略的生成。

1.2　能力

认知电子战能够实时感知电磁环境,高效自主地调整系统以适应目标和环境的变化,提高系统的反应力、精确性和适应水平等综合效能。结合 1.1 节中的定义与内涵,本文从感知、判断、决策三个方面对电子战系统的能力进行描述。

一是感知能力,即实现对复杂电磁环境中雷达、通信等不同辐射源的精确检测、分析、识别、测向定位等能力,并能对辐射源的工作模式进行智能分析;二是判断能力,即实现对敌辐射源行为规律的精确建模及异常检测,从较长时间尺度上对目标进行深层次认知,并能推断辐射源及所在平台的意图的能力;三是干扰决策能力,即实现最佳干扰决策并生成最佳干扰波形,能基于实时评估干扰效果实现干扰策略优化,具备先发致人式、预测性干扰能力。

2　典型认知电子战项目

自 2008 年起,美国军方和工业界就陆续启动了多个认知电子战项目,分别从关键技术攻关、系统架构、应用集成和演示验证等方面推动认知电子战的发展[11]。

在关键技术攻关方面,美国海军实施的反应式电子攻击措施项目重点聚焦雷达信号探测和分类技术,用于识别敏捷雷达威胁目标,并计划应用于 EA-18G“咆哮者”电子战飞机;美国国防部建立的“算法战跨职能小组”开展基于人工智能的海量光电侦察数据态势分析、目标识别、光电对抗等技术研究;美国 DeepSig 公司于 2020 年开发了一套 OmniSIG 人工智能软件,开展信号检测、识别、推理等关键技术验证,为动态频谱感知与决策提供支撑。

在系统架构研究方面,DARPA 资助的“宽带传感器系统的处理器重构”项目聚焦开发高吞吐量、流数据处理器,大幅提升硬件反应速度和处理能力,为认知电子战提供实时运算平台支持;“射频机器学习系统”聚焦研究如何将机器学习等人工智能理念与方法应用于射频系统设计。美国空军针对认知电子战面临新威胁的特点,实施了“电子支援关键试验”项目,试验具有新目标适应能力的开放式机载电子攻击系统。

在应用集成和演示验证方面,美国工业界在 DARPA 的资助下分别针对雷达对抗、通信对抗等开展了验证。在雷达对抗方面,主要代表项目是“自适应雷达对抗”项目;在通信对抗方面,主要代表性项目包括“自适应电子战行为学习”“认知干扰机”“城市军刀”等。而“极端射频频谱条件下的通信”项目则聚焦认知通信防御问题,提高在遭受干扰压制情况下的通信自适应能力和灵活性。2022 年,美国空军发布的“怪兽”项目是美军公开的认知电子战最新项目,其包括了数据框架、硬软件架构(软件无线电研究)、多频谱模拟仿真环境、可重构的电子攻击处理、实时算法开发、关键技术重编程(检测、分选、识别、去模糊和跟踪等)、分布式对抗等,实现机载认知电子战能力的全面验证。

3　认知电子战系统架构

综合国内外研究,认知电子战系统架构一般由可重构射频模块、侦察感知模块、干扰生成模块、推理学习模块、动态知识库等组成,如图 1 所示。可重构射频模块主要负责与电磁环境的交

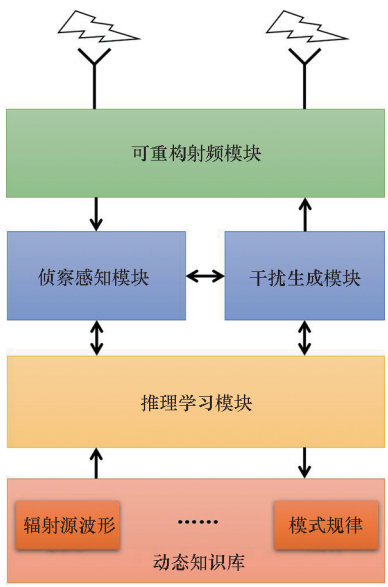

图 1　通用的认知电子战系统体系结构

Fig. 1　General architecture of cognitive electronic warfare system

互,包括接收环境中的射频信号与发射干扰信号。侦察感知模块主要负责射频信号接收与智能分析识别、信息提取以及辐射源行为分析、意图识别等,为对抗决策提供输入依据,同时也为在线干扰效果评估提供输入依据;干扰生成模块主要负责对抗策略以及干扰波形的实时生成;推理学习模块为整个系统提供运算条件,支撑离线学习以及在线运算等,充当认知电子战系统的大脑;动态知识库存储感知判断得到的目标辐射源波形、模式规律等知识并能够进行动态更新。认知电子战系统的核心特征是通过智能赋能,动态适应电磁环境和目标变化,敏锐发现、精确识别和高效干扰威胁目标,并能自适应实现资源动态调度,通过学习不断优化策略。

在系统架构的基础上,认知电子战系统还可以进一步根据不同的功能层次进行详细设计与划分。

根据自顶向下的设计原则,采用分层架构将认知电子战系统划分为用户层、应用层、算法层、数据层和硬件层,如图2所示。层次越向上,其抽象层次就越面向业务、面向用户;层次越向下,其抽象层次就变得越通用、面向设备。

