基于多维云模型和熵理论的机载娱乐系统安全风险评估

王 静[a,b],漆书凡[c],李 国[c]
(中国民航大学 a.安全科学与工程学院;b.信息安全测评中心;c.计算机科学与技术学院,天津 300300)

摘 要: 针对现有机载娱乐系统风险评估方法存在一定的不确定性、随机性和模糊性,其评估指标也具有很强的主观性,导致评估结果不够准确和客观等问题,本文提出一种基于多维云模型和熵理论的机载娱乐系统风险评估方法。首先使用更为全面、细粒度和客观的系统漏洞作为评估指标,并基于该指标数据生成多维云模型图,直观展现不同风险的隶属度大小;然后结合安全事件发生的可能性及安全事件损失的可能性来计算整个核心组件的风险值,并与风险对照表进行比较得出整个系统的风险评估结果。多次实验结果表明,本文方法的评估结果具有更好的稳定性、准确性和客观性。

关键词: 风险评估;云模型;熵权法;机载娱乐系统
中图分类号: V243;TP39 **文献标志码:** A **文章编号:** 1674-5590(2024)06-0009-08

Security risk assessment of airborne entertainment system based on multidimensional cloud model and entropy theory

WANG Jing[a,b], *QI Shufan*[c], *LI Guo*[c]
(a. *College of Safety Science and Engineering*; b. *Information Security Evaluation Center*;
c. *College of Computer Science and Technology, CAUC, Tianjin* 300300, *China*)

Abstract: In response to the certain uncertainty, randomness, and fuzziness of existing risk assessment methods of airborne entertainment system, as well as the strong subjectivity of their evaluation indicators, which leads to inaccurate and non-objective evaluation results, this paper proposes a risk assessment method of airborne entertainment system based on multidimensional cloud model and entropy theory. Firstly, more comprehensive, fine-grained, and objective system vulnerabilities are used as evaluation indicators, and based on this indicator data, a multidimensional cloud model graph is generated to visually display the membership degree of different risks. Then, the risk value of the entire core component is calculated based on the probability of security events occurring and the probability of security events losses. And compared with the risk comparison table, the risk assessment result of the entire system is obtained. Multiple experimental results have shown that the evaluation results of the proposed method in this paper have better stability, accuracy, and objectivity.

Key words: risk assessment; cloud model; entropy weight method; airborne entertainment system

机载娱乐系统是飞机客舱网络域中重要的组成部分[1],过去由于其功能较为简单且网络环境相对封闭,暴露的网络接口较少,存在的安全风险也较小,因此,对机载娱乐系统的安全性分析及风险评估工作也较少。但随着新一代飞机机载娱乐系统功能的多样化,其网络环境也越来越复杂[2],使得当前机载娱乐系统所面临的风险也日益增多,曾有黑客声称乘坐飞机时成功入侵了机载娱乐系统[3],诸如此类的报道近年来也时有发生,而这种攻击一旦出现,将会导致客舱通信功能中断、乘客恐慌,甚至影响飞行安全,因此,机载娱乐系统的安全风险问题不容忽视,其风险分析和评估工作至关重要。

然而目前针对机载娱乐系统的安全风险分析和评估工作较少,主要研究工作还集中在对部分机载软件或机载网络的安全性进行探索方面,如文献[4]通过故障注入的方式对机载娱乐软件进行测试分析,以证明其

收稿日期: 2023-03-07; **修回日期:** 2023-05-13
基金项目: 国家自然科学基金民航联合基金重点项目(U2033205, U2233214);中国民航大学信息安全测评中心开放基金资助项目(ISECCA-202006)
作者简介: 王静(1980—),女,山西太谷人,副教授,博士,研究方向为网络安全、智能运维、大数据民航应用.

风险性的存在;文献[5–6]对机上娱乐数据链进行了安全性分析与仿真,并给出了其中可能存在的一些安全风险;文献[7]则针对机载客舱无线网络提出了一种基于 ARINC822 的机载无线网络安全架构设计,以尽可能地减少安全风险。以上这些工作虽未涉及机载娱乐系统的风险评估,但证明了其风险的存在,为后续的安全风险评估工作提供了有效依据。而在机载系统整体的风险评估工作方面:文献[8]在 RTCA DO–326 标准的基础上提出了适用于民用飞机机载系统的安保风险评估过程,对研究机载娱乐系统的风险评估具有一定的指导作用;文献[9]则针对机载网络整体提出了一种基于威胁状态辅助风险源计算风险等级的模型,使用灰色定权聚类法计算定权聚类系数,提高了风险评估的准确性和鲁棒性,但其风险评估过程中使用的指标偏于模糊化和主观化,导致评估结果缺乏一定的客观性。在机载娱乐系统的风险评估工作方面,文献[10]提出了一种基于模糊层次分析法的攻击树模型,对机载娱乐系统面临的风险进行分析,结合系统自身和叶节点攻击行为的特点,构造模糊一致判断矩阵,确定叶节点各安全属性权值,计算攻击树叶节点实现概率,但由于其评估指标较少,不容易客观确定叶节点安全属性值,且计算过程中存在一定的不确定性和随机性,使得其评估结果不够客观准确。

其他领域相关研究中:文献[11–14]分别从不同角度针对不同问题提出了各种风险评估方法,大多采用定性分析与定量计算相结合的方法,典型的方法有层次分析法、故障树分析法、灰色理论、神经网络、模糊数学以及云模型等,其中,多维云模型允许对数据的不确定性进行更加灵活的建模,并能够处理更为复杂的决策问题,因此在风险评估领域得到了广泛应用;文献[15]在电力压力测试研究中采用了多维云模型进行风险评估,有效地通过图的形式展现了不同风险等级下的风险水平,使评估结果更加直观准确,但该评估方法存在权重模糊的问题,使评估结果缺少客观性;文献[16]则将熵权理论融入风险评估工作中,引入权值分配的思想,以衡量信息的复杂性和难以预测性,使结果更加客观准确。

