

一、项目名称

面向智能无人系统的多维威胁模型与安全防御方法

二、提名者及提名意见

提名者：中共陕西省委军民融合发展委员会办公室

提名意见：智能无人系统兼具“新质生产力”与“新质战斗力”双重战略价值，是把握科技革命机遇、筑牢国家安全屏障的战略必争之地。然而，智能无人系统面临对抗样本攻击、虚假数据注入攻击、协同窃听攻击三个维度（即“多维”所指）的安全威胁，本项目立足智能无人系统的体系化安全需求，在国家自然科学基金面上项目等7项课题资助下，从威胁感知建模、模型鲁棒防御、攻击检测识别与安全可靠传输四个层面，系统建立了智能无人系统安全防御的理论体系。

项目在网络空间安全和通信领域等领域核心刊物发表SCI检索论文45篇，获得全军优秀博士学位论文奖1项、陕西省优秀博士学位论文奖1项，授权国家发明专利20项；特别地，5篇代表性论文均为SCI中科院一区/二区论文，Web of Science核心合集引用共516次、他引467次，单篇最高他引143次（谷歌学术上引用次数达到225次），其中包括ESI全球前0.1%热点论文1篇、ESI全球前1%高被引论文5篇，获得80位国内外院士、IEEE Fellow等的正面评价。

成果材料齐全、规范，无知识产权纠纷，人员排序无争议，符合陕西省自然科学奖提名条件，特提名为陕西省自然科学奖二等奖。提名该项目为陕西省自然科学奖二等奖。

三、项目简介

属计算机科学与技术前沿领域。智能无人系统兼具“新质生产力”与“新质战斗力”双重战略价值——民用领域催生数万亿级低空经济新业态，军事领域重塑未来战争形态与力量编成，是把握科技革命机遇、筑牢国家安全屏障的战略必争之地。党的二十大报告明确“加快无人智能作战力量发展”，习近平主席强调“逐步构建智能化军事体系”；“十五五”规划将低空经济列为战略性新兴产业集群，国务院部署全空间无人体系建设，多地出台专项政策，多层次支撑体系初步形成。然而，智能无人系统面临对抗样本攻击、虚假数据注入攻击、协同窃听攻击三个维度（即“多维”所指）的安全威胁，本项目立足智能无人系统的体系化安全需求，从威胁感知建模、模型鲁棒防御、攻击检测识别与安全可靠传输四个层面，系统建立了智能无人系统安全防御的理论体系。

本项目的四个科学发现遵循认知威胁与防御威胁的研究链条，逻辑递进、环环相扣。发现点（1）从攻击者视角系统揭示三类攻击的数学本质、隐蔽机理与级联效应，回答“威胁从何而来、如何起作用”的问题，为后续防御设计提供理论基础。发现点（2）针对智能算法面临的对抗样本攻击，从模型训练层面提出集成对抗训练与鲁棒蒸馏的动态防御机制，回答“如何在算法层面抵御感知欺骗”的问题。发现点（3）针对虚假数据注入攻击的检测难题，从数据表征层面建立时空特征深度融合的检测理论，回答“如何在数据层面识别数据污染”的问题。发现点（4）针

对通信链路面临的窃听威胁，从物理层安全角度建立人工噪声与资源分配的协同防御理论，回答“如何在传输层面防止信息泄露”的问题。四个发现点形成威胁建模—感知防御—数据检测—通信安全的理论闭环。

发现点 1 智能无人系统多维威胁模型。从对抗样本攻击、虚假数据注入攻击与多方协同窃听攻击三个维度构建威胁分析框架。揭示了智能无人系统中深度神经网络在感知层对微小扰动存在“误差传递放大”的固有脆弱性，建立智能无人系统中扰动误差逐级传递、非线性累积直至系统级失效的内在规律；揭示虚假数据注入攻击的数学本质是构建满足动力学物理约束且与正常量测统计特性不可区分的错误状态估计，进一步从信息融合视角证明，攻击隐蔽性的核心成因在于多源传感信息互补性约束的精确破坏；揭示无线通信链路的空间广播特性构成窃听威胁的物理根源，阐明窃听者数量增加对信息熵和安全容量的影响规律。进一步发现三类攻击并非孤立存在，而是可相互组合、级联放大，形成针对智能无人系统的闭环攻击链。（攻击链用闭环修饰是否合适）