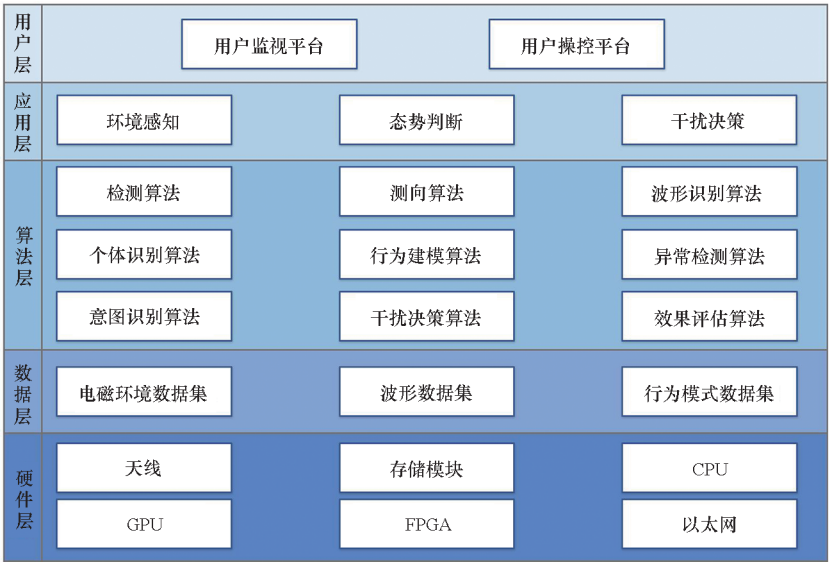

图2　认知电子战系统的分层架构

Fig. 2　Layered architecture of cognitive electronic warfare system

4　认知电子战关键技术

认知电子战的核心是感知能力、判断能力、决策能力。考虑到感知、判断、决策每个方面具有不同评价方式,认知电子战的效能函数可以表示为

$$\max_{\boldsymbol{c}} U(\boldsymbol{m}_{\mathrm{ob}}(\boldsymbol{c}_{\mathrm{ob}}),\boldsymbol{m}_{\mathrm{or}}(\boldsymbol{c}_{\mathrm{or}}),\boldsymbol{m}_{\mathrm{de}}(\boldsymbol{c}_{\mathrm{de}}),\boldsymbol{w})$$
$$\text{s.t.}\ \begin{cases} C_{\mathrm{eq}}(\boldsymbol{c}_{\mathrm{ob}},\boldsymbol{c}_{\mathrm{or}},\boldsymbol{c}_{\mathrm{de}})=0 \\ C_{\mathrm{non-eq}}(\boldsymbol{c}_{\mathrm{ob}},\boldsymbol{c}_{\mathrm{or}},\boldsymbol{c}_{\mathrm{de}})\geqslant 0 \end{cases} \tag{1}$$

其中:$\boldsymbol{m}_{\mathrm{ob}}$、$\boldsymbol{m}_{\mathrm{or}}$、$\boldsymbol{m}_{\mathrm{de}}$分别表示感知、判断、决策三个方面的性能指标向量;$\boldsymbol{c}_{\mathrm{ob}}$、$\boldsymbol{c}_{\mathrm{or}}$、$\boldsymbol{c}_{\mathrm{de}}$分别表示感知、判断、决策三个方面的控制参数;$U(\cdot)$表示系统效能函数,将多个性能指标$\boldsymbol{m}$合成单一标量值,$\boldsymbol{w}$是不同模块对应指标的权重系数。通过寻找最优的$\boldsymbol{c}_{\mathrm{ob}}$、$\boldsymbol{c}_{\mathrm{or}}$、$\boldsymbol{c}_{\mathrm{de}}$,使得认知电子战系统的效能函数最大化。$\boldsymbol{m}_{\mathrm{ob}}$、$\boldsymbol{m}_{\mathrm{or}}$、$\boldsymbol{m}_{\mathrm{de}}$等每一个指标的提升都应该会带来认知电子战系统性能的提升,但是单一的指标提升只能在一定程度范围内提升认知电子战系统的效能,而不能无限提高。$C_{\mathrm{eq}}(\cdot)$、$C_{\mathrm{non-eq}}(\cdot)$分别代表优化问题中的等式限制条件与不等式限制条件,即表示认知电子战系统在学习优化控制参数过程中需要遵循的约束条件。例如,电子战系统的干扰样式集、侦察与干扰的开窗时间限制等。

从每个功能模块的角度出发,效能函数可以进一步表示为

$$\begin{aligned} &U(\boldsymbol{m}_{\mathrm{ob}}(\boldsymbol{c}_{\mathrm{ob}}),\boldsymbol{m}_{\mathrm{or}}(\boldsymbol{c}_{\mathrm{or}}),\boldsymbol{m}_{\mathrm{de}}(\boldsymbol{c}_{\mathrm{de}}),\boldsymbol{w}) \\ &=\widetilde{U}[U_{\mathrm{ob}}(\boldsymbol{m}_{\mathrm{ob}}(\boldsymbol{c}_{\mathrm{ob}}),\boldsymbol{w}_{\mathrm{ob}}),U_{\mathrm{or}}(\boldsymbol{m}_{\mathrm{or}}(\boldsymbol{c}_{\mathrm{or}}),\boldsymbol{w}_{\mathrm{or}}), \\ &U_{\mathrm{de}}(\boldsymbol{m}_{\mathrm{de}}(\boldsymbol{c}_{\mathrm{de}}),\boldsymbol{w}_{\mathrm{de}}),\boldsymbol{w}] \end{aligned} \tag{2}$$

其中,$U_{\mathrm{ob}}(\cdot)$、$U_{\mathrm{or}}(\cdot)$、$U_{\mathrm{de}}(\cdot)$分别表示感知、判断、决策模块的效用函数,$\widetilde{U}[\cdot]$代表三个效用函数的耦合函数。下文将从感知、判断、决策三个方面分别介绍其涉及的关键技术。

4.1　感知技术

4.1.1　问题模型

感知的目标是对截获到的信号进行处理,获取信号的基本参数、信号样式、个体身份等信息,

能够为对抗波形生成提供基础参数。其核心在于如何根据不同的需求,构造不同的特征提取模型,可以表示为

$$\max_{\boldsymbol{c}} U_{\mathrm{ob}}(\boldsymbol{m}_{\mathrm{ob}}(\boldsymbol{c}_{\mathrm{ob}}),\boldsymbol{w}_{\mathrm{ob}})$$
$$\text{s.t.}\ \begin{cases} C_{\mathrm{eq}}(\boldsymbol{c}_{\mathrm{ob}})=0 \\ C_{\mathrm{non-eq}}(\boldsymbol{c}_{\mathrm{ob}})\geqslant 0 \end{cases} \tag{3}$$

为了完成对目标的感知任务,需要对接收到的信号进行分步骤处理,包含信号检测、测向、信号识别、个体识别等,从而实现从复杂电磁环境中发现、识别辐射源目标,为后续干扰决策提供目标指引。控制参数 $\boldsymbol{c}_{\mathrm{ob}}$ 中核心控制变量为特征提取函数 $f(\cdot)$,$f(\cdot)$ 在很大程度上决定了感知模块的效能。目前,在认知电子战感知技术研究中,$f(\cdot)$ 一般采用不同的深度学习模型。下面分别对感知技术中涉及的检测、测向、信号识别和个体识别技术进行介绍。

