威胁环境下多无人机协同控制

符小卫　高晓光　著

科学出版社

威胁联网环境下多无人机协同控制

符小卫　高晓光　著

科学出版社

北京

内 容 简 介

无人机越来越多地应用于各种各样的军事任务中。在执行任务时，无人机面临着越来越复杂的威胁环境。威胁联网就是无人机所要面对的一种典型环境。本书系统介绍威胁联网对无人机生存率和无人机执行任务的影响，并深入分析威胁联网概念，建立准确可靠的威胁联网数学模型，设计威胁联网下的基于多步寻优搜索的无人机突防航迹在线规划方法，研究威胁联网下多无人机协同突防与攻击及协同欺骗干扰的一些控制方法。本书紧紧围绕威胁联网问题，深入分析相关概念，建立相关模型，并设计相关方法，为威胁联网下的多无人机协同控制提出了较为系统的解决方案。

本书可供无人机协同控制相关科研工作者和工程技术人员参考，也可作为高等院校无人机相关专业研究生的教学参考书。

图书在版编目(CIP)数据

威胁联网环境下多无人机协同控制/符小卫，高晓光著. —北京：科学出版社，2018.3

ISBN 978-7-03-056882-3

Ⅰ.①威… Ⅱ.①符… ②高… Ⅲ.①无人驾驶飞机-自动飞行控制-研究 Ⅳ.①V279

中国版本图书馆 CIP 数据核字 (2018) 第 048356 号

责任编辑：李 萍 张瑞涛 / 责任校对：郭瑞芝
责任印制：张 伟 / 封面设计：陈 敬

科学出版社出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

北京中石油彩色印刷有限责任公司 印刷
科学出版社发行 各地新华书店经销
*
2018 年 3 月第 一 版 开本：720×1000 B5
2018 年 3 月第一次印刷 印张：9 1/2
字数：200 000

定价：80.00 元

(如有印装质量问题，我社负责调换)

前　言

近十几年来，无人机越来越多地应用于各种各样的军事任务中。在无人机执行任务过程中，防空系统是无人机需要面临的重要威胁。随着信息化理论和网络化作战理论的发展，现代防空体系已实现网络互联，使作战区域内的众多威胁单元能够信息共享和互联互通，形成具有一定信息融合能力、综合指挥控制能力和互操作能力的一体化威胁网络，我们称之为威胁联网。威胁联网的存在基于以下两点，一方面对于无人机协同完成作战任务来说，由于防空系统已不再是孤立的节点，其对无人机的杀伤力不再是多个威胁单元的简单叠加，传统的多无人机协同控制方法已经难以保证威胁联网下无人机的生存率要求；另一方面，由于威胁之间相互有信息交流和共享，传统的多无人机协同对抗联网威胁的软/硬杀伤模式已难以保证无人机作战任务的有效完成。因此，威胁联网从多个方面对多无人机协同控制提出了新的挑战。威胁联网下的多无人机协同运用成为了研究多无人机协同控制的一个重要发展方向。

本书通过分析威胁联网对无人机生存率和无人机执行任务的影响，深入研究了威胁联网的概念，在建立威胁联网数学模型的基础上，设计了威胁联网下的无人机突防航迹在线规划方法、多无人机协同攻击联网目标方法、多无人机协同欺骗干扰控制方法，为威胁联网下的多无人机协同控制提出了较为系统的解决方案。

本书由西北工业大学符小卫副教授与高晓光教授完成，是作者多年以来从事无人机任务规划与指挥控制研究工作的部分总结。书中内容也包含了团队多名博士和硕士研究生的工作，对于他们所做出的贡献表示感谢。

由于作者水平有限，书中难免存在不足之处，敬请同行专家和读者批评指正。

作　者

2017 年 8 月

目　　录

第1章 绪 论

本章主要阐明威胁联网的研究背景，说明无人机在威胁联网下的作战应用研究的意义及目前国内外研究现状。

1.1 研究背景及意义

1.1.1 研究背景

通信网络技术与计算机技术的发展，促使现代战争的作战方式逐步由平台作战扩展到一体化和网络化作战，敌我对抗由单元对抗向体系对抗发展。以网络为中心的作战模式成为信息化战争的主要特点。

