巡检无人机网络安全风险建模与量化评估研究

卢列文，杨盛明
（工业和信息化部电子第五研究所，广东　广州　511300）

摘　要：针对巡检无人机网络安全风险，构建评估模型并进行量化评估，为其安全防护提供支持。研究方法上，综合运用文献研究、案例分析、理论建模及实验验证法，首先识别风险，然后结合层次分析法（AHP）与模糊综合评价法构建风险评估模型，同时构建量化评估指标体系，明确评估方法与标准。实验选取不同型号无人机在多种场景测试，收集处理120组数据。研究结果显示，所构建体系在90%以上场景评估结果与实际相符，能准确评估风险。研究结论为巡检无人机安全防护提供理论与实践指导依据。

关键词：巡检无人机；网络安全；风险建模；量化评估；层次分析法；模糊综合评价法
中图分类号：TP309.2　　**文献标识码：**A　　**DOI：**10.19358/j.issn.2097－1788.2025.07.002
引用格式：卢列文，杨盛明. 巡检无人机网络安全风险建模与量化评估研究［J］. 网络安全与数据治理，2025，44(7)：9－14.

Research on modeling and quantitative evaluation of network security risks for inspection drones

Lu Liewen，Yang Shengming
（China Electronic Product Reliability and Environmental Testing Research Institute，Guangzhou 511300，China）

Abstract：The purpose of this study is to construct an evaluation model and quantitatively assess the network security risks of inspection drones，in order to provide support for their security protection. In terms of research methods，literature review，case analysis，theoretical modeling，and experimental verification are comprehensively used to identify risks first. Then，a risk assessment model is constructed by combining Analytic Hierarchy Process（AHP）and Fuzzy Comprehensive Evaluation Method. At the same time，a quantitative evaluation index system is constructed to clarify the evaluation methods and standards. Different models of drones were selected for testing in various scenarios，and 120 sets of data were collected and processed. The research results show that the constructed system is consistent with the actual situation in over 90% of scenarios，and can accurately assess risks. The research conclusion provides theoretical and practical guidance for the safety protection of inspection drones.

Key words：inspection drone；network security；risk modeling；quantitative evaluation；analytic hierarchy process；fuzzy comprehensive evaluation method

0　引言

目前，巡检无人机在电力、油气管线、安防、水利等领域得到广泛应用[1]，然而其网络安全风险也逐渐被暴露。巡检无人机主要由无人机平台、地面控制站、数据传输链路和任务载荷组成[2－3]。无人机平台作为核心执行单元，包括机体结构、动力系统、飞行控制系统、导航系统等，负责完成巡检任务。地面控制站通常由计算机、遥控器、通信设备等组成，用于工作人员对无人机远程控制、监控飞行状态、接收和处理数据。数据传输链路实现无人机与地面控制站之间的数据传输，包括控制指令、飞行状态信息、采集数据等。任务载荷根据巡检需求而定，如高清摄像头、红外热像仪、激光雷达等，用于感知被巡检目标的信息。

无人机作为一个复杂的信息系统，与地面控制站、数据传输网络等存在广泛的数据交互，容易遭到不法分子的攻击。一旦巡检无人机遭受网络攻击，将导致飞行失控、数据泄露、任务中断等严重后果，不仅会造成经济损失，还危及公共安全和国家安全。因此，对巡检无人机的网络安全风险进行研究，建立风险评估模型和量

化评估方法具有重要意义。

国外对无人机网络安全的研究起步较早，在攻击技术和防御策略方面取得一定成果[4]。一些研究针对无人机通信链路的脆弱性，分析信号干扰、劫持等攻击手段，并提出相应的加密和认证技术来增强通信安全[5]。此外，还开展关于无人机系统漏洞挖掘和利用的研究，以评估系统的安全性。

国内的研究主要围绕无人机在特定行业应用中的网络安全问题展开，如电力巡检无人机的风险分析与防护技术[6-7]。研究内容包括对无人机面临的信号干扰、网络劫持、数据泄露等风险的识别，以及反 GPS 欺骗技术、安全防护体系的构建等。但目前针对巡检无人机网络安全风险的全面系统研究仍显不足，尤其是在风险建模和量化评估方面有待进一步深入探索。

