

基于模糊层次法的改进型网络安全态势评估方法

李方伟, 杨绍成*, 朱江

(移动通信技术重庆市重点实验室(重庆邮电大学), 重庆 400065)

(*通信作者电子邮箱 515085554@qq.com)

摘要:为最大限度降低网络安全问题带来的损失,提出一种基于模糊层次分析法(FAHP)的改进型网络安全态势评估模型。鉴于未来的大规模网络环境,首先建立一套符合实际环境的,由指标层、准则层、决策层三层组成的态势指标体系;针对态势评估中的数据分布不确定性、模糊性对评估结果的影响,利用模糊C-均值(FCM)聚类 and 最佳聚类准则进行数据预处理,得到最佳聚类数和聚类中心;最终建立多因素二级评估模型得到态势评估向量。仿真结果表明,与目前的基于模糊层次法的态势评估方法相比,更好地考虑到某些权重小的因素,因而标准偏差更小,评估结果更加客观、准确。

关键词:模糊层次分析法;指标体系;最佳聚类准则;模糊C-均值;态势评估

中图分类号: TP393 **文献标志码:** A

Improved network security situational assessment method based on FAHP

LI Fangwei, YANG Shaocheng*, ZHU Jiang

(Chongqing Key Laboratory of Mobile Communications Technology (Chongqing University of Posts and Telecommunications), Chongqing 400065, China)

Abstract: To minimize damage from network security problem, an improved network security situation assessment model based on Fuzzy Analytic Hierarchy Process (FAHP) was proposed. First, a set of index system in conformity with actual environment which consists of index layer, criterion layer and decision layer was established in consideration of the large-scale network environment in the future. Aiming at the influence on evaluation by data distribution uncertainty and fuzziness in situation assessment, the proposed model used Fuzzy C-Means (FCM) clustering algorithm and the best clustering criterion for data preprocessing to get the optimal cluster number and cluster center. Finally, multi-factor secondary assessment model was established for situation assessment vector. The simulation results show that, compared with the present situation assessment method based on FAHP, the improved method takes the factors which have small weights into consideration better, so the standard deviation is smaller and evaluation results are more objective and accurate.

Key words: Fuzzy Analytic Hierarchy Process (FAHP); index system; best clustering criterion; Fuzzy C-Means (FCM); situation assessment

0 引言

在网络攻击技术越来越发达的今天,计算机网络与互联网的应用对于各国的教育、经济、政治、文化和科学的发展起着不可忽视的作用,但它的负面影响也日益严峻。所以网络安全一直伴随着网络技术与应用的发展而进步,是一个值得重视的研究课题^[1-4]。

态势感知目前普遍定义为从网络中察觉并获取各种因素,对这些因素进行整合分析,最终对未来的网络安全趋势进行预测以获得网络实时安全状态,所以网络态势评估作为态势感知承上启下的环节已成为网络安全中的研究热点。态势感知这一起源于军事的概念目前已广泛运用到包括制造、交通等各个领域^[5-6],最近被应用到网络安全领域中,人们基于不同方面提出了大量研究方法。

Bass等^[7]将航空控制中的成熟理论和技术结合,第一次提出了网络安全态势的概念,并介绍了一种基于信息融合的

入侵检测系统模型,对网络安全实时监控的实现加强了人们对网络安全态势的管理;但是Bass仅仅给出了模型而没有对其实现。Gorodetsky等^[8]提出了基于异步数据流的网络安全态势评估方法,利用多代理异常检测网络的数据流进行分析,获取安全态势;但是这种方法只考虑了攻击信息而忽略了网络本身的特性。与此同时,国外很多研究机构也已开始着手研制网络安全态势感知系统和工具,OCTAVE和COBRA是其中具有代表性的两种工具。COBRA采用问卷调查形式收集网络系统内的环境数据和相关信息,利用专家知识库和规则对关键资产存在的弱点以及资产面对威胁潜在的损失作出评估,并提供安全措施改进建议;OCTAVE针对信息系统提出一个评估框架,该方法的评估过程由收集并整理资产配置信息及现有安全策略,标识资产存在的弱点并给出等价评价和制定安全管理策略^[9-10]三个步骤组成。陈秀真等^[11]根据入侵检测日志攻击记录情况,结合服务、主机重要性等信息,建立了一个层次化的安全威胁评估模型,并给出了相应的威

收稿日期: 2014-04-11; **修回日期:** 2014-06-19。 **基金项目:** 国家自然科学基金资助项目(61271260, 61301122); 教育部科学研究重点项目(212145); 重庆市教委科学技术研究项目(KJ1400405)。

