网络拓扑层次化安全评估综合熵权算法①

万 巍[1,2], 李 俊[1]

[1](中国科学院计算机网络信息中心, 北京 100190)
[2](中国科学院大学, 北京 100049)

摘 要: 提出了一种网络拓扑层次化安全评估框架, 并基于该框架设计了一种安全评估过程中风险因素权重计算方法. 该方法在传统的层次分析法的基础上进行了改进, 引入熵权法的概念并进行修正, 在实际运用过程中其计算结果更加合理, 为网络安全态势评估奠定良好基础.

关键词: 安全评估; 层次分析法; 熵权

Integrated Entropy Weight on Hierarchical Topology Security Assessment Profile

WAN Wei[1,2], LI Jun[1]

[1](Computer Network Information Technology Center, Chinese Academy of Sciences, Beijing 100190, China)
[2](University of Chinese Academy of Sciences, Beijing 100049, China)

Abstract: This paper proposed a Hierarchical Topology Security Assessment Profile (HTSAP), and based on that designed a security assessment in the process of risk factors for weight algorithm. This algorithm improved the traditional AHP by the introduction of the concept of entropy weight method and correction. In the process of practical application its calculation result is more reasonable, and lays a good foundation for the network security situation assessment.

Key words: security assessment; AHP; entropy weight

1 引言

随着互联网技术的飞速发展, 网络技术的应用已经越来越普及, 但是也出现了越来越多的网络安全问题. 根据国家计算机网络应急技术处理协调中心(CNCERT/CC)发布的《2013 年中国互联网网络安全报告》[1], 2013 年国内共有 420 多万台主机被木马或者僵尸程序控制, 另外有 600 多万手机用户感染移动恶意程序, 并监测发现了 1 万多个针对国内网站的仿冒页面. 在安全漏洞方面, 国家信息安全漏洞共享平台(CNVD)统计, 2014 年新增漏洞进 8000 个, 其中高危漏洞占比三分之一, 主要涵盖微软、IBM、苹果、谷歌、甲骨文等知名厂商的各类主流产品[2].

目前, 网络安全技术已经得到了巨大的发展, 但是, 不断涌现的互联网新技术也面临更多的新的安全威胁和挑战. 网络攻击技术与安全防范手段在一定时期和范围内仍将共同向前发展. 因此, 利用各种安全评估手段, 了解当前网络安全状态信息是解决信息系统安全防范的一个重要手段, 尤其是针对大规模网络的安全态势.

大规模网络安全态势评估不同于单个信息系统或小型局域网的安全风险评估. 在单个信息系统或小型局域网中, 影响安全状态的风险因素相对较少, 安全信息的来源也相对有限, 因此安全风险的评估过程也比较简单. 但是在大规模网络中, 网络拓扑结构非常复杂, 网络节点数量相对庞大, 同时安全信息的来源也非常广泛, 因此针对大规模网络的安全态势评估是一个综合的过程.

本文结合大规模网络的结构特点, 同时参考了传统的安全评估的模式和方法, 设计了网络拓扑层次化安全评估框架(HTSAP). 并在 HTSAP 的基础上重点

① 基金项目:中国科学院"十二五"信息化专项——中国科学院网络安全保障与服务工程
收稿时间:2015-01-23;收到修改稿时间:2015-03-09

研究了影响大规模网络安全评估的风险因素的权值的计算方法.

2 HTSAP介绍

根据已有的信息安全风险评估规范[3]的标准, 典型的安全风险评估过程包括: 分析系统特性、识别威胁、识别脆弱点、分析现有控制措施、确定损害发生的可能性、分析影响、确定风险、提出控制措施建议和评估结果管理等步骤. 在确定风险的过程中涉及到风险的三个重要因素, 即威胁、脆弱点和对资产造成的潜在影响.

利用传统的安全评估方法, 针对一个大规模网络, 我们需要首先识别出该网络中的所有资产, 包括各类网络设备、安全设备、应用系统、终端主机等等, 然后针对每一个资产识别其脆弱点以及外部威胁, 并分析这些威胁利用该资产的脆弱点所产生的影响. 在具体的实践过程中, 上述方法几乎无法实现. 首先, 在一个大规模网络环境下, 资产数量非常庞大, 针对每一个资产进行风险分析计算需要耗费大量的资源. 另外, 通过该方法无法体现各个资产对整个大规模网络的安全态势分析所贡献的比例. 核心层中的一台交换机, 其重要性明显要比在接入层中的一台同样的交换机要高的多, 前者对整个网络的安全态势的贡献也要比后者高. 同样, 在终端层中, 不同的终端用户根据其承载的业务类型其重要性也各不相同.