4.1.2　检测技术

信号检测的目的是从接收的无线电数据中检测出潜在的目标信号,是实现认知电子战感知技术的第一步。传统信号窄带检测方法主要分为匹配滤波法[12-13]、循环平稳法[14]、特征值检测法[15-18]和能量检测法四大类。但是这些经典检测方法重点关注的是信号存在性判定问题,大都未对信号参数估计进行研究,而全面准确的信号参数获取对于后续盲处理是至关重要的。

近几年随着深度学习技术的飞速发展和巨大性能突破,将其引入宽带信号检测效果十分显著。基本思路是以时频图作为输入,预测信号在时频图上的边界框和类型;再将预测的边界框进行简单的转换,即可得到信号的起止时间、中心频率、带宽以及信号类别等参数。Yuan 等在时频图上利用能量检测方法获取感兴趣区域(regions of interest, RoI),然后利用多层卷积神经网络(convolutional neural networks, CNN)组成的分类器对 RoI 进行识别以检测 Morse 信号[19]。该方法的性能瓶颈主要在于能量检测在信道环境复杂时鲁棒性较差。Prasad 等认为信号检测任务复杂性低于通用目标检测,因此采用了一个简化的 Faster R-CNN 模型来从含干扰时频图中检测 Wi-Fi信号,并且对模型不同超参数进行了详细讨论和优化[20]。Zha 等采用单阶段目标检测器从宽带时频图中检测多种调制类型的信号[21]。Li 等采用 YOLOv3 针对宽带时频图中检测多调制类型信号开展了实验验证[22]。

随着新体制信号的出现,信号带宽范围大,一次通联涉及多种不同突发宽度、多频点、多带宽,如何应对时间频域尺度差异较大的不同类型信号的检测成为亟待解决的难题。

4.1.3　测向技术

空间信号波达方向(direction of arrival, DOA)估计,也称为阵列测向,其主要目的是对空间某区域目标信源进行精确的测向。

经典的 DOA 估计方法,即模型驱动类方法,通过预先建立的阵列观测数据与信号角度之间的数学模型,计算出相应准则下的信号方向。该类方法需要经过特征值分解、多维搜索、迭代运算等计算过程,会产生巨大的计算量,并且当预设模型与实际情况不匹配或存在较大偏差时,该类方法的性能将会出现急剧恶化甚至完全失效,难以满足日益复杂的电磁环境下对测向准确性、实时性和稳健性的要求。

近年来,很多国内外研究者开始引入了机器学习技术,如支持向量回归[23-24]、径向基函数[25-26]、深度神经网络[27-29]等来解决 DOA 估计问题。以机器学习为代表的数据驱动类方法能够直接基于对数据的学习提取特征与入射角度之间的非线性映射关系,可表示为 $f(s)\rightarrow\theta'$,对难以建模的复杂环境具有较强的适应性。同时,其在线测试过程能够被硬件高效地并行实现,在计算效率方面也具备显著优势。但对该类方法的研究目前还处于探索阶段,仍然面临着很多问题,如问题条件理想化、先验信息挖掘不充分、少样本问题以及在线学习问题等。

4.1.4　信号识别技术

信号识别是指对接收到的电磁信号进行特征测量,识别信号规格或者信号样式,具体包括雷达、通信信号的调制方式等。

目前,智能信号识别算法根据数据预处理阶段所使用的信号表示技术可以划分为基于序列表示、特征表示、图像表示或它们的组合表示的智能信号识别四类方法。

序列表示是最直观的信号表示,常用的方法是使用同相正交(inphase and quadrature, IQ)序列、幅度相位(amplitude and phase, AP)序列和快速傅里叶变换(fast Fourier transform, FFT)序列等表示信号。文献[30]基于相同 CNN 和 RadioML2016.10a[31]中的相同数据集研究了 IQ 序列、AP 序列和 FFT 序列表示对识别性能的影响,实际应用中应根据具体的场景和信号特点进行综合考虑以选择合适的序列表示方法。

基于特征表示的智能信号识别算法由传统的基于特征提取算法发展而来。它通过提取多个特

征来表示接收信号,再输入深度学习模型完成识别。常使用的特征有高阶累积量、瞬时特征、循环统计量、小波变换特征和近似熵特征等。因为提取的特征数目通常小于接收信号的长度,故可以使用具有较少神经元的简单神经网络。但也存在以下几点不足:一是信号特征的计算导致额外的计算复杂度;二是需要根据候选信号样式选择适当的特征,依赖于专业知识和经验;三是提取信号的某些特征,可能丢失一些关键信息,并影响调制识别的性能。

基于图像表示的智能信号识别算法是在数据预处理阶段将接收信号转换为星座图、特征点图像、模糊函数图像、眼图、谱相关函数图像等,通过图像识别来完成信号识别。

由于单一一种信号表示方式均存在片面性,很难仅利用某一种表示技术完整地表征信号全部特性。因此,现有研究中也有考虑使用多个特征、图像或序列的组合来表示接收信号,作为深度学习模型的输入用于信号智能识别。通过综合运用多种信号表示,多种表示优势互补,解决了单一表示对信号反映不完整的问题,可以提高识别的鲁棒性和准确率。

4.1.5　个体识别技术

特定辐射源个体识别(specific emitter identification, SEI)技术,又称辐射源指纹识别技术,是指对接收的电磁信号进行特征测量,并根据已有的先验信息确定产生信号的辐射源的个体识别过程。现有SEI技术根据特征提取方式可以划分为基于特征工程的辐射源个体识别技术与基于深度学习的辐射源个体识别技术[32]两大类。人工设计指纹特征面临的挑战主要表现在两个方面:一是特征设计函数复杂度较低导致指纹特征表征能力较弱;二是随着加工工艺不断进步,辐射源个体差异日益缩小,同时新体制辐射源信号日益复杂,导致SEI特征设计难度显著增加[32]。

