卫星通信系统电子对抗方法研究

贺群

上海京济通信技术有限公司，上海 201800

摘要：当前信息化时代，卫星通讯系统广泛应用于军事指挥、导航定位、广播电视、远程通信等诸多领域，其战略地位举足轻重，然而随着电子技术的飞速发展，卫星通讯系统面临着日益严峻的电子对抗威胁，敌方可能利用各种电子干扰手段，试图破坏卫星通讯的正常运行，窃取或篡改传输信息，直接影响到国家主权、军事安全以及经济社会稳定。因此，深入研究卫星通讯系统电子对抗的方法，对于提升卫星通讯的抗干扰能力、确保信息传输的安全可靠，具有极其重要的现实价值。

关键词：电子对抗；卫星通信；安全

DOI:10.63887/jeti.2025.1.4.16

引言

卫星通讯系统能够实现远距离、大容量、高可靠性的信息传递，在复杂的电磁环境下，卫星通讯系统极易成为电子对抗的目标，不仅会使通信质量严重下降，甚至可能导致通信中断，引发军事指挥失灵、经济信息泄露等严重后果。本文主要阐述了卫星通信系统面临的电子对抗威胁类型，如电子欺骗、电气干扰、电子窃听等，同时从冗余与备份设计、加密与认证技术、主动防御与反制等方面提出了相应的应用路径，进而为保障军事及民用通信安全提供有力支撑。

1 卫星通信系统面临的电子对抗威胁类型

1.1 电子窃听

卫星通讯系统中，电子窃听主要变现在破解加密通信、入侵通信链路等方面，一些敌方使用高性能的卫星信号接收天线、解调器等专业设备，对卫星通讯信号进行直接截获。这些设备具备高灵敏度和宽频带接收能力，能够覆盖卫星通讯常用的频段，从而获取卫星传输的语音、数据、图像等信息，还可以将监听设备部署在与目标卫星相同的轨道或相近轨道上，实现对卫星通讯信号的近距离截获，该方式可以克服地球曲率和信号传输损耗等问题，提高截获的准确性和效率。若卫星通讯系统采用的加密算法不够强大或密钥管理存在漏洞，敌方就有可能通过密码分析技术来破解加密通信，通过收集大量的加密卫星信号样本，运用数学分析和计算方法，尝试推导出加密密钥或破解加密算法，敌方还可以通过侧信道攻击的方式来获取加密密钥。侵通信链路方面，黑客可以通过入侵卫星通讯的地面控制站、网络管理中心等关键节点，获取对卫星通讯链路的控制权，进而实现对通信内容的窃听和篡改，系统漏洞方面敌方可以利用操作系统漏洞、通信协议栈漏洞、应用程序漏洞等，获取对卫星通讯系统的非法访问权限，进而实现电子窃听[1]。

1.2 电子干扰

电子干扰主要是指通过发射特定频率、功率和调制方式的电磁信号，扰乱或破坏卫星通信链路的正常运行，其表现形式包括信号遮蔽、信号扭曲等，其中信号遮蔽使通过发射强干扰信号，覆盖卫星通信频段，使合法信号无法被接收或解调，瞄准式干扰是针对特定卫星或通信链路，精准施加干扰，效率高且难以防御。电子干扰信号通常针对卫星通信的上行链路或下行链路的频段，可能覆盖整个通信频段或针对特定信道，干扰源可能来自地面、空中或太空，具备方向性天线以集中能量，干扰范围可能覆盖单个地面站、区域或全球，而且干扰可能是持续性的突发性的，尤其随着技术的不断发展，干扰信号可能采用噪声调制、扫频干扰、脉冲干扰或智能调制方式，借助现代干扰技术可动态调整频率、带宽和功率，进而适应卫星通

信的抗干扰措施。

1.3 电子欺骗

电子欺骗是指通过技术手段模拟、伪造或干扰卫星通讯信号，使接收方无法正确识别真实信号，从而达到误导、干扰或破坏通信的目的，其可以伪造与卫星信号相似的虚假信号，冒充合法卫星或地面站，发送错误信息或指令，如模拟导航卫星信号，误导接收设备的定位或导航功能，还可以通过发射与卫星信号频率相同或相近的干扰信号，掩盖或扰乱真实信号，如使用噪声干扰或欺骗性信号覆盖真实信号，使接收方无法正常解码。此外，电子欺骗还包括截获并记录卫星信号，稍后重新播放，制造虚假通信或误导接收方，利用卫星通讯协议的漏洞，伪造或篡改数据包，干扰通信链路，针对导航卫星，通过发射虚假信号或干扰信号，误导接收设备的定位结果。电子欺骗通常不易被察觉，虚假信号与真实信号在频率、波形和协议上高度相似，攻击者可以利用合法信号的“掩护”进行欺骗，难以通过简单手段识别，而且电子欺骗往往针对特定卫星、频段或通信协议，利用其技术特点或漏洞实施攻击，电子欺骗手段可以动态调整，根据卫星通讯系统的变化实时适应，可能导致卫星通讯系统失灵、数据传输错误或卫星失控[2]。

