工程科学学报
Chinese Journal of Engineering

人工智能在军事对抗中的应用进展

张智敏 石飞飞 万月亮 徐阳 张帆 宁焕生

Application progress of artificial intelligence in military confrontation

ZHANG Zhi-min, SHI Fei-fei, WAN Yue-liang, XU Yang, ZHANG Fan, NING Huan-sheng

引用本文:
张智敏, 石飞飞, 万月亮, 徐阳, 张帆, 宁焕生. 人工智能在军事对抗中的应用进展[J]. 工程科学学报, 2020, 42(9): 1106-1118. doi: 10.13374/j.issn2095-9389.2019.11.19.001
ZHANG Zhi-min, SHI Fei-fei, WAN Yue-liang, XU Yang, ZHANG Fan, NING Huan-sheng. Application progress of artificial intelligence in military confrontation[J]. *Chinese Journal of Engineering*, 2020, 42(9): 1106-1118. doi: 10.13374/j.issn2095-9389.2019.11.19.001

在线阅读 View online: https://doi.org/10.13374/j.issn2095-9389.2019.11.19.001

工程科学学报, 第 42 卷, 第 9 期: 1106−1118, 2020 年 9 月
Chinese Journal of Engineering, Vol. 42, No. 9: 1106−1118, September 2020
https://doi.org/10.13374/j.issn2095-9389.2019.11.19.001; http://cje.ustb.edu.cn

人工智能在军事对抗中的应用进展

张智敏[1,2)], 石飞飞[1)], 万月亮[3,4)], 徐　阳[1)], 张　帆[1)], 宁焕生[1,4)]✉

1) 北京科技大学计算机与通信工程学院, 北京 100083　2) 北京科技大学顺德研究生院, 佛山 528300　3) 北京锐安科技有限公司, 北京 100192　4) 北京市网络空间数据分析与应用工程技术研究中心, 北京 100083

✉通信作者, E-mail: ninghuansheng@ustb.edu.cn

摘　要　人工智能特别是近几年深度学习的飞速发展, 深刻的影响着军事领域, 并赋予现代战争智能性、交叉性和破坏性的新特点. 要想在军事对抗中取胜, 不仅需要机器智能, 同样需要人类智慧, 能在军事作战中达到人机高度协同, 是实现人与机器取长补短的重要途径, 也是在愈发复杂的战争形势中取得胜利的关键. 本文将军事对抗中人工智能的应用作为切入点, 罗列了代表性国家在军事领域对人工智能的重视程度, 从对抗策略和物联网三层架构两大角度对发展现状进行总结, 同时指出在目前军事领域使用人工智能存在的不足, 对人机融合智能在军事对抗中的发展趋势进行分析, 并给出可能实现的技术方案, 对未来的研究方向作出展望. 如何实现高度的人机融合, 从而获得“1+1>2”的良好效果, 是人工智能在军事对抗中的下一步研究工作.

关键词　人工智能; 军事对抗; 物联网; 人机融合智能; 技术方案

分类号　TG142.71

Application progress of artificial intelligence in military confrontation

ZHANG Zhi-min[1,2)], *SHI Fei-fei*[1)], *WAN Yue-liang*[3,4)], *XU Yang*[1)], *ZHANG Fan*[1)], *NING Huan-sheng*[1,4)]✉

1) School of Computer & Communication Engineering, University of Science and Technology Beijing, Beijing 100083, China

2) Shunde Graduate School of University of Science and Technology Beijing, Foshan 528300, China

3) Run Technologies Company, Ltd., Beijing 100192, China

4) Beijing Engineering Research Center for Cyberspace Data Analysis and Applications, Beijing 100083, China

✉ Corresponding author, E-mail: ninghuansheng@ustb.edu.cn

ABSTRACT　Artificial intelligence (AI), especially the rapid development of deep learning, has a profound impact on various industries and has continuously changed the traditional production methods and lifestyles. From passive learning with computing power to autonomous learning and enhanced learning, the development of machine intelligence is largely due to the innovation of the AI theory and practice. AI has also had a far-reaching impact on the military field, as it has provided modern warfare with new features such as intelligence, interconnectedness, and destructiveness. Winning in a military confrontation requires not only machine intelligence but also human wisdom. Therefore, human-machine collaboration would combine the strengths and complement the weaknesses of human and machine, which is the key to victory in the increasingly complex war environment. How to achieve a high degree of hybrid human–artificial intelligence to obtain a good result of “1+1>2” is also a problem that needs to be further explored in military confrontation. This paper reviewed the application of AI in military confrontation as the starting point and highlighted the important measures and achievements of representative countries in the use of AI technology in the military development process. Moreover, we analyzed the development status from the two perspectives of confrontation strategy and the three-tier architecture of the Internet of Things,

收稿日期: 2019−11−19

基金项目: 国家自然科学基金资助项目(61872038); 国家自然科学基金民航联合基金资助项目(U1633121); 北京科技大学顺德研究生院科技创新专项资金资助项目(BK19CF010)

revealed the shortcomings of using AI in the current military field, and analyzed the development trend of hybrid human–artificial intelligence in military confrontation. We also presented three possible technical schemes and detailed explanations and finally proposed future research directions. We believe that the future development trend of intelligent military may be based on the hybrid human–artificial intelligence, which will further improve the adaptability of machines to the combat environment and reveal the merits of the integration of human wisdom and machine intelligence; this integration may be the next step of AI research in military confrontation.

KEY WORDS artificial intelligence; military confrontation; Internet of Things; hybrid human –artificial intelligence; technical schemes

1956 年，人工智能（Artificial intelligence, AI）一词正式诞生，并逐渐对众多领域产生深远影响；1997 年，IBM 的“深蓝”在象棋比赛中战胜卡斯帕罗夫，人工智能在经过两次低谷后重回大众视线，但此时机器的良好表现更多要归功于超强的计算能力，它不能像人类一样理解棋局所代表的含义；2006 年，在 Hinton 的带领下，深度学习领域取得重大突破[1]，人工智能进入爆发期；2017 年，拥有“深度学习”大脑的 AlphaGo 强势来袭，击败世界围棋冠军柯洁，机器开始拥有“思考”能力；同年，只通过三天自我博弈与学习的 AlphaGo Zero 出师，不仅击败 AlphaGo，还学会了三种不同的棋类游戏，机器开始拥有“洞察力”[2]. 人工智能特别是深度学习的不断发展，使机器不再受限于特定的程序，转而开始拥有思考能力，机器变得越来越“聪明”；而人类智慧是机器始终无法取代的，如何实现智慧与智能的融合，也就开启了人工智能领域新的研究话题.

纵观军事领域，高科技化军事装备的出现，势必会对作战形势以及取胜机制产生重大影响. 但从目前国内外情况来看，部分先进科技装备不能有效、快速的投入到战斗当中，且面对复杂作战环境时，可能会出现无法发挥正常作战效应的情况，这都会严重妨碍军事力量发展.

随着人工智能及其分支技术的不断发展，军事对抗的作战形态已发生巨大变革，这将从根本上改变作战方式和制胜机理，同时会演化出众多新式武器，未来战争可能会实现由“人对人”到“机器自主杀人”的转变[3]. 目前，众多国家已经开始投入到对人工智能在军事领域的研究当中，并取得了重大的进展，这将加速推进战争形态向智能化迈进.

人工智能下的军事，从对抗策略角度进行分析，需要解决在军事攻击、军事检测和军事防御方面如何有效的将人工智能融入其中这一问题，同时为达到作战一致性，协同配合也需要着重考虑. 而若从物联网三层架构分析军事对抗中的人工智能技术，需要解决软硬件在感知层、网络层和应用层的对抗问题，从而形成完备的军事攻防体系.