因此,基于多维云模型和熵理论在风险评估方法中具有解决不确定性、随机性和模糊性等问题方面的优势,本文首次将多维云模型和熵理论引入机载娱乐系统风险评估工作,提出了一种基于多维云模型和熵理论的机载娱乐系统风险评估方法。采用由面到点,由大到小的方法,逐步深入影响其核心安全的组件中。首先通过系统漏洞分析获取机载娱乐系统可能存在的漏洞,并将其作为风险评估指标,以有效解决传统指标体系过于主观的问题;然后对风险指标进行综合分析,并按照标准划分等级权重,构建评价集隶属度矩阵,并采用熵系数确定风险因素的权重向量,以计算系统的风险值,减小了传统风险评估方法中主观因素的作用,进而提高机载娱乐系统安全风险评估的准确性和客观性。

1　预备知识

1.1　风险评估流程

机载娱乐系统风险评估过程主要是通过恰当的工具和方法来评估系统自身存在的安全风险。首先确定能够对系统资产造成一定风险的威胁属性,通过威胁发生频率及漏洞的严重性来计算安全事件发生的可能性,并通过资产值及漏洞的严重性两方面来计算安全事件损失的可能性,最后评估系统的风险值。计算安全风险值[17]表示为

$$Y = R(A,T,V) = R(L(T,V),F(I_a,V_a)) \tag{1}$$

式中:R 表示安全风险计算函数;A 表示信息系统资产值;T 表示信息系统的威胁性;V 表示信息系统的脆弱性;L 表示安全事件发生的可能性;F 表示安全事件损失的可能性;I_a 表示安全指标的资产值;V_a 表示漏洞的严重性。

风险评估示意图如图 1 所示。

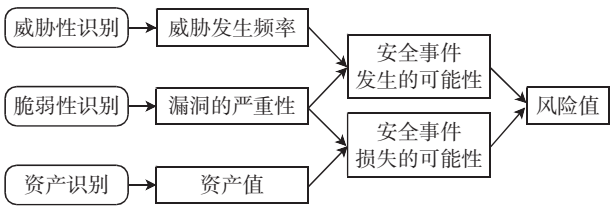


图 1　风险评估示意图

Fig.1　Schematic diagram of the risk assessment

1.2　多维云模型和熵理论

1)多维云模型

为了反映多维定性概念,将一维云模型扩展为多维云模型,其中 U 是一个 m 维场,T 是 U 的定性概念,$(x_1,x_2,\cdots,x_m)$ 是 U 的元素,其在 T 中的隶属度 μ 是稳定趋势的随机数[18]。对 μ 的解释如下

$$U\rightarrow[0,1],\ \forall(x_1,x_2,\cdots,x_m)\in U,\quad (x_1,x_2,\cdots,x_m)\rightarrow\mu \tag{2}$$

假设场的每个维度都是独立的,那么 m 维正态云

模型可以用三维的数字特征来描述：$E_{x1}, E_{n1}, H_{e1}, E_{x2}, E_{n2}, H_{e2}, \cdots, E_{xm}, E_{nm}, H_{em}$。其中：$E_{x1}, E_{x2}, \cdots, E_{xm}$ 是期望；$E_{n1}, E_{n2}, \cdots, E_{nm}$ 是熵；$H_{e1}, H_{e2}, \cdots, H_{em}$ 是超熵。多维云模型的数学期望超平面表示如下

$$\mathrm{MEHS}(x_1, x_2, \cdots, x_m) = \exp\left[-\frac{1}{2}\sum_{i=1}^{m}\frac{(x_i - E_{xi})^2}{E_{ni}^2}\right] \tag{3}$$

2）多维云生成算法

云生成算法称为云生成器，包括正向云生成器（FCG，forward cloud generator）和后向云生成器，正向云生成器也被称为基本的云生成器，m 维正规云的正向云生成器算法如下[18]。

步骤 1　基于期望（$E_{x1}, E_{x2}, \cdots, E_{xm}$）和熵（$E_{n1}, E_{n2}, \cdots, E_{nm}$）生成 k 个 m 维的正规随机向量 $\boldsymbol{x}_i = (x_{i1}, x_{i2}, \cdots, x_{im})$，$i = 1, 2, \cdots, k$。

步骤 2　基于熵（$E_{n1}, E_{n2}, \cdots, E_{nm}$）和超熵（$H_{e1}, H_{e2}, \cdots, H_{em}$）生成 m 维标准随机数的 k 个向量 $\boldsymbol{y}_i = (y_{i1}, y_{i2}, \cdots, y_{im})$，$i = 1, 2, \cdots, k$。

步骤 3　隶属度的公式描述如下

$$\mu_i = \exp\left[-\frac{1}{2}\sum_{j=1}^{m}\frac{(x_{ij} - E_{xj})^2}{y_{ij}^2}\right] \quad i = 1, 2, \cdots, k \tag{4}$$

式中，$(\boldsymbol{x}_1, \boldsymbol{x}_2, \cdots, \boldsymbol{x}_k, \mu_i)$ 作为云滴。对二维正向云生成器的描述如图 2 所示，其中：dt 为生成云滴的间隔时间；N 为云滴的数量；$\mathrm{drop}_i(x_{i1}, x_{i2}, \boldsymbol{y}_i)$ 为云滴参数。