作者简介: 李方伟(1960-),男,重庆南岸人,教授,博士生导师,主要研究方向:态势感知; 杨绍成(1990-),男,重庆璧山人,硕士研究生,主要研究方向:态势感知; 朱江(1977-),男,湖北荆州人,副教授,博士,主要研究方向:认知无线电。

量化方法。该方法采用自下而上,先局部、后整体的评估策略,对目标主机和网络环境进行威胁累加,可以在不同层次上进行态势威胁分析。

前文所介绍的方法为网络态势评估提供了一些实践理念,每种方法都有各自的优点,为态势评估模型及算法的研究奠定了基础。但这些方法也存在一些不足,比如缺乏对安全因素的全面考虑以及单一数据源的获得使得评估结果不够准确,上述定量评估算法的评估指标权重过于主观。因此本文提出一种定性定量相结合的层次化评估模型,并结合最佳聚类准则使指标权重更加符合实际环境,评估结果更加准确。

1 基于模糊层次分析法的网络态势评估建模

1.1 二级模糊综合评估方法流程

本文在广泛研究国内外成果的基础上,认为网络态势评估类似系统的多属性决策,两者都涉及大量不确定因素,故首先建立一套层次式指标体系;而且由于信息具有不确定性,影响因素具有模糊性,因此引入模糊推理^[12]进行量化处理,使得从网络中获取所构成的指标体系中的每一个因素都有一个取值范围,在一定程度上调整评判矩阵构造过程中的偏差,使评价的精确度得到提高。本文详细介绍了其数学原理和具体应用。由于态势评估中的评估因素往往具有不确定性和模糊性,而且每个因素本身的数据分布特点对评估结果有着不可忽视的影响,所以本文采用模糊 C-均值(Fuzzy C-Means, FCM)聚类^[13]对各数据集进行划分,并通过一种最佳聚类准则确定最优的聚类数。最后在态势值计算方面运用了模糊层次分析法(Fuzzy Analytic Hierarchy Process, FAHP)^[14],这是一种定性定量分析相结合的多目标决策分析方法,在目标结构复杂且缺少必要数据的情况下,采用此方法比较实用。本文改进型的态势评估方法流程如图1所示。

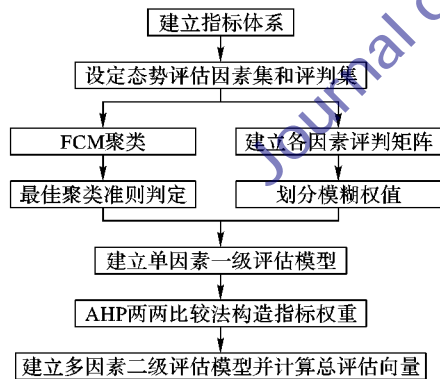


图1 改进型态势评估方法流程

本文的改进型态势评估方法采用多级评估模型,既在一级评估模型中单独地分析每个因素,又在二级评估模型中同时考虑各因素之间的相互关系,采用1~9标度法^[15]对各个评估因素之间进行比较使结果更加科学、客观、合理。

1.2 评估指标体系建立

根据图1可知指标体系是网络态势评估的操作对象。根据信息论相关知识,信息来源越丰富,采用的评估指标越多,对态势的描述就越详尽深刻;但过多的指标将导致计算量巨大,带来不必要的冗余。因此对特定的客观情形选择对当前态势影响深刻的网络特征建立态势指标体系非常重要。根据

上述论述,本文提出如图2所示的网络态势指标体系。

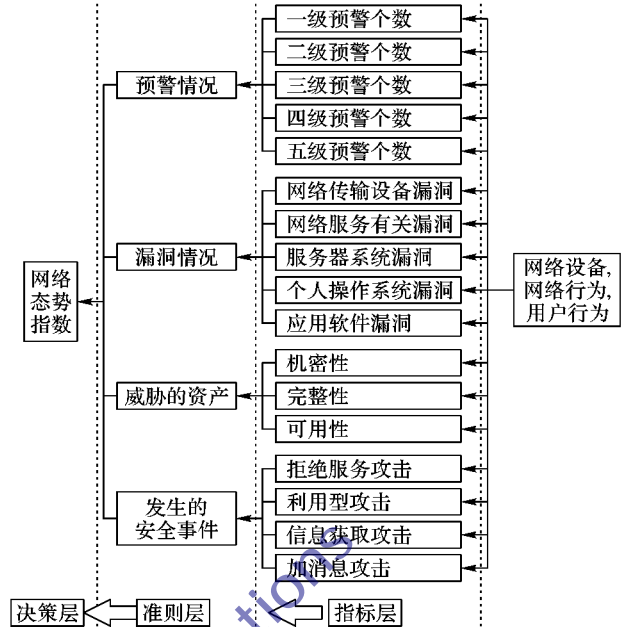


图2 网络态势指标体系

定义1 网络态势指数。对某个时间周期(一般在24 h以上)某网络区域内影响安全态势的各种因素采用一定的方法进行综合量化评估后得到一个反映整个网络安全状况的态势值或向量。