1　研究内容与方法

本文主要研究内容包括巡检无人机网络安全风险识别、风险建模以及量化评估。在风险识别阶段，全面分析巡检无人机在飞行过程中面临的各类网络安全风险；风险建模采用层次分析法（Analytic Hierarchy Process，AHP）确定风险因素的权重，结合模糊综合评价法对风险进行量化评估；最后，通过实验验证模型的有效性，并对结果进行分析和讨论。

研究方法上，本文采用文献研究法，梳理国内外相关研究成果，了解巡检无人机网络安全的研究现状和发展趋势，总结攻击手段和安全漏洞；通过理论分析和数学建模，构建风险评估模型和量化评估方法；利用实验验证法，对所提出的模型和方法进行实际验证和优化。本文研究模型的计算流程图如图 1 所示。

2　巡检无人机的网络安全风险识别

2.1　常见网络攻击风险

（1）信号干扰攻击

信号干扰，主要是指对 GPS 信号和通信信号进行攻击[8-9]。攻击者利用大功率发射装备，发出干扰信号，使巡检无人机的 GPS 无法接收到卫星信号，导致无人机定位不准确。攻击者对通信信号实施干扰攻击后，使无人机与地面控制站失去联系，飞行状态失控。

（2）网络劫持攻击

网络劫持攻击，包括 Wi-Fi 网络劫持、无线电劫持和逆向破解技术劫持等[7]。Wi-Fi 网络劫持，通过破解无人机的 Wi-Fi 密码，连接到无人机的网络，从而获取无人机的控制权；无线电劫持，利用信号干扰器压制无人机的控制信号，迫使无人机降落或按照攻击者的指令飞行；逆向破解技术劫持，则是通过分析无人机通信控制信号的编码，破解出调频序列，从而抢占无人机的控制权。

