电力巡线无人机信息安全风险分析与防护

杨 浩[1],林 楠[1],袁 晨[1],罗 昊[2],苏 盛[2]

(1.国网江西省电力有限公司电力科学研究院,江西 南昌 330000;2.长沙理工大学电气与信息工程学院,湖南 长沙 410114)

摘 要:针对电力行业大量采用民用消费级无人机进行输电线路巡线可能存在的信息安全隐患展开风险分析。首先,结合无人机实时性要求高、通信链路不稳定、GPS 导航信号易篡改和飞航路径需保密等特点,指出应用专业级无人机进行输电线路巡线需要解决的信息安全问题。接着提出无人机及地面控制系统中基于对称密钥的控制信号、航拍数据加密通信与存储、密钥分发机制和基于无人机惯性导航系统的虚构 GPS 信号综合评估与甄别方法,以及基于云安全的无人机恶意软件检测的加固措施,所提方法为专业级巡线无人机的信息安全提供保障。

关 键 词:无人机;输电线路巡线;信息安全;风险分析

DOI:10.19781/j.issn.1673-9140.2021.04.022 **中图分类号**:TM863 **文章编号**:1673-9140(2021)04-0172-09

Cyber security defense of unmanned aerial vehicle in power utilities

YANG Hao[1], LIN Nan[1], YUAN Chen[1], LUO Hao[2], SU Sheng[2]

(1. Electric Power Science Research Institute, State Grid Jiangxi Electric Power Co., Ltd., Nanchang 330000, China; 2. School of Electrical & Information Engineering, Changsha University of Science & Technology, Changsha 410114, China)

Abstract: The paper performs the risk analysis of potential cybersecurity problems in residential consumer unmanned aerial vehicles (UAVs) adopted by power utilities for the transmission line inspection. Considering the real-time requirement, unstable communication links, easy-to-tamper GPS navigation signal, and flight path confidentiality, the paper shows the cybersecurity matters in applying professional UAVs for the transmission line inspection. After that, the paper proposes the evaluation and screening method in UAVs and ground control systems for falsified GPS signals, which is based on the symmetric encryption control signal, encrypted communication and storage of aerial data, key distribution mechanism, and inertial guidance system in UAVs. Moreover, the cloud security malware-detection-based reinforcement measure is also proposed. The proposed method and measure ensure the cybersecurity of professional patrol UAVs.

Key words: UAVs; transmission line inspection; cyber security; risk analysis

随着电网规模的日益扩张,输电线路巡线工作量快速增长,传统人工巡线仅靠肉眼及手持仪器巡检线路,受视角遮蔽影响,难以保障巡线质量。此外,部分线段地形复杂、交通不便,加之巡线环境恶劣,导致巡线效率低下[1-2],人工巡检输电线路已不能满足现代电网高效运维需求。无人机不受地形因素影响[3-4],携带方便、操作简单,还可使用高精度摄像设备进行大范围高精度航拍[5-6],显著提高了输电

收稿日期:2018-10-08;**修回日期**:2019-10-09

基金项目:国家自然科学基金(51777015);湖南省教育厅科学研究项目(重点项目)(15A005)

通信作者:杨 浩(1980-),男,硕士,高级工程师,主要从事电力系统网络安全防护研究;E-mail: 318448632@qq.com

线路巡检效率和质量，在电力系统中得到快速推广和应用。各电网公司均制定了短期内实现机巡为主、人巡为辅的协同巡检工作目标[7]，广东电网还计划到 2025 年将无人机巡线由手工遥控操作全部转变为自动驾驶。

需要指出的是，目前电力系统采用的巡线无人机多为民用消费级产品，为控制成本，该类无人机未考虑电力等专业级用户应用需求。从业务发展来看，基于民用无人机的输电线路巡线在信息安全等方面存在明显隐患，为保障未来全行业普遍应用无人机进行输电线路巡线的信息安全，亟待开展电力系统巡线无人机网络安全风险分析。结合电力行业业务需求特点，在信息安全加固等方面给出指引，提高电力行业无人机整体的安全防护水平。

该文首先对无人机巡视输电线路进行信息安全风险分析；然后，针对性地分析通信系统、导航控制系统、恶意软件入侵检测及其他方面的安全威胁，并提出可用的加固方案；最后，展望无人机信息安全的潜在发展趋势。

1　巡线无人机信息安全风险分析

巡线无人机信息安全风险框图如图 1 所示。民用消费级无人机一般仅用于视距内航拍，载荷能力有限，加之一般仅为个人用户使用，不涉及有强私密性要求的隐私信息，主要考虑满足飞航操控性能需求，对信息安全考虑不足。由于行业背景的差异，电力行业应用的专业级无人机在信息安全防护上派生了以下 2 点安全新需求。