HTSAP 分为三个层次如图 1 所示, 分别是目标层、拓扑层和风险因素层. 目标层即我们需要评估的整体的大规模网络安全态势; 拓扑层包括大规模网络的五个拓扑层次——出口层、核心层、汇聚层、接入层和终端层; 风险因素层即风险评估的三要素——资产影响、威胁和脆弱性.

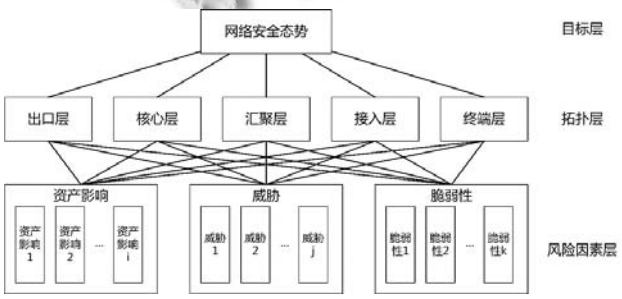

图 1　网络拓扑层次化安全评估框架(HTSAP)

3 层次分析法概述

层次分析法(Analytic Hierarchy Process, AHP)是由匹兹堡大学的T.L.Saaty教授于上世纪70年代提出的[4]. 其基本思想是将一个复杂的问题分解为多个组成元素, 并将这些元素进行分组, 从而形成一个有序的递进层次结构. 由于无法直接给各层次中的组成元素进行权重赋值, 因此通过对每两个元素进行比较确定其相对重要性, 然后结合专家的判断决定各元素相对重要性的总体排序.

如图 2 所示, 通常情况下将一个复杂问题自上而下按照相关因素的属性分解为三个层次: 目标层、准则层和方案层. 上层元素和下层元素存在一定的关联. 假设准则层 B 含有 n 个元素, 方案层 C 含有 m 个元素. 首先可以针对上层次中的某元素确定本层次与之相关的元素的重要性顺序的权重值, 即层次单排序. 然后利用同一个层次中的所有层次单排序结果计算针对上层某元素的本层所有元素的重要性的权值, 即层次总排序[5].

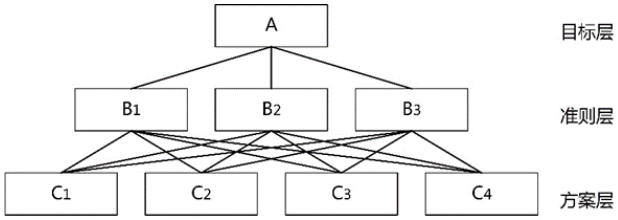

图 2　层次结构图

层次分析法中的一个关键步骤是分析两个元素之间的相对重要度, 以针对目标层 A 为例, 首先是构建基于 A 的准则层 B 的两两比较矩阵 M_{AB}, 则 M_{AB} 是一个 $n\times n$ 的矩阵:

$$M_{AB}=\begin{bmatrix} b_{11} & b_{12} & \cdots & b_{1n} \\ b_{21} & b_{22} & \cdots & b_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n1} & b_{n2} & \cdots & b_{nn} \end{bmatrix} \tag{1}$$

其中 b_{ij} 表示 b_i 相对于 b_j 的重要度. 这里引入 Saaty 提出的九分位[6]标示法来描述 b_{ij}, 如表 1 所示. 其中不难发现: $b_{ij}>0$; $b_{ij}=1/b_{ji}$; $b_{ii}=1$. 因此两两比较矩阵 M_{AB} 是一个三角矩阵. 这里的 b_{ij} 的取值由多个专家根据实际经验进行取值后进行平均.

