Computer Science and Application 计算机科学与应用, 2021, 11(9), 2350-2356
Published Online September 2021 in Hans. http://www.hanspub.org/journal/csa
https://doi.org/10.12677/csa.2021.119240

Hans汉斯

一种基于AHP构建的网络安全态势评估方法评价模型

黄正兴，张　静

武警警官学院信息通信系，四川 成都
Email: hykgg201756@163.com, 1123062430@qq.com

收稿日期：2021年8月15日；录用日期：2021年9月11日；发布日期：2021年9月18日

摘　要

目前网络安全态势评估方法繁多，对其缺乏统一的评价指标，从而导致评估方法在应用时难以选取。针对以上问题，本文提出了一种基于AHP构建的网络安全态势评估方法评价模型。首先介绍层次分析法(AHP)，阐明其实现步骤和计算原理；接着综合分析已有网络安全态势评估方法，得到了五个评价指标；而后基于AHP构建网络安全态势评估方法的评价模型，并阐明了评价步骤；最后以实例证明了该评价模型的有效性。

关键词

AHP，网络安全态势，评估方法，评价模型

An Evaluation Model of Network Security Situation Assessment Based on AHP

Zhengxing Huang, Jing Zhang

Department of Information and Communications, Armed Police College of CAPF, Chengdu Sichuan
Email: hykgg201756@163.com, 1123062430@qq.com

Received: Aug. 15th, 2021; accepted: Sep. 11th, 2021; published: Sep. 18th, 2021

Abstract

At present, although there are many methods of network security situation assessment, there is no unified evaluation index, which makes it difficult to select the evaluation method when people need to use them. In view of the above problems, this paper presents an evaluation model of net-

文章引用: 黄正兴, 张静. 一种基于 AHP 构建的网络安全态势评估方法评价模型[J]. 计算机科学与应用, 2021, 11(9): 2350-2356. DOI: 10.12677/csa.2021.119240

work security situation assessment method based on AHP. Firstly, the hierarchical analysis method (AHP) is introduced. Secondly, through the comprehensive analysis of the existing network security situation assessment method, five evaluation indexes are obtained. Thirdly, the evaluation model of the network security situation assessment method based on AHP is constructed. Finally, the effectiveness of the evaluation model is proved through the case.

Keywords

AHP, Network Security Situation, Assessment Methods, Evaluation Model

1. 引言

作为网络安全态势感知系统的核心，网络安全态势评估技术一直备受关注。近几年，针对传统网络安全态势评估技术存在的缺点，众多改进的网络安全态势评估方法被提出。为了解决网络中多源异构信息导致传统方法评估准确性和效率偏低的问题，引进了层次分析法[1]、D-S 证据理论[1]、理论直觉模糊集[2]、聚类分析[3]等理论对传统方法进行改进；由于传统基于神经网络的评估方法存在效率低、评估精度不高的问题，引进了人工蜂群算法[4]、遗传算法[5]等算法对其进行改进；鉴于传统评估方法依赖于人工标注或经验的问题，提出了基于深度学习和深度自编码的评估方法[6] [7]。众多方法解决的问题不同，导致其优缺点不同。网络安全管理人员应该针对不同的应用场景，结合评估方法的优缺点科学选取评估方法。但目前针对众多评估方法还没有一个公认的评价指标和评价模型，对不同的网络安全态势评估方法无法进行分析比较和综合评价，从而导致在应用时难以抉择，实际应用时达不到理想的效果。

为了解决以上问题，本文建立了评价网络安全评估方法的指标，并基于 AHP 构建了网络安全态势评估方法评价模型，最后通过实例证明了其有效性。

2. 层次分析法 AHP 介绍

层次分析法[8] (Analytic Hierarchy Process, AHP)是美国知名的运筹学家、匹兹堡大学教授 T. L. Saaty 在 20 世纪 70 年代提出的一种优化决策的方法。该方法将定性的指标与量化的权值相结合，将问题分为目标、决策准则和具体方案等层次，方便了人们以一个清晰的思路得到最佳的决策方案。定性的指标是层次与层次之间存在着的关联因素，量化的权值表示每一层的各个元素相对于上一层某个元素的重要程度。层次分析法最后用加权求和的方法得到具体方案对最终目标的相对权值，权值的大小即是衡量方案优劣的标准：权值越大，方案越优；反之，权值越小，方案越差。权值的确定可以为人们得到最佳的方案、做出正确的决策提供重要的参考信息，能够避免人的主观因素影响决策结果。