1）因需要对长距离输电线路或大跨越的远距离输电线路进行巡航，专业级巡线无人机在续航能力和载荷能力上与一般民用无人机有明显差异[7]。为提高无人机对发热性缺陷的检测能力，除配置高精度航拍摄像头外，还要求配置红外甚至紫外摄像头[8]；为满足检测树线净空和杆塔倾斜等需求，未来还可能配置激光雷达系统[9]。一方面，配置完整巡线装备的电力系统巡线无人机价格可能超过 10 万，遭劫持或失控可能直接导致较大的经济损失；另一方面，无人机携带设备从高空失控跌落，将危及周边行人人身安全。

2）电力巡线无人机内部的航迹和航拍视频为机密信息。当无人机远距离巡线时，可根据输电线路沿线杆塔精确地理信息预先设置航迹，然后按预设航迹进行高清晰度航拍[10]。无人机中存储的近距离航拍视频和预设航路数据对应的输电线路精确地理信息为机密信息。一方面，无人机航拍时传输到地面站系统的视频信息存在窃听风险；另一方面，无人机失散后其中存储的航路敏感数据也将失密。

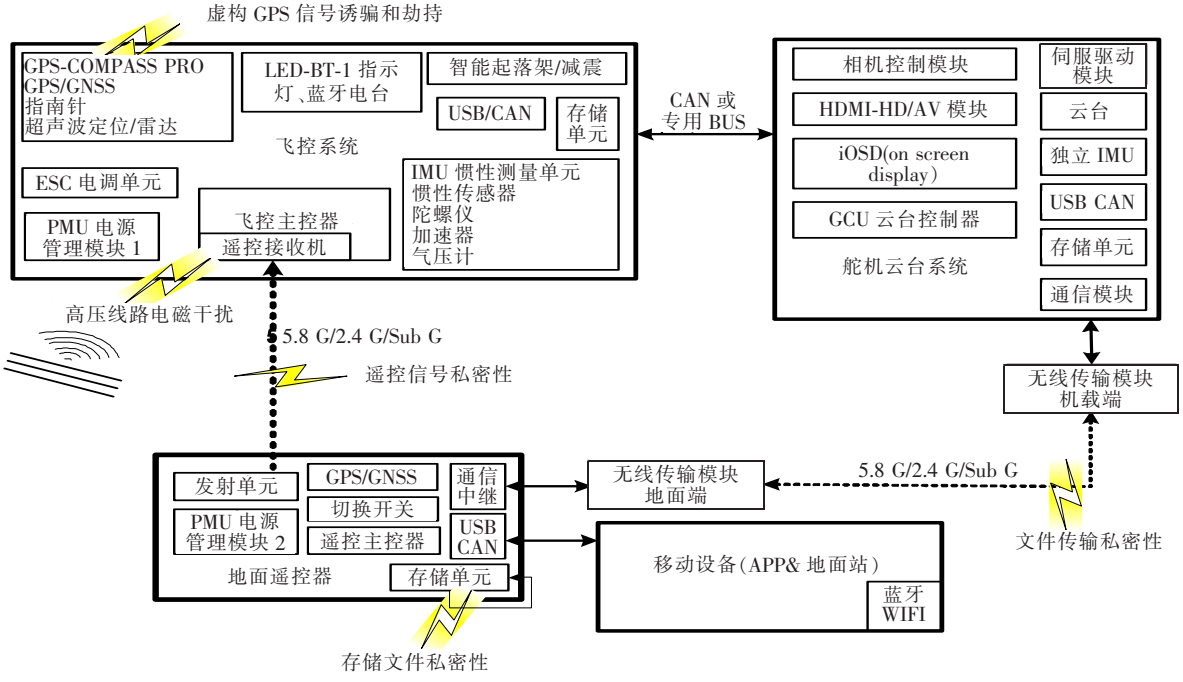

图 1　巡线无人机信息安全风险框图

Figure 1　Vulnerability of patrol UAV

电力巡线无人机作为行业应用专业设备，因价格和内部存储机密信息等因素，不但更容易成为网络攻击目标，同时也放大了遭遇攻击后的损失程度。因此，有必要对巡线无人机进行网络安全风险分析，并对各风险因素寻求针对性的加固与应对措施。

从图 1 结构来看，输电线路巡检无人机系统可分为空中无人机载具、机载终端与地面站系统及配套设备两部分。其中，机载终端包括无人机飞控系统(包括飞控计算机、机载传感器和执行机构等部分)和带有航拍摄像机的云台/吊舱，地面和机载终端间通过无线通信链路通信。无线通信链路负责传输由地面终端发送的控制命令、数据等信号，并将其发送给机载飞控计算机处理，飞控计算机输出控制指令到各执行机构及有关设备，实现对无人机飞行模态控制和任务设备管理。同时，飞控系统也将无人机飞行状态数据及发动机、机载电源系统、任务设备等工作状态参数通过下行链路实时传回地面终端，为控制人员提供无人机及任务设备状态信息。无人机巡线系统主要涉及飞行控制、数据链通讯、现代导航、机载遥测遥感、快速对焦摄像以及输电系统故障异常诊断技术等领域。当前，无人机在遥控信号安全性、抗虚构 GPS 信号干扰、文件传输和存储文件私密性等方面存在明显安全缺陷。