随着信息化理论和空天一体作战理论的发展，现代防空体系早已实现网络互联，防空网已经基本具备了信息共享、探测信息互联互通和网络化火力打击的一体化指挥控制能力。对于无人机来说，防空类地面威胁不再是孤立的节点，地面威胁对无人机的杀伤力不再是多个威胁单元的简单叠加。在信息化条件下，地面防空威胁单元通过有线和无线网络组网，使作战区域内的众多威胁单元形成具有一定信息融合能力、综合指挥能力和互操作能力的一体化威胁网络，本书称之为威胁联网。

在现代战争中无人机往往充当排头兵的角色，需要在有人飞机等我方有生力量进入前，对敌方防空阵地进行渗透和打击压制，摧毁敌方重要指挥中枢，为战争赢得先机。无人机由于自身独特的优势，可以充分利用地形遮蔽等有利条件进行秘密突防，或者携带精确制导导弹或反辐射导弹隐蔽突防到敌方纵深区域，摧毁敌防空系统关键节点，从而为有人飞机任务的安全执行扫清障碍。

在现行技术条件下防空单元不再独立作战，无人机航迹规划必须充分考虑威胁联网对突防的影响。由于威胁单元的联网大大增加了敌方防御力量对无人机的对抗能力，传统的航迹规划方法难以满足当前需求，这就需要对威胁联网下的突防航迹规划进行深入研究。

1.1.2　研究意义

现代战争中，为了减少己方有人战斗机的损伤，世界上各先进国家纷纷采用无人机来进行先期防空压制和对敌方的防空系统进行第一波打击，为有人飞机的进入清除大部分障碍。在战斗初期，由于敌方地面存在完整的防空体系，且通过计算机网络技术将各个防空单元连接在一起，形成防空网，对无人机形成全方位探测和打击。

此时，传统无人机航迹规划方法中的威胁建模方法不再适用。无人机必须充分考虑到威胁的联网特性，建立符合威胁联网实际的威胁模型，才能寻找到最优的隐蔽突防路径。对威胁联网下的突防航迹规划的研究是基于现代战争发展新特点所展开的，是比较符合实际的。对威胁联网的特性，如威胁联网的“四抗”特性 (抗隐身特性、抗低空突防特性、抗毁/反辐射导弹特性和抗干扰特性)、威胁联网的指挥控制一体化特性、威胁联网的协同打击特性等的研究，能够改进传统航迹规划算法的威胁建模方法，使航迹规划中的威胁评估更加真实可信，从而使无人机更好地规避威胁，提高生存概率。同时，可结合低空突防的作战要求，设计满足威胁联网作战环境的实时航迹规划算法，以提高无人机在威胁联网环境下的突发事件应对能力。

1.2　国内外研究现状

1.2.1　无人机的发展现状

无人机是一种有动力、可控制、能携带多种任务设备、执行多种任务并能重复使用的无人驾驶航空器 [1]。与有人战斗机相比，无人机具有低成本、高机动、高隐身等一系列特点，在高危险环境执行任务时，能够体现出更大的优势。在军事领域，无人机获得广泛应用，其遂行的任务从单纯的空中侦察扩展到情报监视、导弹攻击、充当诱饵、电子战等，在五维一体化的战场上显示出了重要的作用 [2]。

随着科学技术的不断发展，现代战争向着“海、地、空、天、电”一体化方向发展，新的军事理论、军事技术与武器平台不断涌现，在信息化与协同作战技术中，无人机正成为其中翘楚，并得到飞速发展。无人机系统具有雷达反射面积小、机动灵活、自主能力强、可重回收利用等优点，在近年来发生的几场局部战争中展现出

了独特的优势，其军事地位不断提高，由执行辅助任务的角色转而成为主要作战力量。可以预见，在未来高度立体化、信息化和一体化的战场上，无人机将成为军事强国空中作战的主要武器之一。