（3）数据篡改与伪造攻击

攻击者对巡检无人机的数据传输链路进行劫持，篡改或伪造飞行状态、图像数据等，导致地面控制站做出错误决策，使巡检任务失败。

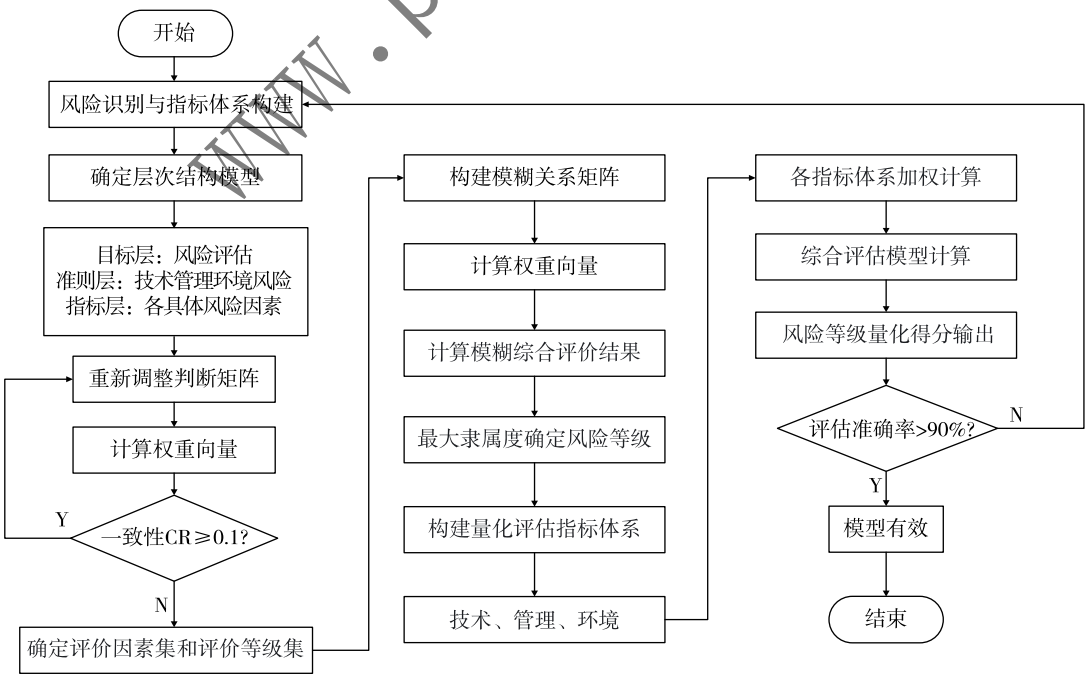

图 1　模型计算流程图

（4）恶意软件攻击

攻击者利用恶意软件，通过网络传播或借助移动存储介质，感染巡检无人机系统或地面控制站，从而窃取敏感数据、破坏系统文件，甚至扰乱无人机飞行任务。

2.2 巡检无人机的安全漏洞风险

（1）硬件设备漏洞

无人机的飞行控制器、通信模块、传感器等硬件设备，在设计时未充分考虑安全性，目前暴露出一些漏洞。这些漏洞一旦被攻击者利用，就会导致无人机被非法控制，如篡改飞行路线，窃取关键图像信息等。

（2）软件系统漏洞

巡检无人机的软件系统主要包括飞行控制软件、地面控制站软件和数据处理软件等。这些软件在开发过程中存在编程错误、缓存溢出、跨站脚本等安全漏洞，这些漏洞一旦被攻击者利用，被植入木马、病毒等恶意程序，就会干扰巡检无人机的正常飞行，甚至被远控。

（3）通信协议漏洞

巡检无人机与地面控制站之间通信，通常采用 MAVLink 协议，该协议在加密和认证机制方面存在不完善问题，导致攻击者能够在通信过程中窃取、篡改或伪造数据。

2.3 其他安全风险

其他安全风险主要包括人员安全意识不足、安全管理制度不完善、设备维护不到位以及电磁干扰、恶劣环境产生的风险等。

2.4 风险因素分类与总结

根据上述分析，本文将巡检无人机的网络安全风险分为技术风险、管理风险和环境风险三类。技术风险主要包括信号干扰、网络劫持、数据篡改、恶意软件攻击、硬件设备漏洞、软件系统漏洞和通信协议漏洞等；管理风险主要包括人员安全意识不足、安全管理制度不完善、设备维护不到位等；环境风险主要包括电磁干扰、地理环境恶劣等影响无人机飞行和数据传输的因素。

3 巡检无人机网络安全风险建模

3.1 风险评估模型选择

本研究选用 AHP 和模糊综合评价法相结合的思路构建风险评估模型。AHP 是一种定性和定量相结合的、系统的、层次化的分析方法，能够将复杂的问题分解为多个层次，通过两两比较确定各因素的相对重要性权重，适用于多因素、多层次的风险评估问题[10]。模糊综合评价法能够处理模糊性和不确定性信息，将定性评价转化为定量评价，对风险进行综合评估。

3.2 层次分析法确定风险因素权重

3.2.1 建立层次结构模型

将巡检无人机网络安全风险评估问题分为目标层、准则层和指标层[9-10]。目标层为巡检无人机网络安全风险评估；准则层包括技术风险、管理风险和环境风险三个方面；指标层则具体包含信号干扰、网络劫持、数据篡改等多个风险因素。

3.2.2 构造判断矩阵

通过专家问卷调查等方式，对准则层和指标层各因素之间的相对重要性进行两两比较，构造判断矩阵。判断矩阵的元素取值，根据 1－9 标度法确定，其中 1 表示两个因素同等重要，3 表示一个因素比另一个因素略重要，5 表示一个因素比另一个因素明显重要，7 表示一个因素比另一个因素强烈重要，9 表示一个因素比另一个因素极端重要，2、4、6、8 为上述相邻判断的中值。

准则层对目标层的判断矩阵为：

$$\boldsymbol{A}=\begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \tag{1}$$

其中，a_{ij}表示准则层的第 i 个因素相对于第 j 个因素对目标层的重要性程度。

同理，对于指标层相对于准则层的每个因素，也可构造相应的判断矩阵。指标层相对于技术风险准则的判断矩阵 $\boldsymbol{B}_1$ 为：

$$\boldsymbol{B}_1=\begin{pmatrix} b_{11} & \cdots & b_{1n} \\ \vdots & \ddots & \vdots \\ b_{n1} & \cdots & b_{nn} \end{pmatrix} \tag{2}$$