建立的层次结构模型可以对信息系统的评估指标进行深入的分析,结构模型主要包括决策层、准则层和指标层三个层次关系,各层之间存在着一定的关系。其中:决策层是最高层,代表态势评估的总体目标;中间层是准则层,主要设定对系统进行态势评估的准则,对态势评估的目标进行分解;指标层处在最低层,是进行网络态势评估的具体评估指标,表示影响目标实现的各种因素,如果指标不能完全表达意思,可以继续划分子层。

1.3 FCM 聚类分析数据分布特点

针对数据分布对评估结果的影响采用FCM聚类对数据进行预处理。

定义2 最佳聚类准则。本文的最佳聚类准则要求类间距离最大,而类内元素距离最小。给出聚类的允许范围 a ,这样就能保证得到聚类结果符合属性特性^[16]。

对于指标层的某个因素的属性 X 和聚类类别 a, x_1, x_2, \dots, x_n 为各属性值,偏差 $\partial^2(x)$ 定义为:

$$\partial^2(x) = \frac{1}{n} \sum_{n=1}^n (x_n - \tilde{x})^2 \quad (1)$$

其中 $\tilde{x} = \sum_{n=1}^n x_n$ 为属性均值。式(1)代表属性 X 的差异,其值越大表示 X 的差异越大;相反,越小说明 X 中的值越相似。同理,聚类 i 的偏差为:

$$\partial^2(x_i, \tilde{x}_i) = \frac{1}{n_i} \sum_{n=1}^{n_i} (x_{ik} - \tilde{X}_i)^2 \quad (2)$$

其中: $X_i = x_{i1}, x_{i2}, \dots, x_{im}$ 为第 i 类数据元素; \tilde{X}_i 为该聚类平均值。则 a 个聚类的平均偏差为:

$$\partial^2(X, \tilde{X}) = \left[\frac{1}{a} \sum_{i=1}^a \partial^2(x_i, \tilde{x}_i) \right] / \partial^2(x) \quad (3)$$

其中: \tilde{X} 为 a 个聚类平均值; $\partial^2(X, \tilde{X})$ 表示类内元素间距离, 也就是聚类平均紧密度, 值小说明 a 个聚类中元素的距离越小, 其值会随着同一类元素距离的增大而增大。

同时, 最佳聚类准则要求类间距离应该尽可能大。 a 个聚类间的平均距离定义为:

$$D(X, R) = \frac{1}{2a} \sum_{i=1}^a \sum_{j=1}^a |r_i - r_j| \quad (4)$$

其中: $D(X, R)$ 为类间距离的度量; R 为聚类中心的集合; r_i 和 r_j 分别为聚类 i 和 j 的中心。 $D(X, R)$ 越大, 说明类间距离越大, 聚类效果越好, 因此期待此值最大化。

前面提到, 最佳聚类准则需要同时考虑类内紧密性和类间的分布性。因此最终的最佳聚类准则定义为:

$$S(X, R) = \frac{\partial(X, \tilde{X})}{\alpha/\beta} + \frac{\alpha}{D(X, R)} \quad (5)$$

其中: $\partial(X, \tilde{X})$ 表示聚类紧密性的效果, 没有考虑几何位置的影响; $1/D(X, R)$ 表示了聚类分布性与聚类中心的关系。由于这两部分的值不在同一范围, 因此定义权值 α 和 β 平衡两个影响因素对聚类准则值的影响以保证最佳聚类准则值前后两项大小始终保持相对平衡。 $\alpha = \min |r_i - r_j| / \max |r_i - r_j|$ 为聚类中心距离最大值与最小值之比; $\beta = D_{a, \max}(X, R)$ 为聚类数最大时聚类中心距离的平均值。 $S(X, R)$ 越小, 聚类结果越好, 所以求最佳聚类的目的就是要最小化 $S(X, R)$, 所得到的聚类数就是最佳聚类数和聚类结果。

1.4 用模糊层次法进行关联分析

1.4.1 隶属函数的确定

目前关于网络安全态势的评估, 往往不是将预警、漏洞或安全事件等都混在一起, 就是将它们孤立分离, 没有较好地考虑威胁的驱动因素及其内在的逻辑联系, 不能把握威胁的本质。在综合各种因素构建指标体系的基础上, 需要对这些指标进行量化。而这些指标都较抽象, 存在诸多不确定性和交互, 所以本文借助模糊逻辑的方法, 通过运用模糊集合中隶属度和隶属度函数的理论, 对存在相互制约关系的诸多影响因素进行数学抽象, 进而建立量化机制并运行模糊推理的方法进行指标间融合计算, 以获取各因素间的联系。