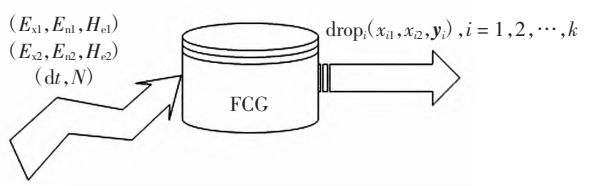


图 2　正向云生成器

Fig.2　Forward cloud generator

3）熵权理论

熵的概念是在热力学中产生的，被用来描述不可逆过程的现象，熵代表了信息论中出现事物的不确定性，并作为不确定性的度量。

假设系统可能有 h 种不同的状态 $s_1, s_2, \cdots, s_h$，p_i 指系统处于 s_i（$i = 1, 2, \cdots, h$）状态时的概率。熵的公式表示如下

$$H(p_1, p_2, \cdots, p_h) = -\sum_{i=1}^{h} p_i \ln p_i \tag{5}$$

式中，$0 \leqslant p_i \leqslant 1$ 且 $\sum_{i=1}^{h} p_i = 1$。

4）乘法

乘法的主要目的是基于两个或多个矩阵中的元素来生成一个新的矩阵中的元素。假设有两个矩阵 $\boldsymbol{\alpha}$ 和 $\boldsymbol{\beta}$，且有另一个矩阵 $\boldsymbol{\theta}$ 依赖于他们，函数 f 可以用作一种乘法方法，则公式的描述如下

$$\boldsymbol{\theta} = f(\boldsymbol{\alpha}, \boldsymbol{\beta}) = \boldsymbol{\alpha} \otimes \boldsymbol{\beta} \tag{6}$$

式中，⊗指 $\boldsymbol{\alpha}$、$\boldsymbol{\beta}$ 中的元素乘后取平方根。

2　机载娱乐系统风险评估模型

2.1　机载娱乐系统架构

机载娱乐系统主要分为在线娱乐系统和无线娱乐系统两部分。在线娱乐系统主要通过飞机自带的乘客座椅背屏上的功能实现，主要包括机载电影、机载音乐、飞机点餐服务等功能；无线娱乐系统则通常是通过乘客自携设备连接机载 Wifi 实现的。而机载娱乐服务主要包括飞行数据服务、视频播放服务、音频播放服务、预制音频通告、外景视频服务以及无线门户服务等。本文研究的机载娱乐系统的架构如图 3 所示。

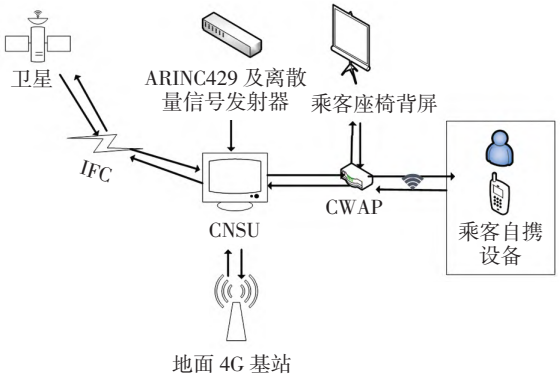


图 3　机载娱乐系统架构

Fig.3　Architecture of airborne entertainment system

图 3 中：ARINC429 及离散量信号发射器主要用来模拟飞机飞行过程中，飞机向客舱网络域中单向传输数据的功能；客舱网络服务单元（CNSU，cabin network service unit）则为整套系统的中枢，负责存放信息数据以及与其他部件进行交互，同时也是整套机载娱乐系统中最为核心的部分；客舱无线接入单元（CWAP，cabin network access point）相当于机载 Wifi，乘客可以通过其无线连接 CNSU 进行访问；乘客座椅背屏同样通过 CWAP 来对 CNSU 中的资源进行访问；机载天线（IFC，in flight connectivity）可以通过卫星、地面网络或两者结合来连接飞机上的 CNSU 设备和乘客设备，为乘客提供在高空中的互联网访问，使其可以在飞行期间收发电子邮件、浏览网页和使用社交媒体等。

ARINC429 信号模拟器采用单向传输的方式向 CNSU 提供飞行高度、经纬度等实时数据[19]，因此在安全等级更高的信息域向客舱网络域传输数据的过程中起到了一定程度的安全隔离作用，因此，其风险较小。而乘客座椅背屏、乘客自携设备、CWAP、IFC 以及地面 4G 基站等之间的交互均是围绕 CNSU 进行的，因此，CNSU 成为了整个结构的中心，风险接入点也往往存在于其中。如今的 CNSU 将传统的乘务员操作面板与娱乐系统信息服务器合二为一，这也就更加强调整个 CNSU 的安全性与稳定性。因此，深入挖掘和研究 CNSU 中的风险因素并进行风险评估至关重要。