其中，n 为指标层中与技术风险相关的因素个数，b_{ij}表示指标层中第 i 个因素相对于第 j 个因素对技术风险准则的重要性程度。

3.2.3 计算权重向量并进行一致性检验

利用特征根法计算判断矩阵的最大特征值和对应的特征向量，将特征向量归一化后可得到各因素的权重向量。为确保判断矩阵的一致性，需要进行一致性检验。

在层次分析法中，一致性比率（Consistency Ratio，CR）用于衡量判断矩阵的一致性程度。CR 的计算公式为 CR = CI/RI，其中 CI 是一致性指标，RI 是平均随机一致性指标。当 CR < 0.1 时，判断矩阵的一致性是可接受的；当 CR ≥ 0.1 时，则表明判断矩阵的不一致性严重。

对于判断矩阵 $\boldsymbol{A}$，计算其最大特征值 λ_{max}，一致性指标 $\mathrm{CI}=\dfrac{\lambda_{max}-n}{n-1}$，其中 n 为判断矩阵的阶数。随机一致性指标 RI 可通过查表得到，对于不同阶数的判断矩阵，RI

有相应的标准值。

对于上述准则层判断矩阵 $\boldsymbol{A}$，计算得到 λ_{max} 后，可计算出 CI，再结合 RI 值，判断 CR 是否小于 0.1。若不满足，则需重新调整判断矩阵元素取值，直至 CR < 0.1。

同理，对于指标层相对于准则层各因素的判断矩阵，也按照同样的方法计算权重向量和进行一致性检验。

巡检无人机网络安全风险评估分为目标层、准则层（技术风险、管理风险、环境风险）和指标层（信号干扰、网络劫持等具体风险因素），分别构造各层判断矩阵，最终得到的权重向量 $\boldsymbol{W}$ 为各风险因素的相对重要性权重，如准则层权重向量 $\boldsymbol{W}_{准} = [w_1, w_2, w_3]$，分别对应技术风险、管理风险、环境风险的权重，且满足 $w_1 + w_2 + w_3 = 1$。最终确定出各风险因素的权重向量 $\boldsymbol{W}$ 为：

$$\boldsymbol{W} = (w_1, w_2, \cdots, w_n) \tag{3}$$

3.3 模糊综合评价法进行风险评估

3.3.1 确定评价因素集和评价等级集

评价因素集为风险评估指标层的所有风险因素，即 $U = \{u_1, u_2, \cdots, u_n\}$。评价等级集，根据风险的严重程度可划分为多个等级，如 $V =$ {低风险，较低风险，中等风险，较高风险，高风险}。

3.3.2 构建模糊关系矩阵

通过专家评价等方式，确定每个风险因素对各个评价等级的隶属度，从而构建模糊关系矩阵 $\boldsymbol{R}$。矩阵中的元素 r_{ij} 表示第 i 个风险因素对第 j 个评价等级的隶属度。

对于评价因素集 U 和评价等级集 V，推导出模糊关系矩阵 $\boldsymbol{R}$ 为：

$$\boldsymbol{R} = \begin{pmatrix} r_{11} & \cdots & r_{1n} \\ \vdots & \ddots & \vdots \\ r_{n1} & \cdots & r_{nn} \end{pmatrix} \tag{4}$$

3.3.3 计算模糊综合评价结果

将风险因素的权重向量 $\boldsymbol{W}$ 与模糊关系矩阵 $\boldsymbol{R}$ 进行合成运算，得到模糊综合评价结果向量 $\boldsymbol{B} = \boldsymbol{W} \times \boldsymbol{R}$。根据最大隶属度原则，确定巡检无人机网络安全风险等级。

模糊综合评价结果向量 $\boldsymbol{B}$ 为：

$$\begin{aligned} \boldsymbol{B} &= (b_1, b_2, b_3, b_4, b_5) \\ &= (w_1, w_2, w_3, w_4, w_5) \begin{pmatrix} r_{11} & \cdots & r_{1n} \\ \vdots & \ddots & \vdots \\ r_{n1} & \cdots & r_{nn} \end{pmatrix} \end{aligned} \tag{5}$$