因此,研究人员提出采用深度学习技术代替人工设计指纹特征步骤,即在损失函数的约束下,通过不断优化网络结构参数,自动提取有效的指纹特征,并完成个体身份识别任务[32-33]。根据网络输入的数据格式不同,该类技术可以划分为两类,即基于原始IQ数据的指纹特征提取与基于信号变换域的指纹特征提取。基于原始IQ数据的指纹特征提取技术的优势在于原始数据无信息丢失,可以为深度学习模型提供全部可用的信息,但却同时带来了冗余信息干扰训练的问题。针对这一问题,部分学者首先将信号映射至变换域再输入深度学习模型,以降低训练难度,进而提高SEI系统识别准确率和鲁棒性。

4.2　判断技术

4.2.1　问题模型

判断的目标是对感知模型输出的信号基本参数、信号样式等特征进行时间维度上建模,分析目标的行为规律,检测是否异常并识别目标意图,能够为对抗策略生成与优化提供支撑。判断模型的效用函数可表示为

$$\max_{\boldsymbol{c}} U_{\mathrm{or}}(\boldsymbol{m}_{\mathrm{or}}(\boldsymbol{c}_{\mathrm{or}}),\boldsymbol{w}_{\mathrm{or}})$$
$$\text{s.t.}\ \begin{cases} C_{\mathrm{eq}}(\boldsymbol{c}_{\mathrm{or}})=0 \\ C_{\mathrm{non-eq}}(\boldsymbol{c}_{\mathrm{or}})\geqslant 0 \end{cases} \tag{4}$$

判断过程包括行为建模、异常检测和意图识别。其输入为侦察感知模块的输出,包括信号识别结果、个体识别结果、信号方向、信号参数等。

式(4)中的判断模块控制参数$\boldsymbol{c}_{\mathrm{or}}$由建模模型$f_{\mathrm{Model}}(\cdot)$、异常检测模型$f_{\mathrm{AD}}(\cdot)$和意图识别模型$f_{\mathrm{IR}}(\cdot)$决定。针对行为建模,当$f_{\mathrm{Model}}(\cdot)$提取的行为描述特征$\boldsymbol{c}_{\mathrm{Model}}$足够代表一个目标或者事件的真实特征$\boldsymbol{c}_{\mathrm{Model}}^{\mathrm{Ture}}$时,建模效果越好。这是一个逐渐逼近不断优化的过程。该行为描述特征也能与后续干扰决策进行联合学习。

在提取行为描述特征后,通过异常检测计算$f_{\mathrm{AD}}(\cdot)$进行判断,根据经验误差设定阈值ρ判别是否为异常行为。

当检测到目标信号波形或工作模式等的异常行为后,可以进一步分析并确定其对应的事件或意图Y_{IR},构建意图识别函数$f_{\mathrm{IR}}(\cdot)$与事件Y_{IR}作对应,即可得到意图识别结果。

4.2.2　行为建模

行为建模是通过对特定辐射源的长期行为观察、描述和统计分析,从数据中获取目标的行为描述和规律特征。电磁目标行为是指目标面对任务需求及外界环境时做出的决策反应。通过建立电磁目标在信号参数和工作状态等方面的行为模型,便于对后续的行为进行判别。

随着智能化认知设备的发展,电磁目标行为分析相关的研究逐渐兴起[34],相继提出雷达行为[35]、电磁辐射源行为学[36]等相关概念。根据现有研究,电磁目标行为可分为个体行为和群体行为。个体行为通常表现为辐射源信号参数的变化、所搭载平台运动规律的改变,以及环境因素等其他能够引起个体行为发生反应并可被非合作单位识别的变化等,例如辐射源扫描方式的改变、电磁目标工作时间段的变化等;群体行为则需要注

重空间相互关系的影响,包括电磁密度、电磁频谱占用度的划分,群体阵列的结构构成,以及任务事件的进程等。要建立庞大的行为知识体系,行为建模不仅要包含个体行为和群体行为,还要考虑时间粒度、空间粒度的划分。目前关于电磁目标行为建模一般采用人工或机器学习的方法提取行为描述特征,也有采用多层级语义建模的方法[37],还有学者构建实时动态的频谱行为知识图谱,利用采集频谱数据中提取的语义与知识进行建模[38]。通过行为建模来获得电磁目标的内部决策机制,进而为后续干扰策略优化提供基础参数。

4.2.3　异常检测

异常检测就是将被视为正常的活动定义与观察到的事件进行比较,以识别显著偏差的过程[39]。深度学习未发展之前,异常检测分析主要基于统计的方法[39]。但随着数据量呈指数型增长且参数灵活多变,过时的模型导致误报率更高,文献[40]证明基于统计的算法在检测图像和序列数据集上的异常值方面性能是次优的。而深度学习的方法可以学习大规模数据的深层特征,从而获得良好的性能。

以标签数据划分,基于深度学习的异常检测可分为有监督、无监督和半监督三类。有监督的异常检测使用标注的正常和异常数据来训练深度分类器,尽管相对于传统方法性能有所提高,但数据类别不平衡,即正类标签的总数远远多于负类标签的总数的问题常常导致性能次优。此外,在电子战领域的辐射源行为特征数据通常难以准确完善地标注,因此有监督的方法不如无监督或半监督的方法有效。无监督的异常检测仅基于数据的内在分布特性来区分异常,大多采用聚类的方法。而半监督的异常检测通常采用正类的单类标签来分离异常,利用异常数据与正常数据的特征差异性,在模型训练时学习正类数据特征,在测试时对包含有正常和异常的数据进行分类,进而识别出异常数据。

4.2.4　意图识别

意图识别[41]也被称为目的识别,是通过分析目标的部分或所有行动,或者分析其行动导致的状态或环境变化来识别意图的任务,而行为预测更侧重于通过分析历史数据来预测未来的行为,这是两个相关但不完全相同的概念。在认知电子战中,既要考虑对方意图具备的欺骗性、动态性以及对抗性等诸多特性,同时还要考虑意图误判的代价敏感性。识别对方意图是一个由诸多细微信息综合提炼、依靠经验数据支持的推理分析和概率计算过程。

由于智能算法在处理复杂大数据的优越表现,意图识别的研究已经逐渐从基于模板匹配、贝叶斯网络[42]以及隐马尔可夫模型等依靠领域专家知识的传统方法转为深度学习的方法。因为作战意图具有时间关联性,目前意图识别中深度学习的方法多采用门控循环单元、长短时记忆网络等时间序列网络模型。但是考虑到认知电子战中决策的时效性,网络模型的快速性同样不可忽视。而且现有方法的参数选择多从信号层面,环境建模较为理想化,要构建更为完善的意图识别系统,还需要综合考虑信号、时间、空间层面,甚至舆论层面的各种因素影响。最终通过不断改进完善,在保证准确率和误判代价的前提下,逐步发展为更具先进性的意图预测[43]。