从综合评估的角度和以往的研究经验出发, 隶属函数的设定应满足以下条件: 1) 首尾两个评估等级的隶属函数应该是单调的; 2) 相邻两个等级的隶属函数必须是交叉的, 体现了“你中有我, 我中有你”的模糊集概念, 不相邻的两个等级之间的隶属函数应该没有交集; 3) 某一个指标的所有隶属程度之和应该为 1。

目前主要采用的隶属函数有梯形、三角型、正态型或者柯西型等^[17]。本文采用梯形型的隶属函数作为样本相似性度量的主要依据, 其相关定义如图 3 所示。

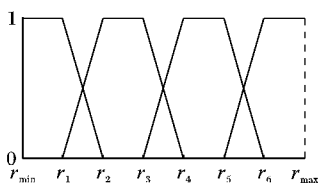


图3 梯形隶属函数

图 3 中 $\{r_1, r_2, \dots, r_c\}$ 为各个评估等级中心集合, 得到隶

属函数的定义如下:

$$f_1(x) = \begin{cases} 1, & x \leq r_1 \\ \frac{r_2 - x}{r_2 - r_1}, & r_1 < x < r_2 \\ 0, & x \geq r_2 \end{cases}$$

$$f_2(x) = \begin{cases} 0, & x \leq r_1 \\ \frac{x - r_1}{r_2 - r_1}, & r_1 < x < r_2 \\ 1, & r_2 \leq x \leq r_3 \\ \frac{r_4 - x}{r_4 - r_3}, & r_3 < x < r_4 \\ 0, & x \geq r_4 \end{cases} \quad (6)$$

$$f_3(x) = \begin{cases} 0, & x \leq r_3 \\ \frac{x - r_3}{r_4 - r_3}, & r_3 < x < r_4 \\ 1, & r_4 \leq x \leq r_5 \\ \frac{r_6 - x}{r_6 - r_5}, & r_5 < x < r_6 \\ 0, & x \geq r_6 \end{cases}$$

$$f_4(x) = \begin{cases} 0, & x \leq r_5 \\ \frac{x - r_5}{r_6 - r_5}, & r_5 < x < r_6 \\ 1, & x \geq r_6 \end{cases}$$

1.4.2 确定指标集和评判集得到单因素一级评估模型

指标集 U 顾名思义就是指指标体系的指标层中各个因素组成的模糊集合, 记为 $U = \{U_1, U_2, \dots, U_n\}$, $U_i = \{u_1, u_2, \dots, u_a\}$ 为其中第 i 个因素的模糊集合。评判集 V 是这些因素评估等级的集合, 记为 $V_i = \{v_1, v_2, \dots, v_k\}$; 本文选取 4 个评估等级, 评判集 $V = \{v_1, v_2, v_3, v_4\}$, 分别代表非常安全、安全、普通和严重。通过隶属函数进行单因素评估, 给出从 U 到 V 一个模糊映射, $f: U \rightarrow F(V)$ 。

设 $m_i = (m_{i1}, m_{i2}, \dots, m_{im})$ 为 u_i 到 $f(u_i)$ 的映射, 得到单因素评估矩阵为:

$$M_i = (m_1^i, m_2^i, \dots, m_a^i)^T = \begin{pmatrix} r_{11}^i & r_{12}^i & \dots & r_{1k}^i \\ r_{21}^i & r_{22}^i & \dots & r_{2k}^i \\ \vdots & \vdots & & \vdots \\ r_{a1}^i & r_{a2}^i & \dots & r_{ak}^i \end{pmatrix} \quad (7)$$

代表指标层第 i 个因素针对其 a 个模糊划分以及每个划分对各个评估等级的隶属程度。通过统计每个因素隶属于第 i 个模糊集合对应的权为 $\omega = (\omega_1, \omega_2, \dots, \omega_a)$, 重点考虑模糊集合划分对评估结果的影响, 模糊算子采用扎德算子^[18], 又称为主因素决定型:

$$y_j^i = \vee (r_{aj}^i \wedge \omega_j); a = 1, 2, \dots, k \quad (8)$$

最终得到单因素一级评估结果 $Y = (Y^1, Y^2, \dots, Y^n)^T$, 其中: $Y^i = (y_1^i, y_2^i, \dots, y_k^i)$ 表示第 i 个因素对第 k 个评估等级的隶属度。

