



航空学报  
*Acta Aeronautica et Astronautica Sinica*  
ISSN 1000-6893, CN 11-1929/V

## 《航空学报》网络首发论文

题目： 无人机对雷达组网航迹欺骗综述  
作者： 柏鹏，王玉冰，梁晓龙，张佳强，王维佳  
网络首发日期： 2020-07-20  
引用格式： 柏鹏，王玉冰，梁晓龙，张佳强，王维佳. 无人机对雷达组网航迹欺骗综述. 航空学报. <https://kns.cnki.net/kcms/detail/11.1929.V.20200720.1726.030.html>



**网络首发：**在编辑部工作流程中，稿件从录用到出版要经历录用定稿、排版定稿、整期汇编定稿等阶段。录用定稿指内容已经确定，且通过同行评议、主编终审同意刊用的稿件。排版定稿指录用定稿按照期刊特定版式（包括网络呈现版式）排版后的稿件，可暂不确定出版年、卷、期和页码。整期汇编定稿指出版年、卷、期、页码均已确定的印刷或数字出版的整期汇编稿件。录用定稿网络首发稿件内容必须符合《出版管理条例》和《期刊出版管理规定》的有关规定；学术研究成果具有创新性、科学性和先进性，符合编辑部对刊文的录用要求，不存在学术不端行为及其他侵权行为；稿件内容应基本符合国家有关书刊编辑、出版的技术标准，正确使用和统一规范语言文字、符号、数字、外文字母、法定计量单位及地图标注等。为确保录用定稿网络首发的严肃性，录用定稿一经发布，不得修改论文题目、作者、机构名称和学术内容，只可基于编辑规范进行少量文字的修改。

**出版确认：**纸质期刊编辑部通过与《中国学术期刊（光盘版）》电子杂志社有限公司签约，在《中国学术期刊（网络版）》出版传播平台上创办与纸质期刊内容一致的网络版，以单篇或整期出版形式，在印刷出版之前刊发论文的录用定稿、排版定稿、整期汇编定稿。因为《中国学术期刊（网络版）》是国家新闻出版广电总局批准的网络连续型出版物（ISSN 2096-4188，CN 11-6037/Z），所以签约期刊的网络版上网络首发论文视为正式出版。

**引用格式：**柏鹏，王玉冰，梁晓龙，等. 无人机对雷达组网航迹欺骗综述[J]. 航空学报, 2021, 42(1):023912. BAI P, WANG Y B, LIANG X L, et al. Overview On Phantom Track Deception Against Radar Network Using UAVs [J]. Acta Aeronautica et Astronautica Sinica, 2021, 42 (1):023912 (in Chinese). doi: 10.7527/S1000-6893.2020.23912

# 无人机对雷达组网航迹欺骗综述

柏鹏<sup>1,2</sup>，王玉冰<sup>1,\*</sup>，梁晓龙<sup>1</sup>，张佳强<sup>1,2</sup>，王维佳<sup>3</sup>

- 1. 空军工程大学 空管领航学院，西安 710051
- 2. 空军工程大学 国家空管防相撞技术重点实验室，西安 710051
- 3. 军事科学院 系统工程研究院系统总体研究所，北京 100101

**摘 要：**未来战争对体系作战的需求不仅仅是靠规模“以量取胜”，更要有战术上的智谋“以活胜僵”。通过干扰敌方对我方的意图推断，甚至设计出让敌方相信的假意图，能够在双方的博弈中塑造态势，取得先手，从顶层设计和战术策略上掌握主动权。运用无人机对敌方组网雷达进行航迹欺骗就是一种有效的对抗手段，能够在实现对敌探测的同时，消耗敌方雷达组网的计算资源，干扰敌方雷达及幕后指挥员对我方作战意图的推断，同时提高己方态势感知能力和生存力。本文首先介绍了航迹欺骗干扰的概念，并以时间为序，分类梳理了国内外各研究团队在航迹欺骗领域取得的技术成果；然后针对航迹欺骗干扰的特点，详细分析了虚假航迹设计和生成、由不确定性误差导致的估计问题、延时转发策略和同源检验准则，以及动力学约束问题等四个方面的关键问题和技术难点；最后展望了航迹欺骗的应用前景和下一步研究方向。

**关键词：**航迹欺骗；无人机；雷达组网；意图推断；体系作战

**中图分类号：**V249    **文献标识码：**A    **文章编号：**1000-XXXX (2020) XX-XXXXX-XX

无人机之间通过深度协同，可以实现整体作战性能提升与涌现，其卓越的战场能力已经在实战中予以显现，被美军列入改变未来空战样式的“颠覆性技术”并开展了多项相关项目研究<sup>[1, 2]</sup>。随着分布式协同研究与无人机技术的飞速发展，将无人机应用于电子战受到了广泛关注。同时，雷达组网的出现和应用使得雷达系统的整体抗干扰性能得到大幅度提升，单一的电子对抗设备已经很难实现对敌方雷达组网的有效对抗。因此，以“集群”对“组网”的博弈样式成为未来电子战的

重要选项。  
美国防部发布《2017~2042财年无人系统综合路线图》将无人机集群列为15项关键技术之一，指出其将具备侦察和干扰一体化能力，将对未来航空装备体系构成和作战样式产生重大影响，可见利用无人机执行干扰任务具有极大的应用潜力和研究价值<sup>[3-5]</sup>。2016年5月美国空军发布了首份专门针对小型无人机系统的《2016~2036年小型无人机系统飞行规划》<sup>[6]</sup>，新增了无人机系统对空/对地电子干扰的能力，并将欺骗干扰列

网络出版时间：  
网络出版地址：  
基金项目：国家自然科学基金（61703427）  
\*通讯作者. E-mail: [wyb\\_fd@163.com](mailto:wyb_fd@163.com)

为重点技术之一<sup>[7]</sup>。

当前无人机对组网雷达的干扰方式主要分为：无源干扰与有源干扰。无源干扰由雷达信号对非目标物体的散射或反射产生，常见的方式有箔条云和雷达诱饵等<sup>[8]</sup>。有源干扰一般分为压制性干扰和欺骗式干扰。其中压制性干扰主要通过噪声或者伪噪声的干扰信号淹没或压制含有目标状态信息的回波信号，从而导致组网雷达无法正常发现目标和测量目标参数<sup>[9, 10]</sup>。压制干扰实施过程中，由于平台进行有源辐射且辐射功率要求较大，自身平台的安全性需要实时保证，在实际运用中具有一定的局限性。欺骗干扰通过信号延时转发，能够在战场生成虚假目标，兼有扰乱敌方态势感知同时保护自身平台安全的特点<sup>[11, 12]</sup>。因此，欺骗干扰技术成为电子战领域的研究热点，被美军列为制胜电磁频谱战的新兴技术和未来十年无人技术发展的前十军事目标之一<sup>[13-15]</sup>。

运用无人机遂行作战任务具有诸多优势。一方面，出于无人机成本低廉的特质，可以将大量无人机投入敌方空域作为诱饵，通过航迹欺骗联合其他手段（例如RCS增强等）伪造出虚假目标甚至特定型号的高价值假目标，误导敌方判断，诱使敌方防空火力和雷达对虚假目标做出反应，在保护我方力量的同时，消耗敌方防空资源，暴露敌方装备位置，以很小的成本代价消耗敌方高成本武器，获取高价值敌方情报；另一方面，出于无人机作战运用灵活机动的优势，搭载电子战

设备后可根据任务需求实现高度协同，进行战场侦察，并对敌方的预警雷达、制导武器进行压制干扰或欺骗干扰，为后续作战力量开辟安全走廊，成为强大的电子支援力量<sup>[16]</sup>。

航迹欺骗是欺骗干扰中的一种高级形式，无人机可搭载数字射频存储器（Digital radio frequency memory, DRFM），通过飞行航迹和信号延时转发的协同配合，形成虚假航迹欺骗敌方组网雷达。在和平时期，对已知的敌方雷达实施航迹欺骗干扰，可同时侦察其工作参数和工作模式，甚至诱使隐蔽的雷达开机，实现情报、监视和侦察；而在战时，航迹欺骗干扰形成的逼真性较强的假目标可以吸引敌方雷达注意力，占用敌方的计算资源，使其虚警率大幅提高，扰乱敌方的跟踪和制导，掩护己方飞机的作战，即使敌方采取硬杀伤方式，也可能命中的是假目标，消耗敌方武器装备，提高我方作战力量的生存力<sup>[17]</sup>。

如图 1 所示，是无人机协同作战的场景示意图，当无人机与敌方距离较远时，可以充分发挥分布式侦察定位的优势来完善观测信息、提高定位精度，为后续的航迹欺骗等行动提供准确的情报支撑。随着与敌方距离逐渐接近，无人机可采用航迹欺骗联合RCS欺骗、闪烁干扰等其他干扰手段进行佯装和诱骗，迷惑敌方雷达及幕后指挥员对战场态势和我方意图的判断，消耗其计算资源，在进入近距后，航迹欺骗还可起到自卫和保护我方高价值作战平台的作用。