4.3　决策技术

决策技术,即干扰决策,其目标是基于感知和判断的结果实时生成最佳的干扰策略与波形。

4.3.1　问题模型

最佳干扰策略的关键是最佳干扰波形序列的生成,包括干扰样式、干扰时刻、干扰能量等。在此基础上,根据干扰目标不同状态变化情况,对干扰效能进行评估,进而优化干扰策略,对后续的干扰资源调度进行引导,从而保证干扰持续有效。核心目标是基于可观测参数向量$[\boldsymbol{o}(0),\cdots,\boldsymbol{o}(t)]$(如目标信号特征、干扰信号特征、接收机状态、环境因素、任务目标等)、不可观测参数向量$[\boldsymbol{z}(0),\cdots,\boldsymbol{z}(t)]$(如未知环境因素、未知辐射源状态等)和控制参数向量$[\boldsymbol{c}(0),\cdots,\boldsymbol{c}(t-1)]$(如干扰信号$j(t)$生成参数、干扰模式、发射机参数、节点部署方式等)来确定控制参数向量$\boldsymbol{c}(t)$,使得效用函数$U(t+1)$最大,目标函数表示为

$$\begin{aligned}\boldsymbol{s}(t) &= \arg\max_{\boldsymbol{c}(t)} U(t+1)\\ &= \zeta(\boldsymbol{o}(0),\cdots,\boldsymbol{o}(t),\boldsymbol{c}(0),\cdots,\boldsymbol{c}(t),\boldsymbol{z}(0),\cdots,\boldsymbol{z}(t))\end{aligned} \tag{5}$$

其中满足条件的$\boldsymbol{c}(t)$构成t时刻最佳干扰策略$\boldsymbol{s}(t)$。

4.3.2　认知干扰策略生成

在传统对抗过程中,获取目标信号侦察信息后主要依靠从预设干扰策略库中或凭借经验制定干扰策略,选取预存储的干扰波形进行对抗,而当目标先验缺失、目标信号参数动态变化或出现新目标时,传统基于“剧本”的对抗方式无法自适应地调整干扰策略以完成有效干扰,对抗效果将会

被极大地削弱甚至完全失效。

现有的认知干扰重点是基于侦察中获取的目标特征信息进行最优化干扰决策,其能够适应数据库中有类似波形对抗策略的未知目标对抗问题。

目前,认知干扰策略生成的主要方法是基于强化学习的决策方法。常用的强化学习算法主要包括动态规划、时序差分学习、Q-Learning 等[44]。但该类方法实现的前提是实时获取并修正干扰奖励函数,而对于快速变化的对抗场景,奖励函数的定义本身就是一个难题。因此,该类方法目前只能针对特定缓慢变化目标的干扰任务,当目标信号参数快速变化时,仍然难以发挥作用。另外,对于多种已有波形组合或者是全新波形的对抗问题,一般性的推理和决策也难以找到最优的干扰波形。

认知干扰决策难题在于如何基于对威胁目标未知波形的认知实现实时高效对抗策略的优化。生成式深度学习技术[45-46]、零样本学习技术[47]以及知识-数据联合驱动学习技术[48]的兴起为解决这个问题提供了新的思路。面对潜在未知目标波形,由于学习过程中数据样本的缺失,需要融合领域知识进行联合驱动,使系统具有对信号的"深度"理解能力,进而缩短对未知威胁的干扰反应时间,提升电子战系统干扰成功率。

4.3.3　在线效果评估

传统电子战不能实时评估干扰效果,感知—判断—决策—行动环始终是"侦察—干扰"的开环模式,无法实现"侦察—干扰—侦察"的闭环模式。闭环对抗要实时获取干扰效果信息,即要能够做到基于干扰方的干扰效果评估。以雷达对抗为例,雷达在受到干扰后,在工作模式、行为特征、信号特征等方面会存在一定的变化,主要包括:工作模式切换如跟踪模式受到干扰后会切换到搜索模式,或者采用一些抗干扰措施如频率捷变、重频抖动、功率管控等。通过工作模式、行为特征、信号特征等的变化能评估雷达受到干扰的效果。

目前,在线干扰效果评估是认知电子战领域的研究难题。学术界的研究成果较少,其核心在于构建目标电子系统的状态变化集、状态变化集如何与干扰决策过程进行耦合,以及修正干扰目标奖励函数并共同引导决策过程在线优化。

5　未来挑战与发展

认知电子战概念自提出以来,已经经历了十多年的发展,但现有的系统距离真正意义上的"认知能力"还具有一定的差距,本节将阐述认知电子战所面临的挑战与其关键技术发展方向。

5.1　未来挑战

虽然人工智能技术已经在计算机视觉、自然语言处理领域得到了广泛应用,但是在与电子战结合的过程中依旧面临诸多挑战,主要表现为开放性电磁环境带来的变化引起的智能学习过程的非鲁棒性。

一是未知目标。认知电子战中的信号识别、个体识别、行为建模、意图识别等环节都面临着新增的未知目标的挑战。一方面,随着电子信息系统的数量与种类不断增加,新的波形层出不穷,信号识别与个体识别等任务必须具有开集识别和新目标认知能力;另一方面,不同目标执行的任务多导致信号工作模式等更加多样化,未知行为分析和意图识别挑战大。

二是未知环境。现代战场的电磁空间斗争激烈,多种电磁信号、干扰和噪声相互交织。检测、测向、信号识别、个体识别等环节均易受到复杂多变环境的影响,即复杂多变的电磁环境使平时积累的数据分布特性与模型应用时实时接收到的数据分布特性存在不同程度的差异,从而导致学习训练模型失配,性能大幅度下降。

三是频谱对抗。现实中大部分侦察活动面临着干扰的挑战。干扰技术旨在破坏或掩盖原始信号,通常采用高功率、捷变频等手段,使侦察系统难以检测和区分所需的信号和干扰信号。现有列装的设备大多依赖于时域或频域分离信号。如何应对时频混叠干扰信号的威胁,保证干扰条件下侦察系统的可靠性、稳定性、准确性(即扰中侦),已成为重中之重。