1.2.2 威胁联网研究现状

威胁联网的概念，最早是由国外的学者 Szczerba 提出 [3]，并通过建立威胁源的相互支援信息表 (threat netting cost look-up, TNCLU) 来对威胁联网进行建模。在 TNCLU 列表中，包含了威胁类型、威胁传感器和武器作用距离范围、威胁通信能力、天气条件、任务类型和任务时间等信息。这种方法的威胁代价列表的确定较难，威胁信息的量化比较复杂，容易偏离实际。

近几年来，国内陆续有学者开始研究威胁联网下的无人机路径规划，并取得了一定成果。但从目前来看，以往学者对威胁联网研究的方法大多具有一定的局限性。例如，文献 [4] 将威胁类型作为主要属性，建立了相应的威胁支援信息表，并使用 A* 搜索算法来研究威胁联网下的无人机路径规划。采用威胁源类型为研究属性，可以很好地解决威胁联网状态下各个威胁之间通信的建模，但是由于相互支援信息表是根据实际经验离线建立的，不便于在线迅速调整，从而不能够及时、准确反映瞬息万变的战场环境对威胁联网代价的影响。

文献 [5] 将地图划分成网格，然后根据先验经验计算出网格平均威胁等级构建威胁网，并用蚁群算法进行航迹仿真。在穿越某一个或多个威胁区域后，通过更新威胁概率网格进行航迹重规划，一定程度上反映威胁联网的实时性，但其威胁变化仍然不是实时的，且对威胁联网的整体特性反映不全面。

文献 [6] 对威胁联网的体系结构进行了研究，提出距离函数的连接度概念和目标指示概念，并以雷达组网探测公式作为威胁代价函数，对威胁联网的评估有一定的改进。但是，真正意义上的威胁联网不仅仅是雷达的组网，还包括威胁单元间火力打击的网络化和一体化。

整体而言，对威胁联网的理论研究相对较少。现有文献对威胁联网的研究均停留在研究威胁联网对威胁范围和威胁代价大小的影响上，而没有对威胁联网作战效能会根据目标状态的不同而产生实时变化这一现实进行研究，即没有对威胁联网如何增强威胁作战效能的机制进行研究。

威胁联网的初期研究多是概念化的，没有战场实例可供参考。如今，随着网络

技术和信息技术的发展，地面防空力量的联网作战已经开始应用于现实作战。例如俄罗斯“铠甲”防空系统就实现了不同分布层级的系统互联和对目标的多次拦截。当今一些先进国家的导弹防御系统已成为现实版的威胁联网系统。

从实际应用角度来说，可以将威胁联网看作是多传感器组网探测和防空火力协同打击的优化组合。如今，无人机的攻击手段增多，已经可以应用到电子对抗领域。因此，针对复杂的电子对抗环境对威胁联网的“四抗”特性进行分析就越加显得重要。

1.2.3　多无人机协同控制研究现状

近年来，国外开展了大量面向不同任务的多无人机协同控制和任务规划的研究项目。其中，美国在多无人机协同控制领域内的研究始终占据最前沿，在军事和民用研究领域都取得了大量研究成果，最负盛名的是自治编队混合主动控制项目[7,8]。该项目是由美国国防部高级研究计划局领导的，对多无人机协同控制多项关键技术进行了研究，包括分布式控制结构、编队飞行控制算法、仿真模拟技术等。该项目旨在通过新的有效手段提高无人机的自主控制、智能控制和协同控制能力，来减少地面操作人员对无人机的操作控制。

除美国外，其他西方发达国家也纷纷加大了对多无人机任务规划与协同控制领域的投入。英国奎奈蒂克公司为了实现多无人机自组织作战，从智能体行为协调入手展开研究，研发了相关推理软件，并进行了多无人机协同攻击地面目标的仿真验证研究[9,10]；澳大利亚悉尼大学的自主系统高级研究中心研究了多无人机的实际应用问题，通过小型无人机平台开展协同目标跟踪的技术验证，并进一步研究了多机协同定位、分布式滤波和目标跟踪的问题[11]。