层次分析法的实现主要有 4 步：

1) 对要素进行分类，建立层次结构模型。一般将要素分为三类：一是目标类，属于决策的结果；二是准则类，是影响决策的定性指标；三是措施类，即实现目标的方案。根据因素的分类将各因素排列于不同层次，自上而下为目标层、准则层和措施层。

2) 建立判断矩阵。决策者依据经验给出各层中每个元素相对于上一层中某个因素的权值，得到相应的判断矩阵，接着进行修正以使判断矩阵达到一致性标准。

3) 计算组合权值。通过加权求和得到措施层每个方案对于目标层的相对权值，进而对各方案的优劣进行确定，使决策者容易做出决策。

3. 网络安全态势评估方法的评价指标分析

自网络安全态势评估提出以来，相关评估方法的提出者便从某些指标验证了所提方法的有效性，但这些指标未统一标准。论文[1]为了能够评测多源融合的性能，提出了包括融合算法准确率、误警率等指标；论文[4]为了验证其基于人工蜂群优化的神经网络安全态势评估方法的有效性，提出了收敛速度、训练和预测精度、鲁棒性等指标；论文[6]主要从效率、准确性、灵活性等指标对比传统网络安全态势评估方法；文献[9]在研究 JDL 模型威胁评估层的过程中，提出了融合准确性、先验知识需求、计算机资源需求、负载、通信带宽和算法性能等参数用于衡量多传感器融合的性能。Sabata 和 Ornes [10]提出 DIR (Data to Information Ratio)来衡量态势评估，DIR 的含义是大量的数据转化为信息的比率，目的是对 NSSA 处理数据的能力进行衡量。文献[11]提出了三个评价指标，分别是态势符合度、态势报警比、时效性，为评测态势评估方法提供客观的评价标准。

通过分析我们发现以上某些评价指标存在共性，比如融合算法准确率、DIR 和态势报警比，它们均对网络安全态势评估方法处理海量数据的能力进行评价，对于这些指标，如果同时考虑会造成评价结果偏重于某一方面，因此只需选取其中一个进行考虑。所以，通过研究分析，本文得到的网络安全态势评估方法的评价指标为：时效性，敏感性，态势符合度，具体性，态势报警比。下面对各评价指标的概念进行说明。

时效性：指评估方法满足实时性的程度。根据此指标，可以衡量网络安全态势评估方法是否能够在威胁来临时做出及时响应，从而更好地对网络信息系统安全进行保障。

敏感性：指评估方法在网络受到威胁时反映出来的灵敏程度。根据此指标，可以衡量网络安全态势评估方法是否能够灵敏地感知网络安全的变化，从而准确地对网络安全存在的具体问题进行识别。

态势符合度：指评估方法对当前态势的评估准确程度。根据此指标，可以衡量网络安全态势评估方法是否可以准确地评估网络安全态势，从而准确地判断出网络事件对网络安全态势的影响程度。

具体性：指评估方法对当前态势具体影响因素的感知程度。根据此指标，可以衡量网络安全态势评估方法是否可以在知道网络安全态势的情况下还能得知造成网络安全问题的具体攻击事件类型，从而便于管理员有针对性地采取防御或补救措施。

态势报警比：指评估方法对原始报警的约简程度。通过此指标，可以衡量网络安全态势评估方法是否可以对网络安全态势的影响因素进行约简，从而降低网络管理员的负担。

4. 基于 AHP 构建网络安全态势评估方法的评价模型

根据层次分析法的实现步骤可知，基于层次分析法从众多网络安全态势评估方法中择优选取最合适的目标方法时，首先需要建立层次结构模型。

本文将目标方法设置为层次分析结构的目标层元素，将本文所提出的网络安全态势评估方法的评价指标设置为层次分析结构的准则层元素，将候选的网络安全态势评估方法设置为层次分析结构的措施层元素，其模型如图 1 所示。

