

doi:10.1631/FITEE.1700032

题目：无人机网络中的安全连通性分析

摘要：无人机网络的独特特征包括高动态网络拓扑、高移动性以及野外无线环境可能使得无人机网络容易受到攻击和威胁。本文基于无人机行为、运动模式和无人机之间的信道特征，为无人机网络提出一种新颖的信任模型。该信任模型由直接信任、间接信任、信任集成和信任更新 4 部分组成。基于信任模型，提出一种无人机网络中安全链路的概念，该概念仅在两个无人机之间既有物理链路又有信任链路时存在。此外，利用两架无人机之间的物理连通概率和安全连通概率，分析无人机网络的连通性。通过随机几何方法，推导得到考虑和不考虑多普勒频偏情况下的物理连通概率和安全连通概率的解析表达式。仿真结果表明，与具有和不具有恶意攻击的物理连接概率相比，提出的信任模型可以保证无人机之间的安全通信和可靠连接，并在无人机网络面临恶意攻击和其他安全隐患时提高网络性能。

关键词：无人机网络；信任模型；安全连接；多普勒频移