表 1 九分位标示法

标记值	说明
1	ib_i 与 j 的重要度一样
3	i 相对于 jb_j 略显重要
5	i 相对于 j 明显重要
7	i 相对于 j 非常重要
9	i 相对于 j 特别重要
2、4、6、8	介于以上各重要程度之间
以上数值的倒数	以上 j 相对于 i 的重要程度

针对两两比较矩阵 M_{AB} 计算满足方程 $M_{AB}W_{AB}=\lambda_{\max}W_{AB}$ 的特征根和特征向量. 其中 $\lambda_{\max}$ 是 M_{AB} 的最大特征根, 如果 $W_{AB}=(w_1,w_2\cdots w_n)^T$ 是对应于 $\lambda_{\max}$ 的归一化特征向量, 那么 w_i 就是对应元素 i 的层次单排序的权值. 利用方根法, 有:

$$w_i=\frac{\sqrt[n]{\prod_{j=1}^{n}b_{ij}}}{\sum_{i=1}^{n}\sqrt[n]{\prod_{j=1}^{n}b_{ij}}} \tag{2}$$

$$\lambda_{\max}=\sum_{i=1}^{n}\frac{(M_{AB}W_{AB})_i}{nw_i} \tag{3}$$

当两两比较矩阵 M_{AB} 具有完全一致性时, $\lambda_{\max}=n$. 但是通常情况下由于专家对任意两个元素进行比较时, 无法保证 n 个元素的重要度的一致性, 因此引入两两比较矩阵的一致性判断指标:

$$CI=\frac{\lambda_{\max}-n}{n-1} \tag{4}$$

当 $CI=0$ 时, 两两比较矩阵 M_{AB} 具有完全一致性; 当 CI 越大时, 两两比较矩阵 M_{AB} 的一致性就越差. 这里引入平均随机一致性指标 RI 来检验两两比较矩阵 M_{AB} 的一致性程度. 对于固定的值 n, 我们随机构造正互反矩阵 $R_{n\times n}$, 其元素值取 1~9 及其相应的倒数. 实验中, 我们取 1000 个样本保证样本空间足够大, 计算 $R_{n\times n}$ 的最大特征值的平均值 k, 则:

$$RI=\frac{k-n}{n-1} \tag{5}$$

通过实验计算出 RI 的值如表 2. 一般情况下, 1 阶矩阵和 2 阶矩阵总是具有完全的一致性, 因此 1 阶矩阵和 2 阶矩阵的 $RI=0$.

表 2 平均随机一致性指标 RI

n	1	2	3	4	5	6
RI	0	0	0.5173	0.8746	1.4112	1.2612

对于 2 阶以上的矩阵, 定义两两比较矩阵的随机一致性比率 CR, 它是 CI 和 RI 的比值. 规定一个阈值 ε, 当 $CR<\varepsilon$ 时, 判定两两比较矩阵 M_{AB} 基本一致; 当 $CR\geq\varepsilon$ 时, 判定两两比较矩阵 M_{AB} 不满足一致性要求, 则需要对两两比较矩阵 M_{AB} 进行修正, 直到 $CR<\varepsilon$ 为止. 一般情况下, $\varepsilon=0.1$.

依据层次结构模型, 分别计算出每一层中所有元素针对上一层元素的权重比例, 通过递归计算, 最终可以计算出方案层中的元素相对于目标层的组合权重.

下一步计算方案层 C 中所有元素针对准则层 C 中第 i 个元素的权重 $W_i^{(BC)}$. 根据上述方法有 $W_i^{(BC)}=(\omega_{i1},\omega_{i2}\cdots\omega_{im})^T$. 则通过递归计算, 可以计算出方案层 C 中所有元素相对于目标层 A 的组合权重 $W^{(AC)}=(W_1,W_2\cdots W_m)^T$. 其中:

$$W_i=w_i\sum_{j=1}^{n}\omega_{ij};\left(w_i\in W^{(AB)},\omega_{ij}\in W_i^{(BC)}\right) \tag{6}$$

4 基于AHP的综合熵权算法

通过层次分析法可以对 HTSAP 中各元素的权重进行计算, 它可以将一个复杂的网络进行层次化, 并将复杂的问题分解为有序的递进层级. 但是层次分析法在计算HTSAP中各元素权重时也存在一些问题. 首先, 根据层次分析法可以把负责的HTSAP分解为递进的层次, 它仅仅关注了上一层次中的元素对下一层次中的元素的约束关系, 但是同一层次中的元素之间的关系则认为是独立的, 从而忽视了元素间的关联关系对上一层次的贡献. 其次, 层次分析法中的两两比较矩阵中的两个元素间的重要度赋值完全依赖于专家的经验, 具有很强烈的主观性, 从而忽视了 HTSAP 中个元素之间客观存在的属性, 因此不同专家的判断之间会存在比较大的偏差. 另外, 层次分析法中给两两比较矩阵赋值的九分位标示法显得比较粗糙, 虽然现在也有其他的标示法, 比如三角标示法、分数标示法、指数标示法等[7], 但是总体上来说仍然显得不够精准.