2 卫星通信系统电子对抗方法的研究

2.1 加密与认证技术

卫星通信的链路层面，企业应对从地面站到卫星以及卫星之间转发的信号进行加密，可以采用先进的对称加密算法，对数据流进行实时加密，当数据在卫星链路上传输时，即使被敌方截获，由于没有正确的密钥，也无法解析出原始的通信内容，确保通信的保密性，同时为了应对可能的密钥破解风险，应建立动态密钥更新系统，根据通信场景、时间周期或者特定的触发条件，定期或不定期地更换加密密钥，可以通过安全的密钥分发渠道，将新的密钥分发给合法的通信节点，使得敌方难以通过长期监听和分析来获取有效的解密密钥。企业可以在卫星通信的终端设备之间实现端到端加密，将终端设备的身份认证与加密紧密结合，还应积极构建多层次的加密体系，还应考虑到卫星通信系统可能与其他通信系统进行交互，建立跨系统的加密兼容机制。认证技术应用中，企业在卫星通信系统中，应对每个卫星终端设备进行严格的身份认证，预先植入的设备标识，在设备接入卫星通信网络时进行认证，只有通过认证的设备才能接入卫星通信系统，防止非法设备接入网络，还应及时更新设备的身份认证信息，建立设备认证的备份和恢复机制，以应对设备丢失、损坏等突发情况，确保合法设备能够快速恢复通信权限。对于使用卫星通信服务的用户，企业应采用多因素认证方式，除了传统的用户名和密码认证外，结合生物特征识别、动态口令等多种认证手段，根据用户在卫星通信系统中的角色和职责，设置不同的认证权限和访问级别，在卫星通信链路建立阶段，对链路的两端进行双向认证，通信发起方和接收方通过交换认证信息，验证对方的身份和链路的合法性，通信链路建立后，持续对链路进行认证监测，并对链路中的数据传输进行完整性验证，通过添加消息认证码或者使用数字签名等技术，确保数据在传输过程中没有被篡改[3]。

2.2 干扰检测与定位技术

干扰检测技术应用中，企业应利用频谱分析仪等设备，对卫星通讯信号的频域特性进行监测，对比正常信号和实际接收信号的频谱特征，鸡儿呢检测到是否存在干扰以及干扰的大致频域位置，积极采用快速傅里叶变换等算法对接收的信号进行频域转换和分析，设置合适的频域分辨率和监测时间窗口，实时或近实时地检测频域上的干扰变化情况。企业应观察卫星通讯信号的时域波形特征，通过示波器等设备直接观察时域波形，或者利用数字信号处理技术对采集的时域信号进行分析，可检测到时域上的干扰迹象，还应分析信号的统计特性，通过与正常信号的统计特性进行对比和阈值判断，实现干扰检测，如当信号的方差突然增大超过一定阈值时，可能表示有干扰加入，影响了信号的稳定性。企业可以采用基于机器学习和人工智能的检测方法，先从大量的卫星通讯信号样本和已知干扰信号样本中提取特征，利用这些特征向量对机器学习模型进行训练，采用深度学习中的卷积神经网络或循环神经网络等架构对信号的原始数据直接进行

处理和学习，实际运行中，将实时采集的卫星通讯信号输入到训练好的机器学习模型中进行检测，模型会根据学习到的特征模式对输入信号进行分析和判断，输出是否存在干扰以及干扰类型的预测结果。

干扰定位技术应用中，企业应使用多个天线组成的天线阵列，来接收卫星通讯信号和干扰信号，测量不同天线单元接收到的信号的相位差或到达时间差等信息，利用天线阵列的几何关系和电磁波传播原理，计算出干扰信号的来波方向，通过多个不同方向的天线阵列组合或旋转天线阵列，进一步确定干扰信号在三维空间中的方位角和俯仰角，从而实现对干扰源的精确测向定位。企业还可以在不同的地理位置设置多个监测站，每个监测站都配备有测向设备，当卫星通讯系统受到干扰时，各监测站同时对干扰信号进行测向，获取干扰信号在各个监测站处的来波方向信息，然后根据各监测站的位置坐标和测向来波方向数据，利用三角定位原理或多站定位算法计算出干扰源的位置。基于时差技术应用，企业应在多个监测站点同步采集卫星通讯干扰信号，精确记录每个站点接收到干扰信号的时刻，通过测量这些时间差，结合各监测站点之间的位置关系和电磁波传播速度，利用 TDOA 定位算法计算出干扰源的位置，基于空域滤波技术中应利用自适应空域滤波器对接收的卫星通讯信号和干扰信号进行处理，使滤波器在空域上形成特定的滤波特性，从而抑制来自特定方向的干扰信号，不断调整滤波器权值并监测输出信号的质量，进而确定干扰信号的主要来向[4]。