2.2　风险评估流程

基于多维云模型和熵理论的风险评估流程如图 4 所示。

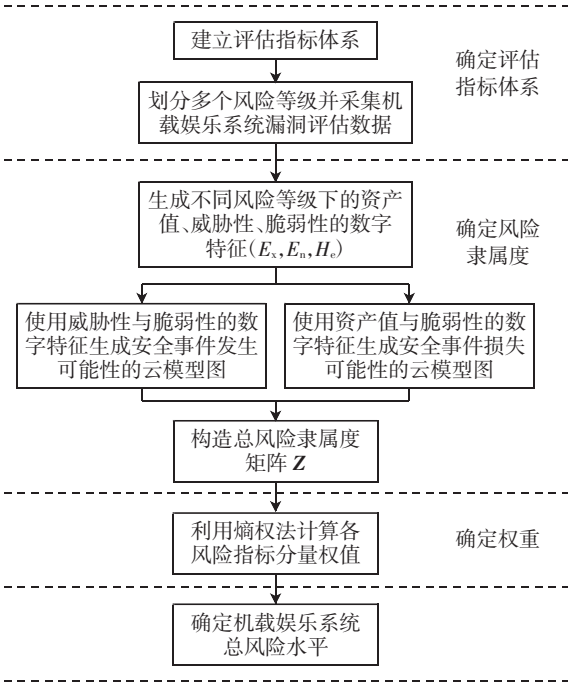


图 4　基于多维云模型和熵理论的风险评估流程

Fig.4　Process of risk assessment based on multidimensional cloud model and entropy theory

该模型主要包括 3 个部分，分别为确定评估指标体系、确定风险隶属度以及确定权重。其中，确定评估指标体系部分的主要任务是通过漏洞挖掘的方式对机载娱乐系统内部可能存在的威胁漏洞进行分析，得到不同等级下的漏洞评估数据；确定风险隶属度部分首先基于统计数据计算出不同风险程度下的期望、熵和超熵(E_x,E_n,H_e)，并分别将资产值、威胁性和脆弱性呈现，接着，使用威胁性和脆弱性的数字特征生成不同风险下安全事件发生可能性的云模型图，并使用资产值和脆弱性的数字特征生成安全事件损失可能性的云模型图，然后，结合二者构造总风险隶属度矩阵 $\boldsymbol{Z}$；确定权重部分主要是利用熵来度量各风险指标的相对重要性，并分别赋予不同风险指标相应的权值；最后计算出机载娱乐系统的总风险值。

2.3　建立风险评估指标体系

本文通过漏洞挖掘的方式对所研究的机载娱乐系统进行安全检测，根据检测结果大致可以将影响其安全性的因素分为 5 个方面，其主要威胁指标如表 1 所示。

表 1　CNSU 安全风险评估指标体系

Tab.1　Index system of CNSU security risk assessment

安全类别	指标名称	指标编号
系统安全	系统日志等级参数配置不当	1
	内核版本未更新	2
	核心文件命令未禁用	3
	诊断信息命令未禁用	4
	内核符号表命令未禁用	5
	地址空间配置随机加载未启用	6
	内核配置文件未禁用	7
	存在已知漏洞	8
通信安全	IPv6 数据包重定向发送未禁用	9
	IPv4 源路由数据包被接受	10
	IPv4 可疑数据包未记录	11
	IPv4 广播 ICMP 请求未被忽略	12
	IPv4 伪造的 ICMP 响应未被忽略	13
	IPv4 反向路径过滤未启用	14
	IPv4 TCP 同步包 Cookies 未启用	15
	IPv4 数据包重定向发送未禁用	16
	IPv6 源路由数据包被接受	17
	Wifi 配置不当	18
	Wifi 固件检测	19
服务安全	存在敏感服务运行	20
	SSH 配置文件权限配置不当	21
	SSH Root 用户登录未被禁止	22
	SSH 空密码未被禁止	23
	进程映射虚拟地址重复	24
	进程虚拟内存权限错误	25
文件系统安全	文件系统权限配置不当	26
	Dev 目录权限配置不当	27
	挂载配置读写方式不当	28
	挂载配置 nodev 设置不当	29
	挂载配置 nosuid 设置不当	30
	挂载配置 noexec 设置不当	31
	挂载配置 dm–verity 不当	32
	存在已知漏洞	33
信息安全	存在 SUDO 命令	34
	存在 SU 命令	35
	存在命令历史记录文件	36
	存在敏感私钥	37
	存在通用资源识别号(URI)密码	38
	用户使用弱密码	39

在计算过程中，每个指标中的资产值、威胁性和脆弱性将根据其严重程度按照风险等级赋值表给予一定的赋值，其中的主要威胁漏洞例如潜在漏洞（内

核版本未更新)、运行出错(核心文件命令未禁用)、网络错误(IPv6 数据包重定向发送未禁用)、越权攻击(存在 SU 命令、存在 SUDO 命令等)、信息泄露(存在敏感私钥、存在通用资源识别号(URI)密码)等在计算时给予相对较高的值。

2.4 构造多维云模型

构造多维云模型主要分为 3 部分。首先通过采集数据计算云数字特征(E_x,E_n,H_e);然后通过云数字特征生成安全事件发生可能性和安全事件损失可能性的云模型图;最后,构造安全事件发生可能性的隶属度矩阵以及安全事件损失可能性的隶属度矩阵,并计算出机载娱乐系统的总风险隶属度矩阵 $\boldsymbol{Z}$。具体过程如下。

(1)通过正向云生成器算法计算云数字特征(E_x,E_n,H_e)。

正向云生成器算法过程如下。

输入:样本数据 $X_i(i=1,2,\cdots,N)$。

输出:数字特征 E_x,E_n,H_e。

算法步骤:

步骤 1　通过样本数据计算出样本均值 $\overline{X}=\frac{1}{N}\times\sum_{i=1}^{N}X_i$,样本的一阶绝对中心矩为 $\frac{1}{N}\sum_{i=1}^{N}|X_i-\overline{X}|$,样本的方差为 $S^2=\frac{1}{N-1}\sum_{i=1}^{N}(X_i-\overline{X})^2$;

步骤 2　计算样本的期望 $E_x=\overline{X}$;

