

# 基于综合云的移动自组织网络信息安全评估

程华福, 郑越峰, 邹凯, 陈彦龙

(国网信息通信产业集团有限公司信息通信共享服务分公司, 北京 102211)

**摘要:** 大数据的复杂性让以单一权重为主的信息安全评估过程, 易受信息差异性、不均衡性等问题的干扰, 评估效率较低, 为此提出基于综合云的移动自组织网络信息安全评估方法。采用改进k均值聚类算法对移动自组织网络信息实行聚类处理, 降低信息之间的差异性; 采用组合权重算法得到网络信息的综合权重, 解决单一权重不均衡的问题; 将综合权重与云模型生成的逆向云相结合得到综合云, 通过计算相似性, 完成移动自组织网络信息的安全评估。测试结果显示, 设计的信息安全评估方法的评估时间短、评估误差小。

**关键词:** 信息聚类; 判断矩阵; 评估指标; 正则化运算; 信任数字特征集; 风险值

中图分类号: TP393 文献标识码: A 文章编号: 1003-7241(2025)05-0066-05

## Information Security Evaluation of Mobile ad Hoc Network Based on Integrated Cloud

CHENG Hua-fu, ZHENG Yue-feng, ZOU Kai, CHEN Yan-long

(Info & Telecom Shared Service Branch, State Grid Info & Telecom Group, Beijing 102211 China)

**Abstract:** The complexity of big data makes the information security assessment process based on single weight vulnerable to the interference of information differences, imbalance and other issues, and the assessment efficiency is low. Therefore, a mobile ad hoc network information security assessment method based on comprehensive cloud is proposed. The improved k-means clustering algorithm is used to cluster the information in mobile ad hoc networks to reduce the difference between the information; The combined weight algorithm is used to obtain the comprehensive weight of the network information to solve the problem of unbalanced single weight; The comprehensive cloud is obtained by combining the comprehensive weight with the reverse cloud generated by the cloud model. The security assessment of mobile ad hoc network information is completed by calculating the similarity. The test results show that the evaluation time of the designed information security evaluation method is short and the evaluation error is small.

**Keywords:** information clustering; judgment matrix; evaluation metrics; regularization operation; trust digital feature set; value at risk

### 0 引言

随着大数据时代的来临, 移动自组织网络信息被广泛应用于数据处理<sup>[1]</sup>、制造业、自动化等领域。信息智能化为我们的生活提供巨大便利的同时, 也存在信息贩卖、隐私泄露等弊端。因此网络信息安全的评估一直是相关工作人员的关注重点。国内外学者在网络信息安全评估方面研究投入较多, 不仅在基础电子设备的防护上做出相关对应战略, 也在评估网络信息安全的技术研发等方面设计了有效的应对方案。

刘道远<sup>[2]</sup>等人首先采用Delphi压缩法计算出移动自组织网络信息中的权重系数, 找出权重系数最大的信息点, 对其做加固处理, 最后将模糊二级评判算法投入到信息中, 完成移动自组织网络信息的安全评估。赵冬梅<sup>[3]</sup>

等人首先将信息分离技术和深度解析技术相融合, 得到具备三层组合单元的神经网络模型, 然后用三维矩阵表达移动自组织网络信息, 并输入到模型中, 最后采用时间因子构建关于信息的安全空间映射, 完成移动自组织网络信息安全的评估。李佳玮<sup>[4]</sup>等人首先利用粗糙集和辨别函数将移动自组织网络信息简约化, 然后通过GEP算法提高小生境模型的计算速度, 最后将信息输入到模型中, 通过遗传算法完成移动自组织网络信息的安全评估。

以上方法的信息安全评估过程以单一权重为主, 评估复杂性较高的大数据时, 易受信息差异性、不均衡性、冗余性等问题的干扰。为了解决上述方法中存在的问题, 提出基于综合云的移动自组织网络信息安全评估方法。