2 通信系统安全分析与加固

2.1 通信系统的安全威胁

因只能通过无线通信远程遥控，无线通信链路是无人机网络安全最突出的薄弱环节[11]。消费级无人机对网络安全没有严苛要求，主要依靠跳频技术来保障通信的私密性和抗干扰性。无人机射频通信模块一般有上百个跳频频点，通过频点的选择可组合出大量跳频方案。为避免同型号无人机遥控器间相互干扰，无人机起飞前还要将遥控终端和无人机对频，即选择一定数量的频点作为跳频组合，之后无人机和控制终端间即可按约定跳频序列同步高速跳频来保持数据链路和收发控制。以大疆无人机为例，地面系统控制无人机采用单向通信，地面遥控终端定期发送描绘控制杆和开关状态的 32 字节控制指令包，其中前 31 字节为状态位而末字节为 CRC 校验码。无人机接收到数据后根据控制指令执行飞行控制。当无人机和地面站系统失去同步或通信链路中断时，会进入同步搜索状态进行重新同步。

跳频通信具有很强的抗搜索、抗截获和抗干扰能力，有效提升了协议破解难度，但仅依赖跳频通信可能存在防护纵深不足的问题。跳频通信安全性严重依赖于跳频控制数字频率合成器，一旦跳频通信机制遭攻击破坏，将无法抵御。在 2015 年，安全机构就曾在反向工程的基础上发现了大疆无人机所用调频控制器设计缺陷，获取跳频序列信息后劫持并取得了无人机最高控制权。

2.2 通信安全加固

无人机与地面遥控终端之间采用的调频通信难以达到保障专业级应用的防护需求。无人机控制信号采用明码通信，单点突破跳频通信防护机制后，可获取无人机控制权。一般信息系统中多采用加密和身份认证技术进行安全防护，但无人机通信环境不稳定、控制指令简单重复，该 2 种安全防护手段均难以适用。

目前，在身份认证方面主要有基于密钥和非密钥的身份认证机制两大类。

1)基于密钥的认证机制要求在每次通信前确认身份。无人机无线通信链路易受建筑物、地形或植物阻挡而中断重连，地面控制终端将控制指令分解为 32 字节单向传输数据包，以保证在不稳定通信链路下保持敏捷的飞航控制。如采用 128 位的 SM1 国密算法进行身份认证，需要在控制指令数据包基础上附加 16 字节数字签名，将显著增加通信流量，并可能在远距离通信和跨障碍通信时影响飞航控制品质。尽管可以采用硬件加/解密的方式进行加速，但输电线路巡线无人机电磁信号干扰强，尤其在远距离巡线时通信链路可能经常中断[12]。基于密钥的身份认证机制将明显增加控制通信流量，对飞航控制特性产生不利影响，需深入研究才可采用。

2)近年来出现的基于硬件指纹的非密钥身份认证机制可利用制造射频通信模块时的细微差异形成的频谱特征硬件指纹识别身份[13]。该方法仅需检测通信对象频谱特征而无需增加通信流量，但无人机飞航时接收信号的频谱指纹可能受天气因素及通信距离影响，该方法的适用性有待进一步研究。

数据通信中常使用数据加密保障通信安全。数据加密可采用硬件或软件实现。因无人机控制系统实时性要求高，宜采用集成密钥的安全芯片进行硬件加/解密以提高响应速度。无人机系统存在密钥分配问题，如无人机及遥控器都和电表一样采用集成 SM1 国密算法的安全芯片进行对称加/解密，将造成密钥分发困难。可考虑对同一单位的多台无人机及地面控制系统采用含相同密钥的安全芯片，但地面控制终端遥控指令数量有限，攻击方在有限状态组合下较易搞清密文对应控制参数。在大量无人机系统共用相同密钥条件下，加密通信的安全防护价值将大打折扣。

为提高无人机纵深防护水平，可参照智能电表的安全防护模式进行密钥分发，并在后台系统中登记各无人机的密钥信息。在起飞前对无人机和地面遥控系统进行跳频序列配对的同时，根据无人机序号从密钥管理系统取得对应的密钥，再由地面控制终端和无人机执行对称加/解密。为提高地面遥控终端的加密实时性，可根据后台系统取得的密钥进行 FPGA 编程，然后由 FPGA 进行硬件加密，同时保持系统的安全性、实时性和灵活性。

3　无人机数据安全

3.1　数据安全威胁分析

无人机数据安全分为视频传输、外部文件存储和内部文件存储安全三部分。

1）为方便管理监控无人机飞行状态和读取航拍视频，无人机航迹数据和航拍视频分别存储于内部和外部存储器[14]，预设航路的航迹规划文件存储于内部存储器。民用无人机对存储器没有访问控制措施，拔除外部存储卡后可经读卡器读取视频文件，内部存储的航迹信息和航路规划文件则可通过 micro USB 接口读取。内部存储文件采用专用格式，利用专业软件可解析获取无人机前期飞行信息。