步骤 3　计算样本的熵 $E_n=\sqrt{\frac{\pi}{2}}\frac{1}{N}\sum_{i=1}^{N}|X_i-E_x|$;

步骤 4　计算样本的超熵 $H_e=\sqrt{|S^2-E_n^2|}$。

依据统计原理,期望为(E_{x1},E_{x2},$\cdots$,E_{xm}),熵为(E_{n1},E_{n2},$\cdots$,E_{nm}),超熵为(H_{e1},H_{e2},$\cdots$,H_{em})。

给定的样本指标点越多,用正向云生成器算法还原所得到的参数估计值误差越小。

(2)依据最新的国家安全风险评估标准[20]将机载娱乐系统的风险划分为 5 个等级,根据先前求得的特征值生成各自风险等级下的云模型图,并且得到安全事件发生可能性的隶属度矩阵 $\boldsymbol{P}$ 以及安全事件损失可能性的隶属度矩阵 $\boldsymbol{L}$,即

$$\boldsymbol{P}=\begin{bmatrix} p_{11} & \cdots & p_{1k} \\ \vdots & & \vdots \\ p_{q1} & \cdots & p_{qk} \end{bmatrix}\quad \boldsymbol{L}=\begin{bmatrix} l_{11} & \cdots & l_{1k} \\ \vdots & & \vdots \\ l_{q1} & \cdots & l_{qk} \end{bmatrix} \tag{7}$$

式中:q 表示风险等级的数量;k 为正规随机数的个数。

(3)采用乘法计算总风险隶属度矩阵 $\boldsymbol{Z}$,表示漏洞的威胁造成的风险损失程度,即

$$\boldsymbol{Z}=\boldsymbol{P}\otimes\boldsymbol{L}=\begin{bmatrix} z_{11} & \cdots & z_{1k} \\ \vdots & & \vdots \\ z_{q1} & \cdots & z_{qk} \end{bmatrix} \tag{8}$$

2.5 根据熵权法确定权重

基于熵权理论测量安全风险成分的熵值

$$F_i=-\frac{1}{\ln k}\sum_{j=1}^{k}z_{ij}\ln z_{ij} \tag{9}$$

式中,z_{ij} ($j=1,2,\cdots,k$)等价时,熵为最大值,$0\leqslant F_i\leqslant 1$。

若风险成分对系统风险评估的贡献最大,则其熵值最大,使用 $1-F_i$ 来测量安全风险分量 z_{ij} 的权重,同时将该权重标准化后得到 ϕ_i,表示如下

$$\phi_i=\frac{1}{q-D}(1-F_i) \tag{10}$$

式中:$D=\sum_{i=1}^{q}F_i$;$0\leqslant\phi_i\leqslant 1$,$\sum_{i=1}^{q}\phi_i=1$。

根据风险分类,不同评估因子(b_1,b_2,$\cdots$,b_k)对应赋予不同的权重(c_1,c_2,$\cdots$,c_k),且 $\sum_{i=1}^{k}c_i=1$。

从上述算法中,可以得到总风险隶属度矩阵 $\boldsymbol{Z}$、安全风险成分权重 $\boldsymbol{\phi}=[\phi_1\ \phi_2\ \cdots\ \phi_q]$和评估集中风险等级权重 $\boldsymbol{C}=[c_1\ c_2\ \cdots\ c_k]$。计算最终风险值

$$R=\boldsymbol{\phi}\cdot\boldsymbol{Z}\cdot\boldsymbol{C}^{\mathrm{T}} \tag{11}$$

将计算得出的风险值与表 2 所示的风险对照表进行对比,可以得到最后评估的机载娱乐系统风险水平结果。

表 2　风险对照表

Tab.2　Comparison table of risk

风险等级	R	风险等级	R
非常低	[0,0.2)	高	[0.6,0.8)
低	[0.2,0.4)	非常高	[0.8,1.0]
中等	[0.4,0.6)		

3　模型实验分析

本文以实验室搭建的机载娱乐系统作为研究对象,使用安全分析工具获取其数据指标,主要的安全评估集合为:系统安全、通信安全、服务安全、文件系统安全和信息安全,各类安全事件的子集为其评估指标,每个指标 g 含有资产值、威胁性和脆弱性 3 个参数(A_g,T_g,V_g),按照表 3 所示的赋值标准,通过专家打分的方式分别给 3 个参数赋予不同的值。表 4 中以系统安全指标中的 1~8 为例,将对应的(A_g,T_g,V_g)参数作为输入,按照正向云生成器算法即可得到样本指标的期望、熵与超熵,并依据风险对照表得到其预估风险等级。

表 3　风险等级赋值表

Tab.3　Assignment table of risk level

风险等级	数值	风险等级	数值
非常高	5	低	2
高	4	非常低	1
中	3		

表 4　系统安全指标数据

Tab.4　System security index data

指标编号	资产值 A_g	威胁性 T_g	脆弱性 V_g	预估风险等级
1	2.8	2.5	2.9	中
2	3.4	3.6	3.3	高
3	4.3	4.5	4.7	非常高
4	0.9	0.7	0.8	非常低
5	1.3	1.6	1.8	低
6	4.6	4.9	4.7	非常高
7	2.6	2.4	2.2	中
8	3.8	3.3	3.7	高

3.1　风险特征值的确定

在对机载娱乐系统的实验结果及指标赋值分类后，根据正向云生成器算法，按照 5 种等级分别统计数据并计算出指标资产值、脆弱性及威胁性在不同风险等级下的期望、熵、超熵。具体结果如表 5—表 7 所示。