因此本文将在层次分析法的基础上对 HTSAP 中元素权值的计算进行改进, 为了减小层次分析法中因为依赖主观因素对最终计算结果造成的影响, 采用熵权的计算进行修正.

熵最早是热力学中的一个物理量, 它用来表示分子状态混乱的程度. 1948 年, 香农借用热力学中熵的理论, 提出了信息熵[8]的概念. 在信息论中, 信息熵表示信号在被接收之前, 在传输过程中损失的信息量. 信息熵用来测量不确定性, 是一个随机变量可能出现

的期望值. 一个信息出现的机会越多则其概率越大, 那么它的不确定性则越小; 同理, 一个信息出现的机会越少则其概率越小, 那么它的不确定性越大.

假设随机变量 $X=\{x_1,x_2\ldots x_n\}$, 则可以定义 X 的熵 $H(X)$:

$$H(X)=kE(I(X)) \tag{7}$$

其中 k 为常数, E 代表了数学期望函数, 而 $I(X)$ 则表示 X 所含的信息量, 它也是一个随机变量. 假设 $P(x_i)$ 代表 X 处于 x_i 状态的条件概率, 则 X 的熵可以表示为:

$$H(X)=k\sum_{i=1}^{n}P(x_i)I(x_i)=-k\sum_{i=1}^{n}P(x_i)\log_b P(x_i)\lim_{x\to\infty} \tag{8}$$

其中 b 的取值可以是 2、10 或者自然对数 e. 在信息论中, 一般取 $b=2$.

在本文中, 考虑使用熵权法[9]对上文权值计算过程中的 $W^{(AB)}$ 和 $W_i^{(BC)}$ 进行修正. 熵权法是利用信息熵的概念来计算一个元素的权重. 一个元素的熵越小, 则该元素提供的信息量越大, 其指标值的差异度越大, 表现为该元素的权重越大; 相反, 一个元素的熵越大, 则该元素提供的信息量越小, 其指标值的差异度越小, 表现为该元素的权重越小.

假设某一层 A 的一个元素包含下一层 B 中的 n 个元素, 共有 m 个专家对 B 中的 n 个元素进行评价, 建立两两比较矩阵 $M_l=(b_{ij}^{(l)})_{n\times n}$, 它表示第 l 个专家构造的两两比较矩阵, b_{ij} 为依据表 1 对第 i 项和第 j 项元素进行的重要性比较并取值.

设 M_l 中第 i 行的向量 $V_{il}=\{b_{i1}^{(l)},b_{i2}^{(l)}\cdots b_{in}^{(l)}\},i\in[1,n],l\in[1,m]$, 它表示第 l 个专家针对元素 i 与其他所有元素的两两比较值的集合. 定义专家矩阵 R_i, 它表示所有专家针对元素 i 与其他所有元素的两两比较值的矩阵:

$$R_i=\begin{bmatrix}V_{i1}\\V_{i2}\\\vdots\\V_{im}\end{bmatrix}=\begin{bmatrix}b_{i1}^{(1)}&b_{i2}^{(1)}&\cdots&b_{in}^{(1)}\\b_{i1}^{(2)}&b_{i2}^{(2)}&\cdots&b_{in}^{(2)}\\\vdots&\vdots&\ddots&\vdots\\b_{i1}^{(m)}&b_{i2}^{(m)}&\cdots&b_{in}^{(m)}\end{bmatrix} \tag{9}$$

对矩阵 R_i 中的每一行进行归一化, 得到归一化后的专家矩阵 R_i':

$$R_i'=(r_{lj})_{m\times n}=\begin{bmatrix}r_{11}&r_{12}&\cdots&r_{1n}\\r_{21}&r_{22}&\cdots&r_{2n}\\\vdots&\vdots&\ddots&\vdots\\r_{m1}&r_{m2}&\cdots&r_{mn}\end{bmatrix} \tag{10}$$

$$r_{lj}=\frac{1}{n}\sum_{j=1}^{n}b_{ij}^{(l)},l\in[1,m],j\in[1,n] \tag{11}$$

在上面的分析过程中, V_{il} 记录了元素 i 与其他元素的重要度两两比较结果, 如果 V_{il} 中各个值的结果比较相近即差异度较小, 说明元素 i 对整体评价的贡献比较低, 则该元素的权重较小, 反映出来的熵较大; 同理, 如果 V_{il} 中各个值的结果差异度较大, 说明元素 i 对整体评价的贡献比较高, 则该元素的权重较大, 反映出来的熵较小.