发现点 2 基于集成对抗训练与鲁棒蒸馏的对抗样本攻击安全防御机制。突破传统静态防御的局限，首次揭示对抗训练中决策边界动态演化与鲁棒泛化的内在关联规律。将专家判别先验、历史演化轨迹与实时攻击反馈纳入统一分析框架，揭示三者协同驱动下决策边界向最优鲁棒区域收敛的演化路径，证明专家集成机制可在特征空间中形成更平滑且泛化能力更强的鲁棒决策边界。进一步发现教师与一学生模型中间特征层的动态匹配可在特征空间中建立“知识迁移通道”，使系统在继承鲁棒判别能力的同时保持对正常样本的高精度识别，揭示该通道的有效性取决于对齐误差与判别信息损失之间的动态平衡，特定条件下系统可达精度与鲁棒性的帕累托最优。

发现点 3 基于时空特征深度融合的虚假数据注入攻击防御方法。针对现有检测方法依赖单一时域分析的理论局限，揭示量测数据天然具有空间关联属性——相邻节点间的协同演化规律，攻击行为在时间维度呈现异常突变的同时必在空间维度破坏节点间一致性，该双重特征构成检测攻击的本质依据。首次提出将一维时序数据重构为融合时间周期与空间关联的二维矩阵映射方法，建立时空特征联合表达的理论框架。进一步将时序卷积与递归记忆机制统一于 ConvLSTM 网络框架，揭示该网络在同时捕获全局周期趋势与局部突变特征过程中的联合优化机理，从理论上证明时空联合学习是实现高泛化虚假数据注入攻击检测的充分条件。

发现点 4 基于人工噪声与资源分配的抗多方协同窃听攻击安全防御理论。针对智能无人系统通信链路面临的多方协同窃听威胁，揭示了保密传输的理论瓶颈，提出了基于人工噪声零陷设计与动态资源分配的统一安全防御理论。一方面，揭示了多用户非正交通信中可靠性与保密性的耦合制约机理，证明通过将服务质量约束嵌入功率分配可行域，可最小化可靠用户的连接中断概率且不牺牲保密用户的可靠性，明确了协同优化的可行边界。另一方面，发现将人工噪声置于合法信道零空间的设计可有效压制外部协同窃听，首次推导出保密中断概率的闭式表达式，发现其独立于窃听信道条件的统计规律，并量化了分集阶数为发射天线数减 2。该发现为智能

无人系统提供了明确的天线配置准则与性能评估基准。

本项目从威胁感知建模、模型鲁棒防御、攻击检测识别与安全可靠传输四个层面，构建了完整的智能无人系统安全防御理论体系。五篇代表性论文发表于《IEEE Transactions on Information Forensics and Security》《IEEE Transactions on Dependable and Secure Computing》《IEEE Transactions on Vehicular Technology》《IEEE Internet of Things Journal》等本领域权威期刊，1篇入选 ESI 全球前 0.1% 热点论文，3 篇入选 ESI 全球前 1% 高被引论文，得到国内外学者的正面引用与评价。研究成果揭示了智能无人系统在对抗环境下的脆弱性本质与安全边界，为构建兼具感知可信、决策鲁棒与传输保密的智能无人系统提供了理论基础与方法论支撑，对推动智能无人系统从“功能实现”向“安全可信”的范式跃迁具有重要的科学价值。发表 SCI 检索论文 45 篇，获得全军优秀博士学位论文奖 1 项、陕西省优秀博士学位论文奖 1 项，授权国家发明专利 20 项；特别地，5 篇代表性论文均为 SCI 中科院一区/二区论文，Web of Science 核心合集引用共 516 次、他引 467 次，单篇最高他引 143 次（谷歌学术上引用次数达到 225 次），其中包括 ESI 全球前 0.1% 热点论文 1 篇、ESI 全球前 1% 高被引论文 5 篇，获得 80 位国内外院士、IEEE Fellow 等的正面评价。本项目成果培养了智能安全、通信对抗等技术领域的优秀青年科技人才，多名项目完成人入选万人领军、军队高层次学科拔尖人才、中央网信办“国家网络安全优秀教师”、科协/军事青托、陕西省优青/科技新星等国家和省部级人才，享受国务院政府特殊津贴和省部级专业技术人才岗位津贴，入选全球前 2% 顶尖科学家和中国知网高被引学者，并受邀担任 IEEE Transactions on Communications、IEEE Internet of Things Journal、Computers & Security、《网络与信息安全学报》、《网络空间安全学报》等国内外顶尖期刊副主编/编委。依托项目成果，团队人员获得多项奖励，包括陕西省计算机学会科学技术奖二等奖、“锦囊-2024”未来战争场景与创意征集一等奖（排名第一）、第八届全军军事建模竞赛特等奖、全国研究生信息安全对抗技术竞赛一等奖等。