基于图 1 所示模型，实现网络安全态势评估方法评价的步骤如下：

第一步：确定措施层。本步骤主要由决策者了解现有网络安全态势评估方法，根据应用场景需求事先确定候选的网络安全态势评估方法，作为评估模型的措施层。

第二步：建立判断矩阵，检验一致性。本步骤主要由决策者依据经验将措施层相对于准则层各个因素

的重要程度和准则层相对于目标层的重要程度做两两比较，从而建立判断矩阵。本步骤是网络安全态势评估方法评价模型中的关键步骤，其主要内容有两部分：一是判断矩阵的量化；二是判断矩阵的一致性检验。

为了量化判断矩阵，往往使用文献[12]提出的 1~9 标度，见表 1。

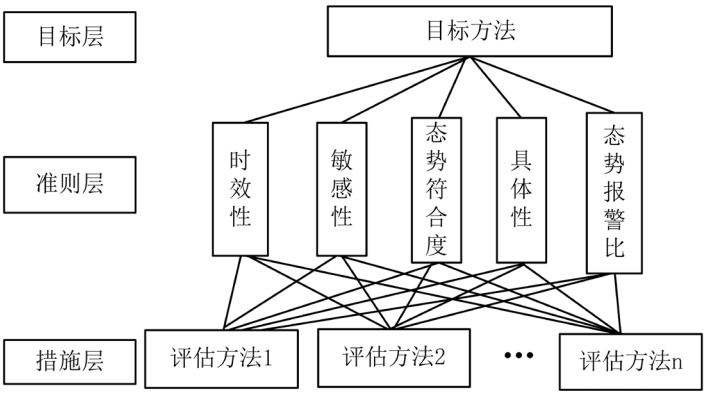

Figure 1. An evaluation model of network security situation assessment based on AHP
图 1. 基于 AHP 的网络安全评估方法评价模型

Table 1. The definition of scale
表 1. 标度的定义

标度 a_{ij}	定义
1	因素 i 的重要程度等于因素 j 的重要程度
3	因素 i 的重要程度略大于因素 j 的重要程度
5	因素 i 的重要程度较大于因素 j 的重要程度
7	因素 i 的重要程度非常大于因素 j 的重要程度
9	因素 i 的重要程度绝对大于因素 j 的重要程度
2, 4, 6, 8	界于以上判断的中间状态
倒数	以上因素前后互换所得比值

而检验判断矩阵一致性普遍使用的指标为 CR，当 CR 的值低于 0.1，则判断矩阵已经达到了一致性的要求；当 CR 的值等于或高于 0.1，则判断矩阵还不满足一致性的要求，需要继续进行修正。CR 的计算公式为：

