·信息安全技术·

**熵权法和神经网络的信息系统安全评价模型**

顾兆军1，辛倩2

（1．中国民航大学，信息安全测评中心，天津 300300；

2．中国民航大学 计算机科学与技术学院，天津 300300）

**摘 要：**为了提高信息系统安全评价的准确性，提出一种将熵权法和神经网络相结合的信息系统安全评价模型（熵权-BP）。该模型采用熵权法计算评价指标权重，避免了主观方法确定指标权重的随意性和不确定性，并筛选出权重较大的评价指标传递到BP神经网络中，提高它对知识的学习能力。通过BP神经网络非线性的分析处理评价指标数据，得到评价结果。采用民航信息系统评价数据进行实验，结果表明，与其他同类型评价模型相比，该模型提高了信息系统安全评价的精度，评级结果可以为系统管理员提供科学的参考依据。

**关键词：**信息系统 熵权法 神经网络 评价模型 主观方法 非线性

**中图法分类号：** TP393.08 **文献标识码：**A **DOI:**

Information System Security Evaluation Based on Entropy Method and Neural Network,

Zhao Jun Gu1, Qian Xin2

(1．Information Security Evaluation Center, Civil Aviation University of China, Tianjin 300300;

2. college of Computer Science and Technology, Civil Aviation University of China, Tianjin 300300）

**Abstract:** In order to improve the accuracy of information system security evaluation, an information system security evaluation model (entropy weight -BP) combining entropy weight method with neural network is proposed. The entropy method is used to calculate the weight of the evaluation index, which avoids the subjective method to determine the randomness and uncertainty of the index weight, and selects the evaluation index with large weight to be passed into the BP neural network to improve its learning ability. The evaluation data were evaluated by BP neural network nonlinear analysis and the evaluation results were obtained.The experiment was carried out using the civil aviation information system evaluation data. The results show that the model improves the accuracy of information system security evaluation compared with other types of evaluation model

**Key words:** information system; entropy weight method; neural network evaluation model; subjective method; nonlinearity

# 引言

随着各行各业对信息系统的依赖程度日益增加，一些重要的信息系统已经成为国家重点保障的关键信息基础设施。然而国内外连续不断地出现比较严重的信息系统安全事故，如浙江温州有线电视网络系统被黑客攻击，乌克兰电力信息系统遭受恶意代码攻击，尤其是最近刚爆发的全球大规模蠕虫勒索软件感染事件等等，这些安全事故将会给企业甚至国家带来无法估计的损失和影响。因此，信息系统的安全状况成为人们当前关注的主要问题，如何准确地评价信息系统的安全状况对保障信息系统安全具有重要的研究价值和意义。

信息系统安全评价方法主要分为定性评价方法、定量评价方法和综合评价方法。由于影响信息系统的安全因素难以量化，大多数学者采用层次分析法、熵权法、模糊理论、故障树等[1,4]定性与定量相结合的综合评价方法建立信息系统安全评价模型，但这些方法计算复杂、评价结果受主观因素影响较大。为了避免这些问题，国内外学者采用DS证据理论[5]、支持向量机[6]、神经网络[7]、贝叶斯网络[8]等人工智能算法构建信息系统安全评价模型，取得了较好的评价结果。de Gusmão A P H [9]使用事件树分析与模糊决策理论相结合，通过专家鉴定，确定场景和事件的，模糊评估和排序这一系列步骤对信息安全进行分析，但在确定事件发生时没有统一的方法，导致不同方法设置事件发生的概率不同；马丽仪[10]等人采用模糊神经网络评价信息系统的安全风险，将风险因子进行模糊化后输入到神经网络训练，提高了神经网络对模糊性的识别能力，但隶属度矩阵和权重均采用专家评判，客观性较差，在一定程度上影响整个模型的实用性；赵保华[11]采用层次分析法和神经网络构建信息系统风险评价模型，层次分析法确定评价指标重要性时完全依赖评价者的主观判断，可能会误剔重要指标，而且评价指标较多容易出现残缺判断矩阵。赵刚[12]等人使用熵权法计算指标权重，使模糊合成中的权重更加客观，但是当信息系统有较多不确定因素时，缺乏学习和自适应能力。

为了进一步提高评价的准确性，针对信息系统的安全影响因素较多、因素之间相互可能相互影响、变化性等特点，本文提出熵权法和BP神经网络（Back-Propagation Neural Network）相结合的信息系统安全评价方法（熵权-BP），并采用具体的实例验证模型的有效性。