表 5　期望

Tab.5　Expected value

因素	风险等级				
	非常高	高	中	低	非常低
资产值	4.8	3.7	2.9	1.8	0.9
威胁性	4.9	3.8	2.9	1.9	0.7
脆弱性	4.7	3.9	2.7	1.7	0.8

表 6　熵

Tab.6　Entropy

因素	风险等级				
	非常高	高	中	低	非常低
资产值	1.51	1.53	1.58	1.59	1.56
威胁性	1.54	1.50	1.55	1.53	1.57
脆弱性	1.59	1.57	1.59	1.57	1.52

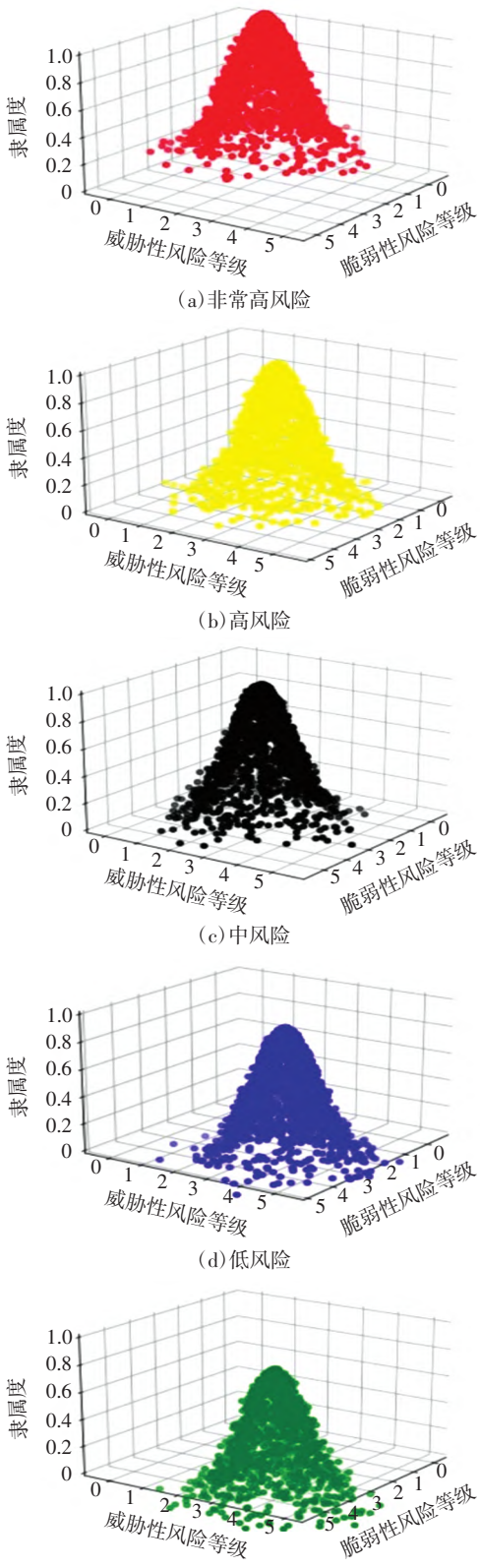
表 7　超熵

Tab.7　Hyperentropy

因素	风险等级				
	非常高	高	中	低	非常低
资产值	0.21	0.22	0.25	0.24	0.22
威胁性	0.22	0.26	0.21	0.27	0.29
脆弱性	0.23	0.25	0.26	0.23	0.28

3.2　构造多维云模型

(1)在取得各指标相应的特征值之后，在多维云模型生成代码中将威胁性和脆弱性的特征值作为输入，得到安全事件发生可能性云模型图及其隶属度矩阵(隶属度范围为 0~1)，如图 5 所示。



(a)非常高风险　(b)高风险　(c)中风险　(d)低风险　(e)非常低风险

图 5　安全事件发生可能性的云模型图

Fig.5　Cloud model diagram of the probability of security events occurring

由图 5 可知，该模型生成的云图呈现出了在不同风险等级下的指标隶属度的变化，随着风险等级的逐

渐降低,云模型的隶属度也在逐渐降低,最后生成一组代表安全事件发生可能性的隶属度矩阵

$$\boldsymbol{P}=\begin{bmatrix}0.742\,3 & 0.952\,2 & 0.431\,9 & 0.103\,6 & 0.013\,3\\ 0.038\,6 & 0.503\,9 & 0.963\,7 & 0.771\,1 & 0.338\,9\\ 0.040\,4 & 0.569\,9 & 0.963\,4 & 0.735\,5 & 0.274\,6\\ 0.011\,2 & 0.438\,8 & 0.793\,7 & 0.762\,5 & 0.338\,8\\ 0.011\,3 & 0.335\,7 & 0.807\,6 & 0.792\,3 & 0.365\,9\end{bmatrix}$$

(2)将先前获取的资产值以及脆弱性的期望、熵、超熵(E_x,E_n,H_e)作为输入,生成安全事件损失可能性的云模型图如图 6 所示。

由图 6 可知,该模型生成的安全事件损失可能性云图也呈现出了在不同风险等级下的指标隶属度的变化,随着风险等级逐渐降低,云模型的隶属度也在逐渐降低,最后生成一组代表安全事件损失可能性的隶属度矩阵

$$\boldsymbol{L}=\begin{bmatrix}0.807\,7 & 0.961\,5 & 0.596\,9 & 0.146\,6 & 0.006\,9\\ 0.121\,5 & 0.510\,7 & 0.950\,7 & 0.812\,3 & 0.247\,7\\ 0.150\,6 & 0.634\,4 & 0.957\,6 & 0.756\,7 & 0.186\,7\\ 0.083\,3 & 0.543\,8 & 0.751\,6 & 0.764\,4 & 0.262\,4\\ 0.070\,8 & 0.479\,8 & 0.703\,9 & 0.797\,6 & 0.253\,0\end{bmatrix}$$