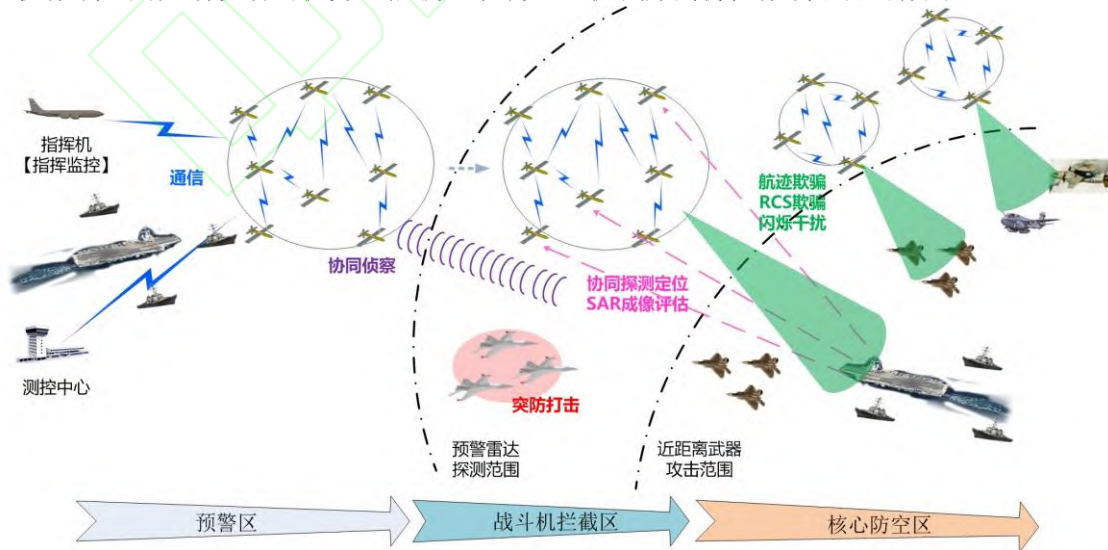


图 1 无人机协同作战中航迹欺骗与侦察/干扰/打击一体化任务示意图

Fig. 1 UAV cooperative operation of phantom track deception and reconnaissance / jamming / strike mission

由于航迹欺骗干扰的实施有诸多约束条件, 目前的研究大多处于理论探索和试验阶段。从实验室走向战场运用, 其原理和具体实施还存在瓶颈有待突破, 本文将重点针对无人机对雷达组网航迹欺骗进行分析和研究。一方面对国内外各研究团队在航迹欺骗领域取得的技术成果进行梳理和总结; 另一方面, 针对航迹欺骗干扰的特点, 详细分析虚假航迹设计和生成、由不确定性误差导致的估计问题、延时转发策略和同源检验准则, 以及动力学约束问题等四个方面的关键问题和技术难点, 从而为无人机对雷达组网航迹欺骗方法提供指导。

本文的章节组织如下: 文章共分5部分, 其中第1节介绍航迹欺骗干扰的基本概念; 第2节对国内外相关公开文献进行梳理归纳; 然后根据航迹欺骗干扰的特点, 在第3节中提炼出四个关键问题和技术难点, 并分别介绍常用解决思路方法和仍存在的不足; 围绕未来作战运用需求, 第4节探讨航迹欺骗的应用前景和可行的下一步研究方向, 最后第5节对全文进行总结。

## 1 航迹欺骗干扰概念

如图2所示, 是假目标欺骗的工作原理。无人机基于截获到的敌方雷达信号, 利用数字射频存储器进行处理后, 延迟(或超前)一定时间后再发射出去, 使雷达接收到一个或多个比该目标真实距离靠后(或靠前)的回波信号, 实现假目标或多假目标欺骗。小型无人机属于低慢小目标, 会给雷达探测带来一些困难, 以此保证无人机自身的生存能力; 或者无人机具有一定的隐身性能, 避免雷达对无人机平台的直接探测识别, 使得雷达只能依靠包含虚假目标信息的回波信号来计算和判断目标位置和类型。

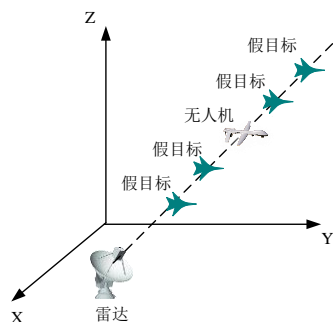


图2 对雷达实施距离假目标欺骗干扰示意图  
Fig. 2 Deception jamming of range phantom target to radar

在此基础上, 多个连续的假目标点可以形成一段虚假航迹, 利用多无人机平台间的深度协同实施更高级别的虚假航迹欺骗干扰。如图3所示, 通过协同控制无人机的飞行航迹, 可在敌方的组网雷达系统中形成一条或多条欺骗干扰航迹, 迫使敌方加强空情处置, 达到欺骗目的。

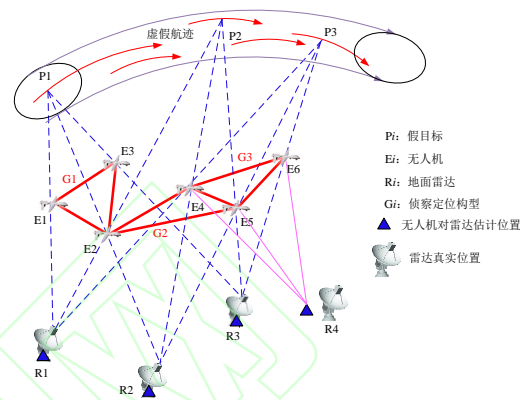


图3 无人机协同干扰组网雷达系统示意图  
Fig. 3 The cooperative phantom track jamming against radar network using UAVs

组网雷达自身具有抗干扰特性, 通常采用聚类分析、多站联合检测、回波相关性处理以及数据级融合等方法进行信号、信息处理[18]。在组网雷达探测跟踪下, 真目标和有源假目标在空间状态(如位置、速度等)上表现出显著的差异: 对于真目标, 其空间状态与雷达部署位置无关, 在统一坐标系中, 各雷达探测出的真目标空间状态基本一致, 可以认为它们是源自于同一个目标(同源); 对于假目标, 它们存在于雷达与干扰机连线以及延长线上, 其空间状态由干扰机和雷达部署位置共同决定, 不同雷达量测到的有源假目标的空间状态一般是不一致的, 组网雷达信息融合中心就会将假目标剔除。这种利用真假目标在组网雷达观测下的空间状态差异来进行假目标鉴别的思想简称为“同源检验”, 它是组网雷达对真假目标甄别的理论依据。

当采用无人机对组网雷达进行欺骗干扰时, 利用平台之间协同产生的虚假目标信息作用于雷达的信号接收系统, 以致雷达组网中每部雷达都接收到包含虚假目标信息的回波信号, 雷达在接收到该信号后, 将会改变天线波束指向或跟踪波门等对该虚假目标进行定位与跟踪。

根据航迹欺骗原理, 多无人机节点可进行灵活选择, 形成多个假目标和虚假航迹。例如, 无



人机E1, E2, E3分别欺骗雷达R1, R2, R3, 无人机与雷达视线(line of sight, LOS)的延长线交汇于一点P1, 即通过了这三部雷达同源检验的假目标点。同理, 无人机E2, E4, E5分别欺骗雷达R1, R2, R3, 无人机与雷达LOS的延长线交汇于一点P2, 即通过了这三部雷达同源检验的另一个假目标点。多个连续假目标点可形成多段虚假航迹。在进行航迹欺骗的同时, 无人机可对地面组网雷达进行侦察定位, 通过优化空间构型提高定位精度。例如无人机E4, E5, E6在侦察定位构型G3下对雷达R4进行协同定位, 同时对雷达R1, R2, R3进行航迹欺骗, 形成假目标P3及

其航迹。同理, E1, E2, E3在侦察定位构型G1下形成假目标P1及其航迹, 无人机E2, E4, E5在侦察定位构型G2下形成假目标P2及其航迹。

## 2 航迹欺骗国内外研究现状

航迹欺骗的概念一经提出就备受关注, 美国、印度、韩国等国家的学者都开展了大量工作, 中国在这方面的研究起步较晚, 但随着对电子战领域愈发重视, 目前也取得了阶段性成果。如图4所示, 是运用无人机对雷达组网进行航迹欺骗的分类归纳图。

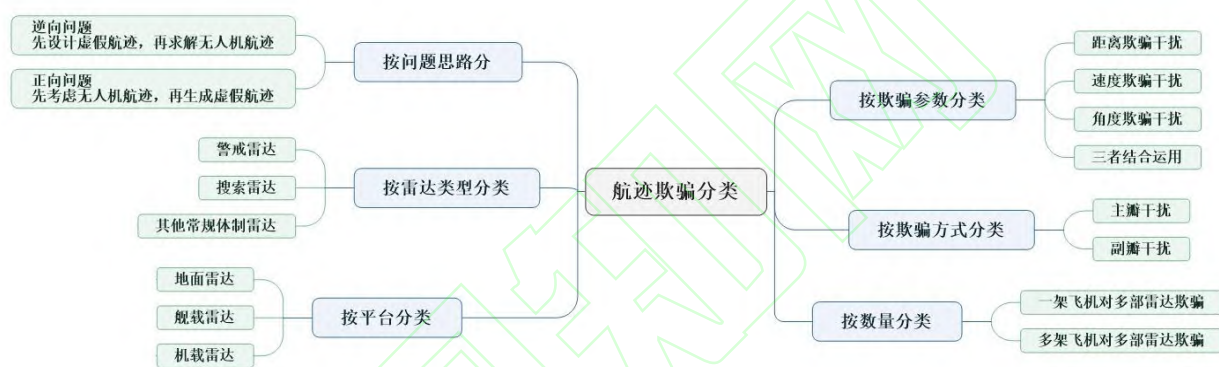


图4 航迹欺骗分类归纳图

Fig. 4 Classification diagram of phantom track deception

按照欺骗参数的种类, 对单个参数的欺骗可以分为距离、速度、角度欺骗三类, 但由于仅在单个参数上进行改变很容易被雷达组网识别出来, 欺骗效果不佳, 因此常常对多个参数进行同时欺骗, 将三者结合运用形成最为复杂也最难被识别的航迹欺骗。同时, 根据欺骗信号进入的是雷达主瓣还是副瓣, 还可分为主瓣干扰和副瓣干扰<sup>[19, 20]</sup>。按照欺骗雷达数量的分类, 有“一对一”和“一对多”两类, 是否能够利用无人机实现“一对多”的干扰, 其根本是由无人机干扰系统的计算能力和资源决定的。前者主要针对自发自收体制的雷达组网, 每架无人机只需欺骗一部雷达, 通过多架无人机的高度协同来完成对整个雷达组网的欺骗, 在无人机计算能力和系统资源允许的情况下, 采用距离欺骗和角度欺骗的综合运用也可以实现对普通单基地组网雷达的“一对多”航迹欺骗干扰; 后者主要针对收发分置体制的雷达组网, 一架无人机可同时欺骗多部雷达接收机。