### 1 移动自组织网络信息聚类与综合权重

#### 1.1 移动自组织网络信息的聚类处理

\*基金项目: 北京市国网信息通信创新科研项目(2020GX004519)

收稿日期: 2023-10-18

采用改进k均值算法对移动自组织网络信息聚类处理<sup>[5]</sup>,使属于同一类别的信息之间的距离无限缩小,为网络信息安全评估过程打下基础。具体步骤如下:

(1) 将移动自组织网络信息作为待聚类处理的样本,从其中任意挑选几个信息点作为第一轮聚类的中心点,公式如下所示:

$$\begin{cases} A = [(a_i, b_i) | i = 1, 2, \dots, c_n^3] \\ c = [(c_{a_i}, c_{b_i}) | i = 1, 2, \dots, l] \end{cases} \quad (1)$$

式中,  $A$  代表的是异性自组织网络样本集合;  $a_i, b_i$  均表示集合中的第  $i$  个样本点;  $c$  为聚类中心;  $l$  代表的是初始聚类个数;  $n$  为样本点的数量;  $c_n^3$  为待聚类的样本。

(2) 计算出剩余移动自组织网络信息样本点与各个聚类中心点之间的距离  $d$ , 并标记出与聚类中心距离最短的信息点, 再将该信息点调拨到新的聚类计算中。公式如下所示:

$$\begin{cases} d = \{d_{ij} | i = 1, 2, \dots, (c_n^3 - l); j = 1, 2, \dots, l\} \\ 1 \leq i \leq (c_n^3 - l) \\ 1 \leq j \leq l \end{cases} \quad (2)$$

式中,  $d_{ij}$  为第  $i$  个点与第  $j$  个点之间的距离。

(3) 基于综合云的信息安全评估方法, 将所有的样本点都投入到新一轮的聚类过程中, 以形成不同层次的聚类。其中任意聚类都包含原始的聚类中心点。然后利用如下公式计算更新后的聚类中心点, 直到找出所有聚类的新聚类中心。

$$\begin{cases} A_{a_i}' = \left(\frac{1}{l_i}\right) \sum a_i \\ A_{b_i}' = \left(\frac{1}{l_i}\right) \sum b_i \\ A' = \{(A_{a_i}', A_{b_i}') | i = 1, 2, \dots, l\} \end{cases} \quad (3)$$

式中,  $A', A_{a_i}', A_{b_i}'$  均代表更新后的聚类中心。

(4) 当任意两个相邻的聚类中心点不再发生变动时, 代表此时已完成最终聚类, 得到移动自组织网络信息的聚类结果。否则返回步骤(2)继续计算。公式如下所示:

$$\begin{cases} 0 & A = A' \\ 1 & \text{otherwise} \end{cases} \quad (4)$$

由此完成网络信息的聚类处理。为了提高评估效率, 需要对信息权重进行融合。

## 1.2 基于组合权重的综合权重生成

得到聚类后的移动自组织网络信息后, 采用组合权重算法将网络信息的主、客观权重融合到一起, 得到综合权重, 具体步骤如下:

(1) 引入判断矩阵<sup>[6]</sup>, 确定矩阵中的最大特征值  $\alpha_{\max}$ , 以及  $\alpha_{\max}$  对应的特征向量, 然后计算出移动自组织网络信息的主观权重, 公式如下所示:

$$\begin{cases} O = [e_{pq}]_{m \times m} \\ w_i = \frac{\alpha_{\max}}{\sum_{p=1}^m \alpha_{\max}} \\ p, q = 1, 2, \dots, m \end{cases} \quad (5)$$

式中,  $O$  表示引入的判断矩阵;  $e$  代表评估指标之间的判断性;  $w_i$  表示移动自组织网络信息的主观权重;  $p, q$  均表示评估指标;  $m$  表示的是指标的数量。