四、客观评价

本项目 5 篇代表性论文全部发表在 SCI 中科院一区/二区等领域顶级期刊，Web of Science 核心合集引用共 516 次、他引 467 次，单篇最高他引 143 次（谷歌学术上引用次数达到 225 次），其中包括 ESI 全球前 0.1% 热点论文 1 篇、ESI 全球前 1% 高被引论文 5 篇，获得 80 位国内外院士、IEEE Fellow 等的正面评价。

代表性论文 1：加拿大工程院院士、ACM/IEEE Fellow、香港理工大学教授杨强在 COMST 发文正面评价了代表性论文 1，认为田继伟等人的研究表明攻击者可利用这些漏洞进行攻击，如成员推断或梯度泄漏等，以从设备中提取本地训练数据。（“...adversaries can exploit these vulnerabilities to perform attacks such as membership inference or gradient leakage [277]-[279], aiming to extract local training data from devices. ([278]为代表性论文 1)”）。

代表性论文 2：加拿大工程院院士、IEEE Fellow、卡尔顿大学教授 Fei Richard Yu 和欧洲科学院院士、IEEE Fellow、香港科技大学教授郭嵩在 ACM Computing

Surveys 联合发文正面评价了代表性论文 2，指出代表性论文 2 证明了对抗攻击对无人机集群网络中深度学习的危害。（“…authors in Reference [87] demonstrate the harm of adversarial attacks for DL in UAV swarm networks.（[87]为代表性论文 2）”）。

代表性论文 3：俄罗斯工程院外籍院士、IEEE/AAAS Fellow、国家高层次人才、合肥工业大学教授吴信东在 IEEE Transactions on Emerging Topics in Computational Intelligence 发文（FedSTAFN: A Secure and Efficient Privacy-Preserving Federated Learning Model for Electricity Theft Detection），指出代表性论文 3 将数据转换为时空序列，并使用多层 ConvLSTM 网络进行处理，解决了检测精度低的问题（“These methods rely on one-dimensional electricity data, limiting their ability to capture periodic features and reducing detection accuracy. To address this, Xia et al. [23] transformed the data into spatiotemporal sequences and processed them using a multi-layer ConvLSTM network.（[23]为代表性论文 3）”）。

代表性论文 4：加拿大工程院院士、IEEE Fellow、卡尔顿大学教授 Fei Richard Yu 和 IEEE Fellow、伦敦玛丽女王大学教授 Arumugam Nallanathan 在 TVT 联合发文高度评价了代表性论文 4，称其开创性考虑了非正交多址的内部窃听问题，并建立了非正交多址抗内部窃听攻击的基本框架（“While existing studies [13], [14] have established foundational frameworks for NOMA transmission against internal eavesdropping, they primarily consider scenarios with a single fixed internal eavesdropper.（[13]为代表性论文 4）”）。

代表性论文 5：IEEE Fellow、皮奥伊联邦大学教授 Joel J. P. C. Rodrigues 在 TCE 发文称赞代表性论文 5 提出的联合人工噪声与功率分配策略可有效推进高密度且高可靠的 6G 网络接入点部署（“…necessitating the rapid evolution and integration of diverse and dense reliable 6G network access points [6].（[6]为代表性论文 5）”）。

五、代表性论文专著目录

代表性论文专著目录

（不超过 8 条。其中代表性论文不超过 5 篇，代表性专著不超过 3 部）

序号	论文专著名称	刊名	作者	年卷 页码 （xx 年 xx 卷 xx 页）	发表 时间 （年 月 日）	通 讯 作 者 （ 含 共 同 ）	第 一 作 者 （ 含 共 同 ）	国 内 作 者	他 引 总 次 数	检 索 数 据 库	知 识 产 权 是 否 归 国 内 所 有
----	--------	----	----	---------------------------------------	---------------------------	---	---	------------------	-----------------------	-----------------------	---