针对元素 i, 定义第 l 个专家对其评估的熵为:

$$H(i,l)=-k\sum_{j=1}^{n}r_{lj}\log_2 r_{lj} \tag{12}$$

假设在极端情况下, V_{il} 中的各个值差异度一致 $r_{lj}=1/n$, 也就是元素 i 对整体评价的贡献最低, 权重最小, 此时的熵最大, 令 $H(i,l)=1$, 则:

$$-k\sum_{j=1}^{n}\frac{1}{n}\log_2\frac{1}{n}=1\Rightarrow k=\frac{1}{\log_2 n} \tag{13}$$

计算元素 i 的熵权 ϕ_{il}, 由于熵值越大熵权越小, 通过归一化, 求出:

$$\phi_{il}=\frac{1-H(i,l)}{n-\sum_{l=1}^{m}H(i,l)} \tag{14}$$

令 $\Phi_i=(\phi_{i1},\phi_{i2}\cdots\phi_{im})$, 则经过熵权法修正后的 AHP 两两比较矩阵 M' 可以表示为:

$$M'=(\Phi_1R_1',\Phi_2R_2',\cdots\Phi_nR_n')^T \tag{15}$$

根据公式(2)即可计算出基于 AHP 的综合熵权 W'.

5 实验分析

本文以中国科技网骨干网为例, 基于HTSAP框架, 中国科技网骨干网的拓扑层可以分为出口层、核心层、汇聚层、接入层、终端层. 其风险因素层包括资产影响、威胁和脆弱性.

资产影响包括资产的保密性、完整性、可用性和业务相关性 4 个因素; 威胁包括物理环境问题或自然灾害、物理破坏、软硬件故障、操作失误、恶意代码攻击、越权或权限滥用、网络攻击、失泄密、篡改、抵赖、管理缺失 11 个因素; 脆弱性包括该脆弱点的影响级别、技术难度、利用价值、管理漏洞、防范措施 5 个因素.

实验中我们邀请 10 位专家分别进行评估, 这 10 位专家由核心运维人员 3 人、安全管理人员 3 人和终端用户网络管理员 4 人组成.

首先构建拓扑层针对目标层的两两比较矩阵，分别计算其随机一致性比例 CR，结果均小于 0.1，因此可以认为该 10 名专家构建的两两比较矩阵满足一致性要求.

分别计算归一化后的专家矩阵，熵权值和修正后的两两比较矩阵，最终求得综合权重向量为 $W_{AB}'=(0.0482,0.3267,0.0619,0.5041,0.0592)$. 通过未加改进层层次分析法求出的权重向量 $W_{AB}=(0.1555,0.1996,0.3085,0.0845,0.2519)$. 如表 3 所示:

表 3 拓扑层权重分析

拓扑层	层次分析法权重(%)	综合熵权法权重(%)
出口层	15.55	4.82
核心层	19.96	32.67
汇聚层	30.85	6.19
接入层	8.45	50.41
终端层	25.19	5.92

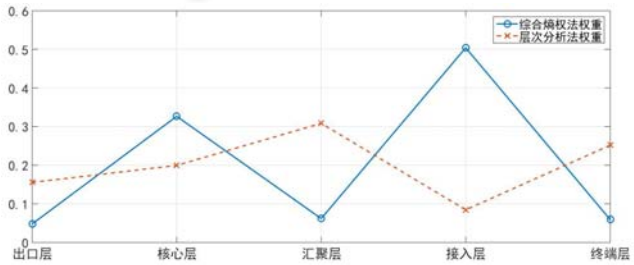

图 3 拓扑层权重结果分析

从表 3 和图 3 中我们可以分析拓扑层相对于整体安全态势的权重分布. 根据层次分析法计算的结果显示，汇聚层的权重最高，其次是终端层，核心层和出口层的权重相似，接入层的权重显著较低. 而根据综合熵权法计算的结果显示，接入层的权重最高，核心层的权重其次，其他三层的权重显著较低.