2）在早期，无人机对图传和视频不做加密防护。2009 年，伊拉克武装分子就曾监控美军无人机航拍视频判断美军动向。目前，民用无人机与地面终端多采用 TCP 协议通过 Wi-Fi 传输视频，并采用 WPA2 标准进行加密防护。Wi-Fi 图传时视频文件被分解为 512 字节数据包，传输时首先要通讯握手，传输有误时还需重传并确认完整性后再传输下一数据包，在极限距离及树障影响条件下易导致视频卡顿。针对视频传输对实时性要求高于可靠性的特点，新推出的 Lightbridge 图文传输采用 UDP 通信协议，无需错误校验和数据重传，并可根据距离远近、延时和信道通畅程度优化通信，能显著提高图传和视频监测效果。

3）无人机航拍图片存储为可交换的图像文件格式（Exif），该文件格式是在 JPEG 等文件基础上附加应用标记字段，可存储航拍时的经纬度、海拔、无人机方位角、云台角度与俯仰角等信息。如航拍照片中包含杆塔所属线路和杆塔编号，再结合文件中标记字段的经纬度和海拔信息，实质上就泄露了输电线路的精确位置信息。因此，对航拍图片导出后需做脱敏处理，消除潜在信息泄露风险。

3.2　数据安全加固

基于 Wi-Fi 的图文传输主要依靠 WPA2 进行加密防护。2017 年出现的密钥重装攻击（KRACK），利用 WPA 协议层逻辑缺陷，多次重传握手过程中的第三次握手消息，导致重放随机数和重播计数器。利用该协议存在的密钥重装攻击后客户端安装数值为全零密钥的缺陷，可随意监听网络、注入数据。对服务器和客户端更新补丁可修补该缺陷。尽管防护强度不高，但窃取航拍视频文件后果不严重，可考虑沿用已有措施。

大疆无人机采用的 Lightbridge 图文传输协议相对较新，在传输加密等安全性上较 Wi-Fi 协议有更深入考量，目前未见对其安全性分析的相关报道。在图文传输中，常见攻击模式是查找网络中开放的 FTP/Telnet 服务端口后利用漏洞进行提权渗透。接入无人机通信系统后通过 nmap 扫描获得设备目录，并重启 Telnet 服务器获得对无人机和地面终端的 root 访问权限，然后施行攻击。因此，需关闭不必要的服务，及时更新补丁以提高安全防护等级。

无人机内部存储数据接入 micro USB 接口即可利用专业解析软件读取和解析，缺乏控制措施，容易出现私密性问题。因无人机多发摔落、遗失，在不影响无人机有效载荷能力前提下，可对航迹文件及存储视频进行硬件写入加密。巡检人员回收无人机

后可根据无人机编号获取对应的密钥并按对称方式解密,即可取得记录内容。非法用户即便获取 SD 卡也无从解密机密信息。

4 导航控制安全

4.1 导航控制安全威胁模型

为提高巡线效率,降低无人机巡线过程人为干预,近年来出现了针对特定线路的航迹规划和路径定位巡线技术,可按照电力线模型和地形数据预先规划航迹。自主巡航过程依赖 GPS 导航,在航线附近进行 GPS 信号干扰或伪造 GPS 信号都可诱骗劫持无人机[15]。据报道,伊朗就曾于 2011 年发布虚构 GPS 信号,诱捕美国的 RQ-170 无人机。德克萨斯大学也研发了低成本 GPS 诱骗设备,并通过实验测试证明可发布虚构 GPS 信号劫持军用无人机。

GPS 是具有时间同步和定位功能的无源系统,GPS 卫星负责发射导航电文,地面接收机根据接收的导航信号进行时钟同步和导航定位。导航电文包括如图 2 所示的载波、测距码和数据码三部分。其中,载波是导航电文的基础频率;测距码分为加密传输的军用 P 码和明文传输的民用 C/A 码。无人机采用明文传输的民用 C/A 码进行定位和导航,易遭攻击。

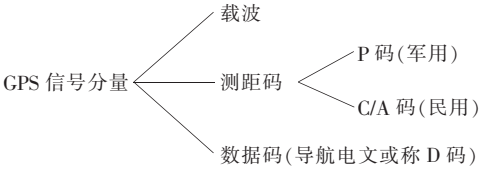

图 2 GPS 信号分量组成

Figure 2 Composition of GPS signal

GPS 导航电文包含时间、卫星运行轨道、电离层延时等用于定位和获取 GPS 参数的重要信息,并以帧、子帧的组帧方式形成数据流。卫星以帧为单位发送导航电文,每帧 1 500 bit,每比特长 20 ms,期间 C/A 码重复 20 个周期,一帧时长 30 s。每帧由 5 个子帧组成,每个子帧有 300 bit,一个子帧 6 s,总共 10 个字组成。每个字长 30 bit,GPS 接收机按从高位到低位的顺序接收解算。