2.3 冗余与备份设计

卫星通讯系统电子对抗中，冗余与备份设计中，企业在构建卫星通信星座时，应规划一定数量的备份卫星，在低轨卫星通信系统中，根据业务需求和服务区域，设计冗余的卫星数量，对于关键通信任务，采用热备份卫星，配置冷备份卫星，作为长期储备，在需要时经过快速激活和调试后加入通信网络。卫星通信天线是易受攻击的关键部件，采用多副天线冗余设计，在一颗卫星上安装多副相同规格的通信天线，当一副天线受到干扰或损坏时，其他天线可自动切换承担通信任务，保证信号的收发，还应对卫星上的通信转发器、放大器等核心通信载荷进行冗余配置，采用双套或多套通信载荷设备，卫星电源设计冗余的电源模块和储能装置，使用多个太阳能电池板和蓄电池组，通过冗余切换电路连接。软件层面，卫星通信系统具备多种通信协议，支持传统的频分复用、时分复用协议以及新兴的码分多址、正交频分复用等协议，开发智能的协议自适应调整软件，自动选择最优的通信协议和参数设置，在卫星通信地面站和卫星上均设置数据备份机制，采用分布式数据处理软件架构，将通信数据的处理任务分散到多个处理节点。

2.4 主动防御与反制

企业应利用先进的频谱分析仪等设备，对卫星通信频段进行全方位、不间断的扫描，实时捕捉到空中的电磁信号，当监测到信号后，运用数字信号处理技术对信号的特征进行提取，识别信号的来源和用途，如对于采用特定编码方式的军事卫星通信信号，通过分析其编码序列，可以判断该信号是否属于己方或友方的通信系统，还是敌方的干扰信号，还可以根据信号强度的变化来判断干扰源的距离和功率大小。企业应基于提取的信号特征，建立信号数据库和识别算法，将监测到的信号与数据库中的正常通信信号模式进行对比，从而区分出正常通信信号、友好干扰信号和敌方干扰信号。主动干扰抑制与反干扰中，企业可以采用自适应滤波器来抑制干扰信号，卫星电视接收中，在面对相邻频道干扰或者同频干扰时，自适应滤波器可以根据接收到的信号和干扰的强度、频率等特性，动态地调整滤波器的通带和阻带，保证电视图像和声音的质量，卫星通信系统自身可以采用跳频和扩频技术来提高抗干扰能力，积极通过功率控制，合理调整卫星通信发射端的功率。欺骗式干扰与反制中，企业可以发射与卫星通信信号相似的假信号来欺骗敌方，在频率上与敌方卫星通信频率相同或相近，但在调制方式、编码内容等方面进行精心设计，使敌方接收设备误以为是正常通信信号而进行接收和处理，模拟敌方卫星指挥控制信号，向敌方卫星地面站发送虚假的指令信号，并加强信号认证和加密技术[5]。

结束语

综上所述，卫星通讯系统电子对抗是一场持续演进的技术博弈，面对层出不穷的干扰手段，单一的防御策略已难以奏效。电子对抗中，相关企业应进一步融合多学科技术，注重干扰检测、干扰定位、认证技术、加密等技术等应用，持续投入研发资源，加强创新性研究，融合人工智能、量子通信等新兴技术，进而应对不断升级的安全威胁，为国防建设与社会发展筑牢坚实的通信保障基石。

参考文献

[1]徐建国,杨志谋,杨庆,等.联合对海突击背景下电子对抗任务规划研究[J].系统工程与电子技术,2024,46(11):3736-3743.

[2]张轶,吴晗,刘涛.卫星通信系统智能电子对抗研究综述[C]//中国通信学会卫星通信委员会,中国宇航学会卫星应用专业委员会.第十九届卫星通信学术年会论文集.中国空间技术研究院西安分院;2023:50-57.

[3]王勇,赵青松,王迪,等.NC-OFDM 卫星通信方法及系统仿真[J].计算机仿真,2022,39(07):60-63+212.

[4]郝坤.基于临近空间平台电子对抗系统及作战运用构想[D].国防科技大学,2020.

[5]林锦顺,徐建敏,詹毅,等.毫米波卫星通信网络体系侦察技术分析[J].航天电子对抗,2020,36(02):14-16.

作者简介：贺群（1982.10.13），男，汉，吉林榆树人，博士研究生，研究方向为卫星通信