航迹欺骗的对象通常是警戒雷达、搜索雷达等常规体制雷达, 其装载平台可以是多种类型, 例如地面雷达、舰载雷达和机载雷达等。

在研究航迹欺骗问题时, 常用的解决思路有两大类, 一是先设计好虚假航迹, 再根据虚假航迹和雷达的相对位置逆推求解出无人机的实际飞行航迹, 这类思路被称为“逆向问题”; 另一类则与之相反, 在给定的无人机飞行航迹下, 通过控制延时转发策略, 根据无人机和雷达的相对位置计算可能形成的虚假航迹, 这类思路被称为“正向问题”。

正向问题中, 无人机通常情况下以执行侦察、定位、打击等其他任务为主, 无人机与雷达的空间位置没有经过预先设计, 如果无人机与雷达间LOS不能汇聚于一点, 那么无论延时转发时间如何改变, 都无法使得假目标位于雷达组网的同一个SRC内, 即无法形成有效的假目标, 因此航迹欺骗成功率较低, 容易出现无解的情况<sup>[21]</sup>。

此时进行航迹欺骗主要起到执行侦察、定位、打击等任务的辅助作用,一方面尽可能形成空间连续的虚假目标点,保护自身平台安全,迷惑敌方判断;另一方面,通过大量转发雷达信号,消耗敌方雷达运算资源<sup>[21]</sup>。

对于特意以航迹欺骗为目标的干扰任务,往往具有战术意图和特定目的,而能够体现出意图设计的方式是先设计好虚假航迹再逆推出无人机实际飞行航迹,因此在学术研究中,学者们通常将对航迹欺骗的关注重点集中在逆向问题上,本文的重点也放在逆向问题的解决方法上。

以图 5所示情况为例,一发多收体制下的组网雷达有一部发射机和多部接收机。这种情况下,无人机将发射机发射的信号延时转发后被多部接收机接收,形成了一架无人机对多部雷达的局势,即“一对多”的欺骗形式。

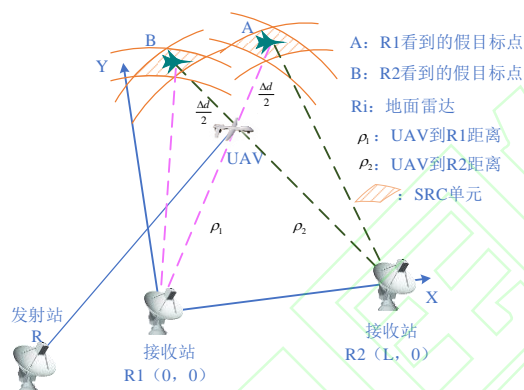


图 5 一发多收体制下的航迹欺骗示意图(修改自[51])

Fig. 5 phantom track deception against radar network with one transmitter and multiple receivers (modified from [51])

虚假航迹欺骗的概念最早由美国学者K. B. Purvis等人提出<sup>[21]</sup>, K. B. Purvis团队针对自发自收体制的雷达组网开展了协同航迹欺骗研究,在二维空间内分析了匀速直线状和圆弧状假航迹对应的无人机航迹可飞区域。针对无人机对雷达组网的定位误差,建立了非线性协同欺骗系统模型,分别分析在TDOA无源定位体制下雷达站址误差对航迹欺骗效果的影响<sup>[22]</sup>以及无人机速度误差对可飞区域造成的影响<sup>[23]</sup>,并针对多无人机的分布式控制问题,运用多智能体思想求解了可行航迹<sup>[24]</sup>。在处理无人机运动约束时,运用最优控制方法,在代价函数中添加平滑惩罚函数<sup>[25]</sup>;针对雷达站址误差影响航迹欺骗成功率的问题,提出了欺骗与定位双任务联合优化的思路,通过计

以图 6所示情况为例,自发自收体制下的组网雷达,每部雷达都独立发射并接收信号,可通过一架无人机欺骗一部雷达,协同形成虚假航迹,即“一对一”的欺骗形式。

受到硬件水平和动力学约束等实际因素的约束,无人机对敌方雷达组网产生航迹欺骗通常要满足几个条件:

(1) 无人机处在雷达与虚假目标的LOS上,即运用主瓣距离欺骗技术来创建欺骗航迹;

(2) 考虑到欺骗效果,一般认为无人机质量和体积较小,或者具有一定隐身性能;

(3) 雷达位置固定或近似固定,无人机和虚假航迹的运动满足动力学约束。

由于以上约束是非常严苛的,如何在满足各类约束的同时设计出合理虚假航迹和求解出可行无人机航迹,就成为了技术难点和研究热点。

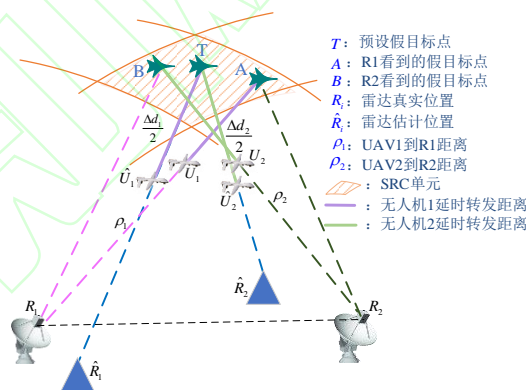


图 6 自发自收体制下的航迹欺骗

Fig. 6 phantom track deception against radar network with distributed radar network

算克拉美罗界CRLB,给出了TDOA定位体制下无人机最佳空间构型的角度准则和协同准则,从而提高航迹欺骗成功率<sup>[26]</sup>。Shima T等人在有通信约束的情况下,采用分布式控制架构,运用EKF滤波,实现状态估计和无人机航迹调整,并对无限时长和有限时长下的航迹欺骗进行了空间构型分析<sup>[27]</sup> <sup>[28]</sup>。XU Y和Basset G运用VMC算法用于无人机航迹求解,并通过计算机仿真验证了仿生智能算法在航迹欺骗问题中的有效性<sup>[29]</sup>。

Maithripala DHA, Jayasuriya S等印度学者也开展了针对自发自收体制的雷达组网航迹欺骗逆向问题研究,主要从控制论和多智能体系统的角度进行分析。该团队将无人机航迹用参数化的微分空间曲线表示出来,考虑了无人机和虚假目

标间的耦合运动学约束<sup>[30]</sup>和平台的机动性能约束<sup>[31]</sup>,提出一种分布式控制架构<sup>[32]</sup>,并基于比例导引律生成虚假航迹,基于LOS导引律控制无人机航迹<sup>[33]</sup>。Hajieghrary H等人考虑了无人机和设定虚假航迹之间的构型参数,运用路径规划算法来确保控制的一致性<sup>[34]</sup>。Dhananjay N利用雷达位置的投影位置设计垂直平面上的虚迹,推导出了可行航迹的充分条件<sup>[35]</sup>。

韩国学者Lee I-H 和 Bang H 在三维空间内进行航迹欺骗问题的求解,主要从控制论的角度展开分析,将无人机航迹求解问题转化为最优化控制问题,运用可行序列二次规划法求解<sup>[36]</sup>;或转化为基于预测控制器的LOS导引律问题<sup>[37]</sup>,提出基于输入输出反馈的导引律方法,求解出预设假航迹下的无人机航迹解析解<sup>[38]</sup>。

中国学者开展欺骗相关研究虽然起步较晚,但更加注重战术和技术的结合。在战术方面,马亚涛,赵国庆等人提出一种利用单架飞机对雷达网内某个特定雷达进行假目标航迹欺骗干扰,其余飞机对网内其他雷达进行相参噪声压制干扰的航迹欺骗战术<sup>[39]</sup>。李修和提出一种由地面控制站和空中干扰机构成的空地有源组网干扰系统,将有源压制和假目标欺骗相结合<sup>[40]</sup>。由于雷达网在不同位置的探测精度不同,李小波提出在假航迹规划时,可根据雷达网探测精度的弱点确定相应的延时转发策略<sup>[41]</sup>。