(2) 由评估指标构成的矩阵称之为指标信息矩阵, 对其实行常量纲化与正则化<sup>[7]</sup>处理, 可以降低逆向指标的冗余量, 公式如下所示:

$$\begin{cases} u_\alpha = \frac{v_\alpha}{v'} \\ s_\alpha = 1 - u_\alpha \end{cases} \quad (6)$$

式中,  $u_\alpha$  代表经过无量纲化处理后的指标;  $v_\alpha$  表示各指标代表的信息;  $v'$  表示规定指标的数值;  $s_\alpha$  表示的是正则化处理后的指标。

(3) 经过无量纲化与正则化计算后的评估值, 计算出指标的信息熵  $g$  与升级因子  $k$ 。再通过信息熵与变异系数得到移动自组织网络信息的客观权重  $w_2$ , 公式如下所示:

$$\begin{cases} g = -r \sum_{\alpha=1}^m s_\alpha \ln s_\alpha \\ k = 1 - g \\ w_2 = \frac{k}{\sum_{\alpha=1}^m k} \end{cases} \quad (7)$$

式中,  $r$  表示一般常数,  $\alpha$  为网络信息特征值。

(4) 组合权重法将主观权重与客观权重相结合, 得到移动自组织网络信息的综合权重  $w$ , 公式如下所示:

$$\begin{cases} w = w_1 \times x + w_2 \times y \\ x \neq y \neq 0 \end{cases} \quad (8)$$

式中,  $x, y$  分别表示权重系数。

## 2 网络信息安全评估方法设计

将上节获得的综合权重与逆向云相结合得到综合云, 再计算出综合云与评价云之间的相似性, 最终与风险值结合, 实现网络信息的安全评估, 具体步骤如下:

(1) 逆向云生成

1) 当移动自组织网络信息的安全评估指标个数为  $m$  个时, 设其对应属性的数量为  $o$ , 则云模型生成的逆向云  $RC$  对应的信任数字特征集合可用  $\{Ex_1, Ex_2, \dots, En_1, En_2, \dots$

$He_1, He_2, ]$ 表示,计算其中的信任隶属度<sup>[8-10]</sup>与样本均值,公式如下所示:

$$\begin{cases} \beta = m \frac{2 \ln(\frac{1}{2})}{o} \\ \bar{a} = \frac{\sum_{i=1}^o \left[ a_i \left( \beta + \frac{1}{2} \right) \right]}{o} \end{cases} \quad (9)$$

式中,  $Ex_o, En_o, He_o$ 分别代表逆向云的期望值、计算熵、超级熵;  $a_i$ 代表第  $i$  个信息样本点;  $\beta$  代表的是信任隶属度;  $\bar{a}$  为样本均值。

2) 其中,逆向云的计算熵与超级熵的计算公式如下所示:

$$\begin{cases} En_o = \sqrt{\frac{\sum_{i=1}^o (a_i - Ex_o)^2}{o-1}} \\ He_o = \sqrt{\frac{\sum_{i=1}^o (En_o - En_o')^2}{o-1}} \end{cases} \quad (10)$$

式中,  $En_o'$  代表的是计算熵的标准值。

(2) 获取综合云与评价云

1) 由于在信息安全评估过程中,移动自组织网络信息的各个属性都存在一定差异,所以云模型需要根据逆向云的数字特征以及综合权重得到更新后的综合信任云<sup>[11-12]</sup>,公式如下所示:

$$\begin{cases} Ex = \sum_{i=1}^o (Ex_o \cdot w) \\ En = \sqrt{\sum_{i=1}^o (En_o \cdot w)} \\ He = \sum_{i=1}^o (He_o \cdot w) \end{cases} \quad (11)$$