由于技术水平有限，在目前的军事对抗中，还无法完全交由机器进行实时响应、紧急决策处理；在未来的一段时间内，无法实现武器装备完全自主控制. 这表明在执行过程中，依旧需要人工操纵与控制，来确保整个作战过程不出现偏差. 通过让机器承担操作性的任务，让人承担决策性的工作，从而实现人与机器的高度融合，优势互补，是未来军事对抗的发展方向.

人机融合智能，是一种强人工智能，简单来说就是可以将人与机器优势相互结合的一种智能形势. 人类与机器在态势感知、数据处理、决策分析等方面可以做到优势互补，是弥补人类与机器各自缺点的重要方式. 能否实现多种作战方式，将取决于人机融合智能能否有效的应用于军事对抗中，也取决于人与机器在实际对抗中遇到各类突发情况时是否能够默契配合.

人机融合智能在军事对抗中的应用，以人工智能在军事对抗中的应用为基础，以如何在各类战争角色中实现人–机高度协同为主要研究内容，在有人进行监督参与的情况下，使机器以不同方式配合实现在“防御–检测–攻击”的高效运作，最终实现“1+1>2”的对抗效果.

在目前，人机融合智能在军事对抗中仍有很多问题需要解决，这些问题主要有：

（1）赋予机器的假设条件是有限的，面对复杂的作战环境，这种有限性限制了决策的多样性；

（2）环境高度复杂化、高度不确定化，导致数据量急剧增加，但目前人机之间的信息传递效率低，具有滞后性，在不同编队的情况下，如何实现数据高速共享也是需要思考的问题；

（3）由于作战任务高度复杂且对时间精度要求较高，干预问题成为人机融合智能在军事对抗中不可忽略的问题之一，何时由人获得主控权，何时由机器获得主控权，需要对人机融合系统进行充分设计.

人机融合智能在军事对抗中的应用，可以认为是智能系统与决策技术的高度融合，这将是多学科交叉的研究成果. 如何实现人机协同打击工

作, 如何对人机承载能力进行合理划分, 如何在人机协同时进行态势感知, 如何对出现的突发事件进行实时检测与分析, 如何协同处理好各项任务, 是实现“1+1>2”作战效果的关键.

1　人工智能在各国军事发展中的应用现状

2008 年, IBM 公司开始进行脉冲神经网络芯片的研制, 随后与美国空军联合进行大脑启发式超算系统的开发[4]; 2014 年, 美国军方提出“第三次抵消战略”, 将研究重心向机器学习、机器辅助作战等方向转移; 2016 年, 评估通过了 ALPHA 智能超视距空战系统, 该系统主框架采用“模糊学习树”技术, 并搭载专家系统, 可在协同空战中迅速作出决策, 但系统评估在相对固定的空战环境进行, 与实际空战环境有一定差距; 2017 年, 美国国防部正式发布名为“Project Maven”的备忘录, 旨在进一步发展人工智能等技术在战争中的重要作用[4]; 2018 年, 美国战略与预算评估中心发布《未来地面部队人机编队》报告, 报告阐述的主要内容有: 发展未来地面部队人机编队的主要推动因素、可使未来地面部队在战争中获得竞争优势的三大人机编队形式、发展未来人机编队面临的主要挑战、以及通过人机编队提高未来地面部队作战效能的战略; 2019 年, 美国空军发布《2019 年人工智能》战略, 特别强调出人工智能在目前军事发展中的重要性, 同时这也是针对国防部提出的人工智能战略的细化, 更加关注人工智能在军事领域的应用.

俄罗斯认为未来军事的主要竞争力将会围绕人工智能展开, 因此俄罗斯正在大力发展类人机器人、机器人部队. 从 2016 年起, 俄罗斯每年都会召开“俄罗斯联邦武装力量自动化”军事科技会议; 据国防部长谢依盖·绍伊古称, 最近 3 年俄罗斯武装力量成立了 10 个大型科研院所和中心, 这些科研院所和中心正在研究人工智能等众多领域; 普京表示, 人工智能不仅仅是俄罗斯, 更是全世界的未来. 目前, 俄罗斯军事工业委员会已经批准, 计划于 2030 年从远程控制和人机智能机器人平台上获得 30% 的作战力量.

以色列向来就有“初创国度”的美誉, 其在军事技术中的表现也成为该国科技创新的重要突破口. 2008 年, 为加强监视加沙地区边界, 以色列开始在实战中使用准自动军用车, 这也是全球首个在实战中使用准自动军用车的国家. 目前, 在军事部署中使用全自动机器人, 是以色列军方研究的重点领域; 2016 年 7 月, 以色列军方开始使用自主驾驶汽车进行边境巡逻. 在此基础上, 以色列国防军准备在汽车上安装例如机关枪等武器, 并准备不断部署到边境地区; 同时以色列军方也在考虑如何将机器人与士兵进行混合编队, 最终实现更好的对抗效果. 据了解, 以色列正在研制一款具有智能功能的护目镜, 该护目镜可以远程得到医疗指导, 在战争环境中可以提供紧急援助功能. 不论是部署的摄像头还是安装在坦克上的传感器, 以军通过大量装备及多种途径进行数据的采集, 这些信息可以实现共享, 不仅指挥部与军官可以使用, 战场上的作战部队也可以对数据进行处理. 2019 年, 拉斐尔公司的 Spice 炸弹又有了新的技术突破, 在原有目标自动识别的基础上, 又加入了人工智能与场景匹配技术, 这也显示出以色列军方对人工智能的高度重视.

而我国也同样重视人工智能在军事中的发展. 2017 年 7 月, 国务院公布了到 2030 年前把中国变成“人工智能领域的领先国家和全球创新中心”的详细战略. 该战略表示会加大对人工智能在国防领域的研究与投资, 并注重人工智能在自动化与预测中的应用; 2019 年, 我国发表《新时代的中国国防》白皮书, 对战争形态、作战方式在人工智能的推动下发生的巨大变革进行进一步的阐述. 此外, 英国、日本等国家也十分重视人工智能与军事对抗的融合与发展.

2　人工智能在军事对抗中的技术发展现状

本节首先从对抗策略对人工智能在军事对抗中的发展进行简单阐述, 随后从物联网三层架构分析军事对抗中的人工智能技术.

2.1　对抗策略

2.1.1　智能防御

面对敌方的高强度打压, 如何进行有效的防御是军事对抗中需要重点考虑的问题. 而目前, 战争形态越来越趋向于信息化、数字化, 如何能提高数据样本的抗干扰能力, 在面对敌方扰动时如何采取有效的策略进行应对, 是防御阶段首要考虑的问题. Lecuyer 等[5] 将密码学差分隐私用到对抗样本的防御上, 同时在原始深层神经网络(Deep neural networks, DNN)中加入噪声层, 可以有效达到防御对抗样本的目的; Papernot 等[6] 基于 DNN 提出防御蒸馏模型, 该模型在应对对抗性样本时具有良好的效果, 相比于原先的蒸馏方法, 该方法鲁棒性和泛化性有所提升; 除 DNN 外, 也可以在其他的神经网络中加入防御特性: 如新的防御算

法 ADV-BNN[7]，是以贝叶斯网络为基础对随机性建模，并且通过构造贝叶斯网络中的最小极大值问题来学习在攻击下的最优模型分布，从而得到一个对抗训练的贝叶斯神经网络，在强攻击下拥有较好的防御性能.