1.4.3 多因素二级态势评估模型

在确定诸因素在整个问题中所占的比重时, 遇到的主要困难是这些比重常常不易量化。此外, 当影响某问题的因素

较多时,常常会因为考虑不周全、顾此失彼而使决策者提出与他实际认为的重要性程度不相一致的数据,甚至可能提出一组隐含矛盾的数据。

定义3 现在要比较指标集 $U = \{U_1, U_2, \dots, U_n\}$ 的 n 个因素在整体中各占多大比重。结合多属性决策的方法、过程、方法体系等基本理论,认为确定诸因素比重既是一个统计活动过程,又是一个定量的思维过程。本文采取对因素进行两两比较建立对比矩阵的方法,即每次取两个因素 U_i 和 U_j ,以 a_{ij} 表示 U_i 和 U_j 对总体的影响大小之比,全部比较结果用矩阵 $A = (a_{ij})_{n \times n}$ 表示,称 A 为对比矩阵。若矩阵 $A = (a_{ij})_{n \times n}$ 满足:

$$1) a_{ij} \geq 0;$$

$$2) a_{ij} = a_{ji}^{-1} (i, j = 1, 2, \dots, n);$$

则称 A 为正互反矩阵(容易看出 a_{ij} 与 a_{ji} 互为倒数且 $a_{ii} = 1$)。

对比矩阵 A 把一个复杂的决策问题表示为一个有序的递阶层次结构,通过比较判断,实现定性向定量的转化,需要有定量的标度,在确定 a_{ij} 的值时引用数字 1~9 及其倒数作为标度^[17]。这是一种将思维量化的方法,因为人们在区分事物的差别时,总是用相同、较强、强、很强、极端强的语言,再进一步细分,可以在相邻的两级之间插入折中的提法,因此,1~9 级的标度对于大多数决策判断来说都是适用的。另外从心理学观点来看,需要考虑的因素太多会超越人们的判断能力,既增加了作判断的难度,又容易因此而提供虚假数据,而构造对比判断矩阵的办法能减少其他因素的干扰,较客观地反映出一对因素影响力的差别。然后通过一致性检验进行模糊一致矩阵的调节,最后通过和法或方根法得到所需要的权值向量 $\psi = (\psi_1, \psi_2, \dots, \psi_n)$ 。根据一级评估结果和所有因素的影响权值,得到所有影响因素对第 i 个评估等级的隶属度结果,模糊算子仍然采用扎德算子,也就是主因素决定型。

2 实验分析

本文使用的数据来自于某网络安全公司的防火墙日志,该日志一共提供了 6 d,合计 868 个漏洞、预警、安全事件。针对图 2 指标体系中各指标,漏洞数目由扫描工具 nessus 获得;预警信息本文特指 snort 捕获的 event 事件;发生的安全事件是指经过 snort 规则分析匹配过的事件;而影响的资产则通过评估模型获得。为了从时间上完整表达网络的安全状态,本文选用了其中 4 d 的数据,即 2013-11-04T00:00:00 至 2013-11-07T23:59:59 之间合计 96 h,共 695 个报警事件作为实验数据。

2.1 最佳聚类进行数据预处理

设定聚类范围为 2~10,采用模糊 C 均值进行聚类,得到每个因素的聚类准则值如图 4 所示。

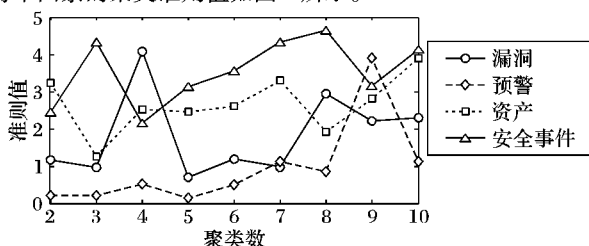


图4 各属性聚类准则值

图 4 表示每个影响因素的聚类准则值随着聚类数的变化情况。从图中可以看出,以预警为例,在聚类数范围 2~8 进行聚类,当聚类数为 5 时准则值 $S(X, R)$ 最小,也就是说当预警的聚类数为 5 时效果最好。通过这一系列处理找到最佳聚类数和聚类中心可以使每个属性更好地反映数据特性,避免由专家指定而造成的主观影响。同理适用于其他影响因素得到其最佳聚类数和聚类中心如表 1 所示。

表1 FCM 聚类情况

属性	最佳聚类数	聚类中心
漏洞	5	178.3;120.4;108.2;92.3;81
预警	5	41.9;21;15;13.1;12.5
资产	3	5.2;3.7;2.19
安全事件	4	0.727;0.488;0.31;0.27