5.2　关键技术发展

5.2.1　基于零样本学习的信号与目标认知

如前文所述,认知电子战的最大优势在于可以针对未知目标进行分析识别,这一过程所涉及的关键技术为零样本学习。

零样本学习允许人工智能模型识别以前从未见过的目标或概念。与传统的监督学习不同,模型从训练实例中学习,只能在它所训练的类别中对物体进行分类,零样本允许人工智能模型使用语义属性和关系来建模所学的目标。

在零样本学习中,模型学习信号数据和特征语义信息之间的映射,如信号不同特征描述、信号属性的层次和关系。根据这些语义属性为新的未知目标预测一个标签。因此,在认知电子战关键

技术研究中,面对潜在的未知目标与未知波形,需要融合关于辐射源信号领域知识进行语义建模与关联,实现对未知波形的特征提取。

5.2.2　鲁棒性学习推理

认知电子战技术发展和系统研制离不开多样化数据的支撑,这就要求研究人员以及工程师们高度重视电子战数据工程问题。但是,现有研究揭示了以深度学习为代表的人工智能模型存在明显的脆弱性[49-50],以对抗样本为代表的攻击技术将会制约未来智能化手段部署到电子战装备中的安全性。因此,认知电子战模型的鲁棒性和安全性不容忽视。近年来,世界各主要军事强国在智能化电磁频谱对抗样本攻防领域的研究飞速发展[51-60]。

自 2019 年始,对抗样本的研究成果开始应用于电磁信号领域。Sadeghi 等首次在基于深度学习的无线信号调制识别任务中提出了一种白盒对抗攻击方法和通用对抗攻击方法[61]。结果表明对抗攻击可以在极小的扰动下大大降低智能调制识别的分类性能,这给使用基于深度学习的识别算法带来了重大的安全性问题。随后,不同研究人员先后开展各类对抗样本攻击算法在调制识别、个体识别等领域的应用。2021 年开始,研究人员开始结合真实物理场景,结合领域特有的知识,优化对抗样本的生成算法,不断增强对抗样本对真实物理场景的适应能力。

综上,现有认知电子战关键技术中基于深度学习模型的各类方法由于缺乏可解释性,极容易受到对抗样本攻击的威胁,给模型在复杂电磁环境下强对抗场景中的实际应用带来严重安全隐患,亟待开展适应对抗样本波形的鲁棒性学习推理方法研究。

5.2.3　时频混叠信号实时分离

在实际对抗过程中,当电子战系统实施干扰时,由于干扰信号与目标时频重叠,无法同步开展侦察,这就带来两个挑战:一是无法实时侦测目标信号的变化从而及时做出反应,导致认知电子战过程无法持续进行;二是干扰过程中无法侦察到目标信号的变化从而直接影响在线效果评估。因此,需要开展时频混叠信号实时分离技术研究,为实现认知电子战过程中的“干扰中侦察”以及在线效果评估提供实时不断的目标数据。

5.2.4　分布式认知对抗技术

群体智能是一个受社会昆虫群落集体行为启发的概念,其中个体代理在本地相互作用以实现全球目标。这一概念已成功应用于各个领域,包括机器人、优化和决策。通过利用群体的集体智慧,可以实现卓越的性能并克服传统集中式方法的局限性。在认知电子战的背景下,群体智能可以增强其分布式感知和通信、自适应和弹性行为、合作干扰和欺骗、动态任务分配等能力,大幅提升系统适应性、弹性和有效性。

6　总结

随着人工智能理论的高速发展和不断涌现,更加先进的机器学习算法和技术将会不断出现,认知电子战技术将逐渐成熟并进入应用,不断提升电子战在强对抗、快变化电磁环境下的敏捷性与整体作战能力。

参考文献(References)

[1] 周一宇, 安玮, 郭福成, 等. 电子对抗原理与技术[M]. 北京: 电子工业出版社, 2014.
ZHOU Y Y, AN W, GUO F C, et al. Principles and technologies of electronic warfare system [M]. Beijing: Publishing House of Electronics Industry, 2014. (in Chinese)

[2] 苏周, 韩俊, 刘飞, 等. 美军认知电子战发展特点和趋势研究[J]. 中国电子科学研究院学报, 2022, 17(11): 1057-1064.
SU Z, HAN J, LIU F, et al. Research on characteristics and trends of the development of cognitive EW in the US military[J]. Journal of China Academy of Electronics and Information Technology, 2022, 17(11): 1057-1064. (in Chinese)

[3] 张春磊, 杨小牛. 认知电子战初探[J]. 通信对抗, 2013, 32(2): 1-4, 20.
ZHANG C L, YANG X N. Elementary study on cognitive electronic warfare [J]. Communication Countermeasures, 2013, 32(2): 1-4, 20. (in Chinese)

[4] 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.
WANG S F, BAO Y F, LI Y. The architecture and technology of cognitive electronic warfare[J]. Scientia Sinica (Informations), 2018, 48(12): 1603-1613. (in Chinese)

[5] HAIGH K, ANDRUSENKO J. Cognitive electronic warfare: an artificial intelligence approach [M]. Boston: Artech House, 2021.

[6] DARPA. Behavioral learning for adaptive electronic warfare, DARPA-BAA-10-79 [R]. Arlington, USA: Defense Advanced Research Projects Agency, 2010.

[7] 张春磊, 杨小牛. 认知电子战与认知电子战系统研究[J]. 中国电子科学研究院学报, 2014, 9(6): 551-555, 562.
ZHANG C L, YANG X N. Research on the cognitive electronic warfare and cognitive electronic warfare system[J]. Journal of China Academy of Electronics and Information Technology, 2014, 9(6): 551-555, 562. (in Chinese)

[8] KNOWLES J. Regaining the advantage: cognitive electronic warfare[J]. Journal of Electronic Defense, 2016, 39(12): 56-62.

