高技术前沿

据国外媒体报道，2023年9月，受“GPS欺骗”影响，多架飞机在伊拉克、伊朗空域飞行时，航线出现明显偏差，其中一架飞机险些在未经许可的情况下误入伊朗领空，形势一度十分紧张。

无独有偶。2013年，美国德克萨斯大学Humphreys团队利用一台笔记本电脑和仅公文包大小的自制设备，伪造GPS信号，成功操控一艘造价8000万美元的“白玫瑰”号超级游艇偏离航线，而游艇上的船员始终没有觉察。

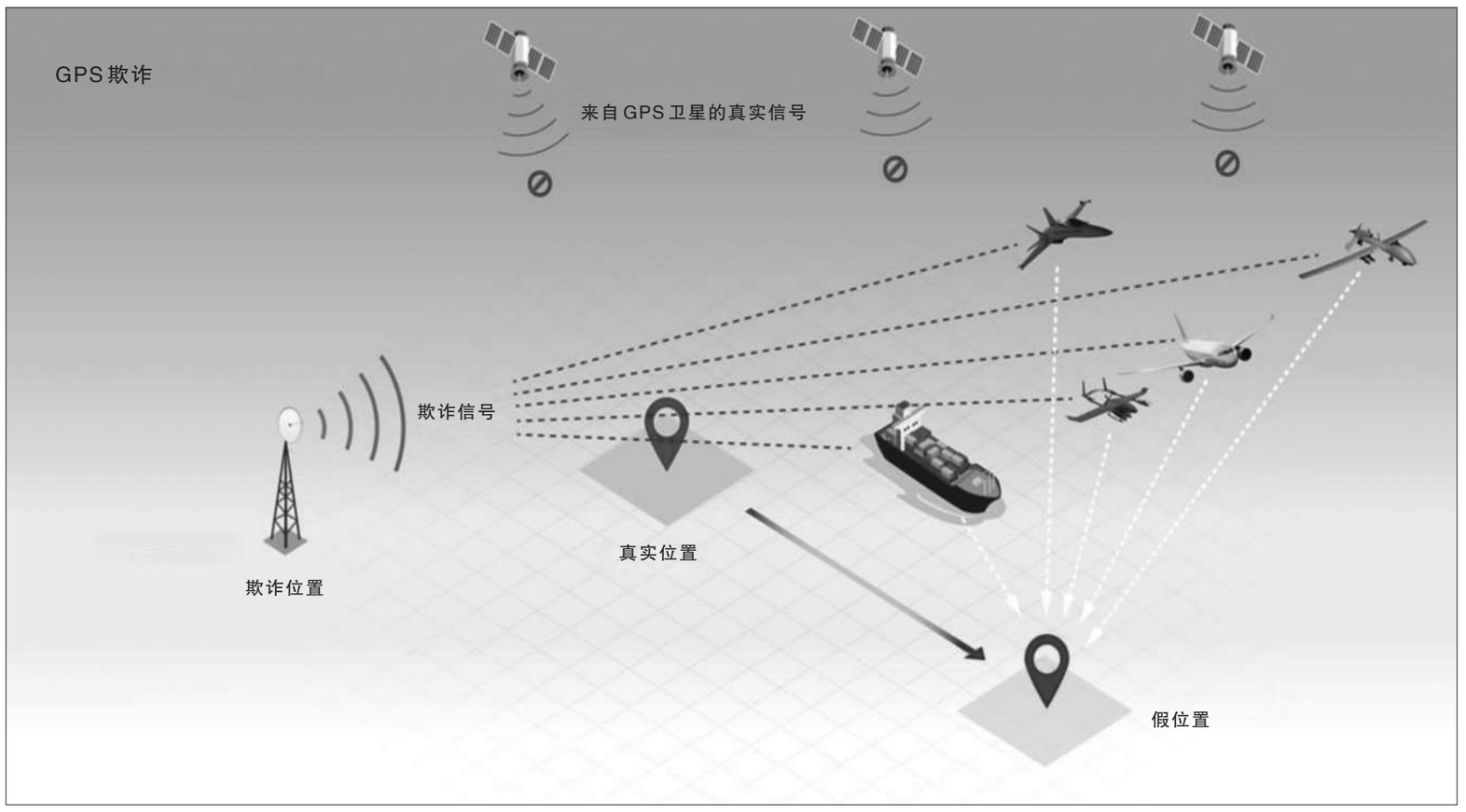
这为人们揭开了“卫星导航欺诈技术”的神秘面纱——当我们依赖的定位系统被随意篡改，所有基于位置的服务都将陷入信任危机。而从军事角度来看，这项技术或将对数字时代的攻防格局产生难以估量的影响。