GPS 干扰可分为压制式和欺骗式干扰两类,前者施放高功率虚构 GPS 信号来压制真实信号,使目标无法准确定位[16]。但所需欺骗信号功率大,容易识别。欺骗式干扰影响对接收机伪距测量,使其解算出错误位置,实现欺骗干扰。欺骗式干扰又可细分为生成式和转发式欺骗干扰[17]。

1)生成式欺骗干扰是欺骗系统直接发射伪造导航信号,使目标接收机跟踪后解算得出错误定位结果,可根据欺骗目的自主设定欺骗坐标。因军码带加密防护,该方法不能攻击军用对象。

2)转发式欺骗干扰是将接收的卫星信号延时、放大后转发,使目标接收机接收并产生定位错误。该方法无需了解信号具体结构,可攻击军码接收机。

为确定某点的三维位置(x_0, y_0, z_0),可进行定位求解,即

$$\rho_i = \sqrt{(x_i - x_0)^2 + (y_i - y_0)^2 + (z_i - z_0)^2} + c \cdot \Delta t \tag{1}$$

式中 ρ_i 为第 i 颗卫星伪距(卫星到接收机的距离),因测算距离不是卫星到接收机的真实距离,故名伪距;(x_i, y_i, z_i)为第 i 颗卫星三维位置,可由卫星导航电文解析得到;c 为卫星信号在大气层中的传播速度;钟差 Δt 为接收机时钟与 GPS 时钟之差。

因 GPS 时钟和接收机时钟不完全同步,它们的伪随机码序列存在同步误差。因不同卫星的原子钟之间存在钟差,取某卫星时钟 t 作为 GPS 时钟也将同样存在误差。为此,接收机根据 GPS 信号定位解算的 GPS 时钟需要进行修正,再通过接收机锁相环调整得到无累积误差、频率为 1 Hz 的高精度脉冲信号,方可用于校正本地时钟系统。GPS 授时原理:利用 GPS 秒脉冲没有累计误差的特点,通过本地晶振输出脉冲对 GPS 秒脉冲计数;测量得到 GPS 秒脉冲和计数后秒脉冲的相位差;将相位差进行卡尔曼滤波,将滤波后的相位差经 DAC 转换为模拟电压值;再用模拟电压值去控制压控晶振输出频率,从而保持本地时钟与 GPS 时钟同步。

式(1)有 4 个未知量,即 x_0、y_0、z_0 和 Δt,搜索 4 颗卫星联立方程组即可求出未知量。对 GPS 的

欺骗式干扰实施过程如下。

1）欺骗系统对每一接收到的可见卫星信号产生相应伪造信号。最初，欺骗系统产生的伪造信号和真实信号几乎同时到达目标接收机，信号码相位（仅几米误差）、信号强度及多普勒频移也都基本一致，此时伪造信号不对目标接收机造成影响。

2）欺骗系统逐渐增加码率使得伪造信号码相位向真实信号对齐，并不断增强伪造信号功率直至高于真实信号。

3）在虚构 GPS 信号增强过程中，鉴相结果会逐渐偏向虚构 GPS 信号的码自相关峰，直至将真实 GPS 信号码自相关峰完全剥离。然后，调整虚构信号的多普勒频移，使得其与真实信号的多普勒频移保持一致。最后，目标接收机跟踪环路持续跟踪虚构信号。

4.2　导航控制安全加固

针对虚构 GPS 信号的检测，文献[18]提出在惯性系统信息辅助下，利用转发式欺骗信号在空间传播方向上的一致性，通过实时观测载波相位差测量值，检测转发式欺骗；文献[19]提出了基于自适应天线技术的虚假 GPS 检测方法，将多根天线接收到的卫星发射信号处理形成定向性很强的波束，可区分不同位置终端，降低其他位置终端干扰；文献[20]提出增加北斗定位模块，通过北斗和 GPS 的相互校核增强无人机抗干扰能力。上述虚构 GPS 信号检测方法需增加硬件配置，且北斗卫星信号同样可遭攻击，还可能使得无人机硬件复杂化并降低可靠性。

除卫星导航系统外，无人机还配置有测量三轴姿态角（或角速率）及加速度的惯性测量单元。惯性测量单元一般包含 3 个单轴的加速度计和陀螺仪，加速度计检测加速度信号而陀螺仪检测角速度信号。无人机还带有磁罗盘和气压计，磁罗盘用于辨别飞行方位，气压计测量飞行高度。利用无人机携带的陀螺仪、加速度计、磁罗盘和气压计等多路冗余导航传感器，可根据其他系统提供的加速度、海拔高度、移动方位与 GPS 定位位置之间的关联性，检验 GPS 定位结果的真实性。此外，在缺乏雷达辅助的条件下，一般虚构信号发送装置无从确定无人机精确位置及其是否进入其控制范围，当无人机进入虚构信号发送装置的控制范围时，将出现 GPS 定位位置和时钟跳变。根据该跳变，同样可检测 GPS 导航系统异常。主要方法：