在现代技术的支撑下，仅凭一两件先进武器装备进行作战是不现实的，必须综合多个编队进行协同控制，通过相应的信息处理技术，将多平台互联互通，以信息网络为中心，进行实时数据交互，最终协同完成作战任务. 在编队方面，目前集中对多智能体（Multi agent）展开研究，因为具有自治性等众多优良的特点[8]，同时能够根据外界环境的变化进行自适应并采取相应行动，使其在分布式人工智能领域具有十分重要的作用. 早期多智能体协同编队的研究以机器人为主，以设计可以融合跟随领航者法的编队模式[9]为目标，为实现队形的灵活变换，建立出多智能体编队控制图[10−11]，同时根据全向视觉的相关内容，设计出多机器人编队及队形变换实验[12]；多智能体的理论与方法也可以和生物免疫系统相结合，用来构建免疫多智能体网络（Immune multi-agent network, IMAN）模型[13]，可以为舰艇编队协同防空体系研究提供一种新的范式；在多智能体中引入梯度估计，用于解决在多智能体的交换结构和拓扑结构实现源搜索的问题，该过程可以有效寻找多智能体编队中心[14]；分布式人工智能的发展也促进了多智能体分布一致性理论的研究，如将分布式协同控制协议用在多智能体中[15]，这种协议不仅可以改变编队结构，还可以在固定的无人机拓扑结构下达成一致，运用 Lyapunov 稳定性理论还可以实现对编队误差系统的定义.

如何进行智能规避，同样是在防御中需要考虑的问题. 目前，越来越多的无人机参与作战，但相比有人机，无人机进行规避具有更高的难度性，需要大量传感器的数据处理与交互和智能规避算法进行支撑. 对大、中型无人机和小、微型无人机差异进行分析，采用分层的感知与规避流程，提出针对不同体型无人机关于感知与规避方面的定义和架构[16]，可以针对无人机规模设计合理的规避方案；有效结合视觉方法，也可实现较好的规避效果：如结合无人机光电平台，将图像阈值法与帧差法进行融合，可以实现实时跟踪的效果，并引入人工势场法，实时计算航路点，实现对目标的规避[17]；Li 等[18]则使用到多传感器信息融合技术，并利用多模态图像，对无人机感知与规避进行深入研究. 尽管目前国内外众多学者致力于无人机规避研究，但目前仍有许多问题需要解决，如：如何使用传感器收集到精确的数据并进行有效的传输，面对复杂多变的环境形势如何进行自主决策等. 以上方法总结见表 1.

表 1 智能防御方面典型方法总结

Table 1 Summary of typical methods in intelligent defense

Research angle of intelligent defense	Method/structure	Main technology	Citation number
Data anti-interference	PixelDP DNN	Adding noise layer to the original DNN; introducing cryptography differential privacy	[5]
	Defense distillation model	Redesign of the DNN; new architecture based on defensive distillation; flexible setting of distillation temperature	[6]
	ADV-BNN	Modeling randomness in Bayesian neural network; constructing minimax problem	[7]
Intelligent cooperative formation	Leader-follower strategy formation	Leader-follower strategy	[9]
	Arbitrary switching of multi-agent formation	Multi-agent formation control chart	[10−11]
	Multi-robot formation and formation switching	Omnidirectional vision	[12]
	Immune multi-agent network	Combining biological immune system mechanisms with multi-agent approaches	[13]
	Switching formation and topology in cooperative multi-agent source seeking	Gradient estimation	[14]
	Distributed cooperative control for UAV	Distributed cooperative control protocol and implementation of error system	[15]
Intelligent avoidance	The definition and framework of UAV perception and avoidance	Layered perception and avoidance process	[16]
	Vision-based UAV perception and avoidance system	Target detection combining image threshold method and frame difference method and based on the artificial potential field method to avoid target	[17]
	UAV perception and avoidance based on multi-source information fusion	Multi-sensor information fusion technology; multi-modal image technology	[18]

2.1.2　智能检测

在作战中, 如何对危险进行检测并进行风险评估, 是攻击与防御阶段的重要基础. 目前, 战争愈发演变成信息化战场, 对信息安全风险进行全面评估是一项必不可少的环节, 人工智能可以承担起这项任务. 在目标威胁评估中, 可结合模糊优选理论[19], 根据影响目标威胁评估的因素指标, 将模糊信息数值化, 确定威胁程度优选值; 也可以在信息安全风险评估中使用人工智能技术[20], 建立起基于知识和模糊逻辑的数据库管理系统信息安全风险评估模型, 并对评估结果进行改进; 在信息传输过程, 有效使用遗传算法和神经网络, 同样可以更敏感的察觉到可能存在的风险[21].

智能装备对环境感知的重要元件是传感器, 但单一类型传感器只能反映出部分环境信息, 面对复杂的作战环境, 为提高整个作战团队的稳定性, 多传感器进行协作配合成为必然要求. 雷达经过多年的发展, 已成为无人作战系统环境感知中的重要传感器, 但若直接使用雷达数据, 可能无法精确的得到数据处理结果. 如果可以在这些数据中使用到人工智能的相关技术方法, 可以在环境感知方面取得重大突破[22]; 主流的研究思路主要是根据雷达生成的不同图像, 利用人工智能中的不同方法对图像进行处理, 结合神经网络强大的自学习能力, 来对环境进行有效感知. 但是, 一个性能表现优良的神经网络需要大量数据进行支撑, 才能有效的完成分类任务, 这与军事领域时间短、信息少的作战环境产生巨大冲突, 导致人工智能难以融入环境感知中. 基于以上原因, 一种新的观点被提出, 即认知学识别在实时对抗复杂环境下可能会发挥巨大作用, 可将认知学识别理解为深度强化学习, 是带真正推理、反馈能力的强人工智能[23], 深入挖掘人工智能对电磁环境的认知能力、推理能力, 从而实现人工智能与军事环境感知的高度融合. 以上方法总结见表 2.

表 2　智能检测方面典型方法总结

Table 2　Summary of typical methods in intelligent detection

Research angle of intelligent detection	Method/structure	Main technology	Citation number
Risk assessment	Threat assessment based on the preferred value of threat degree	Fuzzy optimization theory	[19]
	Information security risk assessment model	Knowledge and fuzzy logic	[20]
	Risk assessment model of information transmission security	Combination of genetic algorithm and neural network technology	[21]
Environmental perception	Environment-sensing radar	Interdisciplinary fusion of microwave remote sensing technology and AI technology	[22]
	Integration of AI and radar technology	Cognitive recognition	[23]

2.1.3　智能攻击

进行作战攻击时, 需要在短时间内确定攻击对象, 明确作战武器, 计算攻击效果, 为此, 需要对攻击行为进行建模研究, 来适应战争突发性、不确定性的特点. 目前, 多使用数学模型以及专家系统来进行仿真, 并使用分布式计算来均衡负载. 如在多智能体中部署的协同作战系统行动规划方法[24], 以编队协同反舰作战为背景, 将多智能体(Multi agent system, MAS)理论引入决策过程, 并将各个作战平台抽象为智能体, 从而建立起基于多智能体的编队协同模型, 并以主从重叠结构作为规划方法, 同时拥有集中与分布的优点; 或总结现代作战仿仿真的不足, 提出一种新的适用于现代战争的仿真方法——基于多智能体的复杂自适应系统[25], 并结合实例说明在作战中使用多智能体系统的优势.