# 1 熵权法和BP神经网络理论

## 熵权法简介

在信息系统安全评价时，各评价指标在整个评价体系中的重要程度不同，指标权重的设定是否合理直接会影响评价结果的准确性。权重赋值的方法主要有专家咨询法、德尔菲法、层次分析法和熵权法等，其中专家咨询法、德尔菲法、层次分析法属于主观赋权法，主观随意性较大，而熵权法属于客观赋权法，根据各评价指标的变异度，利用信息熵计算得到权重，从而得到较为客观的指标权重，避免了主观方法确定指标权重的严重缺陷，使指标权重更具有科学性和说服力。

## 1.2 BP神经网络理论

BP神经网络即误差反向传播神经网络，具有较强的自学习和自适应能力，目前被广泛用在综合评价领域。BP神经网络可以处理“多输入-多输出”高度非线性的映射。BP神经网络通过输入信息号正向计算误差和反向调整网络权值和阈值这两个阶段不断的交替进行，神经网络就会获得不断的学习机会。当误差信号减到预定值或学习次数达到最大规定次数，学习过程结束，此时BP神经网络内部已经存储了大量的学习知识。

# 2 熵权-BP神经网络信息系统安全评价模型的设计

## 2.1构建评价指标体系

评价信息系统的安全状况首先是构建评价指标，即信息系统的安全影响因素。安全影响因素的选取是否科学合理，直接影响评价结果的真实性。目前，信息系统安全评价主要是根据《信息安全技术 信息系统安全等级保护测评要求》[13]，从技术和管理两大层面构建了递阶层次结构的信息系统安全评价指标体，如图2所示。



图1 信息系统安全评价指标体系

## 2.2 熵权法确定指标权重

由于不同信息系统的评判专家可能不同，受专家主观因素影响，同一指标在不同信息系统的权重可能也不同。因此，本文根据各评价指标在不同信息系统的变异度，采用信息熵计算出各评价指标的权重。

2.2.1构建评价指标矩阵

从已评价的信息系统中筛选*m*个具有代表性的信息系统，与*n*个评价指标形成矩阵***R***=(*rij*)*nm*：

 (1)

其中*rij*(*i*=1,2,..,*n*;*j*=1,2,…,*m*)为第*j*个信息系统的第*i*个指标的实际评价结果值。

2.2.2 计算评价指标的权重

1）根据2.2.1节构建的评价指标原始数据矩阵***R***，计算第*i*个评价指标下第*j*个信息系统的评价指标值的比重*pi*j。

 (2)

2）计算第*i*个评价指标的熵值*ei*

  (3)

由熵的极值性可知，若某评价指标*i*的熵*ei*越小，说明该评价指标在不同信息系统中的变异程度越大 ，提供的信息量越多，在综合评价中起的作用就越大，其权重也应该越大。

3）用ln(m)对各评价指标的熵值进行归一化处理：

 (4)

4）引入差异系数1*-ei* 来正向度量评价指标*i*的熵值，得到评价指标*i*的权重：

 (5)

## 2.3 熵权-BP神经网络结构的构建

为了避免BP神经网络在学习过程中出现过拟合，采用熵权法筛选出权重相对较大的评价指标作为BP神经网络的输入，降低BP神经网络的输入维数，提高评价指标的质量，从而提高BP神经网络的学习能力。熵权-BP神经网络结构如图3所示：



图2 熵权-BP神经网络结构

图中*u*表示指标体系的所有评价指标，*x*表示权重较大的评价指标，*y*表示隐含层神经元的输出，*z*表示输出层神经元的网络输出值。*wij*和*wj*分别为传递层到隐含层与隐含层到输出层之间的连接权值。*l、n*和*m*分别比为输入层、传递层和隐含层神经元的个数。

参照上图，熵权-BP神经网络建模过程：

**Step1：**第1层为输入层，其神经元的个数为信息系统安全评价指标体系的14个评价指标；

**Step2：**第2层为指标筛选层，通过构造评价指标矩阵采用熵权法计算第1层评价指标的权重，并选取其中权重较大的评价指标；

**Step3：**第3层为传递层，将第2层选取出权重较大的评价指标传递到BP神经网络中；

**Step4：**第4层为隐含层，主要处理评价指标到评价结果间的非线性映射，隐含层神经元个数的选取是BP神经网络学习成功的关键，借助经验公式：

 (6)