在仿真验证和工程实践方面,龚旻提出了一种结合平方倍频算法和DRFM技术的低截获概率雷达转发式欺骗航迹干扰方法,解决工程运用中传统测频接收机无法检测隐藏在基底噪声下的LPI雷达信号和对LPI雷达进行转发式欺骗航迹干扰的问题<sup>[42]</sup>。罗金亮分析得出多目标航迹欺骗较易于实现对双基地雷达的干扰,并估算了干扰机在实际运用时所需的干扰功率及位置部署<sup>[43]</sup>。张国兵等人通过半实物仿真系统计算了两批假目标预定航迹的置信度,验证了多假目标航迹欺骗技术应用的可行性和有效性<sup>[44]</sup>。针对无人机的空时协同问题,杨忠提出一种基于集中航迹规划和分布航迹协同的雷达网航迹欺骗干扰技术,选取基准雷达坐标系设计基准航迹<sup>[45]</sup>。

在模型建立和求解方法上,针对真假目标空间状态不一致的问题,周续力<sup>[46]</sup>提出一种产生具

有空间相关性和时间相关性的可控欺骗航迹的算法。高彬等人提出一种基于RGPO的航迹欺骗方法,基于ECAV、雷达和虚假航迹点三者共线关系,削减搜索空间,解决动力约束下无人机轨迹规划约束最优化难题<sup>[47]</sup>。朱宇等人在分析组网雷达数据处理方法的基础上,得出使网中各雷达对假目标观测的空间状态差异保持在雷达网检验门限范围内,组网雷达系统就不能有效地剔除假目标的结论<sup>[48]</sup>。郭淑芬等人针对无人机任务过程中的运动特点,提出一种可直接求解无人机的运动状态的简化模型,减少无人机运动状态的控制量<sup>[49]</sup>。

王国宏团队针对实际应用中的航迹欺骗性能问题,分析了雷达站址误差和融合中心K近似域(K-NN)航迹关联准则对航迹欺骗干扰的影响<sup>[50]</sup>。赵珊珊,张林让等人针对一发多收体制的雷达组网,推导了无人机在远场和近场情况下对其形成有效航迹欺骗的延时转发策略<sup>[51]</sup>。柳向对无限时长和有限时长虚假航迹分别给出了基于航迹控制因子的无人机航迹计算方法,并对距离偏差和角度偏差采取了补偿措施<sup>[52, 53]</sup>。范振宇运用TDOA算法进行对组网雷达的定位从而减小站址误差<sup>[54]</sup>。李飞利用勒让德伪谱法将无人机航迹求解问题转化为了非线性规划问题,采用CFSQP软件包进行求解<sup>[55]</sup>。

在欺骗干扰对象上,周续力<sup>[46]</sup>和李森<sup>[56]</sup>针对警戒雷达的欺骗干扰进行了研究,原伟<sup>[57]</sup>等人对机载预警脉冲多普勒雷达的航迹欺骗干扰技术进行研究,黄勇<sup>[58]</sup>分析了“空对空”、“动对动”航迹假目标欺骗干扰的关键技术和难点问题,进一步扩展了航迹欺骗的应用范围。

国内学者也在雷达组网抗欺骗干扰方面取得了一定研究成果,由于干扰和抗干扰技术是在博弈中相互促进的,抗欺骗干扰的成果能够从反面为欺骗干扰的发展提供思路和指导。国防科技大学赵艳丽,王雪松<sup>[59, 60]</sup>等针对距离多目标欺骗干扰下的组网雷达跟踪进行了研究,分析了组网雷达同源检测门限对假目标识别的影响,从反面为假目标欺骗干扰提供了效能评估方法。海军航空工程学院王国宏团队<sup>[61, 62]</sup>也从多元统计分析理论、基于角度量测统计特性差异和基于目标状态估计等多种方法进行了组网雷达抗航迹假目标欺



骗干扰的研究,从反面为虚假航迹设计提供了注意事项和改进思路。由于篇幅限制,更多抗欺骗干扰的相关内容在本文中暂不赘述。

归纳以上研究成果可以看出,航迹欺骗问题在具体分析时,要考虑多种因素和约束,例如:有无雷达坐标的先验信息、欺骗何种体制的组网雷达、组网雷达静止或运动、采用何种检验准则、满足何种运动约束等,都影响着航迹欺骗的效果,这也是航迹欺骗从理论研究走向实际应用的难点所在。

### 3 航迹欺骗的关键问题和技术难点

现有公开文献中,对航迹欺骗问题的研究通常在以下合理假设的基础上进行:

- (1) 无人机运动状态可控,通过无人机之间的协同完成多对多的航迹欺骗;
- (2) 对敌方雷达的位置已知或具有一定先验信息;
- (3) 无人机平台上装备有相应的电子对抗设备,可对截获的雷达信号进行转发式干扰。

如前文所述,航迹欺骗可以分为“正向问题”和“逆向问题”,能够体现出意图设计的是先设计好虚假航迹再逆推出无人机实际飞行航迹的方式,因此“逆向问题”更加受到关注。这就对虚假航迹的设计提出了要求。在给定航迹欺骗起点和终点的情况下,首先要有一套合理的评估方法,来衡量什么是对我方而言“好”的虚假航迹,既能够对敌产生足够的迷惑性,又具有较高可飞性。在此基础上,下一步就是采用合理的算法,求解出能够形成设定虚假航迹的无人机实际飞行航迹,在这个过程中需要综合考虑多无人机的分布式协同控制问题、无人机与敌方雷达的相对空间位置关系、每个航迹点上对应的延时转发量以及无人机动力学约束和硬件性能限制。因此,航迹欺骗要完成从实验室到战场的跨越,首先要解决上述关键问题。本文将以上内容归纳分类如下:

- (1) 为无人机选择“最佳”虚假航迹的分布式协同控制问题;
- (2) 使虚假目标点能够通过雷达组网同源检验或关联准则的延时转发策略;
- (3) 雷达/无人机位置不准确和时间延迟产生的估计问题;

(4) 速度/天线/虚假目标速度等无人机的动力学约束问题,以及DRFM等硬件的性能约束。

在进行以上四个问题研究的基础上可以进一步进行航迹欺骗效果评估,根据评估情况采取对应的补偿措施,从而提高航迹欺骗成功率。整体研究方法如图7所示。

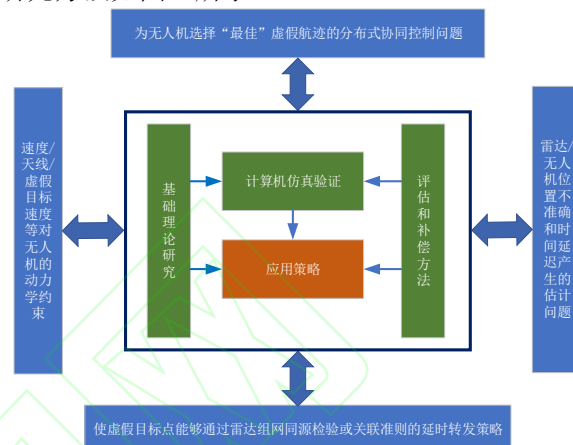


图7 航迹欺骗整体研究方法

Fig. 7 The research route map of phantom track deception

#### 3.1 虚假航迹设计和生成

在虚假航迹生成问题中,无人机和虚假航迹的运动学和动力学不仅各自存在约束,而且两者之间高度耦合,存在着严格的等式和不等式约束,限制了无人机的可飞范围和运动空间。在设计过程中需要考虑上述因素,选择合理的空间位置,使得虚假航迹既满足我方战术意图,又满足动力学约束,并且对应的无人机实际飞行航迹在满足动力学约束的同时还具有较好的可飞性。这也是虚假航迹设计和生成的难点所在。

目前,该部分常用的方法有基于LOS导引律的航迹生成算法、基于比例导引的航迹生成算法、基于分布式控制的航迹生成算法。这些方法都可以得到给定起点和终点的一段虚假航迹,但是缺乏对航迹的评估。研究现状如表1所示。

表1 虚假航迹设计及生成

Table 1 Design and generation of phantom track

虚假航迹类型	求解方法	维度及对应参考文献
直线状航迹	基于航迹控制因子求解	二维: [21] [16] [17] [18] [19] [20] [25]
		三维: [22]



圆弧状航迹	基于曲线微分求解	二维: [21] [15] [16] [17] [23] [25]
折线状航迹	基于航向角选择求解	二维: [18] [19] [21] [25]

实际上, 尽管诸多文献将“虚假航迹生成”作为题目或关键词, 但内容更偏重于在给定虚假航迹之后求解对应的无人机飞行航迹。Pachter et al.<sup>[21]</sup>, Purvis et al.<sup>[23]</sup>, 和Maithripala, Jayasuriya<sup>[30]</sup>分析了无人机运动与虚假航迹之间的二维数学关系。Pachter et al.求解了生成特定虚假航迹(如直线和圆形航迹)的无人机可飞行区域, 并考虑了无人机的速度、天线的工作范围和虚假航迹的速度等空间约束, 提出了虚假航迹生成的分布式协同策略。

有关虚假航迹生成的一些文献讨论了滚动优化控制方法<sup>[24, 30-32, 63]</sup>。Maithripala根据每架无人机在速度和航向速率约束下的飞行距离, 生成了穿过下一个时间步长速度扇区的虚假航迹。虚假航迹的速度矢量是从当前速度方向到下一时刻航迹点的指向, 这个方法相对简单, 只需要边界航向角和虚假航迹方向这两类信息。Mears提出了一种带约束的滚动优化优化方法来解决这个问题<sup>[63]</sup>, 构造了代价函数来惩罚或奖励虚假航迹和无人机的机动行为。Purvis和Chandler研究了一种基于虚假航迹和无人机飞行可行域的制导律, 并证明了该制导律的可行性<sup>[24]</sup>。在无人机可行域中, 提出了与虚假航迹平行飞行的最佳点。当无人机与虚假航迹平行飞行时, 系统是可控的, 这使得该算法具有很强的鲁棒性。