当前, 军事作战多以集群为组织形式, 为达到迅速确定攻击对象、明确作战武器的目的, 如何进行数据快速传输和信息按需共享与分发, 实现数据的按需服务, 成为军事领域一项重要研究内容. 早在 1989 年, 就提出了人工智能与数据库(Database, DB)两大技术相融合的观点, 这将会成为未来信息系统的发展趋势; 通过两者优势互补, 将同时有利于两者的发展, 并会对计算机信息系统产生巨大的影响[26]; 针对这一方面的研究主要包括: 如何构建智能数据库系统, 即将人工智能技术融入到数据库中, 而该使用怎样的融合方法, 需要在这一过程中详细论述[27]; 如何使用数据挖掘、数据融合等新兴人工智能技术, 提出我军军事信息中心构建思路和基本架构[28]; 如何结合现代战争的特点, 探讨与研究对多传感器进行数据融合的方法, 提出针对现代化战场信息融合系统的作

战体系结构与功能体系结构[29]. 目前，AI 与 DB 有效融合的研究还在继续开展，同时，如何结合现代化战争的特点进行数据快速交互也是目前的研究重点.

在军事智能化中，经常需要使用态势感知进行安全风险评估. 可以从态势感知的定义入手，针对网络空间战争提出态势感知的系统框架，并基于态势感知对雷达网络进行设计[30]；也可以在态势感知中引入注意力机制，为设计新型智能模型提供新的研究思路[31]. 以色列正在研发“兰博”地面无人车，态势感知、侦查等能力将在其中有所体现. 以上方法总结见表 3.

表 3 智能攻击方面典型方法总结

Table 3 Summary of typical methods in intelligent attack

Research angle of intelligent attack	Method/structure	Main technology	Citation number
Attack behavior modeling	Cooperative combat system action planning method based on multi-agent system	Agent abstraction; using the MAS theory in decision process and planning strategy of master-slave overlapping structure	[24]
	Application of multi-agent system in combat simulation	Fusion of multi-agent system and complex adaptive system	[25]
Fast data transfer and on-demand shared distribution	Intelligent database system	Integration of database technology and AI	[27]
	Construction of military information center based on data processing	Data mining, data fusion, and other AI technologies	[28]
	Multi-sensor information fusion	Data-level fusion, feature-level fusion, and decision-level fusion	[29]
Situational awareness	Situation awareness based on radar network in cyberspace	Design of radar network based on situation awareness framework in cyberspace war	[30]
	Attention mechanism of battlefield situation awareness	Introduced attention mechanism into situation awareness decision and action	[31]

2.2 从物联网三层架构分析军事对抗中的人工智能技术

在目前的军事对抗中，信息化是主要特点，为此，如何保证信息安全，成为现代化战争的一项重要任务. 目前，有众多学者针对物联网三大层次进行研究，致力于在各个层次中保证数据安全. 本节主要从物联网三大层次出发，主要阐述在各个层次中实现数据安全的算法与协议，并进行比较.

2.2.1 感知层

感知层位于整个物联网的最底端，主要通过传感器对周围数据进行采集，并需要同时考虑到传感器自身、已采集数据以及传感器网络的安全问题. 传感器作为数据收集的起点，其准确性与安全性将直接影响后续数据的处理过程. 但在实际的对抗环境中，传感器节点十分容易受到损坏与干扰，部署到敌方的传感器可能并没有进行数据加密，容易造成数据的泄漏与篡改，因此，如何提升传感器的安全性是需要考虑的问题. 尽快提升传感器安全等级，保证数据安全，是目前业界的一致看法[32]；在保证数据安全方面，哈希（Hash）算法发挥着重要的作用：如使用基于 Hash 的对称加密机制，在一定程度上可以保证节点中的数据安全[33]；使用单向 Hash 将节点的公钥认证进行替换，通过所有传感器的公钥来建立 Merkle 树森林，在保证传感器数据安全的同时，还可以降低通信与计算开销，节省传感器电量[34].

在感知层中，传感器网络通过众多传感器之间的互联操作共同实现数据传输. 为此，如何保证传感器网络安全，实现数据准确无误的传输，是搭建传感器网络需要设计的环节. 这一方面的研究主要包括如下内容. (1)从传感器网络安全协议方面进行建模与分析：如根据目前无线传感器网络数据发现和分发协议的缺点，提出安全性更高的分布式数据发现和分发协议——DiDrop 协议[35]；(2)从入侵检测角度，对传感器网络安全性进行研究，同时针对目前的大多数技术只针对传感器网络的特定层进行攻击监测，为实现跨层入侵检测，可使用移动代理的手段[36]；(3)如何进行有效的访问控制，也是提升无线传感器网络安全性的重要方式之一，希望可以从是否对用户授权等方面进行安全性探究：如通过设计 THC 算法[37]，可以实现即便用户移动也可使传感器及时收到用户认证信息的机制，这使得对传感器的访问控制不仅适用于静态用户，也同样适用于移动用户；也可对无线传感器网匿名性进行研究，通过将 Hash、消息验证码等多种技术相结合，在数据保持完整的前提下可对伪造数据进行防御，从而增强整个物联网感知层的安全性能[38]；(4)通过使用密码与密钥管理来设法增强网络安全性：目前已有对对称与非

对称加密在传感器网络中的应用的详细对比[39], 通过不断研究, 也有越来越多新的密码算法应用于无线传感器网络当中, 如在无线传感器网络数据聚合过程中实现数据和密钥隐私保护[40], 改进混沌序列密码[41] 等. 此外, 还可以从安全路由、拒绝服务攻击等多种角度展开研究, 这都有助于发展无线传感器网络安全.

在目前信息化战场中, 只使用单一或某一类型传感器进行数据收集是远远不够的, 为此, 许多研究侧重在如何收集到多传感器数据, 并进行多传感器数据融合方面做出巨大的努力. 这些努力包括: (1)从提升数据融合精度进行研究, 如基于自回归滑动平均(Auto-regressive and moving average, ARMA)信息模型和增广状态空间模型, 结合误差方差与互协方差公式, 设计出精度更高的多传感器信息融合预报器[42]; (2)针对特定武器装备进行研究, 如提出在无人机传感器方面中的数据融合设计要求[43], 结合无人机作战中的状态, 有针对性的提出涉及高度及姿态角的算法, 通过在多传感器数据融合中加入高度通道和姿态通道, 将更有利于在无人机飞行系统中实现; (3)从数据融合算法着手, 如提出一种基于模糊方法的信息融合通用框架, 并且特征的提取与融合是通过隶属函数来实现的[44]; 使用超光谱传感器数据[45], 通过特征融合和决策融合两个层面对数据进行处理, 并通过神经网络得以实现. 与此同时, 小波分析理论、主成分变换、图像回归算法、专家系统等方法都开始应用于多传感器数据融合当中, 这都会促进信息化战争作战模式的高速转变. 感知层所述技术已在表 4 中进行总结.