由表 1 得到的各个最佳聚类数及聚类中心,然后通过式 (6) 即可得到每个属性的模糊划分和隶属函数。

2.2 模糊合成及多级评估结果

在每个属性得到其模糊划分和隶属函数后,则得到隶属度 U , 结合各待评价阶段参数得到每个影响因素的评估矩阵如表 2 所示。

表2 各个因素评估矩阵

属性	隶属度			
漏洞	0	0	0.6319	0.3681
	0	0.2061	0.7939	0
	1	0	0	0
	0.4218	0.5782	0	0
	0	0	0.5231	0.4769
预警	0	0	0.2190	0.7810
	0	0.9755	0.0245	0
	0.1883	0.8117	0	0
	0.7169	0.2831	0	0
	0	0	0	1
资产	0	0	0.2061	0.7939
	0	0.2061	0.7939	0
	0.2190	0.7810	0	0
安全事件	0	0	0.1249	0.8751
	0	0.6841	0.3159	0
	0.3455	0.6545	0	0
	0.9045	0.0955	0	0

统计隶属于各个模糊集合的历史数据得到每个模糊集合的权值分配如表 3 所示。

表3 各因素模糊划分权值

属性	权值
漏洞	0.17;0.22;0.22;0.22;0.17
预警	0.23;0.19;0.14;0.24;0.2
资产	0.29;0.42;0.29
安全事件	0.21;0.28;0.29;0.22

根据表 2 表 3 得到的数据,进一步通过式 (8) 得到单因素一级评估矩阵如表 4 所示。

由 1~9 标度方法分析每个属性的重要程度,建立态势评估各影响因素之间的比较矩阵,如表 5 所示。

表4 单因素态势评估结果

属性	非常安全	安全	普通	严重
漏洞	0.1223	0.2542	0.5167	0.1067
预警	0.2123	0.5708	0.0528	0.1640
资产	0.0657	0.3188	0.3853	0.2302
安全事件	0.2901	0.4083	0.1179	0.1838

表5 各因素对比矩阵

属性	漏洞	预警	资产	安全事件
漏洞	1	1/2	2	2/3
预警	2	1	5	3
资产	1/2	1/5	1	1
安全事件	2/3	1/3	1	1

长期的研究表明,决策者对事物两两比较的判断要比同时对多个事物同时比较的判断容易和准确得多。上述构造成对比矩阵的办法虽然能够减少其他因素的干扰,较客观地反映出一对因素影响力的差别。但综合全部比较结果时,其中难免包含一定程度的非一致性。所谓比较思维的一致性是指在判断事物重要性时,各判断之间协调一致,不至于出现互相矛盾的结果,对于实际问题建立的对比矩阵满足不一致性,其原因是由于客观事物的复杂性和人们认识上的多样性及可能出现的片面性而产生的判断的不完全一致性。对于对比矩阵来说,最基本的要求是不能出现违反常识的情况,例如“*A*比*B*重要,*B*比*C*重要,而*C*又比*A*重要”,这在逻辑上就是错误的。因此为了保证层次分析法得到的结论合理,表5中的因素还应满足一致性指标:

$$CR = CI/RI \quad (9)$$

经过验算 $CR = 0.019 < 1$, 对比矩阵没有逻辑错误,可以接受,通过和法或方根法得到各因素的影响权值向量如表6所示。

表6 所有影响因素权值

因素	权值	因素	权值
漏洞	0.18851	资产	0.18654
预警	0.38449	安全事件	0.24312

最后通过一级态势评估结果和所有影响因素权值得到二级态势评估结果如表7所示。

表7 多因素二级态势评估结果

评估等级	隶属度	评估等级	隶属度
非常安全	0.1884	普通	0.2115
安全	0.4221	严重	0.1615

本文提出的改进型FAHP多级态势评估相对于普通FAHP在划分模糊集和隶属函数进行关联分析基础上,运用FCM聚类对漏洞、预警等数据进行预处理,摆脱了专家事先给定模糊集划分的瓶颈;提出的最佳聚类准则使聚类数、最小密度、初始值等参数与实际特性相符,最终使各单因素作为威胁程度参差不齐的若干聚类集而不是单单一个整体完成一级推理过程;而且充分考虑各因素在整体评估中的比重,并通过对比矩阵减少各因素之间的干扰,在二级推理过程中比较各因素之间的重要程度。通过方根法确定二级评估的权值向量,最终对各因素作出全面、客观的评估。从表7可知,通过最佳聚类准则进行预处理后得到评估结果与通常的评估结果

相比,目前常用的态势评估方法在数据、影响因素量大时容易“淹没”某些权重小的因素,难以真实地反映各因素在整体中的地位,使态势评估得不到真实的意义。实验结果比较如图5所示,改进型FAHP各个评估等级隶属度差别明显,而普通FAHP评估得到的评估结果中各个危险等级的隶属度比较接近,存在2个危险等级隶属度相同而无法评估的情况,改进型FAHP多级态势评估可以更加有效地为决策提供支持,使得到的结果更加符合实际,效果更好。