Maithripala和Jayasuriya进行了虚假航迹生成的可行性分析和实现平行飞行航迹的概念<sup>[31, 32]</sup>。基于微分几何观点, Maithripala和Jayasuriya推导出了可行解存在的充分条件, 并利用为编队控制开发的运动规划算法生成虚假航迹。

以往研究的一个主要假设是, 无人机在初始时刻满足生成虚假航迹的约束, 并且在整个任务期间该约束是不放松的。问题是这样的约束往往比较严格, 无人机很难一直满足生成虚假航迹的条件并执行任务, 例如无人机受到风力或湍流影响时, 很容易不再满足生成虚假航迹的约束。此外, 以往的研究大多数是在二维中进行的, 当把问题拓展到三维时, 求解方法需要重新制定, 计

算复杂度也大幅增加。

一种常用的方法是引入航迹控制因子, 来表征假目标点、无人机和雷达三者之间的位置关系, 通过推导航迹控制因子来实现对无人机飞行航迹的生成<sup>[37]</sup>。由虚假航迹欺骗原理知, 无人机需要处于雷达和假目标的LOS上, 为后续表示方便, 引入航迹控制因子 $p$ 如下:

$$p = \frac{r}{R} \quad (1)$$

其中,  $r$ 为无人机与雷达的距离,  $R$ 为假目标点与雷达的距离。引入航迹控制因子的航迹生成算法, 优点在于给定起始航迹点、终止航迹点及无人机初始位置参数时可直接求解出一条确定的无人机飞行航迹, 但不足之处在于没有给出全部可行解, 并且计算出的航迹没有考虑无人机的运动学约束, 是否具备真实条件下的可飞性还有待具体分析。

在虚假航迹生成问题上, 如何对虚假航迹的性能进行评估并指导虚假航迹的生成, 以及给定虚假航迹之后求解具备可飞性的无人机航迹仍然有待进一步研究。

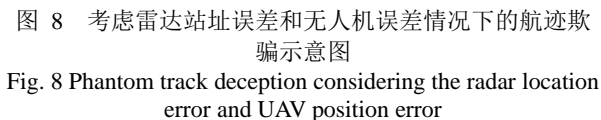
### 3.2 由不确定性误差导致的估计问题

在已有的公开文献中, 由不确定性误差导致的估计问题主要包含两大类: 一是由于先验信息不足, 无人机对组网雷达定位误差等原因导致的雷达站址位置估计问题, 即对航迹欺骗效果产生影响的站址误差<sup>[16,20,33,36-37,40]</sup>; 二是受到动力学约束、硬件系统误差、控制误差和风力影响等原因导致的无人机位置误差<sup>[17,19,26,36-37]</sup>, 如表2所示。

表2 由不确定性误差导致的估计问题

Table 2 Estimation problem caused by uncertain error

误差类型	造成误差的原因	解决方法	维度及对应参考文献
雷达站址误差	无人机对雷达定位的量测误差	采用复合定位方法提高无人机对雷达的定位精度	二维: [22] [26] [50] [54]
			三维: [52] [53]
无人机位置误差	平台性能约束, 无人机控制误差, 风力影响等因素	采取偏差补偿措施	二维: [23] [25] [33]
			三维: [52] [53]



出于非合作特性,我方无人机通过预先侦察获得敌方雷达的大概位置,但存在雷达站址定位误差。在实际航迹欺骗过程中,站址误差导致我方无人机通过延时转发形成的预设假目标点并不是严格处于雷达和无人机连线形成的LOS上。不同雷达视角下观测到的假目标点在空间中出现“分裂”,如图 9和图 10所示。当“分裂”程度较小,两部雷达观测到的假目标点仍处于同一个空间分辨单元(Space resolution cell, SRC)内时,假目标点可以通过这两部雷达间的同源检验;反之,雷达组网将识别并剔除假目标点。因此,分析站址误差对虚假航迹带来的影响是实现航迹欺骗的基础。

Fig. 9 phantom target split in the space because of radar location error under distributed radar network (modified from reference [26])

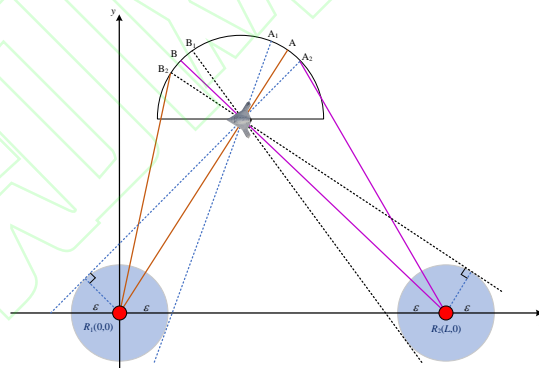


Fig. 10 phantom target split in the space because of radar location error under one transmitter and multiple receivers

考虑站址误差的无人机对一发多收体制雷达的欺骗干扰如图10所示。以侦测的接收站1位置为原点建立直角坐标系, 侦测的接收站2置于x轴上, 与侦测的接收站1间基线长度为 $L$ 。设无人机坐标为 $(x_0, y_0)$ , 延时转发产生的假目标距无人机距离为 $\Delta d/2$ , 在两个雷达接收站的侦测位置视角看, 延时转发后产生的假目标点分别为点A和点B, 如图10所示。然而, 侦测位置和真实位置之间存在站址误差, 范围是半径为 $\varepsilon$ 的圆形区域。当雷达真实位置与无人机位置形成的LOS与误差圆相切时, 产生假目标点最大距离和角度偏差, 此时接收站1对应产生的假目标点为 $A_1$ 和 $A_2$ , 接收站2对应产生的假目标点为 $B_1$ 和 $B_2$ , 将以上四个假目标点称之为误差边界点。

在对不确定性误差导致的估计问题的分析基础上, 可以进行对应的偏差补偿。常见的偏差补偿包括两个部分: 距离偏差补偿和角度偏差补偿。文献<sup>[52]</sup>中指出, 角度偏差相对于距离偏差对航迹欺骗效果的影响要大的多。此外, 距离偏差可以通过减少无人机的延时转发量来进行补偿。但是, 进行该类补偿的前提是具备足够的先验信息, 在掌握敌方雷达精确位置的基础上确定每一时刻雷达与假目标点的LOS, 然后采取相应的补偿措施。实际上, 出于非合作特性, 敌方雷达的精确坐标是很难获得的, 如何在先验信息有限的情况下进行偏差补偿, 将成为提高航迹欺骗效果的关键。

### 3.3 延时转发策略和同源检验准则

在设定虚假航迹之后, 需要对应求解每架无人机的实际飞行航迹和延时转发策略, 即每个时刻每架无人机的位置和对应的转发延时量。由此在空间中形成的假目标点能够通过雷达组网同源检验, 称之为一个有效的假目标点, 多个连续有效假目标点形成一段有效的欺骗航迹。

由于无人机、组网雷达、设定虚假航迹三者的位置不断变化, 延时转发策略的计算具有一定复杂性。针对这个问题, 文献<sup>[51]</sup>中针对一发多收体制的雷达组网, 根据无人机距雷达的位置划分出远场区域和近场区域两类情况, 推导出了一发多收体制下能够形成有效航迹欺骗需要满足的延时转发策略, 并运用SRC同源检验准则进行了有效性验证。对于自发自收体制的雷达组网, 对应的延时转发策略目前还没有见诸公开文献。

要通过组网雷达SRC同源检验的条件如下:

$$\begin{cases} |AR_1 - BR_1| \leq \delta_1 \\ |AR_2 - BR_2| \leq \delta_2 \end{cases} \quad (2)$$

其中,  $\delta_i$  表示雷达  $i$  的距离分辨率。当考虑站址误差时, 上式很容易拓展运用, 只要假目标点在最大偏差情况下仍满足SRC条件, 则假目标点可以通过两部雷达的同源检验。

此外, 组网雷达使用何种方法进行同源检验, 也对欺骗效果有重要影响。目前, 组网雷达常用的同源检验方法有: 基于雷达空间分辨单元的同源检验<sup>[33, 41, 51]</sup>; 基于N/M准则的同源检验<sup>[21, 52, 53]</sup>; 基于K近邻准则的同源检验<sup>[50, 64]</sup>。计算航

迹欺骗通过同源检验的成功率, 可以为假航迹生成提供闭环反馈和设计指导。

### 3.4 动力学约束问题

在航迹欺骗过程中, 无人机的飞行要遵循动力学约束, 否则不具备可操作性; 同时, 由多个虚假目标点形成的虚假航迹也要符合动力学约束, 才能更好地起到迷惑敌方雷达的作用。本文将航迹欺骗中的动力学约束进行归纳, 如图 11 所示, 可分为无人机动力学约束、虚假目标动力学约束、以及无人机和虚假目标的耦合约束三大类。其中, 耦合约束是指无人机和假目标在每个时刻的动力学特性要满足一定的几何关系, 这也是使虚假航迹欺骗更加逼真的关键。