表 4　感知层安全典型技术总结

Table 4　Summary of typical technologies of perceptual layer security

Research angle of perceptual level	Method/structure	Main technology	Citation number
Sensor security	Internet of Things authentication and key management	Symmetric encryption mechanism based on Hash	[33]
	Public key authentication scheme for sensor networks	One-way Hash function used in public key authentication, and Merkle tree established with public key	[34]
Sensor network security	DiDrip protocol	Distributed design and using different security parameters to improve security	[35]
	Cross-layer intrusion detection in wireless sensor network using mobile agent	Fusing cross-layer features such as the MAC layer and network layer	[36]
	Access control of wireless sensor network based on information coverage	Design of a THC algorithm; introducing the Merkle Hash tree and one-way chain	[37]
	Access control of wireless sensor networks with strong anonymity	Integrating Hash function, message verification code and other technologies	[38]
	Data and key privacy protection in data aggregation of wireless sensor networks	Organizing nodes in sensor network into tree structure and encryption in homomorphism	[40]
	Application of chaotic sequence cipher in wireless sensor network	Improved chaotic sequence cipher	[41]
Multi-sensor data fusion	Multi-sensor information fusion predictor	Based on ARMA information model and augmented state space model combined with two kinds of variance formulas	[42]
	Fuzzy method of multi-sensor data fusion	Feature extraction and fusion based on fuzzy method and membership function	[44]
	Super dimensional data fusion in hyperspectral sensor	Feature and decision fusion by maximum rule, neural network and other technologies	[45]

2.2.2　网络层

在目前的信息化战场上, 如何保证自身数据传输安全, 实现远距离数据传输, 是网络层中不可小觑的问题. 目前, 数据量急剧增加, 在整个数据传输过程中, 可能会导致网络层负载过大的风险; 同时, 随着协议的不断扩充, 数据间进行格式转换也同样会带来巨大开销; 如何能实现数据传输过程的动态分配、负载均衡, 提高网络层数据传输利用率, 是目前众多学者研究的热门话题. 早在 1999 年, Bass 与 Gruber[46] 就提出网络态势感知这一概念, 并开始与网络技术紧密结合, 致力于全面加强网络层安全防护等级; Bass 认为, 当前一代入侵检测系统(IDSes)在技术上还不够先进, 没有办法有效监控和保护这些网络所需的态势知识; 而下一代智能决策支持系统将对数据进行融合, 将短期传感器与长期知识数据库结合, 创建出网络态势感知.

Tsochev 等[47] 根据多智能体系统并结合人工智能技术, 提出针对网络方面的安全模型, 该模型由两个主要的多智能体框架组成, 分别是基于主机的监控系统, 用以对操作系统资源和用户活动进行监控, 以及网络网关的监控系统, 用以监测与

防止 TCP/IP 攻击；也可以将径向基函数神经网络（Radial basis function neural network, RBFNN）用于网络安全态势预测[48]，在神经网络中同时融合布谷鸟搜索算法、模拟退火算法和动态发现概率机制，预测精度得到明显改善；还可以结合支持向量机的优势[49]，将支持向量回归的预测方法用于网络态势感知时间序列预测中，在网络态势感知中引入支持向量回归方法，通过网络攻击态势预测训练模块对实验数据进行建模与训练，并设计预测模块，根据入侵检测系统提供的新数据，完成对网络态势的预测，而使用支持向量回归算法，可以达到更好的预测效果．总结如表 5 所示．

表 5 网络漏洞评估与安全态势感知典型技术总结

Table 5 Summary of typical technologies of network vulnerability assessment and security situation awareness

Network vulnerability assessment and security situation awareness	Method/structure	Citation number
Multi-agent network security model	Using a two-tier multi-agent framework to integrate AI to monitor resources and attacks	[47]
Prediction of network security situation based on RBF neural network	Based on an RBFNN neural network and the integration of the cuckoo search algorithm, simulated annealing algorithm, and dynamic discovery probability mechanism in the neural network	[48]
Time series prediction of network situation awareness	Prediction method with support vector regression	[49]

2.2.3 应用层

物联网层次结构的最顶级，即为应用层．面对海量数据，如何在时间紧张、任务繁重的工作环境中准确无误、高速快捷的得到满意的实验结果，是军事对抗在应用层中的一大诉求．目前，很多人工智能技术都支持对海量数据处理，结合云计算等新兴处理方式可以实现良好的效果．一个已建立的海量小文件处理模型正是基于云计算技术[50]，并使用改进的 K 最近邻（K-nearest neighbor, KNN）算法实现对文件的分类，构建基于可扩展标记语言（Extensile markup language, XML）和可同时映射多值的改进 MapReduce 模型可以进行快速数据处理，并通过改进遗传算法，可以实现云数据存储的动态分配与负载均衡，从而有利于海量数据处理，这也利于在军事中对海量小文件进行快速分类与处理；目前，应用层程序种类繁多，需针对特定应用进行方法设计，既要实现应用层与人工智能的结合，也要很好的适应信息化战争的作战特点．

3 人工智能缺陷与人机融合智能的发展趋势

尽管人工智能在军事领域取得了长足的发展，但就目前而言，人工智能的一些缺陷还是限制了其在军事对抗领域的发展，表 6 简单罗列出人工智能的一般缺点和在军事对抗中会出现的问题．

表 6 人工智能缺点及衍生在军事对抗中的问题

Table 6 Shortcomings of AI and the associated problems in military confrontation

Defects of AI	Possible problems in military confrontation
Unable to implement complex reasoning	In the face of a complex battlefield environment, reasoning is likely to go beyond the scope of AI understanding, resulting in “thinking” stagnation.
Support from a large number of samples	In the battlefield environment, data collection and processing speed may not meet the needs of AI, and the good self-learning ability of AI cannot be reflected.
Essentially a software program	There may be defects in program design; errors may occur in high-intensity use, or the program may be attacked and interfered by enemies.
High requirements for computing power	In the battlefield environment, the batteries of equipment are limited and the power supply is tight, but AI usually requires large power consumption for modeling and training.
No social history [51]	Machines cannot think on their own. They can only be used to replace part of human thinking activities. They have no purpose or feelings. In the battlefield environment, they will not accurately judge a new situation.

目前，一种新型的人工智能——人机融合智能正在快速发展，这将是人工智能新的发展趋势，同时也更利于人工智能在军事对抗中的应用．人机融合智能，是将人的智慧与机器智能相结合，从而在决策、态势感知等方面实现优势互补的一种新型智能．机器可以快速处理海量数据，并可以得到精度很高的运算结果，但其在进行重大问题抉择方面就表现的差强人意；相反，人具有独立性，在面对复杂多变的环境时可以快速准确的做出反应，但同时也需要计算机进行辅助，由机器提供支撑数据，从而更好的辅助相关人员进行决策．在目前的军事对抗体系中，机器无法完全脱离人类实现自主控制，在很多场景下，仍旧需要人工加以支持，随着人机融合智能的应用而生，两者实现融合成为一种可能，并可能会带来更好的收益．

2017 年，DARPA 局长认为人机融合已经开始，

但他并不认为人类已经做好准备; 2019 年 2 月, 为促进人机融合的发展, DARPA 发布“智能神经接口”和“人工智能科学和开放世界新奇学习”项目公告; 2019 年 10 月, 第五届中国(杭州)国际机器人西湖论坛召开, 本次论坛的主题为“人机共融”, 人机融合被认为是机器人领域重要的发展趋势; 2019 年 11 月, 美国国防部收到名为《2050 年机械战士: 人机融合与国防部的未来》的报告, 美军开始“Cybrog 战士”的研发.

目前, 人机融合智能的研究尚处于起步阶段, 在军事对抗领域已经开始展露锋芒. 同时, 人工智能在军事对抗中出现的问题已经显现, 只有攻克这几个问题才可以实现更进一步的发展. 以下部分将一一阐述人机融合智能如何解决当前人工智能在军事对抗中的缺陷.

3.1　人机融合智能可应对复杂战场环境

目前的人工智能, 只能依靠输入数据对指定类型进行快速判断与处理, 这对于使用环境相对稳定的场景足够发挥人工智能的优势. 但是在信息化战场中, 战场形势总是在改变, 不断出现的新形势将无法及时反馈给人工智能系统, 造成人工智能系统无法给出准确的裁决, 从而无法在信息化战场中发挥优势. 而人具有思考能力及应急能力, 在遇到新情况时可以及时作出判断并进行处理, 这是机器所无法拥有的人所特有的优势, 若能将两者进行优势互补, 则可以充分发挥人–机联动处理能力, 从而在信息化战场中获得更大的收益. 为了实现人与机器优势互补, 可以将人在回路系统融入到军事对抗决策当中, 如图 1 所示.