那么，什么是“卫星导航欺诈技术”？其有哪些技术特点？又该如何应对？请看本期关注。

卫星导航欺诈技术——

不容小觑的“定位漂移”

■文兆阳 姚昌松



卫星导航欺诈技术概念图。 阳 明供图

悄然出现的威胁

遍观世界各国，人们的生活几乎已经离不开卫星导航系统。

作为现代社会的重要基础设施，卫星导航系统就像是人们的眼睛，是许多领域的重要支撑，能为交通运输、通信、金融、能源、军事等领域提供准确的同步时间和位置信息，其应用直接关系到经济发展、社会稳定和国家安全。

自20世纪70年代美国研制出全球定位系统以来，卫星导航技术发展迅速，应用日益广泛。据一份市场调研数据报告显示，2023年全球卫星导航系统产业规模已达2082.5亿美元。

然而，令人们不得不高度警惕的是，伴随着全球卫星导航技术的快速发展，其受恶意攻击的事件发生频率也在呈增加趋势。

一旦卫星导航系统的卫星接收机遭受欺诈信号干扰，就可能导致定位错误、时间不准，甚至对关键基础设施和应用系统造成严重威胁。

以海上交通为例，当一艘正在海上航行的货轮受到卫星导航欺诈时，对方会首先发送完全正确的卫星信号让系统信任，继而慢慢劫持整个系统。这种精密操控常常让船上人员难以觉察到“定位漂移”。直至货轮抵达对方“导航”的目的地时，船员才发现定位系统早已被“电子幽灵”劫持。

从某种意义上来说，越来越多导航欺诈攻击事件的发生，正倒逼着整个导航定位生态的重构。

事实上，卫星导航欺诈技术是一种极为隐蔽和极具针对性的攻击形式，主要根据导航信号和扩频码的特征规律对目标进行攻击。借助欺骗干扰机发射与导航信号相同或相似而功率稍强的欺诈信号，使接收机误以为欺诈信号是真实信号，导致接收机被误导，从而产生虚假导航信息或者无法输出导航信息。

早在2003年，美国德克萨斯州仪器公司的高级技术人员Scott就曾指出，通过构造虚假卫星星座或攻击差分修正链路可以实现导航欺诈。他还大胆预言，随着卫星定位经济效益的激增以及计算能力“全软件化”的发展趋势，导航欺诈或将演变为持续性威胁。

据公开消息，2011年12月，伊朗军队依托某信号干扰技术对RQ-170“哨兵”隐身无人机施展“电子擒拿术”，首次向世界展示了电磁环境的软肋。

这一事件的发生，颠覆了人们的传统认知：曾经高高在上的隐身无人侦察机，竟能被无形电磁波俘获。

虽然伊方始终未透露技术细节，但该事件催化了导航攻防技术的跨越式发展：从单纯信号压制升级为具备战略欺诈能力的“电子木马”。而“导航欺诈”这一曾经技术专家们争论不休的猜想，如今已成为科技领域的研究热点。

高超的“电子障眼法”

想象一下导航欺诈带来的场景：地面道路交通系统突然瘫痪，船舶、飞机的驾驶员也无法意识到轨迹偏离，而问题一旦暴露，一切都为时已晚……相比于其他类型的电磁干扰技术，卫星导航欺诈技术干扰范围大，更具有隐蔽性和威胁性。