式中：*n*表示传递层神经元个数，*β*∈[1,10]的常数。

**Step5：**第5层是输出层，根据实际需要只设定一个神经元，代表信息系统安全评价结果。

此时，熵权-BP神经网络建模已完成，接下里就是第3层到第4层之间的权值与第4层到第5层之间的权值的学习过程。

## 2.4 BP神经网络学习算法

如图3所示，传递层神经元用*i*表示，隐含层神经元用*j*表示。给定*h*组样本的输入和输出分别为：***X***=(***X***1,***X***2,…,***X***3)*T*=(***Xpi***)*h*×*n*、***z’p***=( *z’*1, *z’*2,…, *z’h*) (*p*=1,2,…,*h*)。

BP神经网络学习过程：

（1）随机选取BP神经网络的偏置值以及权值*wij*和*wj*；

（2）BP神经网络隐含层和输出层样本*p*的正向传递：

 (7)

 (8)

 (9)

式中，*θj*表示隐含层神经元*j(j=*1,2,…,*m)*的偏置值，*θ*表示输出层神经元的偏置值；

（3）使用α-η联合算法，反向修正BP网络权值和偏置值：

 (10)

 (11)

 (12)

式中，*f’*为对*f*求导，*η*∈(0,1)为学习速率，加快网络的收敛速度；*α*∈(0,1)为动量因子，避免BP网络陷入局部最优。

（4）*h*组样本拟合误差函数为：

 (13)

 (14)

（15）

式中，*ε*为误差精度，满足(0≤*ε*<1)；当网络误差达到精度要求或者达到学习的最大次数*T*(*t*≤*T*)，BP网络学习过程结束，否则转向步骤2)，继续学习直到满足条件为止。

# 2.5 熵权-BP神经网络信息系统安全评价过程

根据信息系统安全等级保护测评要求建立评价指标体系并搜集已完成安全评价的信息系统数据；采用熵权法利用评价指标原始数据矩阵计算得到更客观的评价指标权重；对评价指标按权重大小进行排序，筛选出权重相对较大的评价指标作为BP神经网络的输入； BP神经网络通过反向调节神经元之间的权值和正向计算误差得到最优的信息系统安全评价模型；最后利用测试样本检验熵权-BP模型的性能，得到信息系统安全评价结果。熵权-BP模型评价过程如1图所示：



图3 熵权-BP模型评价过程

# 3 实例研究

## 3.1 数据来源

本文收集民航已完成安全测评的30个信息系统作为样本数据，如表1。选择前22个作为熵权-BP模型的训练样本，其余8个作为测试样本，测试熵权-BP模型的安全评价效果。

表1 信息系统安全评价数据

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 样本编号 | *u1* | *u2* | *u3* | *u4* |  | *u14* | *z* |
| 1 | 68.4 | 59.43 | 68.43 | 62.7 |  | 80.97 | 0.754 |
| 2 | 75.4 | 65.2 | 75.67 | 82.84 |  | 84.62 | 0.813 |
| 3 | 61.64 | 62.59 | 75.11 | 65.8 |  | 87.37 | 0.676 |
| 4 | 69.28 | 59.66 | 72.35 | 60.27 |  | 76.87 | 0.755 |
| 5 | 70.16 | 73.53 | 75.36 | 72.66 |  | 68.25 | 0.716 |
| 6 | 91.93 | 67.29 | 63.4 | 82.24 |  | 78.72 | 0.832 |
|  |  |  |  |  |  |  |  |
| 30 | 63.42 | 65.9 | 61.25 | 71.23 |  | 63.86 | 0.677 |