1	LESSON: Multi-label adversarial false data injection attack for deep learning locational detection	IEEE Transactions on Dependable and Secure Computing	田继伟, 沈超, 王布宏, 夏小芳, 张萌, 蔺琛皓, 李前	2024年21卷5期 4418-4432 页	2024年1月12日	沈超	田继伟	田继伟, 沈超, 王布宏, 夏小芳, 张萌, 蔺琛皓, 李前	82	WoS 核心合集	是
2	Adversarial attacks and defenses for deep-learning-based unmanned	IEEE Internet of Things Journal	田继伟, 王布宏, 郭戎潇, 王振, 曹堃锐, 王晓东	2022年9卷22期 2239-2240 9 页	2022年11月15日	王布宏, 田继伟	田继伟	田继伟, 王布宏, 郭戎潇, 王振, 曹堃锐, 王晓东	143	WoS 核心合集	是
3	ETD-ConvLSTM: A deep learning approach for electricity theft detection in smart grids	IEEE Transactions on Information Forensics and Security	夏小芳, 蔺健, 贾倩楠, 王潇峦, 马超凡, 崔江涛, 梁炜	2020年18卷 2553-2568 页	2023年4月18日	崔江涛, 梁炜		夏小芳, 蔺健, 贾倩楠, 王潇峦, 马超凡, 崔江涛, 梁炜	65	WoS 核心合集	是
4	Secure transmission designs for NOMA systems against internal and external eavesdrop	IEEE Transactions on Information Forensics and Security	曹堃锐, 王布宏, 丁海洋, 李腾耀, 田继伟, 宫丰奎	2020年15卷 2930-2943 页	2020年3月11日	王布宏, 丁海洋	曹堃锐	曹堃锐, 王布宏, 丁海洋, 李腾耀, 田继伟, 宫丰奎	54	WoS 核心合集	是

5	Achieving reliable and secure communications in wireless-powered NOMA systems	IEEE Transactions on Vehicular Technology	曹堃锐, 王布宏, 丁海洋, 吕璐, 田继伟, 胡航, 宫丰奎	2021年70卷2期 1978-1983页	2021年2月1日	王布宏, 丁海洋	曹堃锐	曹堃锐, 王布宏, 丁海洋, 吕璐, 田继伟, 胡航, 宫丰奎	123	WoS核心合集	是
---	---	---	---------------------------------	-----------------------	-----------	----------	-----	---------------------------------	-----	---------	---

六、主要完成人情况（不超过6人）

姓名	排名	行政职务	技术职称	完成单位	对本项目贡献
王布宏	1	无	教授	空军工程大学	统筹整个项目，代表作1、2、4、5学术思想的提出者和完成人，对发现点1、2、4均有重要贡献。
田继伟	2	副主任	副教授	空军工程大学	代表作1、2、4、5主要学术思想的提出者之一，对发现点1、2、4做出重要贡献。
曹堃锐	3	无	副教授	信息支援部队工程大学	代表作2、4、5主要学术思想的提出者之一，对发现点1、2、4做出重要贡献。
夏小芳	4	无	副教授	西安电子科技大学	代表作2、3主要学术思想的提出者之一，对发现点1、2、3做出重要贡献。
崔江涛	5	院长	教授	西安电子科技大学	代表作3主要学术思想的提出者之一，对发现点1、3做出重要贡献。
丁海洋	6	主任	副教授	信息支援部队工程大学	代表作4、5主要学术思想的提出者之一，对发现点1、4做出重要贡献。

七、主要完成单位情况（不超过3个）

完成单位	排名	对本项目主要贡献
中国人民解放军空军工程大学	1	项目第一完成单位和技术总体单位。统筹整个项目，从威胁感知建模、模型鲁棒防御、攻击检测识别与安全可靠传输四个层面，系统建立了智能无人系统安全防御的理论体系，代表作1-5学术思想的提出者和完成人，对发现点1-4均有重要贡献。
西安电子科技大学	2	主要完成基于时空特征深度融合的虚假数据注入攻击防御方法。代表作2、3主要学术思想的提出者之一，对发现点1、2、3做出重要贡献。
中国人民解放军信息支援部队工程大学	3	主要完成基于人工噪声与资源分配的抗多方协同窃听攻击安全防御理论。代表作2、4、5主要学术思想的提出者之一，对发现点1、2、4做出重要贡献。

八、完成人合作关系说明

本项目由第一完成人王布宏牵头，各完成人围绕智能无人系统安全防御理论体系开展了长期、稳定的合作，主要合作关系如下：

（1）王布宏与田继伟、曹堃锐：田继伟、曹堃锐曾为空军工程大学王布宏教授课题组博士研究生，一直存在天然合作关系。

（2）田继伟与夏小芳：二人长期共同开展智能系统安全防御研究，共同发表

学术论文、共同申请多项发明专利。

（3）夏小芳与崔江涛：夏小芳为西安电子科技大学崔江涛教授课题组成员，长期共同开展数据安全研究，共同开展相关技术攻关，共同发表学术论文、共同授权多项发明专利。

（4）曹堃锐与丁海洋：曹堃锐现为信息支援部队工程大学（原国防科技大学信息通学院）丁海洋教授课题组成员，长期共同开展通信安全研究，共同开展相关技术攻关，共同发表学术论文、共同授权多项发明专利。