这套针对卫星定位系统的“电子障眼法”，核心在于对信号的伪造与渗透，主要存在两种信号生成模式：转发式欺诈和生成式欺诈。

转发式欺诈——首先对真实卫星导航信号进行截获和存储，然后将信号延迟播发，延长信号传播时间，进而达到混淆用户定位结果的目的。转发式欺诈直接利用了真实卫星导航信号，无需分析信号内部结构，所以即使导航信号采用了破译难度较高的军用密码，干扰机也可能对用户设备实施欺诈。

生成式欺诈——生成式欺诈依托高精度卫星信号模拟器，根据截获真实信号的基本特征生成与真实信号强相关的伪随机码，生成与真实电文格式完全相同的欺诈导航电文，最终经天线发射加载该电文的欺诈信号。

在电子战和信号侦察领域，卫星导航欺诈技术通过误导敌方的电子系统，可以实现对敌方高价值目标的捕获或破坏，极大削弱敌方作战能力。

借助卫星导航欺诈技术，攻击者会高度复刻目标系统的卫星信号特征，包括载波频率、导航电文结构及扩频序列等关键参数。由于伪造信号需与真实卫星的时空参数保持毫秒级精准同步，其技术实现存在极高壁垒。这类“隐身式”攻击信号往往与真实电磁环境融为一体，传统导航终端难以通过常规手段识别出异常。

以战场环境中装甲车辆的导航系统为例，当遭遇此类精密欺诈时，车载设备依然会持续输出定位轨迹和运动参数，仪表界面毫无告警提示。在作战人员毫无戒备的情况下，这可能引导部队误入伏击区域或偏离战略要地，而这种隐蔽的位置欺诈往往在任务失败后才会发现。

在电磁频谱对抗领域，传统压制式干扰通常通过发射高强度的噪声信号，进而盖过敌方卫星通信的“声音”。不过，这种方式影响范围有限，并且易被电子侦察系统识别。相比之下，卫星导航欺诈技术可以生成与导航卫星同频的诱导信号，传输时具有空间泛在性优势。试想一下，未来城市作战中，一个精心设置的欺诈源可以影响到周围数公里甚至更大范围内的作战单位，其对作战进程将带来全局性、决定性的影响。

在军事对抗博弈中，掌握制导航权犹如获得战争之眼。卫星导航欺诈技术构建的时空基准网络，堪比战场的视觉感知系统，直接决定着作战部队的机动部署效率和精确打击效能。在信息化智能化技术快速发展的今天，卫星导航应用的潜在安全隐患正在逐步变为现实威胁。能否正确应对卫星导航欺诈技术，已经成为世界各国必须面对的重要安全问题。

多层次防护体系的构建

随着电磁空间的攻防博弈加剧，卫星导航欺诈技术或将继续进化。在这一背景下，全球导航安全保障体系需要进行有效的迭代和升级。

事实上，卫星导航系统在体系设计上已经考虑了抗干扰功能。目前，世界上主流的卫星导航系统已经建成和使用了抗干扰星载测距接收机、终端抗干扰单元等，具备抗干扰能力。

此外，在卫星导航系统密码战的背景下，世界各国还主动改进应对卫星导航欺诈的技术，保证卫星导航系统的安全性和可靠性。比如，美国国防部持续进行新技术研究，通过加强对目标接收机中间相位的准确检测等方式，进一步改进卫星导航系统天线图像识别技术，提高对卫星导航欺诈技术的识别和抗干扰能力。

与此同时，在技术创新领域，量子导航、脉冲星授时等替代性的定位、导航与授时（PNT）技术也正在逐步走出实验室，向实际应用迈进。这些新技术有望在未来为卫星导航技术提供有效的补充和替代方案，增强导航系统的抗干扰能力。美国海军研究实验室开发出一种新型的量子导航系统，利用连续3D冷却原子束干涉仪，实现了在没有GPS信号情况下的高精度定位。这种技术通过将原子冷却到接近绝对零度的方式，极大地减少了外界环境对原子性质的影响，使得测量更加精确。