## 3.2 筛选重要的评价指标

1）使用已完成安全评价的30组评价指标数据形成一个原始数据矩阵***R***,即



2）通过2.2.2节的计算步骤，得出各评价指标的权重*W*=(*w1*,*w2*,…,*w14*)：

***W***=(0.17,0.008,0.006,0.24,0.02,0.03,0.17,0.1,0.04,0.01,0.05,0.09,0.08,0.06)

对评价指标权重进行排序，权重小于0.05的评价指标值的改变对整个评价结果几乎没有影响，故将其剔除，剩下8个权重较大的评价指标 ：

***W’***=(0.24,0.17,0.17,0.1,0.09,0.08,0.06,0.05)

## 3.3 熵权-BP神经网络模型训练

设定样本训练的学习率*η*为0.5，动量因子*α*为0.3，最大学习次数*T*为6000，拟合误差*ε*为0.0001。将权重较大的评价指标数据采用最大最小法归一化处理后输入到BP模型中进行学习训练，当训练4000次时，拟合误差为0.000237，此时熵权-BP模型已达到拟合误差要求。为了比较熵权-BP模型与BP模型的学习能力，同时对两个模型进行训练，其收敛对比曲线如图4所示。

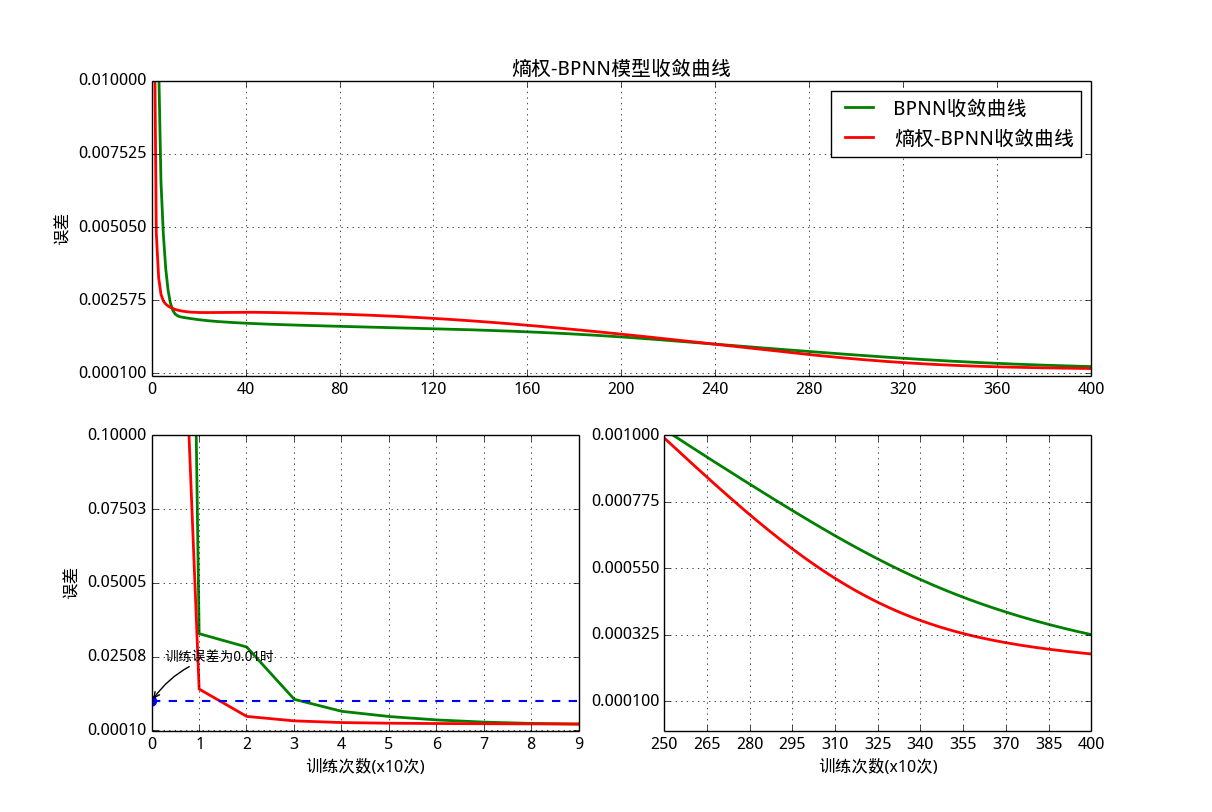


图4 BP神经网络训练集的收敛过程

由图4可知，熵权-BP模型在训练初期的收敛效果明显比单纯使用BP神经网络的效果好。当训练次数达到30次时，误差已经接近0.001，而BP神经网络需要迭代60次才能达到相同的误差，同时，当训练次数从2500-4000次时，熵权-BP模型的收敛速度也明显比BP模型快，最终训练完成后熵权-BP模型得到的误差为0.000237，而BP模型的误差为0.000325，精度提高了37.13%。