美国空军理工学院的 Dustin J. Nowak 研究了在对抗环境下无人机集群的自组织控制，采用部分可观马尔可夫过程建立了集群控制模型，在仿真环境 800km×800km 范围内，进行了无人机集群编队飞行和目标攻击的试验研究，集群无人机数量为 10~30 架，无人机和目标的数量比为 10:3[12]。

相比较而言，国内在多无人机协同控制领域的研究起步较晚，但经过相关研究人员的努力，也取得了一定的理论研究成果。

苏菲[13]在其博士论文中以多无人机协同执行对地打击，进而实现压制敌防空系统的任务为背景研究相应的任务规划方法，分析了多无人机协同执行任务和

有人机引导多无人机协同执行任务两种模式下的作战全过程，建立了无人作战飞机平台模型、装备载荷模型和威胁模型，分析并设计了分布式控制体系结构。同时，研究了面向动态环境下多无人机协同对地打击的分布式在线协同航迹规划方法，提出了多无人机在线协同航迹规划算法和分布式任务协调局部优化算法。

张庆杰 [14] 在其博士论文中较为系统地研究了多智能体一致性理论，并以此为基础来设计多无人机协同控制算法。他在网络受限条件下，设计了多智能体实现平均一致性和鲁棒一致性的相关收敛条件，并进一步从数学上进行了理论证明。同时，基于多智能体一致性理论，设计了实现多无人机任务区集结的协同控制方法和多无人机协同目标观测的状态估计方法。

黄长强教授等 [15] 在 “无人作战飞行器编队协同攻击轨迹规划研究” 一文中研究了无人作战飞机编队对地攻击问题，在多种约束条件下建立单机的质点运动模型，根据任务的编队协同要素分析编队成员相对运动关系，将编队成员之间的安全距离代价和协同时间代价考虑在内设计了性能指标，进而建立了编队协同攻击最优控制模型。

北京航空航天大学高彬等 [16] 在 “基于 RGPO 的编队 ECAVs 协同航迹欺骗” 一文中利用配备有距离拖引技术的电子战飞行器 (electronic combat air vehicles, ECAVs)，对敌防空系统中的组网雷达实施电子干扰来实现假目标欺骗的目的。对于有着电子战能力的 ECAVs 在雷达组网下的协同作战策略进行了研究，分析研究了 ECAVs、雷达和假目标三者之间的耦合关系，并设计了基于动力约束的欺骗干扰航迹规划算法。

总之，面向不同任务的多无人机协同控制和任务规划方法都已有了很多成熟的算法，但是将其应用到威胁联网下的任务规划研究还比较少，而随着通信网络技术的发展以及网络中心战等新型作战理论的不断革新，对适宜威胁联网下的多无人机协同控制与任务规划方法的研究势在必行。

第 2 章　威胁联网与分析

本章对威胁联网的基本概念、基本原理和特性进行研究与分析。由单一防空威胁单元相互连接所形成的一体化威胁网络就称为威胁联网。威胁联网下的电磁对抗呈现一些新的特性，因此，本章对威胁联网的“四抗”特性进行了进一步的分析。

2.1　威胁联网的基本概念

2.1.1　基本概念

现代防空体系中，往往集成了多种类型的防空作战单元。在通信网络一体化技术的支撑下，不仅各个防空单元之间可以互联，而且不同防空单元内的传感器子系统和武器子系统也可以互操作。若以单一防空系统为威胁单元，则多个威胁单元互联互操作就组成一体化的威胁联网体系。威胁联网一般是指整个战场区域内各个主动威胁源 (防空作战单元) 之间通过信息交流与资源共享协同完成整个覆盖空域内的防空任务。也可以理解为，威胁单元之间通过通信链路连接，各自的制导雷达之间可以协同探测，且收集的目标信息可以共享，各自的火力打击武器可以在网络中心的指挥下协同展开拦截与攻击。