这些年，导航信息安全逐渐成为世界各国关注的热点。

目前，世界各国正在加速建设全球卫星导航系统（GNSS）信号监测网络，以实时监测和响应潜在的信号干扰及欺诈行为，保护国家安全和公共利益。

为了安全可靠地使用卫星导航信息，许多国家纷纷采取措施，综合运用多种抗欺诈手段，构建多层次防护体系，反欺诈技术应运而生。首先，在射频前端使用抗欺诈天线，降低欺诈信号的强度。其次，在信号处理阶段，搭建单独的跟踪环路，实时跟踪锁定欺诈信号，并利用欺诈信号参数和其他辅助设备参数比对，消除欺诈信号。再次，通过结合人工智能技术和机器学习技术，将GNSS与其他导航方式相结合，借助不同导航方式的导航结果差异来进行欺诈干扰检测，如果差异超过设定阈值，则判定为受到欺诈攻击，防止用户设备对欺诈信号的误判。

除了构建多层次的卫星导航系统抗欺诈手段，许多国家科研人员还致力于提高对欺诈设备的探测和毁伤能力。在实际工作中，欺诈设备运行时会发出大量特征信号。工作人员通过技术侦察手段，可以对欺诈设备加以探测和定位。

比如，在战时，可以在作战区域范围内广泛设置干扰源监测设备和反干扰定位系统，找出敌方的欺诈设备，并运用反干扰无人机或小型反辐射导弹等武器对其进行精确毁伤，从而直接消除欺诈信号对卫星导航用户设备的威胁。

目前，各国围绕应对卫星导航欺诈技术的相关研究正持续展开，或将迎来卫星导航反欺诈技术更多进步。

新技术为隔空充电提供更多可能

■黄辛舟

热点追踪

近年来，无人机、智能机器人、可穿戴设备等智能硬件广泛应用，但续航能力一直是制约其进一步发展的关键因素。

传统的无线充电技术主要依赖于近距离、接触式的电磁谐振感应，其效率和适用范围受到空间、距离、环境、设备等多重因素的制约。

据公开报道，近日，由西安电子科技大学教授李龙课题组与中国科学院院士、东南大学教授崔铁军课题组共同研发的自适应无线传能技术，为解决这一难题提供了全新方案。

据悉，该技术利用类似WiFi的无线传输方式，将无线能量实时、高效地聚焦并传输到动态的终端设备上，实现无电池供电的感知、计算和通信。该技术构建了一种基于双频超表面、卷积神经网络近场定位的自适应无线传能网络，能进行同步的目标感知定位和波束调控，进而实现自适应追踪的无线能量传输。

凭借高效性、精准性和动态性等优异性能，自适应无线传能技术为隔空充电提供更多可能，未来有望成为无线充电领域的主流技术之一。

环顾世界，不少国家在无线充电技术领域纷纷发力。

美国一家公司开发了一种名为“Cota”的远距离充电技术。借助一个中央发射器，该技术无需连接电线或充电板，就能向多台设备发送无线射频能量。目前，该技术已经应用于电子货架标签和包裹追踪器等场景。

韩国蔚山科学技术院推出了一种新型无线电能传输技术。该技术通过优化收发器的物理结构，采用开放式双线圈配置，增强了电共振能力，使得设备能够在电场中自由定位而不降低充电效率。这种技术能够在三维空间中实现手机、电脑等电子设备的无线充电，且支持多个设备同时充电。

未来，自适应无线传能技术将在多个应用场景中展现出巨大潜力：采用该技术，智能音箱、智能机器人等智能家居设备能够进行稳定、高效的非接触式充电，提高家居环境的整洁度和智能化水平；可植入医疗设备如心脏起搏器、血糖监测仪等也可以采用该技术进行充电，减少手术风险和患者的不便……