1）在正常飞航过程中，单位时间内无人机在水平和垂直方向的移动距离有一定范围，当结合无人机飞航航迹推算的移动距离超出合理范围时，可推断无人机遭劫持；

2）无人机在水平和垂直方向的移动速度和朝向与陀螺仪、加速度计、磁罗盘及气压计存在强关联性，结合各传感器输出亦可诊断无人机是否遭虚构 GPS 信号劫持。

无人机飞航过程中可根据上述方法评估 GPS 信号真实有效性[21]，并综合多因素评分结果诊断无人机是否遭虚构 GPS 信号劫持。在判别为遭劫持时进行告警，由地面控制人员控制无人机返回。

无人机飞行过程中在单位时间上的方位移动可用飞控状态方程描述，根据状态方程推算移动偏移，也可识别虚构 GPS 信号。由于四旋翼无人机飞航状态需要用 15 阶状态方程描述[22]，计算过程繁琐，计算结果有效性受无人机自身多种状态量检测精度和外界风速等因素影响，实用性存疑。

5　无人机恶意软件的检测

5.1　恶意软件的渗透入侵

因涉及实时复杂控制，为方便多进程调度管理，无人机本体及地面控制终端都配置有操作系统，和一般计算机系统一样可能存在恶意软件入侵风险。在 2011 年，美国内华达州克里奇空军基地发现无人机地面控制系统遭恶意软件入侵，可记录飞行过程中飞控人员远程控制的所有操作泄露行动机密数据。事后，美国军方除加强安全检测外，还将无人机地面系统迁移至 Linux 操作系统[23]，以降低攻击几率。

民用无人机多采用基于 Linux 的 Ubuntu 操作系统构建的开源系统，为提高安全性，大疆等公司还将无人机操作系统定制化改造成为类似 Mac-OS 的

非开源平台，通过隐藏系统实现细节降低攻击几率。因攻击方通过逆向工程可获得系统漏洞缺陷信息，该方式并不能杜绝恶意软件渗透入侵，需结合无人机工作场景设计恶意软件检测机制。

5.2 基于云安全的恶意软件检测

与一般信息系统相比，无人机网络安全防护具有鲜明特点。首先，无人机及其地面控制系统在开放通信环境下采用无线通信，易遭攻击破坏；其次，无人机飞航过程通信环境不稳定且对实时性有较高要求，需要将 CPU 负荷率和除飞航控制与视频传输外的背景业务通信流量控制在较低水平，难以采用复杂的防护措施；最后，因为攻击控制通信环节即可达到攻击破坏效果，攻击无人机与地面控制终端的途径与方式可能与一般信息系统不同。恶意软件攻击模式的差异性决定了针对一般信息系统的恶意软件检测方法不一定适用于无人机系统。

传统恶意软件检测机制主要通过比对恶意软件特征码方式检测病毒，需下载恶意软件特征代码库，再将目标文件特征码和特征库内特征代码逐条比对检测恶意软件[24]。用户需在本地存储海量恶意软件特征代码，并定期升级更新病毒库。因病毒库中特征代码数量太过庞大，该方法将明显增加 CPU 占用率，影响飞控品质，难以满足实时控制的需要。

近年来，在新出现的基于云端病毒查杀模式中，用户计算机病毒查杀不再依赖本地病毒特征库，只需枚举所有进程并计算进程哈希值特征码，将其上传到系统后台即可在云端完成恶意代码的比对检测。云端病毒查杀机制将对计算资源有高要求的恶意软件检测工作转移到云端完成，可在无人机及控制终端有限计算资源约束下完成恶意软件检测。

因无人机及其地面控制系统运行环境封闭固定，往往就是操作系统本身和厂家初始安装的业务进程，适合采用白名单机制。在无人机出产前，记录其中运行进程的名称、大小、哈希值特征码及功能描述等相关信息，并将其作为合法进程信息记录于云端形成白名单。因行业用户需结合自身需求进行二次系统开发且绝大部分电力用户为国网和南网用户，还可建立类似苹果的 APP 审查机制。一方面，可对用户二次开发进行审查，根据审查的 APP 和系统自身进程，维护和更新合法程序白名单；另一方面，可促进优秀巡线 APP 的快速推广和普及。

利用云安全和白名单机制进行无人机系统恶意软件检测，可在无人机厂商处架设云端安全服务器，在每次飞航前、后进行云端恶意代码检测，由无人机及地面控制终端枚举进程的哈希值特征码上传到云端安全服务器，即可实现基于云安全的无人机系统恶意软件检测。

6 其他

无人机巡线时需靠近目标对象空中悬停拍摄高清图像。输电线路周边的强电磁场会干扰无人机飞行甚至导致失控坠机。除采用多余度飞控，利用多套飞控系统同时运作、互为备用，降低受电磁干扰误动作概率外，还可采取电磁屏蔽防护和滤波进行防护。电磁屏蔽防护是加装电磁屏蔽外壳及优化设计内部电路，抑制电磁场对内部电路元件的干扰[25]。无人机飞控系统、测量模块（GPS、气压计、磁罗盘等）及信号接收机等需加强电磁防护，可在机身面板和设备外壳增设金属丝网垫或导电布垫屏蔽层，在敏感电子设备和线路整体包覆双绞线和屏蔽线。利用带通滤波器和电源滤波器吸收电磁干扰能量，也可减弱或消除干扰。