训练结果表明，熵权-BP模型通过对筛选出8个权重较大的评价指标样本数据进行训练，可以有效的减少迭代次数，并快速收敛到设定的误差，既可以提高BP神经网络的训练速度，又能保留重要指标的特征，减少非重要指标对BP神经网络模型的干扰，提高BP神经网络评价模型的准确度。

## 3.4 熵权-BP神经网络模型检验

将测试样本分别输入到BPNN、AHP-BP和熵权-BP模型中得到信息系统的网络输出值与实际值的对比关系如图5所示，同时表2给出了各模型的信息系统的安全评价精度，可以得到以下结论:

（1）组合的熵权-BP和AHP-BP模型的评价精度高于单一BPNN模型的评价精度，因为这两种组合模型都对评价指标进行了重要性筛选，使得BP神经网络在反向传播过程中更加逼近真实权值。

（2）熵权-BP模型的评价精度高于AHP-BP模型的评价精度，因为熵权-BP模型通过样本数据计算得到指标的权重，更加客观、真实的反映评价指标的权重，而AHP-BP模型通过专家构造判断矩阵计算指标权重，指标的权重受主观因素影响较大，可能会误删除重要的指标。

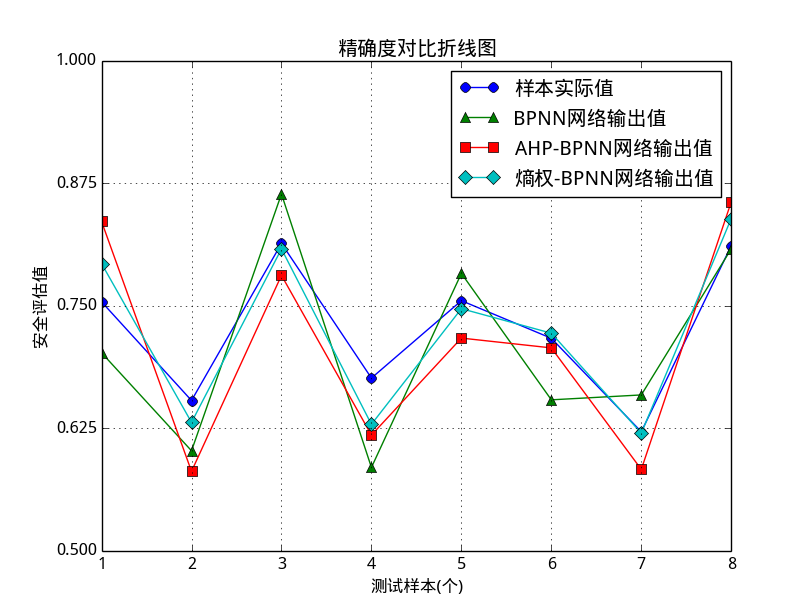


图5 各模型的网络输出值和期望值之间的对比

表2 各模型的信息系统安全评价精度对比

|  |  |
| --- | --- |
| 模型 | 评价精度/% |
| BPNN | 86.72 |
| AHP-BP | 91.39 |
| 熵权-BP | 96.41 |

# 4 结束语

为提高评价结果的准确性，笔者将熵权法和神经网络相结合，提出了熵权-BP神经网络的信息系统安全评价模型。采用熵权法计算各评价指标的权重，筛选出权重较大的指标，提高了评价指标的质量，降低了BP神经网络的输入维数，同时结合具有高度非线性处理能力的BP神经网络，解决了各评价指标之间的相互影响，弥补了传统评价方法无法处理非线性关系的不足。该模型推进了信息系统安全评价的研究，有深厚的理论基础和实用价值。不过本文的安全评价指标体系只是从等保测评中选取了具有代表性的几大类安全影响因素，而每类因素还包括许多具体的测评项，不同安全等级的信息系统每个因素的测评项可能会有些许不同。后续需要对各类因素进行细分，是评价结果能够为系统管理员提供更有效的参考依据。