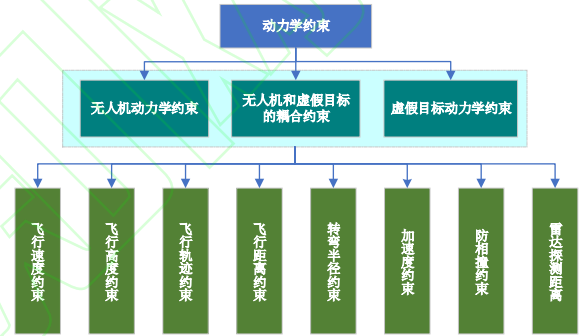


图 11 航迹欺骗研究中的运动学约束

Fig. 11 Kinematic constraints in the phantom track deception

#### (1) 飞行速度约束

在实际运用中, 无人机受到硬件性能的约束, 其飞行速度  $v_E$  应在最小速度  $v_{Emin}$  和最大速度  $v_{Emax}$  之间, 即  $v_{Emin} \leq v_E \leq v_{Emax}$ , 从而保证无人机的正常工作。同样, 为了使假目标具有逼真的运动特性, 假目标的飞行速度也需要在合理的区间范围内。

#### (2) 飞行高度约束

出于硬件性能的限制以及避免被敌方雷达探测发现的战术需要, 无人机的实际飞行高度  $h_E$  应控制在合理飞行范围的最小值  $h_{Emin}$  和最大值  $h_{Emax}$  之间, 即满足  $h_{Emin} \leq h_E \leq h_{Emax}$ 。假目标的飞行高度也要在合理的区间范围内。

#### (3) 飞行轨迹约束

无人机的实际飞行航迹和形成的虚假航迹都要满足飞行轨迹约束。常见的假设无人机做匀速直线运动、匀速圆周运动等简单运动, 这种假设的优点是利于理论计算, 当然也可以采用更加



复杂的运动方式。但不论无人机如何运动,在每个时刻,无人机都要位于该时刻虚假目标点和雷达的LOS上,即假目标点、无人机和雷达三者要满足共线关系。

#### (4) 飞行距离约束

此处的飞行距离约束包括两个含义:一是相邻时刻对应的航点距离需要是可行的,即无人机飞行速度可达;二是总的飞行距离不应超过无人机的续航距离。

#### (5) 转弯半径约束

实际飞行中无人机的飞行方向无法瞬变,调整航向时具有转弯半径约束  $r_{turn} \geq r_{turnmin}$ ,这也是无人机航迹求解过程中不可忽视的约束。

#### (6) 防相撞约束

随着无人机数量的增多,在协同执行航迹欺骗任务时,无人机间距  $d$  需要控制在安全距离  $d_{safe}$  以上,防止出现无人机相撞导致的损毁和任务失败情况,即  $d \geq d_{safe}$ 。

#### (7) 雷达探测距离约束

由于与雷达相距超过雷达探测距离  $d_{range}$  的假目标会直接被雷达系统删除,产生无效假目标点,造成不必要的资源浪费,因此假目标点的设置要满足雷达探测距离约束,即  $R \leq d_{range}$ 。

#### (8) 无人机与虚假目标的耦合约束

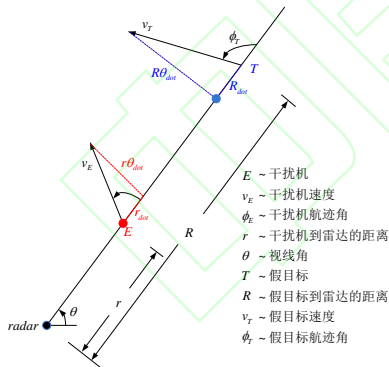


图 12 干扰机和假目标参数及其关系

Fig. 12 The relationship between parameters of UAV and phantom target

由于假目标位于雷达和无人机LOS的延长线上,其运动学参数满足图 12所示的关系。假目标是在模拟一架真实空中飞行器的状态,因此其速度同样有上下限。根据假目标的运动状态和无人机的运动状态,就可以得到无人机和假目标距离变化率和角度变化率的边界限制。从而使UAV和假目标的飞行域呈现的环形域如图 13所示。

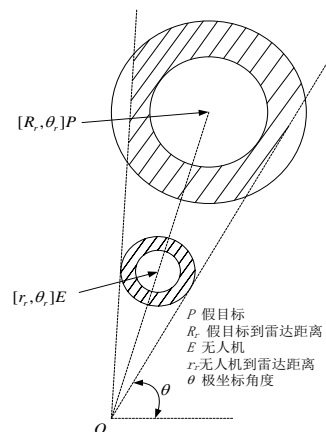


图 13 无人机和假目标在速度边界下的速度可行域

Fig 13 The feasible velocity zone of UAV and phantom target under the velocity constraint

#### (9) 加速度约束

出于硬件性能和机动性能因素,实际飞行中无人机的加速度  $a$  是具有一定界限的,即  $a_{min} < a < a_{max}$ 。

(10) 实际中无人机可机动飞行,但为减少控制误差,无人机尽可能少做转弯、爬升、俯冲等机动动作。

由上可得,动力学约束数量多,要求严苛,极大限制了无人机的可飞区域和可行航迹,是航迹欺骗从理论到实际应用的重要转化环节,也是航迹欺骗从实验室走向战场应用的关键限制条件。在进行航迹欺骗理论研究时,如何能够在满足动力学约束的条件下找到可行解,是难点问题。在实际应用中,严苛的运动约束问题可以通过增加施放航迹欺骗的无人机数量来弥补,采用无人机间接力、闪烁转发等多种形式来提高无人机飞行区域和延时转发策略的灵活性,实现航迹欺骗效果。

## 4 应用前景和下一步研究方向

航迹欺骗作为一种干扰手段,配合战术使用可以起到诱敌、迷敌、扰敌的效果,主动设计意图、塑造态势,使我方掌握战术主动权,是一种对组网雷达的有效对抗方式。尤其在未来体系作战中,可充分发挥灵活机动、易于扩展运用的优势,与情报/监视/侦察和攻击任务联合遂行,形成作战任务一体化样式,进一步增强整体作战效能。围绕航迹欺骗的关键问题,下一步研究方向可从如下几个方面考虑:

(1) 如何开展一体化任务, 进行航迹欺骗与情报/监视/侦察等其他任务的联合优化, 减少施放航迹欺骗时对先验情报的依赖, 提升整体作战效能;

(2) 根据战术意图进行航迹欺骗样式设计, 使无人机作战运用不仅依靠规模优势, 更依靠“智谋”取胜, 具有更加灵活的协同策略;

(3) 针对不同体制、不同类型的组网雷达, 例如车载、舰载或机载等机动目标, 或相控阵雷达等新体制雷达的航迹欺骗方法。

在未来战争的体系对抗背景下, 协同作战体系通过作战节点的泛在分布和节点之间的深度协同, 通过协同探测实现对战场目标的精确全面探测, 通过虚假航迹欺骗迷惑干扰对手, 形成探测干扰一体化的新型作战模式。

## 5 结 论

在未来战争中, 作战意图的推断是赢得先机的关键。通过干扰敌方对我方的意图推断, 甚至设计出让敌方相信的假意图, 能够使我方在博弈中塑造态势, 取得先手, 从而在顶层设计和战略战术上掌握主动权。尤其是处在军事智能高速发展的时期, 制胜战场已不再是仅仅依靠规模取胜, 而是要像人一样具备智谋, 学会伪装自己, 诱骗敌人, 以“活”胜“僵”, 取得四两拨千斤的效果。运用无人机对敌方组网雷达进行航迹欺骗就是一种有效的对抗手段。

本文介绍了航迹欺骗的概念提出和技术发展, 梳理了目前航迹欺骗的国内外研究现状。从总体研究角度, 提炼了航迹欺骗的四个关键问题和技术难点, 分别是虚假航迹设计和生成, 由不确定性误差导致的估计问题, 延时转发策略和同源检验准则, 以及动力学约束问题。针对每个关键问题, 归纳了公开文献中的常用解决方法和存在的不足。最后围绕未来作战需求, 探讨了航迹欺骗的应用前景, 并结合目前研究进展和技术难点, 提出了航迹欺骗的未来可行研究方向。