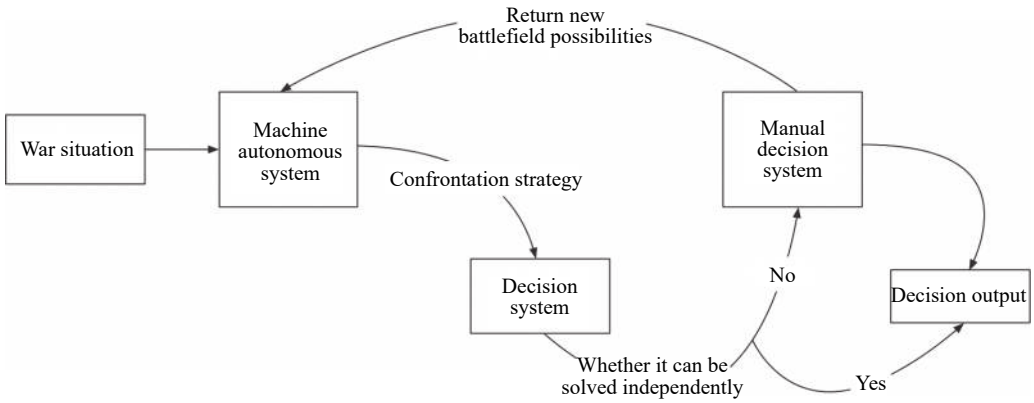

图 1　人在回路决策系统中的人机融合智能

Fig.1　Hybrid human–artificial intelligence in loop decision system

军事对抗中的人在回路系统主要分为两个子系统, 分别是机器自主系统与人工决策系统, 在收到某一战争情形后, 先由机器自主系统进行自检索, 确定是否可以交由机器进行处理, 如若可以进行处理, 将需要判断机器是否可进行完全处理, 是否需要借助人工处理; 如若可以交由机器进行处理, 则给出最终的裁决结果; 如若机器无法进行处理或需要人工介入, 则需将战争情形交给人工决策系统进行处理, 在人工决策系统中, 由作战人员对战争情形进行详细分析, 在经过缜密分析后给出决策结果, 并将决策结果输出; 同时为增加人–机交互的联动性, 将此类战争情形和决策结果重新返回给机器自主系统, 用以丰富机器自主系统知识库, 再次遇到相似情形时, 可以由机器进行自主处理, 从而可以缩短处理周期, 达到对战争情形快速处理的目的, 这也是人机融合在军事对抗中所需要实现的目标.

3.2　人机融合智能可实现数据快速交互

随着战争形势趋向于信息化方向发展, 数据成为战争中需要重点保护的对象, 在收集到众多数据后, 如何进行海量数据的快速交互是军事对抗中急需要解决的重要问题. 在目前的作战集群中, 主要使用综合数据链进行数据的快速传输与情报数据的快速交换, 这是信息化战争发展的重要标志. 但随着研究的深入, 不难发现综合数据链也存在着一些弊端, 如传输速率较低, 在数据传输过程中容易被检测与截取, 这些都会对数据的传输造成干扰, 造成数据传输的不稳定, 并容易产生数据滞后的问题. 为此, 在军事对抗中进行数据传输时, 需要尽量避免上述问题的产生, 尽可能实现数据的快速流动. 为此, 可以设计如图 2 的方案, 将赛博空间的电磁频谱相关技术融入到机器自主系统和人工决策系统中.

在赛博空间中, 由于使用电磁频谱技术, 各个

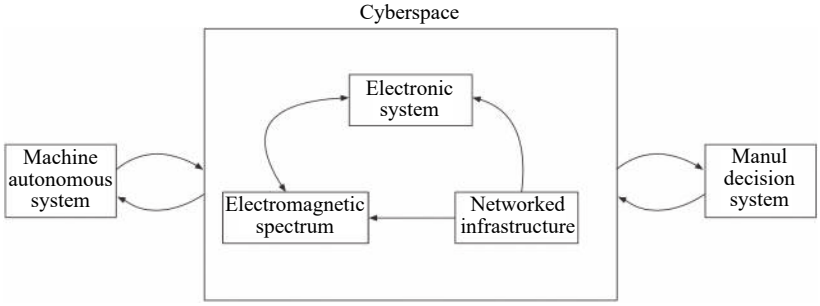

图 2 数据高速处理中的人机融合智能

Fig.2 Hybrid human–artificial intelligence in high-speed data processing

节点数据传输速度快，甚至可以达到光速的传播速度，极适合进行数据快速传输与共享；并且在其中可以对节点进行实时更新，具有高可靠性，在某一设备出现问题时，可以及时进行判断与修正，尽可能降低数据故障. 在军事对抗中，可以将机器自主系统和人工决策系统通过电磁技术进行数据链接，而不是使用传统的有线或无线链路进行数据传输，从而可以将赛博空间的优势充分融合到人机融合系统中，达到信息传输在军事对抗中的要求. 同时，由于不受地域等因素的影响，赛博空间使用范围更广，并且，赛博空间具有很好的隐蔽性，在数据互联互通的过程中，不容易受到数据拦截与泄漏的问题，使数据安全性有所提升.

3.3 人机融合智能可实现负载动态分配

人机融合智能在军事对抗中的设计，还需要考虑动态负载分配问题. 在高强度与高压力的作战环境下，何时将控制权交由机器进行操纵，何时交由人工进行操作，是实现人机高度融合过程中所必须考虑的问题. 为此，设计如图 3 的基于人机融合的动态分配系统，用来实现控制权的自动化分配. 在机器自主系统进行任务处理时，首先计算负载量，当负载量没有超过阈值，即可由机器进行处理时，进入机器处理阶段，并将处理结果返回给机器自主系统，以便使用处理结果；当负载量超过阈值时，可以实现控制权的转移，将控制权转给人工决策系统，由人工决策系统进行接替处理，并将处理结果保存到人工决策系统以备使用；同样，当人工决策系统遇到诸如海量数据处理等实现较困难的情况，工作量明显超过阈值，或由于人为因素（如情绪波动）需要将控制权进行转交时，由人工决策系统将控制权让出，交给机器自主系统进行处理，否则直接由人工决策系统自行处理并给出结果.

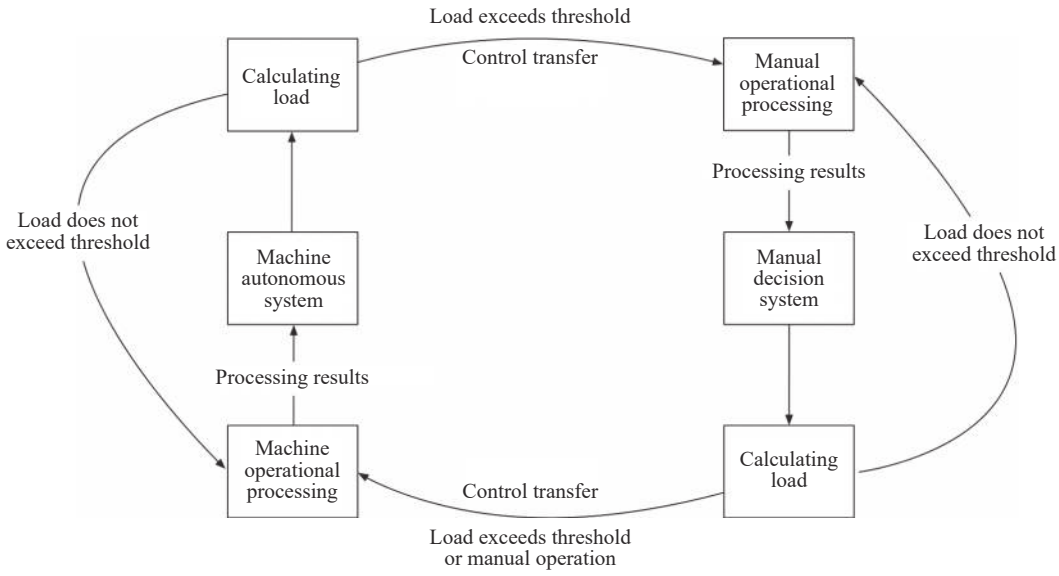

图 3 人机负载动态分配系统

Fig.3 Dynamic distribution system based on hybrid human-artificial intelligence

采用基于人机融合的动态分配系统，可以实现控制权的动态转移，从而使人与机器的协作更加密切，不至于出现任务配置不均匀导致无法及时完成任务的局面. 同时，通过使用该系统，可以

缓解人–机双方工作负担, 利于实现可持续工作的目标.