式中,  $Ex, En, He$  分别表示综合云的期望值、计算熵、超级熵。

2) 在云模型中构建关于移动自组织网络信息安全评估的评价云。评价云主要由三个一级指标与六个二级指标构成,结构如图1所示。

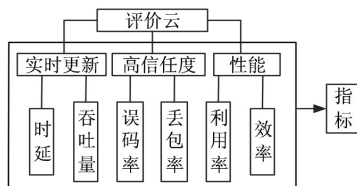


图1 评价云结构

(3) 相似度计算

1) 在评价云和综合云中随机生成若干个正态随机数,计算出二者之间的隶属度,用  $\beta'$  表示。公式如下所示:

$$\beta' = m \frac{(a - En_2)^2}{2(En_2)^2} \quad (12)$$

2) 重复生成正态随机数,直到形成  $o$  个隶属度,可以得到综合云与评价云之间的相似度  $\chi$ ,公式如下所示:

$$\chi = \frac{\sum_{i=1}^o \beta'}{o} \quad (13)$$

3) 根据式(13)得到的相似度以及风险值,并根据规则库中的先验知识判断当前网络信息的安全等级,然后给出安全指示或者由于风险过大的预警指示,完成移动自组织网络信息的安全评估。其中风险值的计算公式如下所示:

$$S = (P, E) = \sum_{i=1}^o G \cdot w \quad (14)$$

式中,  $S$  为风险值;  $P$  表示风险发生概率;  $E$  为风险导致的效果;  $G$  为风险等级。

由此完成移动自组织网络信息安全评估。

### 3 实验与分析

为了验证基于综合云的移动自组织网络信息安全评估方法的整体有效性,需要对其做出如下测试。

将各个方法评估所消耗的运行时间与评估误差作为评价指标,采用基于综合云的移动自组织网络信息安全评估方法、文献[2]方法、文献[3]方法和文献[4]方法完成对比测试,对比方法均为常规单一权重计算方法,与其对比可以检验本文的组合权重评估方法的性能。

(1) 运行时间

自主开发并搭建模拟实验台,为各个方法的安全评估测试提供硬件基础与软件条件。其中实验参数设置如表1所示。测试数据来自2021年辽宁省某运营公司提供的移动自组织网络云平台信息,将安全风险等级划分为高、较高、中、低、较低五个等级。

表1 实验参数

硬件/软件	型号	数量	详细参数
CPU	Inter6-7600	1	Core(TM)i6
操作系统	Centos8	1	Windows 7
内存	Python	1	64 GB
实验环境		1	4.0
编辑器	Pycharm	1	Community2021.1
开源代码	Tensorflow	1	1.14.0
采集卡	NNI-254	1	供电电压:30 V

利用所提方法、文献[2]方法、文献[3]方法安全评估15组移动自组织网络信息。

应用本文所提方法根据云数字特征值在云模型中构建关于移动自组织网络信息的安全综合评估云,结果如

图2所示。利用评估云完成风险评估。

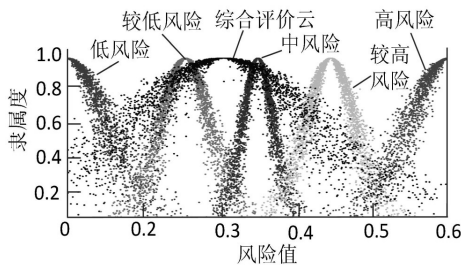


图2 综合评价云

对比不同方法的评估运行时间。运行时间越长,说明方法的评估效率越低;运行时间越短,说明方法的评估效率越高。不同方法的测试结果用表2表示。

表2 不同方法的运行时间

实验次数/组	运行时间/s		
	法方提所	法方[2]献文	法方[3]献文
1(较低风险)	43	52	64
2(较低风险)	46	57	68
3(较低风险)	47	60	73
4(低风险)	48	63	78
5(低风险)	48	68	81
6(低风险)	49	72	86
7(中风险)	51	77	94
8(中风险)	53	81	106
9(中风险)	54	86	114
10(高风险)	62	91	127
11(高风险)	65	95	134
12(高风险)	65	99	157
13(较高风险)	68	102	164
14(较高风险)	68	113	173
15(较高风险)	69	126	196