3.3　构造总风险隶属度矩阵

根据安全事件指标量化后的特征值,生成了安全事件发生可能性的隶属度矩阵 $\boldsymbol{P}$ 以及安全事件发生损失可能性的隶属度矩阵 $\boldsymbol{L}$,通过式(8)计算总风险隶属度矩阵为

$$\boldsymbol{Z}=\begin{bmatrix}0.774\,3 & 0.956\,8 & 0.507\,1 & 0.123\,2 & 0.009\,6\\ 0.068\,5 & 0.507\,3 & 0.957\,2 & 0.753\,7 & 0.289\,7\\ 0.078\,0 & 0.601\,3 & 0.922\,3 & 0.746\,0 & 0.432\,1\\ 0.030\,5 & 0.447\,4 & 0.772\,4 & 0.763\,4 & 0.298\,2\\ 0.028\,3 & 0.401\,3 & 0.754\,0 & 0.794\,9 & 0.304\,3\end{bmatrix}$$

3.4　用熵权法计算权重

根据式(9)计算安全风险成分的熵值 F_i,并且通过式(10)计算风险成分权重,得到 $\boldsymbol{\phi}$,再根据风险分类赋值得到风险等级权重 $\boldsymbol{C}$,分别为

$\boldsymbol{\phi}$ = [0.372 6　0.193 7　0.185 7　0.103 5　0.144 5]

$\boldsymbol{C}$ = [5/15　4/15　3/15　2/15　1/15]

3.5　计算机载娱乐系统总风险值

根据式(11)计算可得系统的总风险值

$R=\boldsymbol{\phi}\cdot\boldsymbol{Z}\cdot\boldsymbol{C}^{\mathrm{T}}=0.532\,7$

计算出的风险值与风险对照表(表 2)进行对比可知,机载娱乐系统当前的风险水平为 0.532 7 处于[0.4,0.6)的区间位置,因此可以得出结论:整个机载娱乐系统在以 CNSU 为核心的风险评估当中,风险的总体测定为中等水平,因此初步判定,此时的整个系统处于一个较为安全的状态,其核心组件并未面临太大的风险。如果该系统需要增加安全性,则需要采取进一步的措施来消除潜在的风险,最终进一步降低风险值。

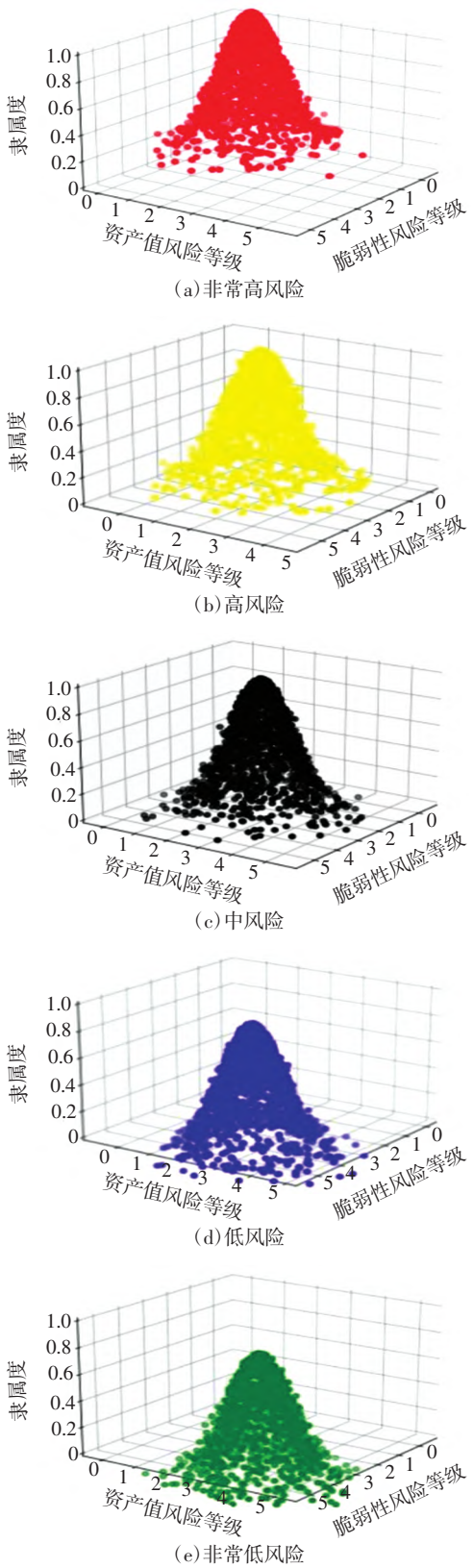


图 6　安全事件损失可能性的云模型图

Fig.6　Cloud model diagram of the probability of security events losses

3.6　实验结果对比分析

由于隶属度的生成具有一定的随机性，为了使最后的评估结果更加可靠，因此本文参照以上多维云模型与熵理论模型采用相同步骤重复进行了 5 次实验，风险值依次为 0.542 6，0.553 3，0.561 6，0.512 1，0.576 9。6 次实验的所有实验结果折线图如图 7 所示。