人机融合智能的研究处在刚刚起步的状态, 但其明显的优越性得到了众多国内外学者的广泛研究. 人机融合智能用于军事对抗中, 其优势十分明显, 但同时, 需要克服的困难也并不仅仅只有以上列举出来的情况, 就比如人机融合智能在伦理中的问题, 也是目前一直备受争议的话题.

4　总结与展望

从人工智能在军事对抗中的应用作为切入点, 论述了代表性国家对人工智能在军事领域的应用等方面的重视程度, 并从两大角度阐述现阶段人工智能在军事对抗中的应用, 展现出了人工智能强大的优越性. 同时, 针对目前的研究现状提出人工智能在军事对抗中的应用限制, 并引出人机融合智能这项新的发展趋势, 通过设计方案试图解决人工智能在军事领域无法解决的问题, 并展现出了人机融合智能相比人工智能更显著的优势. 有理由相信, 在不久的未来, 人机融合智能会在军事领域占据越来越大的比重, 人机融合智能也会敦促军事领域新型技术的快速发展, 实现高度人机融合, 也将是军事领域发展的必然要求.

参　考　文　献

[1] Hinton G E, Osindero S, Teh Y W. A fast learning algorithm for deep belief nets. *Neural Comput*, 2006, 18(7): 1527

[2] Silver D, Schrittwieser J, Simonyan K, et al. Mastering the game of Go without human knowledge. *Nature*, 2017, 550(7676): 354

[3] Xiao Z Z, Liu Y M. *Intelligent Weapons and Unmanned War*. Beijing: Military Friendship Press, 2001
(肖占中, 刘昱旻. 智能武器与无人战争. 北京: 军事谊文出版社, 2001)

[4] Wang X C. Artificial intelligence algorithm: the invisible hand of rewriting war. *Military Digest*, 2017(21): 19
(王雪诚. 人工智能算法: 改写战争的无形之手. 军事文摘, 2017(21): 19)

[5] Lecuyer M, Atlidakis V, Geambasu R, et al. Certified robustness to adversarial examples with differential privacy // 2019 *IEEE Symposium on Security and Privacy* (*SP*). San Francisco, 2019

[6] Papernot N, McDaniel P, Wu X, et al. Distillation as a defense to adversarial perturbations against deep neural networks//2016 *IEEE Symposium on Security and Privacy* (*SP*). San Jose, 2016

[7] Liu X Q, Li Y, Wu C R, et al. Adv-BNN: improved adversarial defense through robust bayesian neural network // *International Conference on Learning Representations*. New Orleans, 2019

[8] Shi Z Z. *Intelligent Agent and Its Application*. Beijing: Science Press, 2002
(史忠植. 智能主体及其应用. 北京: 科学出版社, 2002)

[9] Desai J P, Ostrowski J, Kumar V. Controlling formations of multiple mobile robots//1998 *IEEE International Conference on Robotics and Automation*. Belgium, 1998: 2864

[10] Desai J P, Ostrowski J P, Kumar V. Modeling and control of formations of nonholonomic mobile robots. *IEEE Trans Robot Autom*, 2001, 17(6): 905

[11] Desai J P. A graph theoretic approach for modeling mobile robot team formations. *J Robot Syst*, 2002, 19(11): 511

[12] Das A K, Fierro R, Kumar V, et al. A vision-based formation control framework. *IEEE Trans Robot Autom*, 2002, 18(5): 813

[13] Wang J, Zhao X Z, Zhang Y H, et al. Cooperative air-defense system of system model for surface warship formation based on immune multi-agent. *J Syst Simul*, 2012, 24(2): 263
(王军, 赵晓哲, 张瑛涵, 等. 基于免疫多智能体的舰艇编队协同防空体系模型. 系统仿真学报, 2012, 24(2): 263)

[14] Sahal M, Agustinah T, Jazidie A. Switching formation and topology in cooperative multi-agent source seeking using gradient estimation // 2019 *International Conference of Artificial Intelligence and Information Technology* (*ICAIIT*). Yogyakarta, 2019: 151

[15] Liu L, Liang X L, Zhu C C, et al. Distributed cooperative control for UAV swarm formation reconfiguration based on consensus theory // 2017 2nd *International Conference on Robotics and Automation Engineering* (*ICRAE*). Shanghai, 2017: 264

[16] Lü Y, Kang T N, Pan Q, et al. UAV sense and avoidance: concepts, technologies and systems. *Sci Sin Inform*, 2019, 49(5): 520
(吕洋, 康童娜, 潘泉, 等. 无人机感知与规避: 概念、技术与系统. 中国科学: 信息科学, 2019, 49(5): 520)

[17] Han J Y, Wang H L, Liu C, et al. Vision-based system design for UAV target detection and avoidance. *Tactical Missile Technol*, 2014(5): 11
(韩静雅, 王宏伦, 刘畅, 等. 基于视觉的无人机感知与规避系统设计. 战术导弹技术, 2014(5): 11)

[18] Li Y J, Pan Q, Yang F, et al. Research on UAV perception and avoidance based on multi-source information fusion // *Proceedings of the* 29th *China Control Conference*. Beijing, 2010: 2861
(李耀军, 潘泉, 杨峰, 等. 基于多源信息融合的无人机感知与规避研究 // 第二十九届中国控制会议论文集. 北京, 2010: 2861)

[19] Huang J P. *Study on Threat Assessment of Surface to Air Missile Forces in Anti-Air Attack Operations*[Dissertation]. Xiamen: Xiamen University, 2009
(黄剑平. 地空导弹部队在反空袭作战中的威胁评估研究[学位论文]. 厦门: 厦门大学, 2009)

[20] Azan Basallo Y, Estrada Senti V, Martinez Sanchez N. Artificial intelligence techniques for information security risk assessment. *IEEE Latin America Trans*, 2018, 16(3): 897

[21] Du G, Han Z Q, Li N X, et al. Risk assessment model of information transmission security based on neural network and

genetic algorithm. J Intell, 2010, 29(Suppl 1): 207
（杜戈, 韩增奇, 李宁霞, 等. 基于神经网络和遗传算法的信息传输安全风险度评估模型. 情报杂志, 2010, 29(增刊1): 207）

[22] Sun X Z, Liu L. Development of unmanned ground combat system and environmental sensing radar. *Sci Technol Vision*, 2017(8): 1
（孙晓舟, 刘露. 地面无人作战系统及环境感知雷达发展概述. 科技视界, 2017(8): 1）

[23] Li B, Ren H M, Xiao Z H. Limitation and development prospect of artificial intelligence in radar application. *Military Digest*, 2019(3): 42
（李波, 任红梅, 肖志河. 人工智能在雷达应用中的限制和发展前景. 军事文摘, 2019(3): 42）