分析表2可知,针对移动自组织网络信息的安全评估,在五个不同的风险等级中,所提方法的评估运行时间均低于文献[2]方法与文献[3]方法的评估运行时间。说明所提方法的评估效率高于文献[2]方法与文献[3]方法的评估效率。并且随着风险等级的不断增加,所提方法的评估运行时间增长缓慢,而文献[2]方法与文献[3]方法的运行时间增长幅度较大。

这是因为所提方法在移动自组织网络信息安全评估过程中,采用改进k均值算法对网络信息做出了聚类处理。预处理后的网络信息中属于同一类别的信息之间的距离无限缩小,进而降低了信息的差异性与冗余性,最为关键的是,本文方法设计了综合权重模式,提高了方法的评估运行时间。

#### (2) 评估误差

在实验(一)的基础上,利用所提方法、文献[3]方法与文献[4]方法安全评估6组移动自组织网络信息,对比不同

方法挖掘到的风险信息(测试值)与风险实际值相比较,得到测试值曲线与真实值曲线的相交面积。相交面积越大,表明方法的评估误差越大;相交面积越小,表明方法的评估误差越小。

测试结果分别用图3表示。

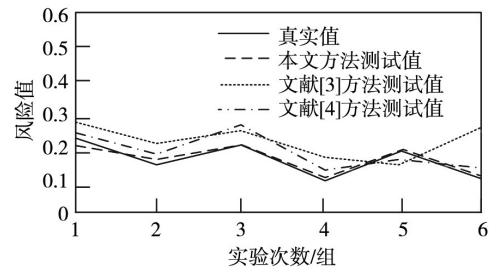


图3 不同方法的评估误差测试结果

分析图3可知,针对移动自组织网络信息的安全评估,无论在哪个组实验中,所提方法的评估测试值都与实际值之间的差距较小,差值小于0.05;文献[3]方法与文献[4]方法评估的测试值与实际值之间差距较大,说明所提方法的评估误差小于文献[3]方法与文献[4]方法的评估误差。

## 4 结束语

目前的移动自组织网络信息安全评估方法存在评估时间过长、评估误差大等问题,为解决以上问题,提出基于综合云的移动自组织网络信息安全评估方法。创新性地结合权重与逆向云获得综合云模型,计算出综合云与评价云之间的相似性,结合风险值,实现网络信息的安全评估。测试结果表明该方法在降低了方法评估时间的同时,一定程度上也降低了方法的评估误差,为网络信息安全评估技术奠定了一定基础。但由于条件有限,该方法获得的综合评价云结构复杂度还有继续提高的空间,未来的研究将进一步扩充评估云的评估指标,提高评估准确性。

### 参考文献:

- [1] 刘常昊,郑万波,杨志全,等.区域煤矿智慧应急管理信息平台的多层次数字预案信息系统[J].能源与环境,2020,42(12):124-129.
- [2] 刘道远,孙科达,周君良,等.模糊综合评判法在电力企业网络信息安全评估中的应用[J].电信科学,2020,36(3):34-41.
- [3] 赵冬梅,宋会倩,张红斌.基于时间因子和复合CNN结构的网络安全态势评估[J].计算机科学,2021,48(12):349-356.
- [4] 李佳玮,吴克河,张波.一种基于小生境遗传算法的电网信息安全风险评估模型[J].电力建设,2021,42(3):89-96.
- [5] 丛培鑫,李晓慧,王俊峰.基于生物信息的未知二进制协议聚类方法[J].四川大学学报(自然科学版),2022,59(3):69-76.
- [6] 李胜利,魏翠萍,宋燕红.基于信任关系和互补判断矩阵的群决策方法[J].控制与决策,2020,35(5):1240-1246.
- [7] 朱奕杰,蔺宏伟.基于正则化一维卷积神经网络的网格模型

(下转第172页)