$$CR = \frac{CI}{RI}, CI = \frac{\lambda_{\max} - n}{n-1}$$

其中，$\lambda_{\max}$ 是判断矩阵的最大特征值，n 是判断矩阵的维度，RI 可以通过查询表 2 获取。

Table 2. The relationship between RI and matrix dimensions
表 2. RI 与矩阵维度的关系

维度数	1	2	3	4	5	6	7	8	9	10	11
RI	0	0	0.58	0.90	1.12	1.24	1.32	1.41	1.45	1.49	1.51

第三步：计算措施层评估方法i分别相对于准则层的权重W_{ip}和准则层相对于目标层的权重W_{pt}。权重计算方法为：判断矩阵的特征向量即为所求权重的值。

第四步：组合计算措施层相对于目标层的权重W，确定要选取的目标方法。其具体计算公式为：

$$W=\left[W_{1p},W_{2p},\cdots,W_{np}\right]\left[W_{pt}\right]$$

其中，$W_{1p},W_{2p},\cdots,W_{np}$和$W_{pt}$都是以权重的列向量形式存在。

5. 实例分析

运用本文所构建的网络安全态势评估方法评价模型，对论文[2]、论文[7]和论文[13]所提的三种方法进行评价，层次结构如图 2 所示。

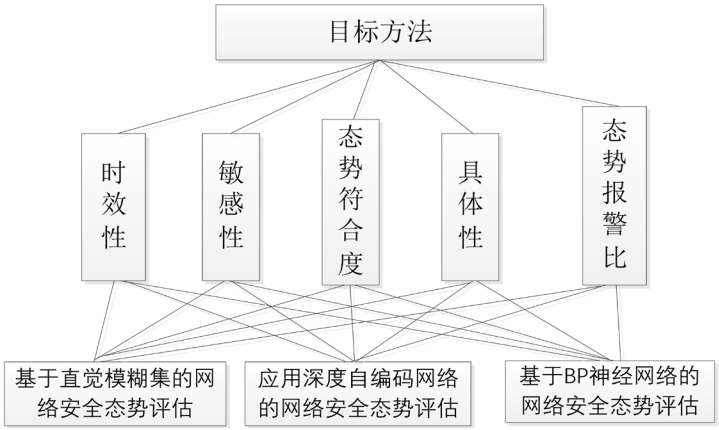

Figure 2. Hierarchy model
图 2. 层次结构

决策者根据表 1 定义的标度，建立判断矩阵见表 3~8。

Table 3. The evaluation indicator's judgment matrix relative to the target method
表 3. 评价指标相对于目标方法的判断矩阵

相对目标方法	时效性	敏感性	态势符合度	具体性	态势报警比
时效性	1	2	7	5	5
敏感性	1/2	1	4	3	3
态势符合度	1/7	1/4	1	1/2	1/3
具体性	1/5	1/3	2	1	1
态势报警比	1/5	1/3	3	1	1

Table 4. The evaluation method's judgment matrix relative to the time-sensitive indicator
表 4. 评估方法相对于时效性指标的判断矩阵

相对时效性	基于直觉模糊集的网络安全态势评估	应用深度自编码网络的网络安全态势评估	基于 BP 神经网络的网络安全态势评估
基于直觉模糊集的网络安全态势评估	1	3	8
应用深度自编码网络的网络安全态势评估	1/3	1	3
基于 BP 神经网络的网络安全态势评估	1/8	1/3	1

Table 5. The evaluation method's judgment matrix relative to the sensitivity indicator
表 5. 评估方法相对于敏感性指标的判断矩阵

相对敏感性	基于直觉模糊集的网络安全态势评估	应用深度自编码网络的网络安全态势评估	基于 BP 神经网络的网络安全态势评估
基于直觉模糊集的网络安全态势评估	1	1/2	5
应用深度自编码网络的网络安全态势评估	2	1	3
基于 BP 神经网络的网络安全态势评估	1/5	1/3	1

Table 6. The evaluation method is a judgment matrix relative to the situation compliance indicator
表 6. 评估方法相对于态势符合度指标的判断矩阵

相对态势符合度	基于直觉模糊集的网络安全态势评估	应用深度自编码网络的网络安全态势评估	基于 BP 神经网络的网络安全态势评估
基于直觉模糊集的网络安全态势评估	1	1	3
应用深度自编码网络的网络安全态势评估	1	1	3
基于 BP 神经网络的网络安全态势评估	1/3	1/3	1

Table 7. The evaluation method is a judgment matrix relative to the specificity indicator
表 7. 评估方法相对于具体性指标的判断矩阵

相对具体性	基于直觉模糊集的网络安全态势评估	应用深度自编码网络的网络安全态势评估	基于 BP 神经网络的网络安全态势评估
基于直觉模糊集的网络安全态势评估	1	3	4
应用深度自编码网络的网络安全态势评估	1/3	1	1
基于 BP 神经网络的网络安全态势评估	1/4	1	1

Table 8. The evaluation method is a judgment matrix relative to the situation alarm ratio
表 8. 评估方法相对于态势报警比的判断矩阵

相对态势报警比	基于直觉模糊集的网络安全态势评估	应用深度自编码网络的网络安全态势评估	基于 BP 神经网络的网络安全态势评估
基于直觉模糊集的网络安全态势评估	1	4	1/2
应用深度自编码网络的网络安全态势评估	1/4	1	1/4
基于 BP 神经网络的网络安全态势评估	2	4	1