[24] Yang F, Wang Q, Wu Z D. Cooperative combat system action planning method based on multi-agent system // 2010 *Second International Workshop on Education Technology and Computer Science*. Wuhan, 2010: 490

[25] Liu Y F, Zhang A. Multi-agent system and its application in combat simulation // 2008 *International Symposium on Computational Intelligence and Design*. Wuhan, 2008: 448

[26] Brodie M L, Cui J. Future intelligent information system: the combination of AI and DB technology. *Comput Sci*, 1989(3): 23
（Brodie M L, 崔靖. 未来的智能信息系统: AI与DB技术的结合. 计算机科学, 1989(3): 23）

[27] Nihalani N, Silakari S, Motwani M. Integration of artificial intelligence and database management system: An inventive approach for intelligent databases // 2009 *First International Conference on Computational Intelligence, Communication Systems and Networks*. Indore, 2009: 35

[28] Shao J, Wu H, Chen L. Construction of military information center based on correlation techniques of data processing. *Microcomput Inform*, 2006, 22(3): 89
（邵军, 吴华, 陈蕾. 基于数据处理相关技术的军事信息中心构建. 微计算机信息, 2006, 22(3): 89）

[29] Niu Z Y. Research on multi-sensor information fusion technology in modern war. *Comput Inform Technol*, 2006(3): 71
（牛志一. 现代化战争中的多传感器信息融合技术研究. 计算机与信息技术, 2006(3): 71）

[30] Yang X, Shan W, Jia L. Technology of situation awareness based on radar network in cyberspace //*Proceedings of the* 2013 *IEEE International Conference on Green Computing and Communications and IEEE Internet of Things and IEEE Cyber, Physical and Social Computing*. Beijing, 2013: 1505

[31] Kong Y S, Hu X F, Zhu F, et al. Attention mechanism in battlefield situation awareness. *J Syst Simul*, 2017, 29(10): 2233
（孔亦思, 胡晓峰, 朱丰, 等. 战场态势感知中的注意力机制探析. 系统仿真学报, 2017, 29(10): 2233）

[32] www.cecb2b.com. Experts call for a higher level of sensor safety. *Comput Telecommun*, 2014, 11(11): 21
（元器件交易网. 专家呼吁提升传感器安全层级. 电脑与电信, 2014, 11(11): 21）

[33] Chen L. *Research on Authentication Technology and Key Management in Internet of Things*[Dissertation]. Changsha: Central South University, 2013
（陈雷. 物联网中认证技术与密钥管理的研究[学位论文]. 长沙: 中南大学, 2013）

[34] Du W L, Wang R H, Ning P. An efficient scheme for authenticating public keys in sensor networks // *Proceedings of the* 6th *ACM International Symposium on Mobile Ad Hoc Networking & Computing*. Urbana-Champaign IL, 2005: 58

[35] Ghormare S, Sahare V. Implementation of data confidentiality for providing high security in Wireless Sensor Network // 2015 *International Conference on Innovations in Information, Embedded and Communication Systems* (*ICIIECS*). Coimbatore, 2015: 1

[36] Gandhimathi L, Murugaboopathi G. Cross layer intrusion detection and prevention of multiple attacks in Wireless Sensor Network using Mobile agent // 2016 *International Conference on Information Communication and Embedded Systems* (*ICICES*). Chennai, 2016: 1

[37] Du Z Q, Shen Y L, Ma J F, et al. Two-hop cover-based access control scheme for wireless sensor networks. *J Commun*, 2010, 31(2): 113
（杜志强, 沈玉龙, 马建峰, 等. 基于信息覆盖的无线传感器网络访问控制机制. 通信学报, 2010, 31(2): 113）

[38] Chen T, Lu J Z, Jiang J H. An access control scheme with strong anonymity in wireless sensor network. *Comput Eng*, 2015, 41(1): 126
（陈婷, 卢建朱, 江俊晖. 一种具有强匿名性的无线传感器网络访问控制方案. 计算机工程, 2015, 41(1): 126）

[39] Jin N, Zhang D Y, Gao J Q, et al. A study on the application of symmetric ciphers and asymmetric ciphers in wireless sensor networks. *Chin J Sens Actuators*, 2011, 24(6): 874
（金宁, 张道远, 高建桥, 等. 对称密码和非对称密码算法在无线传感器网络中应用研究. 传感技术学报, 2011, 24(6): 874）

[40] Akila V, Sheela T. Preserving data and key privacy in data aggregation for wireless sensor networks // 2017 2nd *International Conference on Computing and Communications Technologies* (*ICCCT*). Chennai, 2017: 282

[41] Zhao C. *Research on the Application of Chaotic Sequence Cipher in Wireless Sensor Network*[Dissertation]. Beijing: Beijing University of Chemical Technology, 2014
（赵晨. 混沌序列密码在无线传感器网络中的应用研究[学位论文]. 北京: 北京化工大学, 2014）

[42] Mao L, Deng Z L. Multisensor information fusion wiener deconvolution predictor //2007 26th *Chinese Control Conference*. Zhangjiajie, 2007: 1013
（毛琳, 邓自立. 多传感器信息融合Wiener反卷积预报器 // 第二十六届中国控制会议论文集. 张家界, 2007: 1013）

[43] Li N G, Zhao H. The requirements on the data fusion of multiple-sensor of UAV. *Natl Defense Sci Technol*, 2015, 36(5): 52
（李念国, 赵慧. 无人机多传感器数据融合的设计要求. 国防科技, 2015, 36(5): 52）

[44] Ruzzo F, Ramponi G. Fuzzy methods for multisensor data fusion // 1993 *IEEE Instrumentation and Measurement Technology Conference*. Irvine, 1993: 676

[45] Jimenez L O, Morales-Morell A, Creus A. Classification of hyperdimensional data based on feature and decision fusion approaches using projection pursuit, majority voting, and neural networks. *IEEE Trans Geosci Remote Sens*, 1999, 37(3): 1360

[46] Bass T, Gruber D. A glimpse into the future of id[J/OL]. *USENIX* (2001-2-1)[2019-11-19]. http://pdfs.semanticscholar.org/7ac9/8c4f3b72210775b08aa5849d5501de9c7048.pdf

[47] Tsochev G, Trifonov R, Yoshinov R, et al. Some security model based on multi agent systems //2018 *International Conference on Control, Artificial Intelligence, Robotics & Optimization* (*ICCAIRO*). Prague, 2018: 32

[48] Ren W, Jiang X H, Sun T F. RBFNN-based prediction of networks security situation. *Comput Eng Appl*, 2006, 42(31): 136
(任伟, 蒋兴浩, 孙锬锋. 基于RBF神经网络的网络安全态势预测方法. 计算机工程与应用, 2006, 42(31): 136)

[49] Zhang X, Hu C Z, Liu S H, et al. Research on network attack situation forecast technique based on support vector machine. *Comput Eng*, 2007, 33(11): 10
(张翔, 胡昌振, 刘胜航, 等. 基于支持向量机的网络攻击态势预测技术研究. 计算机工程, 2007, 33(11): 10)

[50] Ren C G. *Research on Cloud Computing and Its Key Technologies for Massive Data Processing*[Dissertation]. Nanjing: Nanjing University of Technology, 2013
(任崇广. 面向海量数据处理领域的云计算及其关键技术研究[学位论文]. 南京: 南京理工大学, 2013)

[51] Chu Q W. *On Artificial Intelligence from the Perspective of Philosophy*[Dissertation]. Wuhan: Wuhan University of Technology, 2014
(褚秋雯. 从哲学的角度看人工智能[学位论文]. 武汉: 武汉理工大学, 2014)