## 参 考 文 献

- [1] 胡利平, 梁晓龙, 何吕龙, 等. 基于情景分析的航空集群决策规则库构建方法研究[J]. 航空学报, 2020, 41(S1): 1-15.  
HU L P, LIANG X L, HE L L, et al. Research on the construction method of aviation swarm decision rule base based on scenario analysis [J]. Acta Aeronautica et Astronautica Sinica, 2020, 41(S1): 1-15. (in Chinese)
- [2] 贾永楠, 田似营, 李擎. 无人机集群研究进展综述[J]. 航空学报, 2020, 41(S1): 1-12.  
JIA Y N, TIAN S Y, LI Q. The Development of unmanned aerial vehicle swarms[J]. Acta Aeronautica et Astronautica Sinica, 2020, 41(S1): 1-12. (in Chinese)
- [3] P. Scharre, Robotics on the Battlefield Part II - The Coming Swarm[R]. Center for a New American Security, 2014:1-68.
- [4] Department of Defense. Unmanned Systems Integrated Roadmap 2017-2042[R]. 2018.
- [5] 袁成. 外军无人机蜂群技术发展态势与应用前景[EB/OL]. 中国航空报, 2018. [http://ep.cannews.com.cn/publish/zghkb7/html/1483/node\\_054444.html](http://ep.cannews.com.cn/publish/zghkb7/html/1483/node_054444.html). China Aviation News, 2018.
- [6] United States Air Force. SUAS Flight Plan: 2016-2036[R]. 2016.
- [7] 赵彦杰. 无人机蜂群系统的国外现状与趋势[J]. 网信科技前沿, 2017, 4(21):1-4.  
ZHAO Y J. The current situation and trend of UAV colony system abroad[J]. Internet and information technology frontier, 2017, 4(21):1-4. (in Chinese)
- [8] 李圣衍, 胡东, 周宏宇, 等. 雷达组网的干扰技术研究浅谈[J]. 电子工程师, 2006, 32(11): 4-6.  
LI S Y, HU D, ZHOU H Y, et al. A preliminary study on jamming technologies of netted radar[J]. Electronic engineer, 2006, 32(11): 4-6. (in Chinese)
- [9] 张养瑞. 对雷达网的多机伴随式协同干扰技术研究[D]. 北京理工大学, 2015.  
ZHANG Y R. Research on Key Technologies of Cooperative ECM in Multi-syndrome Jammers for Countering Radar Net[D]. Beijing Institute of Technology, 2015. (in Chinese)
- [10] 向龙, 丁建江, 杨大志, 等. 压制干扰条件下雷达组网检测概率建模与仿真[J]. 火力与指挥控制, 2011(03): 96-98.  
XIANG L, DING J J, YANG D Z, et al. Modeling and Simulation on Detection Probability of Netted Radar In Suppression Jamming Environment[J]. Fire Control & Command Control, 2011(03): 96-98. (in Chinese)
- [11] 赵辉. 雷达组网信息融合及欺骗干扰技术研究[D]. 西安电子科技大学, 2014.  
ZHAO H. A Study of Netted Radar Information Fusion and Deception Jamming Technology Research[D]. Xidian University, 2014. (in Chinese)
- [12] 刘洁怡. 多站雷达系统抗欺骗式干扰方法研究[D]. 西安电子科技大学, 2018.  
LIU J Y. The Methods for Deception ECCM on Multiple-Radar System[D]. Xidian University, 2018. (in Chinese)
- [13] CLARK, B., and GUNZINGER, M. Winning The Airwaves-Regaining America's Dominance In The Electromagnetic Spectrum[R]. The Center for Strategic and Budgetary Assessments, 2017:1-68.
- [14] CLARK, B., GUNZINGER, M., and SLOMAN, J. Winning In The Gray Zone- Using Electromagnetic Warfare To Regain Escalation Dominance[R]. The Center for Strategic and Budgetary Assessments, 2017:1-84.
- [15] CLARK B, MCNAMARA WM, WALTON TA. Winning the Invisible War[R]. The Center for Strategic and Budgetary Assessments. 2019:1-64.

- [16] 李欢. 信息化大幕下的无人机集群作战[J]. 军事文摘, 2018, 5.  
LI H. UAV swarm operation in the information age[J]. Military digest. 2018, 5. (in Chinese)
- [17] 李欣, 王春阳. 航迹欺骗干扰及其对抗技术的研究现状与发展[J]. 控制与制导, 2013, 1(8):64-67.  
LI X, WANG C Y. Research status and development of phantom track deception jamming and Its Countermeasures[J]. Control and guidance, 2013, 1(8):64-67. (in Chinese)
- [18] 马亚涛. 对雷达网的欺骗干扰技术研究[D]. 西安电子科技大学, 2013.  
MA Y T. Research on deception jamming against the network system of radars[D]. Xidian University, 2013. (in Chinese)
- [19] 赵立志, 魏永峰. 欺骗性雷达干扰实现方法分析[J]. 舰船电子对抗, 2013, 36(2): 11-13.  
ZHAO L Z, WEI Y F. Analysis of Implementation Method of Deception Jamming to Radars[J]. Shipboard Electronic Countermeasure, 2013, 36(2): 11-13. (in Chinese)
- [20] 倪建春, 王宝. 有源欺骗干扰及雷达反对抗策略研究[J]. 舰船电子对抗, 2011, 34(3): 5-8.  
NI J C, WANG B. Research into The Active Deception Jamming and Radar Counter-countermeasure[J]. Shipboard Electronic Countermeasure, 2011, 34(3): 5-8. (in Chinese)
- [21] PACHTER M, CHANDLER PR, LARSON RA, PURVIS KB. Concepts for Generating Coherent Radar Phantom Tracks Using Cooperating Vehicles[C]. AIAA Guidance, Navigation, and Control Conference and Exhibit. 2004:1-14.
- [22] PURVIS KB, ASTROM KJ, KHAMMASH M. Estimating Radar Positions Using Cooperative Unmanned Air Vehicle Teams[C]. 2005 American Control Conference. 2005:3512-3517.
- [23] PURVIS KB, CHANDLER PR, PACHTER M. Feasible Flight Paths for Cooperative Generation of a Phantom Radar Track[J]. Journal of Guidance, Control, and Dynamics. 2006, 29(3):653-661.
- [24] PURVIS KB, CHANDLER PR. A Review of Recent Algorithms and a New and Improved Cooperative Control Design for Generating a Phantom Track[C]. Proceedings of the 2007 American Control Conference. 2007: 3252-3258.
- [25] PURVIS KB, STROM KJA, KHAMMASH M. Online Control Strategies for Highly Coupled Cooperative UAVs[C]. Proceedings of the 2007 American Control Conference. 2007:3961-3966.
- [26] PURVIS KB, ASTROM KJ, KHAMMASH M. Estimation and Optimal Configurations for Localization Using Cooperative UAVs[J]. IEEE Transactions on Control Systems Technology. 2008, 16(5):947-958.
- [27] SHIMA T, CHANDLER P, PACHTER M. Decentralized estimation for cooperative phantom track generation. 2005:339-50.
- [28] RATNOO A, SHIMA T. Formation-Flying Guidance for Cooperative Radar Deception[J]. Journal of Guidance, Control, and Dynamics. 2012;35(6):1730-1739.
- [29] XU Y, Basset G. Virtual motion camouflage based phantom track generation through cooperative electronic combat air vehicles[C]. American Control Conference (ACC). 2010:5656-5661.
- [30] MAITHRIPALA DHA, JAYASURIYA S. Radar Deception through Phantom Track Generation[C]. American Control Conference. 2005.
- [31] MAITHRIPALA DHA, JAYASURIYA S. Phantom Track Generation in 3D through Cooperative Control of Multiple ECAVs Based on Geometry[C]. First International Conference on Industrial and Information Systems. 2006:255-260.
- [32] MAITHRIPALA DHA, JAYASURIYA S. Feasibility considerations in formation control: Phantom track generation through multi-UAV collaboration[C]. 2008 47th IEEE Conference on Decision and Control. 2008:3959-3964.
- [33] DHANANJAY N., KUDUVALLI, A., and GHOSE, D. Realistic Coherent Phantom Track Generation by a Group of Electronic Combat Aerial Vehicles[C]. American Control Conference (ACC). 2013.
- [34] HAJIEGHRARY H, JAYASURIYA S. Guaranteed Consensus in Radar Deception With a Phantom Track[C]. Proceedings of the ASME 2013 Dynamic Systems and Control Conference. 2013:1-7.
- [35] DHANANJAY N, GHOSE D, KUDUVALLI A. Generation of a Class of Proportional Navigation Guided Interceptor Phantom Tracks[J]. Journal of Guidance, Control, and Dynamics. 2015,38(11):2206-2215.
- [36] Lee I-H, Bang H. Optimal phantom track generation for multiple electronic combat air vehicles[C]. International Conference on Control, Automation and Systems. 2008:29-33.
- [37] IL-HYOUNG-LEE, Bang H. Phantom Track Generation Using Predictive Control Concept[C]. 11th International Conference on Control, Automation and Systems. 2011:291-293.
- [38] LEE I-H, Bang H. A cooperative line-of-sight guidance law for a three-dimensional phantom track generation using unmanned aerial vehicles[J]. Proceedings of the Institution of Mechanical Engineers, Part G: Journal of Aerospace Engineering. 2012,227(6):897-915.
- [39] 马亚涛, 赵国庆, 徐晨. 现有技术条件下对组网雷达的航迹欺骗[J]. 电子信息对抗技术, 2013, 28(2): 34-37.  
MA Y T, ZHAO G Q, XU C. Research on Track Deception Technology Against the Radars Network System[J]. Electronic Information Warfare Technology, 2013, 28(2): 34-37. (in Chinese)
- [40] 李修和. 基于空地一体的雷达组网干扰技术研究[J]. 航天电子对抗, 2013, 29(4):48-51.  
LI X H. Research on technique radar netted jamming based on integration with air and land[J]. Aerospace Electronic Warfare, 2013, 29(4):48-51. (in Chinese)
- [41] 李小波, 孙琳, 周青松, 等. 多机协同的组网雷达欺骗干扰航迹优化[J]. 现代防御技术, 2016, 44(6): 43-49.  
LI X B, SUN L, ZHOU Q S, et al. Strategy for Track Deception Jamming Against Radar Network Using Cooperative Autonomous Vehicle Teams[J]. Defense Technology, 2016, 44(6): 43-49. (in Chinese)
- [42] 龚旻, 刁晓静, 林涛. 低截获概率雷达转发式欺骗干扰技术研究[J]. 航天电子对抗, 2011, 27(6):31-33.  
GONG M, DIAO X J, LIN T. Research on repeater deception jamming technique on LPI radar[J]. Aerospace Electronic Warfare, 2011, 27(6):31-33. (in Chinese)
- [43] 罗金亮. 双基地雷达航迹欺骗干扰方法研究[J]. 火控雷达技术, 2012, 41(3):6-9.  
LUO J L. Research on Track Deception Jamming against