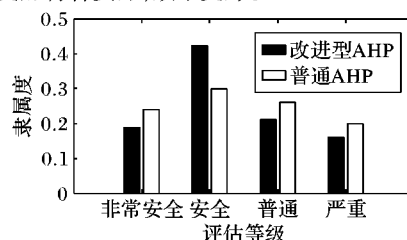


图5 实验结果比较

3 结语

本文提出一种基于模糊层次法的改进型网络态势评估方法,克服了目前模糊层次法评估网络态势中存在的忽略数据分布特点等不足;该方法利用FCM聚类和最佳聚类准则对数据进行预处理,避免了在模糊划分时过度依赖专家,同时提高了评估结果的客观性、准确性;引入对比矩阵并验证其一致性以确保其为模糊一致矩阵,使我们在确定权重时不存在人类思维上的逻辑错误。实验结果表明,本文算法比目前广泛使用的方法所得到的结果更加便于决策者决策。但由于从建立层次结构模型到给出成对比较矩阵,人的主观因素对整个过程的仍有一定的影响,所以方法中的比较、判断以及结果的计算精度有待提高。

下一步工作将分为两个方面:一是引入空间邻域信息加权FCM(Fuzzy C-Means based on Space Neighbor, SNFCM)算法进一步减少人为因素影响。二是进一步完善网络态势计算模型,引入神经网络来完善态势评估体系。由于神经网络模型具有高度的容错性、联想性和自组织、自学习能力,且对复杂系统具有强大的非线性映射和泛化功能,因此可以考虑将其应用在解决态势权重问题方面以提高实时性。

参考文献:

- [1] ZHANG B Y. A quantitative network situation assessment method based on stochastic model [J]. Applied Mechanics and Materials, 2014, 513(6): 768-771.
- [2] FISCHER Y, BEYERER J. Ontologies for probabilistic situation assessment in the maritime domain [C]// CogSIMA: Proceedings of the 2013 IEEE International Multi-disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support. Piscataway: IEEE, 2013: 102-105.
- [3] JANSEN A, MELCHERS K G, LIEVENS F, et al. Situation assessment as an ignored factor in the behavioral consistency paradigm underlying the validity of personnel selection procedures [J]. Journal of Applied Psychology, 2013, 98(2): 326-328.
- [4] ZHENHUA X. Demand-oriented traffic measuring method for network security situation assessment [J]. Journal of Networks, 2014, 9(4): 221-224.
- [5] SHARMA C, KATE V. ICARFAD: a novel framework for improved network security situation awareness [J]. International Journal of Computer Applications, 2014, 87(3): 129-134.

(下转第2644页)