运用 python 编写代码，仿真以上层次模型，运行结果如图 3 所示。

```
=================
准则层：最大特征值5.072084,CR=0.014533,检验通过
准则层权重=[0.47583538 0.26360349 0.0538146  0.09806829 0.10867824]

方案层
          直觉模糊集    应用深度自编码   基于BP神经网络      最大特征值              CR   一致性检验
时效性     0.681725  0.236341  0.081935  3.001542  8.564584e-04    True
敏感性     0.379129  0.507603  0.113269  3.163235  9.068585e-02    True
态势符合度  0.428571  0.428571  0.142857  3.000000 -1.233581e-15    True
具体性     0.633708  0.191921  0.174371  3.009203  5.112618e-03    True
态势报警比  0.344545  0.108525  0.546931  3.053622  2.978976e-02    True

目标层 [[0.54698289 0.29994409 0.15307302]]
```

Figure 3. The result of the simulation run
图 3. 仿真运行结果

从图 3 可以看出，各判断矩阵满足一致性检验，通过计算可以得到评估方法相对于目标方法的权重为[0.54698289, 0.29994409, 0.15307302]。因此，此时根据决策者的需求，应该选择基于直觉模糊集的网络安全态势评估方法。

从实例结果可以看出，相对于传统网络安全态势评估致力于研究改进算法或提出新评估方法的现象，本文提出的评价模型可以为网络安全评估方法使用者在应用层面提供决策辅助，能够基于现有评估方法加以科学利用，使理论向实际应用过渡富有针对性，更加合理化。

6. 总结

本文针对目前网络安全态势评估方法多、评价标准不统一，从而导致评估方法选用困难的问题，通过综合分析现有网络安全态势评估方法评价指标得出了 5 个普适性指标，运用层次分析法构建了网络安全态势评估方法的评价模型，并用实例证明了其可行性，具有一定的应用价值。

参考文献

[1] 常利伟, 田晓雄, 张宇表, 等. 基于多源异构数据融合的网络安全态势评估体系[J]. 智能系统学院, 2021, 16(1): 38-47.

[2] 韩晓露, 刘云, 李旭, 张振江, 吕欣. 基于直觉模糊集的网络安全态势评估方法[J]. 吉林大学学报(工学版), 2019, 49(1): 261-267.

[3] 文志诚, 陈志刚, 唐军. 基于聚类分析的网络安全态势评估方法[J]. 上海交通大学学报, 2016, 50(9): 1407-11414, 1421.

[4] 于海, 李峰, 霍英哲, 尹晓华. 电力信息网络安全态势评估方法[J]. 科学技术与工程, 2021, 21(9): 3642-3648.

[5] 王金恒, 单志龙, 谭汉松, 王煜林. 基于遗传优化 PNN 神经网络的网络安全态势评估[J]. 计算机科学, 2021(6): 338-342.

[6] 杨宏宇, 曾仁韵. 一种深度学习的网络安全态势评估方法[J]. 西安电子科技大学学报, 2021(1): 183-190.

[7] 张玉臣, 张任川, 刘璟, 汪永伟. 应用深度自编码网络的网络安全态势评估[J]. 计算机工程与应用, 2020(6): 92-98.

[8] 孙宏才, 田平. 网络层次分析法与决策科学[M]. 北京: 国防工业出版社, 2011.

[9] Hall, D.L. (2014) Mathematical Techniques in Multisensor Data Fusion. Artech House, Boston, 125-137.

[10] Sabata, B. and Omes, C. (2006) Multisource Evidence Fusion for Cyber-Situation Assessment. *Proceedings of SPIE, the International Society for Optical Engineering*, Kissimee, Florida, 2006, Article ID: 624201. https://doi.org/10.1117/12.663436

[11] 刘效武, 王慧强, 赖积保, 等. 基于多源异质融合的网络安全态势生成与评价[J]. 系统仿真学报, 2010, 22(6): 1411-1415.

[12] Zhang, Y. and Xian, M. (2012) A Study on the Evaluation Technology of the Attack Effect of Computer Networks. *Journal of National University of Defense Technology*, **24**, 24-28.

[13] 黄焱. 基于 BP 神经网络的网络安全态势评估研究[J]. 佳木斯大学学报: 自然科学版, 2020(4): 86-89.