- Bistatic Radar[J]. Fire Control Radar Technology, 2012, 41(3):6-9. (in Chinese)
- [44] 张国兵, 郎荣玲. 基于半实物仿真系统的多假目标航迹欺骗研究[J]. 电子设计工程, 2012, 20(12):1-4.  
ZHANG G B, LANG R L. Multi-range-false-target deception research based on hardware-in-the-loop simulation system[J]. Electronic Design Engineering, 2012, 20(12):1-4. (in Chinese)
- [45] 杨忠, 王国宏, 孙殿星. 雷达网航迹欺骗干扰协同规划技术[J]. 指挥控制与仿真, 2015, 37(6):45-49.  
YANG Z, WANG G H, SUN D X. Collaborative Programming Technic of Radar Network in Presence of Phantom Track Deception[J]. Command Control & Simulation, 2015, 37(6):45-49. (in Chinese)
- [46] 周续力. 对搜索警戒雷达的多目标航迹欺骗[J]. 电子信息对抗技术, 2007, 22:43-45.  
ZHOU X L. Multiple-Target Track Deception Jamming Against Surveillance and Warning Radar[J]. Electronic Information Warfare Technology, 2007, 22:43-45. (in Chinese)
- [47] 高彬, 毛士艺, 孙进平. 基于 RGPO 的编队 ECAVs 协同航迹欺骗[J]. 北京航空航天大学学报, 2011, 37(11):1343-1346.  
GAO B, MAO S Y, SUN J P. Cooperative generation of phantom radar track using a team of ECAVs based on RGPO[J]. Journal of Beijing University of Aeronautics and Astronautics, 2011, 37(11):1343-1346. (in Chinese)
- [48] 朱宇, 罗景青, 田玮. 对组网雷达的多假目标欺骗干扰技术[J]. 电光与控制, 2013, 20(9):93-98.  
ZHU Y, LUO J Q, TIAN W. Research on Multi-False-Target Jamming Against Netted Radar[J]. Electronics Optics & Control, 2013, 20(9):93-98. (in Chinese)
- [49] 郭淑芬, 余国文, 熊鑫, 等. 基于无人机协同的航迹欺骗干扰方法研究[J]. 空军预警学院学报, 2018, 32(1):44-54.  
GUO S F, YU G W, XIONG X, et al. Research on method of track deception jamming based on cooperative control of UAVs[J]. Journal of Air Force Early Warning Academy, 2018, 32(1):44-54. (in Chinese)
- [50] 王国宏, 杨忠, 吴健平. 雷达站站址误差对多机协同航迹欺骗干扰的影响分析[J]. 海军航空工程学院学报, 2015, 30(6):501-510.  
WANG G H, YANG Z, WU J P. Influence Analysis of Radar Location Error on Multi-Aircraft Cooperative Track Deception[J]. Journal of Naval Aeronautical and Astronautical University, 2015, 30(6):501-510. (in Chinese)
- [51] 赵珊珊, 张林让, 李强, 等. 分布式多站雷达转发式欺骗干扰研究[J]. 电子与信息学报, 2017, 39(1):138-143.  
ZHAO S S, ZHANG L R, LI Q, et al. Research on Repeater Jamming Against Distributed Multiple-radar System[J]. Journal of Electronics & Information Technology, 2017, 39(1):138-143. (in Chinese)
- [52] 柳向, 李东生. 对分布式组网雷达的航迹欺骗偏差补偿技术[J]. 系统工程与电子技术, 2018, 40(6):1255-1264.  
LIU X, LI D S. Deviation compensation for phantom tracks jamming against distributed radar network[J]. Systems Engineering and Electronic, 2018, 40(6):1255-1264. (in Chinese)
- [53] Liu X, Li D. A Three-Dimensional Phantom Track Generation for Radar Network Deception [J]. IEEE Access, 2019, 7(1): 27288-27301.
- [54] 范振宇, 王磊, 陈越, 等. 组网雷达航迹欺骗技术研究[J]. 中国电子科学研究院学报, 2010, 5(2): 179-186.  
FAN Z Y, WANG L, CHEN Y, et al. A Technique of Track Deception against Netted Radars[J]. Journal of CAEIT, 2010, 5(2): 179-186. (in Chinese)
- [55] 李飞, 周中良, 苟新禹, 等. 基于多机协同航迹欺骗的组网雷达突防技术[J]. 系统工程与电子技术, 2013, 35(11):2309-2313.  
LI F, ZHOU Z L, GOU X Y, et al. Technology for penetrating radar net based on multiple combat air vehicles cooperation track deception[J]. Systems Engineering and Electronics, 2013, 35(11):2309-2313. (in Chinese)
- [56] 李森, 李彦志, 司瑾, 等. 一种警戒雷达航迹干扰方法及其仿真研究[J]. 舰船电子对抗, 2011, 34(5):19-23.  
LI S, LI Y Z, SI J, et al. A Jamming Method to Surveillance Radar Track and Its Simulation Analysis[J]. Shipboard Electronic Countermeasure, 2011, 34(5):19-23. (in Chinese)
- [57] 原伟, 束坤, 高晨. 对机载预警 PD 雷达的航迹欺骗干扰技术研究[J]. 舰船电子对抗, 2018, 41(4):6-14.  
YUAN W, SHU K, GAO C. Research into Track Deception Jamming Technology of Airborne Early Warning PD Radar[J]. Shipboard Electronic Countermeasure, 2018, 41(4):6-14. (in Chinese)
- [58] 黄勇, 丁宸聪. 针对预警机雷达的机载航迹假目标干扰技术[J]. 现代防御技术, 2015, 43(3): 15-19.  
HUANG Y, DING C C. Track Deception Technology Against Warning Aircraft Radar Based on Airborne Mode[J]. Modern Defense Technology, 2015, 43(3): 15-19. (in Chinese)
- [59] 赵艳丽, 王雪松, 王国玉, 等. 多假目标欺骗干扰下组网雷达跟踪技术[J]. 电子学报, 2007, 35(3):454-458.  
ZHAO Y L, WANG X S, WANG G Y, et al. Tracking Technique for Radar Network in the Presence of Multi-Range-False-Target Deception Jamming[J]. ACTA ELECTRONICA SINICA, 2007, 35(3):454-458. (in Chinese)
- [60] 赵艳丽, 陈永光, 蒙洁, 等. 分布式组网雷达抗多假目标欺骗干扰处理方法[J]. 电光与控制, 2011, 18(3):25-30.  
ZHAO Y L, CHEN Y G, MENG J, et al. A Data Processing Method against Multi-False-Target Deception Jamming for Distributed Radar Network[J]. Electronics Optics & Control, 2011, 18(3):25-30. (in Chinese)
- [61] 李迎春, 王国宏, 孙殿星, 等. 雷达抗自卫转发式航迹假目标欺骗干扰技术[J]. 系统工程与电子技术, 2015, 37(6):1242-1248.  
LI Y C, WANG G H, SUN D X, et al. Technique against Self-Protection Repeating Track False-Target Deceptive Jamming for Radar[J]. Systems Engineering and Electronics, 2015, 37(6):1242-1248. (in Chinese)
- [62] 孙殿星, 王国宏, 李迎春, 等. 距离多假目标干扰下低可观测目标跟踪处理[J]. 电子学报, 2016, 44(4):827-837.  
SUN D X, WANG G H, LI Y C, et al. Low Observable Target Tracking Processing in the Presence of Multi-Range-False-Target Jamming[J]. ACTA ELECTRONICA SINICA, 2016, 44(4):827-837. (in Chinese)
- [63] MEARS, M.J., and AKELLA, M.R. Deception of radar systems using cooperatively controlled unmanned air

- vehicles[C]. IEEE Proceedings of the networking, 2005: 332-335.
- [64] 王国宏, 吉喆. 基于多重判别的雷达网距离向多干扰目标鉴别[J]. 系统工程与电子技术, 2017,39(1):40-48.
- WANG G H, JI Z. Multi-range-false-target jamming for radar network based on multiple discriminations[J]. Systems Engineering and Electronic, 2017,39(1):40-48. (in Chinese)

## Overview on Phantom Track Deception against Radar Network Using UAVs

BAI Peng<sup>1,2</sup>, WANG Yubing<sup>1,\*</sup>, LIANG Xiaolong<sup>1</sup>, ZHANG Jiaqiang<sup>1,2</sup>, WANG Weijia<sup>3</sup>

1. Air Traffic Control and Navigation College, Air Force Engineering University, Xi'an 710051, China

2. National Key Laboratory of Air Traffic Collision Prevention, Air Force Engineering University, Xi'an 710051, China

3. Military Academy of Sciences, Institute of Systems Engineering, Beijing 100101, China

**Abstract:** In the future war, the demand for system operation is not only to "win with quantity" by scale, but also to have tactical wisdom to "win by flexibility". Only by interfering with the enemy's inference of our intention, or even designing the false intention to confuse the enemy's battlefield awareness, can we shape the situation in the game between the two sides, get the first hand, and master the initiative from the top-level design and strategic tactics. Using UAV swarm to cheat the enemy's network radars is an effective countermeasure. It can not only detect the enemy, but also consume the computing resources of the enemy's network radars, and interfere with the enemy's intention inference to our target, so as to improve the perception ability and survival ability of our own state. Firstly, the concept of phantom track deception is introduced, and the current progress of phantom track deception is summarized. Then, this paper extracts the key problems and technical difficulties according to the characteristics of phantom track deception jamming, which are phantom design and generation, the estimation problem caused by uncertain error, time delay strategy and same source testing rule, and dynamic constraints, respectively. Finally, the application prospect and the future research direction of phantom track deception are given.

**Keywords:** phantom track deception; UAV; radar network; intention inference; system operation