可以看出，威胁联网的技术基础就是雷达组网技术和网络化火控技术 [2]。威胁联网的传感器可以是不同频段、不同体制或不同类型的雷达，这些雷达系统在网络内形成与组网雷达类似的探测能力；而威胁联网的各类武器系统作为一体化网络资源，虽然分属于不同的威胁单元，但可以通过通信网络进行互操作。例如，在防空威胁单元的自身探测性能不足的情况下，制导武器可以通过其他威胁单元的制导雷达提供的目标信息对目标进行拦截。

通过统一的调度和协调，威胁联网具有了更好的探测性能和更强的杀伤力。这样的威胁联网对无人机的突防作战与航迹规划的影响也是巨大的。

2.1.2 基本组成

根据文献 [17] 对威胁联网的描述可知：威胁联网是多种类、多数量的防空单元在 “网络中心战”[18] 作战体系下的防空网络，是以无人机突防作战为视角所提出的概念。为了描述方便，威胁联网的基本组成单元可定义如下。

(1) 威胁单元 (threat-unit，TU) 实体：由防空网络指挥通信系统、雷达探测系统和多部导弹发射架所组成的，能够对信息进行收发处理和导弹拦截控制的一个系统集成。威胁单元的组成如图 2.1 所示。

图 2.1 威胁单元的组成

(2) 通信链路 (link，L)：建立两个威胁单元间通信连接的电磁线路。因为威胁网是一个无标度网络 [19]，所以通信链路为全双工通道。用 L_{ij} 表示网络中相邻两节点 i, j 间的通信链路。

(3) 信息路由 (routing，R)：$R_{m\to n}$ 信息从源节点 m 传输到目标节点 n 经过的所有链路组成的通信路径叫做信息路由。

威胁单元实体通过相互间的通信链路实现信息共享和协同控制，多个威胁单元组网形成威胁联网。

威胁联网根据不同的战场环境和作战任务需求如作战空域配合、威胁密度要求等来灵活布站，而威胁联网的拓扑连接与威胁联网的布站情况密切相关。同时，综合考虑威胁联网的抗干扰/打击能力，以及指挥通信效率，可选择星型、线型、环型或者混合型拓扑作为威胁联网的网络拓扑结构。

2.2 威胁联网基本框架结构

2.2.1 防空威胁联网部署结构

根据要地防空对雷达的部署层级 [20]，威胁联网部署结构可以根据保护目标的

重要程度等划分为多个层级。层级不同，威胁部署的密度、方向角范围、数量和网络拓扑都不相同。

图 2.2 所示为防空威胁内部武器区域配合范围，威胁联网内的防空单元如何部署，取决于战场环境、武器的作用范围、上级指挥部要求的火力密度等。防空部署体现的对抗性和众多约束条件，决定了对它的研究是一个综合多种因素、寻求最佳方案的过程。威胁部署要遵循两个原则：一是空域上各武器互相补充；二是重要位置需要加强防御，提高威胁密度。在确定各种威胁单元作用范围的情况下，可以采用图解试探的方法完成威胁单元作用域的空域衔接。