# 参考文献

1. Zhang L, Peng J, Du Y, et al. Information security risk assessment survey[J]. Journal of Tsinghua University Science and Technology, 2012, 52(10): 1364-1369. (in Chinese) [张利, 彭建芬, 杜宇鸽, 等. 信息安全风险评估的综合评估方法综述[J]. 清华大学学报: 自然科学版, 2012, 52(10): 1364-1369.]
2. Gu Z, Han Y. Quantifiable information system security level evaluation[J]. Computer Engineering and Design, 2016, 37(7): 1729-1733. (in Chinese) [顾兆军, 韩迎亚. 可量化的信息系统安全水平评估[J]. 计算机工程与设计, 2016, 37(7): 1729-1733.]
3. Rosqvist T, Molarius R, Virta H, et al. Event tree analysis for flood protection—An exploratory study in Finland[J]. Reliability Engineering & System Safety, 2013, 112: 1-7.
4. Lin Y. Research on Information System Security Risk Assessment Modeling and Application[D]. Dalian: Dalian Maritime University, 2013.(in Chinese) [林洋. 信息系统安全风险评估模型及其应用研究[D]. 大连: 大连海事大学, 2013.]
5. Shi B, Xie X Q. Research on network security situation forecast method based on D-S evidence theory[J]. Computer Engineering and Design, 2013, 34(3): 821-825.(in Chinese) [石波, 谢小权. 基于 DS 证据理论的网络安全态势预测方法研究[J]. 计算机工程与设计, 2013, 34(3): 821-825.
6. Wu L. Risk Analysis of the Information System by Using Factor Analysis and Support Vector Machine[J]. Microelectronics and Computer, 2016, 33(2): 144-148.(in Chinese) [伍浏阳. 因子分析和支持向量机的信息系统风险评价[J]. 微电子学与计算机, 2016, 33(2): 144-148.]
7. Gao N, Gao L, He Y, et al. Dynamic Security Ｒisk Assessment Model Based on Bayesian Attack Graph[J]. Journal of Sichuan University: Engineering Science Edition, 2016, 48(1): 111-118(in Chinese) [高妮, 高岭, 贺毅岳, 等. 基于贝叶斯攻击图的动态安全风险评估模型[J]. 四川大学学报: 工程科学版, 2016, 48(1): 111-118.]
8. Yu F, Xiaoping W, Jia-Sheng W. An approach to information systems security risk assessment based on fuzzy-combinatorial neural network[J]. Journal of Naval University of Engineering, 2010, 1: 18-23. (in Chinese) [付钰, 吴晓平, 王甲生. 基于模糊-组合神经网络的信息系统安全风险评估[J]. 海军工程大学学报, 2010 (1): 18-23.]
9. de Gusmão A P H, e Silva L C, Silva M M, et al. Information security risk analysis model using fuzzy decision theory[J]. International Journal of Information Management, 2016, 36(1): 25-34.
10. Ma L Y, Zhang L F, Yang Y, et al. Evaluation of information system security risk based on fuzzy neural network method[J]. Zhongguo Anquan Kexue Xuebao, 2012, 22(5): 164-169. (in Chinese) . [马丽仪, 张露凡, 杨宜, 等. 基于模糊神经网络方法的信息系统安全风险评价研究[J]. 中国安全科学学报, 2012, 22(5): 164-169. ]
11. Zhao B. Risk Evaluation of Information System Security Based on Neural Network and Analytic Hierarchy Process[J]. Microelectronics and Computer, 2015, 32(10): 163-166. (in Chinese) [赵保华. 层次分析法和神经网络的信息系统风险评估[J]. 微电子学与计算机, 2015, 32(10): 163-166.]
12. Zhao G, Liu H. Practical risk assessment based on multiple fuzzy comprehensive evaluations and entropy weighting[J]. Journal of Tsinghua University Science and Technology, 2012, 52(10): 1382-1387. (in Chinese). [赵刚, 刘换. 基于多层次模糊综合评判及熵权理论的实用风险评估[J]. 清华大学学报: 自然科学版, 2012, 52(10): 1382-1387.]
13. 2012 GBT. Information security technology - Information system security level protection evaluation requirements[S][D]. (in Chinese) [2012 G B T. 信息安全技术-信息系统安全等级保护测评要求 [S][D].

**作者简介：**

顾兆军(1966-)，男，山东蓬莱人，博士，教授，研究方向为网络与信息安全、民航信息系统；

通讯作者：辛倩(1992-)，女，山西省大同市人，硕士研究生，研究方向网络与信息安全、民航信息系统。

# 联系方式：

联系人：辛倩  
联系电话：13516169009

E-mail:13516169009@163.com  
邮编：300300  
地址： 天津市东丽区津北公路2898号中国民航大学北院48号信箱