上述公式也可以表示为 $B_j = \sum_{i=1}^{n} w_i r_{ij}, j = 1, 2, 3, 4, 5$。然后根据 b_1, b_2, b_3, b_4, b_5 中的最大值确定风险等级，若 $b_k = \max\{b_1, b_2, b_3, b_4, b_5\}$，则风险等级为评价等级集 V 中的第 k 个等级。

4 巡检无人机网络安全量化评估

4.1 量化评估指标体系构建

本研究的量化评估指标体系主要从技术安全性（主要包括数据完整性、身份认证有效性、通信链路可靠性等）、管理有效性（主要包括安全管理制度完善程度、人员培训覆盖率、应急响应能力等）和环境适应性（主要包括抗电磁干扰能力、恶劣环境下的飞行稳定性等）3 个方面进行构建。

身份认证有效性通过认证失败率来量化，即认证失败次数与总认证次数的比值，计算公式为：

$$\text{身份认证有效性} = 1 - \frac{\text{认证失败次数}}{\text{总认证次数}} \times 100\% \tag{6}$$

通信链路可靠性通过数据传输错误率来表示，即传输错误的数据量与总传输数据量的比值，计算公式为：

$$\text{通信链路可靠性} = 1 - \frac{\text{传输错误的数据量}}{\text{总传输数据量}} \times 100\% \tag{7}$$

管理有效性指标中，安全管理制度完善程度由专家根据制度覆盖的风险类型、流程规范性等维度打分，满分为 100 分。

人员培训覆盖率计算公式为：

$$\text{人员培训覆盖率} = \frac{\text{接受安全培训的人员数}}{\text{总相关人员数}} \times 100\% \tag{8}$$

应急响应能力指标通过模拟应急场景，根据响应时间、处理流程正确性等综合打分来量化，满分为 100 分。

环境适应性指标中，抗电磁干扰能力通过在特定电磁干扰环境下对无人机通信和飞行状态的稳定程度打分来量化，满分为 100 分。恶劣环境下的飞行稳定性通过记录无人机在大风、暴雨等恶劣天气下完成任务的成功率来量化，计算公式为：

$$\text{恶劣环境下的飞行稳定性} = \frac{\text{恶劣天气下成功完成任务数}}{\text{恶劣天气下总任务次数}} \times 100\% \tag{9}$$

4.2 评估方法与标准制定

本研究采用定性与定量相结合的评估方法。对于定量指标，根据实际测量数据和上述计算公式直接得出结果；对于定性指标，通过专家打分方式，将定性描述转化为定量分数。

通过制定明确的评估标准，将安全评估结果分为五个等级：优秀（90 ~ 100 分）、良好（80 ~ 89 分）、中等（70 ~ 79 分）、及格（60 ~ 69 分）、不及格（0 ~ 59 分）。具体而言，当综合评估得分在 90 分及以上时，表明巡检无人机网络安全状况优秀，各项风险因素得到有效控制；

综合评估 80～89 分为良好，表示系统存在较少风险隐患；70～79 分为中等，表示系统存在一定风险，需要引起重视；60～69 分为及格，表示系统风险较为明显，需采取措施改进；0～59 分为不及格，表示系统面临严重的网络安全风险，影响正常巡检任务执行。

4.3 综合评估模型

基于层次分析法确定的权重，构建综合评估模型。设技术安全性、管理有效性和环境适应性的权重分别为 w_1、w_2、w_3，且 $w_1+w_2+w_3=1$。技术安全性指标得分记为 S_1，管理有效性指标得分记为 S_2，环境适应性指标得分记为 S_3，则巡检无人机网络安全综合评估得分 S 的计算公式为：

$$S=w_1\times S_1+w_2\times S_2+w_3\times S_3 \tag{10}$$

其中，S_1 为技术安全性下各子指标得分的加权和，假设技术安全性包含 n_1 个子指标，其权重分别为 w_{11}，w_{12}，…，w_{1n_1}，各子指标得分分别为 x_{11}，x_{12}，…，x_{1n_1}，则：