当电力行业大规模应用无人机后，电磁兼容问题可能在未来无人机远距离巡线导致遥控信号强衰减场景中凸显，需要针对性进行无人机极限距离电磁兼容性测试。一方面，确定强电磁场干扰条件下的巡线遥控极限距离；另一方面，进一步进行针对性的电磁屏蔽设计，提高远距离巡线安全水平。

7 结语

中国电力行业输电巡线正全面转向无人机巡检，搭载业务系统的升级和巡检距离的提升对巡线无人机网络安全提出了新的挑战。因为应用场景特殊，常用网络安全手段不一定适用。该文结合无人

机巡线实际工作场景，进行了无人机信息安全的风险分析，围绕通信系统安全、数据安全、导航控制安全、恶意软件监测和电磁兼容等方面，分析了存在的问题，提出了针对性的加固措施。

参考文献：

[1] 郭敬东，陈彬，王仁书，等. 基于 YOLO 的无人机电力线路杆塔巡检图像实时检测[J]. 中国电力，2019，52(7)：17-23.
GUO Jingdong，CHEN Bin，WANG Renshu，et al. YOLO-based real-time detection of power line poles from unmanned aerial vehicle inspection vision[J]. Electric Power，2019，52(7)：17-23.

[2] 刘正坤，陈伦清，王昊. 无人机辅助电网巡检作业的应用现状与思考[J]. 南方能源建设，2017，4(2)：115-119.
LIU Zhengkun，CHEN Lunqing，WANG Hao. Application status and reflections of electrical network inspection aided by unmanned aerial vehicle[J]. Sothern Energy Construction，2017，4(2)：115-119.

[3] 钱金菊，麦晓明，王柯，等. 广东电网大型无人直升机电力线路规模化巡检应用及效果[J]. 广东电力，2016，29(5)：124-129.
QIAN Jinju，MAI Xiaoming，WANG Ke，et al. Application and effect of large scale inspection on power lines by using large unmanned helicopter in Guangdong Power Grid[J]. Guangdong Electric Power，2016，29(5)：124-129.

[4] 范亮，汤坚. 架空输电线路三维建模方法现状及展望[J]. 南方能源建设，2017，4(2)：120-125.
FAN Liang，TANG Jian. Expectation and review on overhead transmission lines 3D modeling methods[J]. Sothern Energy Construction，2017，4(2)：120-125.

[5] 张文峰，彭向阳，陈锐民，等. 基于无人机红外视频的输电线路发热缺陷智能诊断技术[J]. 电网技术，2014，38(5)：1334-1338.
ZHANG Wenfeng，PENG Xiangyang，CHEN Ruimin，et al. Intelligent diagnostic techniques of abnormal heat defect in transmission lines based on unmanned helicopter infrared video[J]. Power System Technology，2014，38(5)：1334-1338.

[6] 彭向阳，陈驰，徐晓刚，等. 基于无人机激光扫描的输电通道安全距离诊断技术[J]. 电网技术，2014，38(11)：3254-3259.
PENG Xiangyang，CHEN Chi，XU Xiaogang，et al. Transmission corridor safety distance diagnosis based on point cloud and unmanned aerial vehicle loaded airborne laser scanning[J]. Power System Technology，2014，38(11)：3254-3259.

[7] 麦晓明，刘正军，彭向阳，等. 无人机电力线路安全巡检航线及任务规划软件系统设计[J]. 广东电力，2013，26(12)：81-85.
MAI Xiaoming，LIU Zhengjun，PENG Xiangyang，et al. Design on safe inspection route and mission planning software systems for unmanned aerial vehicle electric power circuit[J]. Guangdong Electric Power，2013，26(12)：81-85.

[8] Kim Hartmann，Christoph Steup. The vulnerability of UAVs to cyber-attacks-An approach to the risk assessment[C]//5th International Conference on Cyber Conflict，Tallinn，Estonia，2013.

[9] Michal Podhradsky，Calvin Coopmans，Nathan Hoffer. Improving communication security of open source UAVs：Encrypting radio control link[C]//International Conference on Unmanned Aircraft Systems，Miami，FL，USA，2017.

[10] Kwanwoong Yoon，Daejun Park，Yujin Yim，et al. Security authentication system using encrypted channel on UAV network[C]//First IEEE International Conference on Robotic Computing，Taichung，China，2017.

[11] 罗昊，苏盛，杨浩，等. 基于 FPGA 的电力巡线无人机硬件加密通信方法[J]. 中国电力，2019，52(7)：11-16.
LUO Hao，SU Sheng，YANG Hao，et al. FPGA-based hardware encryption of power line patrol drones[J]. Electric Power，2019，52(7)：11-16.