- [2] YU S. Design and implementation of sensitive military information search system [D]. Chengdu: University of Electronic Science and Technology of China, 2012. (喻世玺. 军事敏感信息搜索系统的设计与实现[D]. 成都: 电子科技大学, 2012.)
- [3] TAO T, ZHAI C. Regularized estimation of mixture models for robust pseudo-relevance feedback [C]// Proceedings of the 29th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval. New York: ACM, 2006: 162–169.
- [4] CHEN H, DU X, XIA C, *et al.* Query expansion model based on interest ontology [C]// ICMIC 2012: Proceedings of the 2012 International Conference on Information Management, Innovation Management and Industrial Engineering. Piscataway: IEEE, 2012, 3: 474–478.
- [5] CHAUHAN R, GOUDAR R, SHARMA R, *et al.* Domain ontology based semantic search for efficient information retrieval through automatic query expansion [C]// ISSP 2013: Proceedings of the 2013 International Conference on Intelligent Systems and Signal Processing. Piscataway: IEEE, 2013: 397–402.
- [6] GOYAL P, BEHERA L, MCGINNITY T M. A novel neighborhood based document smoothing model for information retrieval [J]. Information Retrieval, 2013, 16(3): 391–425.
- [7] DAMANI O P. Improving Pointwise Mutual Information (PMI) by incorporating significant co-occurrence [EB/OL]. [2014-03-01]. <http://arxiv.org/pdf/1307.0596v1.pdf>.
- [8] LIANG S. VSM information retrieval data sparseness problem analysis and avoidance strategies [J]. Library and Information Service, 2013, 57(1): 142–146. (梁士金. VSM 信息检索中的数据稀疏问题分析与规避策略[J]. 图书情报工作, 2013, 57(1): 142–146.)
- [9] BAI J, NIE J Y, CAO G, *et al.* Using query contexts in information retrieval [C]// Proceedings of the 30th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval. New York: ACM, 2007: 15–22.
- [10] YAN C, GAO K, LI M. Processing natural language based query and context sensitive spelling suggestion in information retrieval [C]// ICMIC 2013: Proceedings of the 2013 International Conference on Modeling, Identification & Control. Piscataway: IEEE, 2013: 269–274.
- [11] LI W, ZHAO T, WANG X. Context-sensitive query expansion [J]. Journal of Computer Research and Development, 2010 (2): 300–304. (李卫疆, 赵铁军, 王宪刚. 基于上下文的查询扩展[J]. 计算机研究与发展, 2010 (2): 300–304.)
- [12] GOYAL P, BEHERA L, MCGINNITY T M. A Context-based word indexing model for document summarization [J]. IEEE Transactions on Knowledge and Data Engineering, 2013, 25(8): 1693–1705.
- [13] PONTE J M, CROFT W B. A language modeling approach to information retrieval [C]// Proceedings of the 21st Annual International ACM SIGIR Conference on Research and Development in Information Retrieval. New York: ACM, 1998: 275–281.
- [14] ZHAI C, LAFFERTY J. A study of smoothing methods for language models applied to information retrieval [J]. ACM Transactions on Information Systems, 2004, 22(2): 179–214.
- (上接第 2626 页)
- [6] CAI B. Evaluation on network security situation based on analytical hierarchy process and information fusion [C]// Proceedings of the 9th International Symposium on Linear Drives for Industry Applications. Berlin: Springer-Verlag, 2014: 619–626.
- [7] BASS T. Multisensor data fusion for next generation distributed intrusion detection systems [C]// INSD 1999: Proceedings of the 1999 IRIS National Symposium on Sensor and Data Fusion. New York: Communications of the ACM, 1999: 24–27.
- [8] GORODETSKY V, KARSAEV O, SAMOILOV V. On-line update of situation assessment based on asynchronous data streams [C]// KES 2004: Proceedings of the 8th International Conference on Knowledge-based Intelligent Information and Engineering Systems, LNCS 3213. Berlin: Springer-Verlag, 2004: 1136–1142.
- [9] YUCEK T, ARSLAN H. A survey of spectrum sensing algorithms for cognitive radio applications [J]. IEEE Communications Surveys & Tutorials, 2009, 11(1): 116–130.
- [10] WEI Y, LIAN Y, FENG D. A network security situational awareness model based on information fusion [J]. Journal of Computer Research and Development, 2009, 46(3): 353–362. (韦勇, 连一峰, 冯登国. 基于信息融合的网络安全态势评估模型[J]. 计算机研究与发展, 2009, 46(3): 353–362.)
- [11] CHEN X, ZHENG Q, GUAN X, *et al.* A hierarchical network security threat situation of quantitative evaluation method [J]. Journal of Software, 2006, 17(4): 885–897. (陈秀真, 郑庆华, 管晓宏, 等. 层次化网络安全威胁态势量化评估方法[J]. 软件学报, 2006, 17(4): 885–897.)
- [12] MAMESSIER S, DREYER D, OBERHAUSER M. Calibration of online situation awareness assessment systems using virtual reality [M]// DHM 2014: Proceedings of the 5th International Conference on Digital Human Modeling, Applications in Health, Safety, Ergonomics and Risk Management, LNCS 8529. Berlin: Springer-Verlag, 2014: 124–135.
- [13] GUO L, LIU G, BAO Y. A study of FCM clustering algorithm based on interval multiple attribute information [J]. Applied Mechanics and Materials, 2014, 444(3): 676–680.
- [14] SHAO C. The implication of fuzzy comprehensive evaluation method in evaluating internal financial control of enterprise [J]. International Business Research, 2009, 2(1): 210–213.
- [15] WANG Z, JIA Y, LI A, *et al.* Network situational quantitative evaluation method based on fuzzy hierarchy analysis [J]. Computer Security, 2011(1): 61–65. (王志平, 贾焰, 李爱平, 等. 基于模糊层次法的网络态势量化评估方法[J]. 计算机安全, 2011(1): 61–65.)
- [16] XIAO C, QIAO Y, HE H, *et al.* Multi-level fuzzy situation assessment model based on the best clustering criteria [J]. Application Research of Computers, 2013, 30(4): 1011–1014. (肖春景, 乔永卫, 贺怀清, 等. 基于最佳聚类准则的多级模糊态势评估方法[J]. 计算机应用研究, 2013, 30(4): 1011–1014.)
- [17] ZHANG X, TANG J, CHENG L. Development and application of online course evaluation system based on FAHP [J]. Computer Technology and Development, 2012, 22(11): 193–196. (张秀琦, 唐吉洪, 程琳. 基于 FAHP 的网络课程评价系统的开发与应用[J]. 计算机技术与发展, 2012, 22(11): 193–196.)
- [18] ZHANG J. The fuzzy analytic hierarchy process [J]. Fuzzy Systems and Mathematics, 2000, 14(2): 80–88. (张吉军. 模糊层次分析法[J]. 模糊系统与数学, 2000, 14(2): 80–88.)