[9] 安红, 张朔, 赵耀东, 等. 面向认知对抗的学习训练与仿真评估系统设计[J]. 太赫兹科学与电子信息学报,

2022, 20(2): 133 – 139.
AN H, ZHANG S, ZHAO Y D, et al. Design of learning training and simulation evaluation system for cognitive electronic warfare[J]. Journal of Terahertz Science and Electronic Information Technology, 2022, 20(2): 133 – 139. (in Chinese)

[10] BIS Research. Cognitive electronic warfare: the rise of AI and ML in modern conflict[EB/OL]. (2023 – 01 – 25)[2023 – 06 – 01]. https://bisresearch.com/news/cognitive-electronic-warfare-the-rise-of-ai-and-ml-in-modern-conflicts.

[11] ZHOU H J. An introduction of cognitive electronic warfare system[C]//Proceedings of International Conference on Communications, Signal Processing, and Systems, 2020.

[12] DIAMANT R. Closed form analysis of the normalized matched filter with a test case for detection of underwater acoustic signals[J]. IEEE Access, 2016, 4: 8225 – 8235.

[13] SHIN Y, NAM S W, AN C K, et al. Design of a time-frequency domain matched filter for detection of non-stationary signals[C]//Proceedings of IEEE International Conference on Acoustics, Speech, and Signal Processing, 2001: 3585 – 3588.

[14] GARDNER W A. Exploitation of spectral redundancy in cyclostationary signals[J]. IEEE Signal Processing Magazine, 1991, 8(2): 14 – 36.

[15] ZENG Y H, LIANG Y C. Maximum-minimum eigenvalue detection for cognitive radio[C]//Proceedings of 2007 IEEE 18th International Symposium on Personal, Indoor and Mobile Radio Communications, 2007.

[16] ZENG Y, KOH C L, LIANG Y C. Maximum eigenvalue detection: theory and application[C]//Proceedings of 2008 IEEE International Conference on Communications, 2008.

[17] ZENG Y H, LIANG Y C. Eigenvalue-based spectrum sensing algorithms for cognitive radio[J]. IEEE Transactions on Communications, 2009, 57(6): 1784 – 1793.

[18] ZENG Y H, LIANG Y C. Spectrum-sensing algorithms for cognitive radio based on statistical covariances[J]. IEEE Transactions on Vehicular Technology, 2009, 58(4): 1804 – 1815.

[19] YUAN Y, SUN Z H, WEI Z H, et al. DeepMorse: a deep convolutional learning method for blind morse signal detection in wideband wireless spectrum[J]. IEEE Access, 2019, 7: 80577 – 80587.

[20] PRASAD K N R S V, D'SOUZA K B, BHARGAVA V K. A downscaled faster-RCNN framework for signal detection and time-frequency localization in wideband RF systems[J]. IEEE Transactions on Wireless Communications, 2020, 19(7): 4847 – 4862.

[21] ZHA X, PENG H, QIN X, et al. A deep learning framework for signal detection and modulation classification[J]. Sensors, 2019, 19(18): 4042.

[22] LI R D, HU J H, LI S Q, et al. Blind detection of communication signals based on improved YOLO3[C]//Proceedings of 2021 6th International Conference on Intelligent Computing and Signal Processing (ICSP), 2021: 424 – 429.

[23] HUANG Z T, WU L L, LIU Z M. Toward wide-frequency-range direction finding with support vector regression[J]. IEEE Communications Letters, 2019, 23(6): 1029 – 1032.

[24] WU L L, HUANG Z T. Coherent SVR learning for wideband direction-of-arrival estimation[J]. IEEE Signal Processing Letters, 2019, 26(4): 642 – 646.

[25] EL ZOOGHBY A H, CHRISTODOULOU C G, GEORGIOPOULOS M. Performance of radial-basis function networks for direction of arrival estimation with antenna arrays[J]. IEEE Transactions on Antennas and Propagation, 1997, 45(11): 1611 – 1617.

[26] EL ZOOGHBY A H, CHRISTODOULOU C G, GEORGIOPOULOS M. Antenna array signal processing with neural networks for direction of arrival estimation[C]//Proceedings of IEEE Antennas and Propagation Society International Symposium 1997. Digest, 1997.

[27] LIU Z M, ZHANG C W, YU P S. Direction-of-arrival estimation based on deep neural networks with robustness to array imperfections[J]. IEEE Transactions on Antennas and Propagation, 2018, 66(12): 7315 – 7327.

[28] WU L L, LIU Z M, HUANG Z T. Deep convolution network for direction of arrival estimation with sparse prior[J]. IEEE Signal Processing Letters, 2019, 26(11): 1688 – 1692.

[29] WU L L, LIU Z M, HUANG Z T, et al. Deep neural network for DOA estimation with unsupervised pretraining[C]//Proceedings of 2019 IEEE International Conference on Signal, Information and Data Processing (ICSIDP), 2019.

[30] KULIN M, KAZAZ T, MOERMAN I, et al. End-to-end learning from spectrum data: a deep learning approach for wireless signal identification in spectrum monitoring applications[J]. IEEE Access, 2018, 6: 18484 – 18501.

[31] O'SHEA T J, WEST N E. Radio machine learning dataset generation with GNU radio[C]//Proceedings of the GNU Radio Conference, 2016.

[32] JAGANNATH A, JAGANNATH J, KUMAR P S P V. A comprehensive survey on radio frequency (RF) fingerprinting: traditional approaches, deep learning, and open challenges[J]. Computer Networks, 2022, 219: 109455.

[33] MCGINTHY J M, WONG L J, MICHAELS A J. Groundwork for neural network-based specific emitter identification authentication for IoT[J]. IEEE Internet of Things Journal, 2019, 6(4): 6429 – 6440.