[12] 黄玲，赵锴，李继东，等. 基于特征金字塔和多任务学习的绝缘子图像检测[J]. 电测与仪表，2021，58(4)：37-43.
HUANG Ling，ZHAO Kai，LI Jidong，et al. Insulator image detection based on feature pyramid and multi-task learning[J]. Electrical Measurement and Instrumentation，2021，58(4)：37-43.

[13] 袁红林，胡爱群. 射频指纹的产生机理与惟一性[J]. 东南大学学报(自然科学版)，2009，39(2)：230-233.
YUAN Honglin，HU Aiqun. Fountainhead and uniqueness of RF fingerprint[J]. Journal of Southeast University(Natural Science Edition)，2009，39(2)：230-233.

[14] 彭福先，张玮，祝晓军，等. 基于激光点云精确定位的输

电线路无人机自主巡检系统研究[J]. 智慧电力,2019,47(7):117-122.
PENG Fuxian,ZHANG Wei,ZHU Xiaojun,et al. Autonomous patrol inspection system of unmanned aerial vehicle for electric transmission lines based on precise positioning of laser point cloud[J]. Smart Power,2019,47(7):117-122.

[15] 吴育武,刘佳陇,陈春,等. 基于多旋翼无人机的输电通道自主巡检技术研究[J]. 电网与清洁能源,2020,36(10):84-89.
WU Yuwu,LIU Jialong,CHEN Chun,et al. Research on autonomous patrol inspection technology of power transmission channel based on multi-rotor UAV[J]. Power System and Clean Energy,2020,36(10):84-89.

[16] 闫占杰,吴德伟,何晶,等. GPS转发欺骗式干扰源部署方法[J]. 现代雷达,2015,37(3):75-79.
YAN Zhanjie,WU Dewei,HE Jing,et al. Deployment method of jammer in GPS repeater deception jamming[J]. Modern Radar,2015,37(3):75-79.

[17] 王海洋,姚志成,范志良,等. 对GPS接收机的欺骗式干扰试验研究[J]. 火力与指挥控制,2016,41(7):184-187.
WANG Haiyang,YAO Zhicheng,FAN Zhiliang,et al. Experiment study of spoofing jamming on GPS receiver[J]. Fire Control & Command Control,2016,41(7):184-187.

[18] 李四海,刘洋,张会锁,等. 惯性信息辅助的卫星导航欺骗检测技术[J]. 中国惯性技术学报,2013,21(3):336-340.
LI Sihai,LIU Yang,ZHANG Huisuo,et al. Inertial measurements aided GNSS spoofing detection techniques[J]. Journal of Chinese Inertial Technology,2013,21(3):336-340.

[19] 董惠,郝鹏飞,王纯,等. GPS欺骗式干扰环境下MVDR算法的性能分析[J]. 计算机工程与科学,2016,38(11):2216-2220.
DONG Hui,HAO Pengfei,WANG Chun,et al. Performance analysis of MVDR algorithm in GPS deception jamming environment[J]. Computer Engineering & Science,2016,38(11):2216-2220.

[20] 史文森,朱海,蔡鹏. 基于接收信号DOA估计的GPS欺骗式干扰信号识别技术[J]. 舰船科学技术,2013,35(4):111-116.
SHI Wensen,ZHU Hai,CAI Peng. The GPS deception jamming identification technology of based on the DOA of received signal[J]. Ship Science and Technology,2013,35(4):111-116.

[21] 史密,陈树新,吴昊,等. 拒止环境实现注入的GPS欺骗干扰[J]. 空军工程大学学报(自然科学版),2015,16(6):27-31.
SHI Mi,CHEN Shuxin,WU Hao,et al. A GPS spoofing patternbased on denial environment[J]. Journal of Air Force Engineering University(Natural Science Edition),2015,16(6):27-31.

[22] Leonard Petnga,Huan Xu. Security of unmanned aerial vehicles:Dynamic state estimation under cyber-physical attacks[C]//International Conference on Unmanned Aircraft Systems,Arlington,VA,USA,2016.

[23] Hichem Sedjelmaci,Sidi Mohammed Senouci,Nirwan Ansari. A hierarchical detection and response system to enhance security against lethal cyber-attacks in UAV networks[J]. IEEE Transactions on Systems,Man,and Cybernetics:Systems,2017,99:1-13.

[24] 朱炳铨,郭逸豪,郭创新,等. 信息失效威胁下的电力信息物理系统安全评估与防御研究综述[J]. 电力系统保护与控制,2021,49(1):178-187.
ZHU Bingquan,GUO Yihao,GUO Chuangxin,et al. A survey of the security assessment and security defense of a cyber physical power system under cyber failure threat[J]. Power System Protection and Control,2021,49(1):178-187.

[25] 宋新明,谢从珍,夏云峰,等. 高压交流电场对WIFI无线通信影响的实验研究[J]. 高压电器,2019,55(12):125-131.
SONG Xinming,XIE Congzhen,XIA Yunfeng,et al. Experimental research of the influence of high voltage AC electric field on WIFI network communication[J]. High Voltage Electrical Apparatus,2019,55(12):125-131.