尽管新技术为隔空充电提供了更多可能，但仍然面临诸多挑战。

比如，该技术在能量传输效率方面仍有待提高，相比有线充电，无线充电过程中会有部分能量以热能等形式损耗。此外，该技术的发射端设备目前体积较大且工艺复杂，使用的射频材料也较为昂贵。

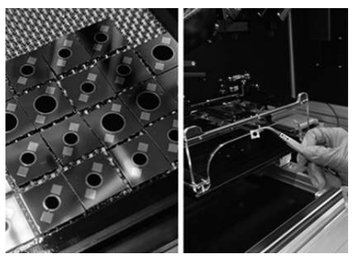
未来，随着磁场增强技术、共振频率控制技术的突破以及无线充电设备的安全防护能力增强，该技术有望实现更远距离的无线充电，满足更多场景下的充电需求，成为未来充电技术的重要发展方向，实现真正意义上的“隔空快充”。

科技云

科技连着你我他

■本期观察：梁佳伟 刘宝双 滕杨

光电传感器



近日，芬兰阿尔托大学的研究团队在光电二极管领域取得了重要突破。他们研制出一种基于锗材料的新型光电传感器，其灵敏度较传统锗基器件提升了35%，这项创新成果已在《光：科学与应用》期刊上发表。

据悉，这种新型器件不仅能够显著提升红外设备的性能，还在成本控制和环保方面展现出明显优势。传统红外光电二极管普遍采用的材料不仅价格昂贵，还存在毒性和致癌隐患。于是，研究团队将目光投向了锗材料，并通过技术创新成功解决了锗材料在红外光捕捉效率方面的局限。

在技术实现方面，研究人员通过在锗基光电二极管表面构建特殊的纳米结构，有效降低了能量损耗，大幅提升了器件性能。为验证这一创新设计的实际效果，团队专门研制了一种测试装置。实验数据显示，这种新型光电二极管的性能指标远超研究人员的预期，展现出广阔的应用前景。

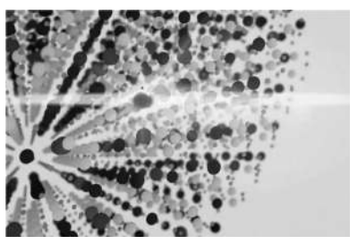
植入式传感器

近期，美国芝加哥某生物中心与美国西北大学的科研人员共同开发了一款植入式传感器，能够实时追踪生物体内蛋白质的变化情况，对炎症反应、糖尿病和心力衰竭等有关蛋白质疾病的诊断具有重要价值，相关研究已在《科学》杂志发表。

相较于传统检测手段，该装置在蛋白质监测的精准度和时效性上具有显著突破。其技术原理模拟“摇树落果”现象，即通过施加交变电场，该传感器能够使自身振动，从而释放捕获的蛋白并捕获新的蛋白，以此来实现持续监控的作用。这一独特设计使得监测过程更加动态、精准。

此外，它还可用于多种蛋白质相关疾病的诊断和治疗，借助实时、准确的生理指标数据，医生能够更及时地了解患者的健康状况，为疾病的早期发现和干预创造有利条件，提高临床诊疗水平。

光子雪崩纳米传感器



近期，哥伦比亚工程学院的科研团队在《自然》期刊上发表了一项突破性研究成果——一种基于光子雪崩效应的新型纳米传感器。据悉，该设备在机械力测量方面展现出前所未有的灵敏度和检测范围，标志着纳米传感技术的重要进步。

这项创新技术采用发光纳米晶体作为核心材料，其独特之处在于通过外力作用，晶体能够改变自身强度或颜色。由于采用光学探测原理，该传感器无需任何物理连接即可实现读数功能。

研究团队指出，该纳米传感器首次实现了单一设备的多尺度、高分辨率检测功能，这意味着只需这一种纳米传感器，就可以用于工程和生物系统中从亚细胞到整个系统水平的力的持续研究。

展望未来，研究团队计划进一步优化传感器性能。他们将重点研究纳米晶体中的集成自动校准功能，使每个纳米晶体都能作为独立的传感单元工作，这将进一步提升传感器的精确度和应用灵活性。