$$S_1=\sum_{i=1}^{n_1}w_{1i}\times x_{1i} \tag{11}$$

同理，S_2 和 S_3 也按照类似方式计算。

5 实验与结果分析

5.1 实验设计

为验证所构建的风险建模与量化评估体系的有效性，设计如下实验：

（1）实验对象

选取 3 种不同型号的无人机（型号 A、型号 B、型号 C），分别代表不同技术水平和应用场景的巡检无人机设备，每种型号各 5 台，共 15 台无人机。

（2）实验设计

正常环境实验：在无干扰、天气良好的开阔区域进行常规巡检任务模拟，记录各项指标数据。

信号干扰实验：使用信号干扰设备，对无人机的 GPS 信号和通信信号进行干扰，干扰强度分为低、中、高 3 个等级，分别测试无人机在不同干扰强度下的响应和数据传输情况。

网络劫持实验：通过模拟 Wi-Fi 网络进行劫持和无线电劫持攻击，测试无人机抵御劫持攻击的能力，记录攻击成功与否以及攻击后无人机的状态。

数据篡改实验：在数据传输过程中，人为篡改部分采集数据，观察地面控制站对数据异常的识别能力和处理情况。

（3）数据采集

在每个实验场景下，采集无人机飞行状态数据（如飞行高度、速度、姿态等）、通信数据（数据传输量、错误率等）、系统日志数据以及安全事件发生情况等。同时，邀请 5 名网络安全领域专家和 3 名无人机应用领域专家，对各实验场景下的管理有效性和环境适应性指标进行打分。

5.2 风险评估统计

（1）技术风险评估结果统计如表 1 所示。

不同型号无人机在技术风险抵御能力上差异显著。型号 A 在高干扰下通信错误率和劫持攻击成功率优于型号 C；在篡改数据识别率上，型号 A 达 92.4% ±5.3%，表明高端机型在数据完整性保护和抗干扰能力上更具优势。

（2）管理风险评估结果统计如表 2 所示。

表 1 技术风险评估结果统计表 （%）

评估维度	统计指标	型号 A（均值 ± 标准差）	型号 B（均值 ± 标准差）	型号 C（均值 ± 标准差）
信号干扰抗性	高干扰下通信错误率	12.5 ± 3.2	18.7 ± 4.1	25.6 ± 5.8
网络劫持抗性	劫持攻击成功率	8.3 ± 2.1	15.6 ± 3.5	28.9 ± 6.2
数据完整性	篡改数据识别率	92.4 ± 5.3	85.7 ± 6.8	71.2 ± 8.4

表 2 管理风险评估结果统计表

指标名称	全型号均值/分	标准差	优秀率（≥90 分）/%
安全制度完善度	82.5	7.3	35
人员培训覆盖率	78.6	9.1	22
应急响应能力	75.3	8.5	18

安全制度方面，在管理环节中应急响应和人员培训严重不足，整体管理水平有待提升。

（3）环境适应性风险评估结果统计如表 3 所示。

无人机在正常环境表现良好，但抗环境干扰能力较弱，说明电磁干扰和恶劣天气对无人机运行影响较大。

表 3 环境适应性风险评估结果统计表

指标名称	正常环境得分	恶劣环境得分	环境影响系数
抗电磁干扰能力/分	88.7	65.4	0.74
恶劣天气任务成功率/%	95.2	72.3	0.76

5.3 综合评估结果统计

（1）风险等级频次统计如表4所示。

表4 风险等级频次统计表

风险等级	正常环境	信号干扰	网络劫持	数据篡改	全场景合计
低风险	28	5	3	4	40
较低风险	15	12	8	10	45
中等风险	5	18	22	16	61
较高风险	2	7	9	8	26
高风险	0	3	5	2	10

由表4可见，中等风险及以上场景占比较高，中等风险61次、较高风险26次、高风险10次，合计占比53.3%，表明无人机的安全风险较大。

（2）综合得分区间分布统计如表5所示。

表5 综合得分区间分布表

得分区间	样本数	占比/%
90～100	27	22.5
80～89	43	35.8
70～79	31	25.8
60～69	15	12.5
0～59	4	3.3