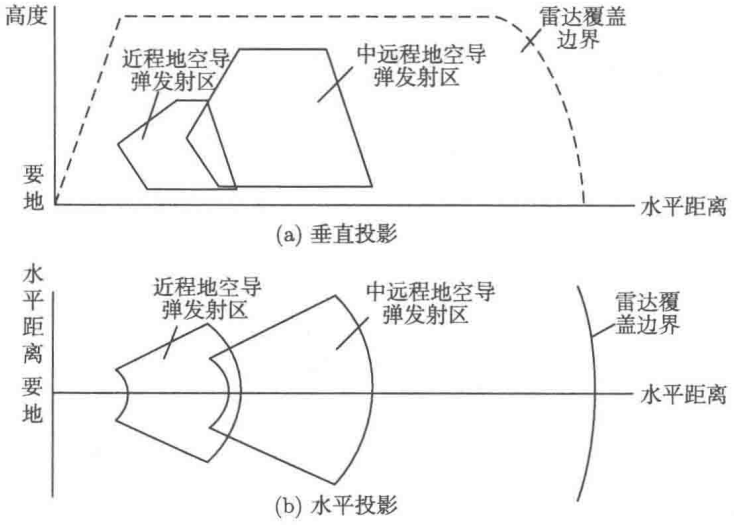

图 2.2　防空威胁内部武器区域配合范围示意图

从几何关系上可将威胁联网的配置方式分为环型配置、线型配置和区域混合型配置，如图 2.3 所示。

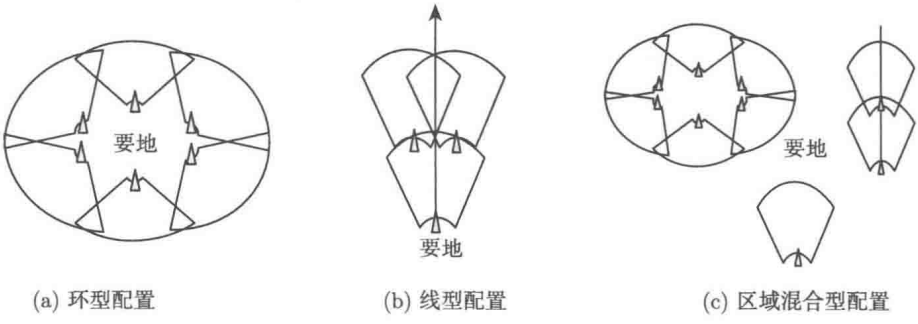

图 2.3　威胁联网三种基本配置方式示意图

当攻击目标的来袭方向不确定或者需要全方位对目标实行保护时，威胁联网的防护范围需要是全方位的，此时可以采用环型配置；当攻击目标来袭方向明确时，威胁联网只需要对一个方向进行防御，这时可采用线型配置。线型配置的优点是正面防御范围大、探测区域重叠范围广且抗干扰能力强。在广域范围内布站，一般采用区域混合型配置，将部署在防空区域内的各型威胁网 (采用线型配置或环型配置) 连接构成有机整体，形成以网络为中心的工作方式，使多个小型威胁网络可以互联互通，从而在作战区域内形成一个大型混合网络。区域混合型配置也是威胁联网最常用的配置方式。

2.2.2 威胁联网指挥控制体系结构

威胁联网的建立必须依托于作战体系的指挥控制结构，目前理论比较成熟的是基于平台中心战的集中式指挥控制结构和基于网络中心战的分布式指挥控制结构。

基于平台中心战的集中式指挥控制结构 [21](图 2.4) 是一种树状指挥结构，即层次化或分级集中管理的体系结构。这种结构的通信组织和指挥控制都比较简单，

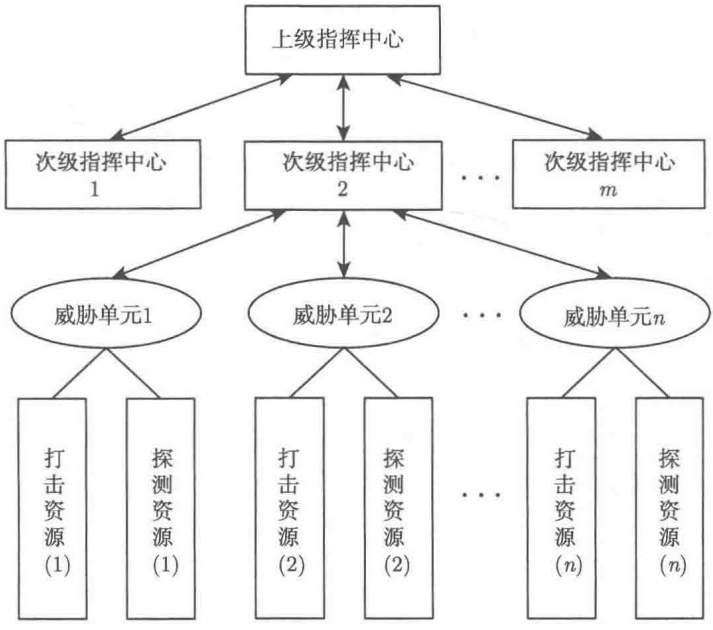

图 2.4 集中式指挥控制结构