[34] 朱玉萍, 王海, 路征. 让电磁态势成为制胜战场的新砝码[N]. 解放军报, 2018 – 02 – 08(7).
ZHU Y P, WANG H, LU Z. Make electromagnetic situation a new weight for winning the battlefield[N]. PLA Daily, 2018 – 02 – 08(7). (in Chinese)

[35] 欧健. 多功能雷达行为辨识与预测技术研究[D]. 长沙: 国防科技大学, 2017.
OU J. Research on behavior recognition and prediction techniques against multi-function radar[D]. Changsha: National University of Defense Technology, 2017. (in Chinese)

[36] 石荣, 肖悦. 行为科学的新分支: 电磁辐射源行为学[J]. 航天电子对抗, 2018, 34(4): 1 – 6.
SHI R, XIAO Y. A new branch of behavioral science: electromagnetic radiation source behaviorology[J]. Aerospace Electronic Warfare, 2018, 34(4): 1 – 6. (in Chinese)

[37] 王铃兰. 基于知识的电磁目标行为分析[D]. 成都: 电子科技大学, 2022.
WANG L L. Analysis of electromagnetic target behavior based on knowledge[D]. Chengdu: University of Electronic Science and Technology of China, 2022. (in Chinese)

[38] 周博, 马欣怡, 况婷妍, 等. 电磁频谱空间态势认知新范

式:频谱语义和频谱行为[J]. 数据采集与处理, 2022, 37(6): 1198 - 1207.
ZHOU B, MA X Y, KUANG T Y, et al. New paradigm of electromagnetic spectrum space situation cognition: spectrum semantic and spectrum behavior [J]. Journal of Data Acquisition and Processing, 2022, 37(6): 1198 - 1207. (in Chinese)

[39] XIE M, HAN S, TIAN B M, et al. Anomaly detection in wireless sensor networks: a survey[J]. Journal of Network and Computer Applications, 2011, 34(4): 1302 - 1325.

[40] CHALAPATHY R, CHAWLA S. Deep learning for anomaly detection: a survey[J/OL]. arXiv: 1901.03407[2023 - 06 - 01]. https://arxiv.org/abs/1901.03407.

[41] SADRI F. Logic-based approaches to intention recognition[M]// Handbook of Research on Ambient Intelligence and Smart Environments. Pennsylvania: IGI Global, 2011: 346 - 375.

[42] 葛顺. 基于规则发现和贝叶斯推理的战术意图识别技术[D]. 哈尔滨: 哈尔滨工程大学, 2015.
GE S. Research on tactical intention recognition based on rule discovery and Bayesian reasoning [D]. Harbin: Harbin Engineering University, 2015. (in Chinese)

[43] 黄苏豫. 基于图学习电磁目标影响关系的入侵意图识别[D]. 北京: 北京邮电大学, 2021.
HUANG S Y. Intrusion intention recognition of electromagnetic target influence relation based on graph learning [D]. Beijing: Beijing University of Posts and Telecommunications, 2021. (in Chinese)

[44] NASIR Y S, GUO D N. Multi-agent deep reinforcement learning for dynamic power allocation in wireless networks[J]. IEEE Journal on Selected Areas in Communications, 2019, 37(10): 2239 - 2250.

[45] GOODFELLOW I, POUGET-ABADIE J, MIRZA M, et al. Generative adversarial networks[J]. Communications of the ACM, 2020, 63(11): 139 - 144.

[46] YANG L, ZHANG Z L, SONG Y, et al. Diffusion models: a comprehensive survey of methods and applications[EB/OL]. (2022 - 09 - 02)[2023 - 06 - 01]. https://arxiv.org/abs/2209.00796/.

[47] POURPANAH F, ABDAR M, LUO Y X, et al. A review of generalized zero-shot learning methods [J]. IEEE Transactions on Pattern Analysis and Machine Intelligence, 2022, 45(4): 4051 - 4070.

[48] DASH T, CHITLANGIA S, AHUJA A, et al. A review of some techniques for inclusion of domain-knowledge into deep neural networks[J]. Scientific Reports, 2022, 12: 1040.

[49] SZEGEDY C, ZAREMBA W, SUTSKEVER I, et al. Intriguing properties of neural networks[C]//Proceedings of 2nd International Conference on Learning Representations, 2014.

[50] GOODFELLOW I J, SHLENS J, SZEGEDY C. Explaining and harnessing adversarial example [C]//Proceedings of International Conference on Learning Representations, 2015.

[51] KIM B, SAGDUYU Y, ERPEK T, et al. Adversarial attacks on deep learning based mmWave beam prediction in 5G and beyond [C]//Proceedings of 2021 IEEE Statistical Signal Processing Workshop (SSP), 2021.

[52] KIM B, SAGDUYU Y E, ERPEK T, et al. Channel effects on surrogate models of adversarial attacks against wireless signal classifiers [C]//Proceedings of ICC 2021: IEEE International Conference on Communications, 2021.

[53] KIM B, SAGDUYU Y E, DAVASLIOGLU K, et al. Channel-aware adversarial attacks against deep learning-based wireless signal classifiers[J]. IEEE Transactions on Wireless Communications, 2022, 21(6): 3868 - 3880.

[54] KIM B, SAGDUYU Y E, DAVASLIOGLU K, et al. Over-the-air adversarial attacks on deep learning based modulation classifier over wireless channels[C]//Proceedings of 2020 54th Annual Conference on Information Sciences and Systems (CISS), 2020.

[55] KIM B, SAGDUYU Y E, DAVASLIOGLU K, et al. How to make 5G communications "invisible": adversarial machine learning for wireless privacy[C]//Proceedings of 2020 54th Asilomar Conference on Signals, Systems, and Computers, 2020.

[56] HOU T, WANG T, LU Z, et al. IoTGAN: GAN powered camouflage against machine learning based IoT device identification [C]//Proceedings of IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), 2021.

[57] SHI Y, ERPEK T, SAGDUYU Y E, et al. Spectrum data poisoning with adversarial deep learning[C]//Proceedings of MILCOM 2018: 2018 IEEE Military Communications Conference (MILCOM), 2018.

[58] SHI Y, DAVASLIOGLU K, SAGDUYU Y E. Generative adversarial network in the air: deep adversarial learning for wireless signal spoofing[J]. IEEE Transactions on Cognitive Communications and Networking, 2021, 7(1): 294 - 303.

[59] KOKALJ-FILIPOVIC S, MILLER R. Adversarial examples in RF deep learning: detection of the attack and its physical robustness[EB/OL]. (2019 - 02 - 16)[2023 - 06 - 01]. https://arxiv.org/abs/1902.06044/.

[60] KOKALJ-FILIPOVIC S, MILLER R, CHANG N, et al. Mitigation of adversarial examples in RF deep classifiers utilizing AutoEncoder pre-training[C]//Proceedings of 2019 International Conference on Military Communications and Information Systems (ICMCIS), 2019.

[61] SADEGHI M, LARSSON E G. Adversarial attacks on deep-learning based radio signal classification[J]. IEEE Wireless Communications Letters, 2019, 8(1): 213 - 216.