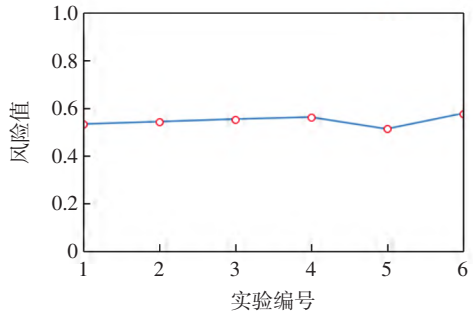


图 7　风险值走势图

Fig.7　Trend chart of risk value

由图 7 可知，在所有实验当中，本文预估的风险值均在[0.4，0.6）的区间范围内，且多次结果波动性较小，说明使用多维云模型和熵理论的评估方法，能够使最终的评估风险值具有较高的稳定性。同时本文使用的威胁指标覆盖面较广，因此能够反映出该结果具有较好的客观性，较高的可信度。因此证明多维云模型与熵理论的风险评估方法能够更加客观有效评估机载娱乐系统的风险。

4　结语

本文提出了基于多维云模型和熵理论的方法对机载娱乐系统进行安全风险评估，该方法采用了系统漏洞作为更加全面的风险评估指标，并引入了熵理论的方法来计算指标的综合权重，充分考虑了安全事件不同等级下的危害性，提高了评估的准确性和客观性。通过多维云模型的方式显示了不同风险等级下的安全水平，使评估结果更加直观。最后也通过多次实验得到了一个较为稳定的风险评估区间，有效消除了单次评估下的随机性影响。

参考文献：

[1] 施俞行，黎　明，邓　振. 基于以太网的民用飞机客舱网络架构设计[J]. 计算机系统应用，2017，26(7)：43–49.

[2] CAO Q X，YAN L F，CHEN B，et al. Enhancing network security strategies against external threats to civil aircraft[C]//2016 IEEE 18th International Conference on High Performance Computing and Communications，December 12–14，2016，Sydney，NSW，Australia. IEEE，2016：110–115.

[3] E 安全. 全球网络安全资讯新传媒：美国国土安全部远程黑掉一架波音 757 [EB/OL]. (2017–11–14)[2023–03–07]. https：//www.easyaq.com/news/1885847208.shtml.

[4] LI Y，LIU J，LI G D，et al. Airborne software testing technology analysis based on fault injection[C]//2020 IEEE International Conference on Information Technology，Big Data and Artificial Intelligence (ICIBA)，November 6–8，2020，Chongqing，China. IEEE，2020：279–282.

[5] AYUB S，PETRUNIN I，TSOURDOS A，et al. In–flight entertainment datalink analysis and simulation[C]//2020 AIAA/IEEE 39th Digital Avionics Systems Conference (DASC)，October 11–15，2020，San Antonio，TX，USA. IEEE，2020：1–10.

[6] SCOTT–HAYWARD S，GARCIA–PALACIOS E. Delivering HD video for wireless in–flight entertainment with IEEE 802.15.3c[C]//IET Irish Signals and Systems Conference(ISSC 2012)，June 28–29，2012，Maynooth，Ireland. Institution of Engineering and Technology，2012：1–6.

[7] 史　岩，朱　佳，范祥辉，等. 基于 ARINC822 的机载无线网络安全架构设计[J]. 硅谷，2014(12)：44–45.

[8] 张　双，孔德岐，李晓东. 机载系统安保风险评估方法[J]. 计算机工程与应用，2013，49(16)：232–235.

[9] 李　国，李静雯，王　静，等. 基于威胁状态的新型机载网络安全风险评估改进模型[J]. 现代电子技术，2019，42(2)：41–45.

[10] 吕宗平，戚　威，顾兆军. 基于模糊层次分析法的攻击树模型[J]. 计算机工程与设计，2018，39(6)：1501–1505，1515.

[11] DENG X H，WANG R，XU T. Risk assessment of tunnel portals in the construction stage based on fuzzy analytic hierarchy process[J]. Archives of Civil Engineering，2018，64(4)：69–87.

[12] SPANIDIS P M，ROUMPOS C，PAVLOUDAKIS F. A fuzzy–AHP methodology for planning the risk management of natural hazards in surface mining projects[J]. Sustainability，2021，13(4)：2369.

[13] AYYILDIZ E，TASKIN GUMUS A. Pythagorean fuzzy AHP based risk assessment methodology for hazardous material transportation：an application in Istanbul[J]. Environmental Science and Pollution Research，2021，28(27)：35798–35810.

[14] WU X P，FU Y，WANG J S. Information systems security risk assessment on improved fuzzy AHP[C]//2009 ISECS International Colloquium on Computing，Communication，Control，and Management，August 8–9，2009，Sanya，China. IEEE，2009：365–369.

[15] 章　亮，杨俊杰. 基于多维正态云模型的电力变压器状态评估[J]. 电测与仪表，2020，57(4)：129–135.

[16] 付　钰，吴晓平，叶　清，等. 基于模糊集与熵权理论的信息系统安全风险评估研究[J]. 电子学报，2010，38(7)：1489–1494.

[17] 赵　刚，吴天水. 结合灰色网络威胁分析的信息安全风险评估[J]. 清华大学学报(自然科学版)，2013，53 (12)：1761–1767.

[18] 郭戎潇，夏靖波，董淑福，等. 一种基于多维云模型的多属性综合评价方法[J]. 计算机科学，2010，37(11)：75–77.

[19] Airlines Engineering Committee. Digital information transfer system (DITS)：ARINC 429[S]. New York：Airlines Engineering Committee，1977.

[20] 国家市场监督管理总局，国家标准化管理委员会. 信息安全技术　信息安全风险评估方法：GB/T 20984—2022[S]. 北京：中国标准出版社，2022.

（责任编辑：明　月）