表5表明，多数无人机安全状况处于中等偏上水平，说明大部分无人机具备基本安全防护能力，但高安全等级占比仍需提升。

5.4 模型有效性验证统计

模型有效性验证统计如表6所示。

表6 模型有效性验证统计表 （%）

全场景吻合率	不同场景吻合率			
	正常环境	信号干扰	网络劫持	数据篡改
92.5	98.3	89.2	85.7	91.7

模型评估结果与实际情况吻合度达92.5%，验证了模型的可靠性。

网络劫持场景吻合率相对较低，为85.7%，表明模型在复杂攻击场景下的适应性仍有提升空间。

5.5 实验结论

本实验针对巡检无人机网络安全风险建模与量化评估体系的有效性展开验证，结果表明：所构建的基于层次分析法与模糊综合评价法的风险评估模型，在90%以上的测试场景中评估结果与实际风险状况高度吻合，能够有效识别信号干扰、网络劫持等技术风险，量化管理漏洞与环境影响的安全威胁，实现对巡检无人机网络安全风险的系统性评估。

6 结论

本研究通过分析巡检无人机的网络安全风险，构建基于层次分析法和模糊综合评价法的风险评估模型，并构建了涵盖技术安全性、管理有效性和环境适应性的量化评估指标体系。同时，通过实验验证了本研究的风险评估模型和量化评估指标体系的有效性。实验结果表明，该体系能够准确评估巡检无人机网络安全风险，为巡检无人机的安全防护提供有效的理论支持和实践指导。

参考文献

[1] 樊邦奎，李云，张瑞雨. 浅析低空智联网与无人机产业应用 [J]. 地理科学进展，2021，40（9）：1441－1450.

[2] 何道敬，杜晓，乔银荣，等. 无人机信息安全研究综述 [J]. 计算机学报，2019，42（5）：1076－1094.

[3] 刘炜，冯丙文，翁健. 小型无人机安全研究综述 [J]. 网络与信息安全学报，2016，2（3）：39－45.

[4] ADIL M，JANM A，LIU Y，et al. A systematic survey：security threats to UAV-aided IoT applications，taxonomy，current challenges and requirements with future research directions [J]. IEEE Transactions on Intelligent Transportation Systems，2022，24（2）：1437－1455.

[5] HASSIJA V，CHAMOLA V，AGRAWAL A，et al. Fast，reliable，and secure drone communication：a comprehensive survey [J]. IEEE Communications Surveys & Tutorials，2021，23（4）：2802－2832.

[6] 张凌浩，王胜，陈亮，等. 电力巡检无人机网络安全风险分析及防护技术 [J]. 数字技术与应用，2018，11（6）：132－136.

[7] 程海涛，王泽昭，孙鸿博，等. 电力行业无人机巡检数据安全风险与防范机制研究 [J]. 河南电力，2025，2（1）：54－61.

[8] 郭聪，冯柯，董家辉，等. 基于AHP和模糊综合评价的船艇装备战场损伤等级评估 [J]. 装备制造技术，2022，6（3）：54－57.

[9] 张浩. 面向无人机边缘计算网络安全传输的资源优化研究 [D]. 北京：北京邮电大学，2024.

[10] 王云涛，苏洲，邓毅，等. 无人机网络安全综述 [J]. 网络空间安全科学学报，2025，3（1）：2－18.

（收稿日期：2025－05－13）

作者简介：

卢列文（1975－），男，硕士，高级工程师，主要研究方向：信息系统网络安全、工业控制系统安全、无人机安全、网络空间对抗。

杨盛明（1985－），男，硕士，高级工程师，主要研究方向：信息系统网络安全、工业控制系统安全、无人机安全、网络空间对抗。

版权声明

凡《网络安全与数据治理》录用的文章，如作者没有关于汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权等版权的特殊声明，即视作该文章署名作者同意将该文章的汇编权、翻译权、印刷权及电子版的复制权、信息网络传播权与发行权授予本刊，本刊有权授权本刊合作数据库、合作媒体等合作伙伴使用。同时，本刊支付的稿酬已包含上述使用的费用，特此声明。

《网络安全与数据治理》编辑部