但是我们在实际的运维过程中发现核心层和汇聚层一般都位于核心机房，设备数量较接入层和终端层少. 另一方面，汇聚层一般情况下都有冗余，因此该层设备即使出现故障也不会对整体网络造成太大的威胁. 而对于广泛分布的接入层和终端层来说，其设备数量比较庞大，单就接入层和终端层来说，接入层的重要性要高于终端层，因为终端层的计算机等设备即使被攻击或者损坏也不会对骨干网造成太大损失，但是接入层负责大量的终端接入，一个设备故障可能导致非常多的终端无法与互联网连接. 因此通过综合熵权法计算出来的权重比较能真实的反映出拓扑层对整体网络安全态势的贡献度.

根据上述方法计算风险因素层各因素针对拓扑层个因素的权重，最后计算风险因素层个因素针对目标层即整体网络安全态势的权值，如表 4.

表 4 风险因素权重分析

类别	风险因素层 风险因素	标记	层次分析法 权重(%)	综合熵权 法权重(%)
资产影响	保密性	P_1	5.48	4.10
	完整性	P_2	4.68	7.29
	可用性	P_3	5.15	5.17
	业务相关性	P_4	4.41	5.81
威胁	物理环境问题	T_1	5.29	4.39
	物理破坏	T_2	4.93	4.77
	软硬件故障	T_3	4.20	5.10
	操作失误	T_4	4.23	4.65
	恶意代码攻击	T_5	5.07	5.06
	越权或权限滥用	T_6	5.16	3.65
	网络攻击	T_7	4.98	6.74
	失泄密	T_8	4.61	5.07
	篡改	T_9	5.79	4.20
	抵赖	T_{10}	4.88	3.28
	管理缺失	T_{11}	4.22	7.52
脆弱点	影响级别	V_1	4.96	4.65
	技术难度	V_2	5.70	4.16
	利用价值	V_3	5.35	4.40
	管理漏洞	V_4	5.26	6.27
	防范措施	V_5	5.65	3.72

从图 4 风险因素权重结果分析中分析发现，基于层次分析法对风险因素计算的权重数值比较平均，都在平均值 5%上下波动，波动大小不超过±1%. 因此基于传统的层次分析法计算的风险因素权值不能明显的表示各个风险因素对整体态势评估的贡献度. 而基于本文提出的综合熵权算法，风险因素的权值则有比较明显区分. 从图中可以看出 P_2、P_4、T_7、T_{11}、V_4 明显比平均值高，其对应的是资产的完整性、业务相关性、网络攻击、管理缺失和管理漏洞，从实际运维的经验来看，这几项对整体安全态势评估的贡献的确要高于其他因素. 另外，T_6、T_{10}、V_5 明显比平均值低很多，其对应的是越权或权限滥用、抵赖、防范措施，它们对整体安全态势评估的共享比较低.

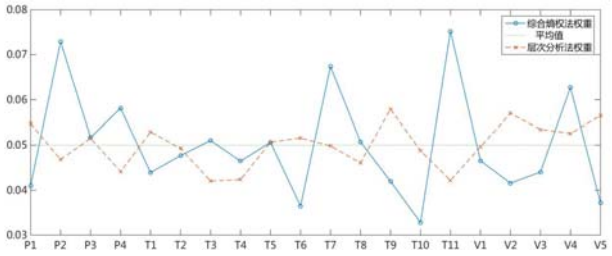

图 4 风险因素权重分析结果

从上述实验结果的分析来看，本文提出的基于 AHP 的综合熵权算法比传统的层次分析法在 HTSAP 的权重计算结果上要更加精确，计算过程更加合理.

6 结语

本文在特定的大规模网络环境下，提出了一种网络拓扑层次化安全评估框架，并基于该框架设计了一种安全评估中风险因素权重的计算方法，通过在中国科技网上的验证，该算法计算结果更加合理. 但是该算法也还存在一些问题，比如当安全因素数量过多时，专家在构建两两比较矩阵时工作量太大，另外构建的矩阵一致性也难以保证，这些都是下一步研究工作中需要解决的问题.

参考文献

1 国家计算机网络应急技术处理协调中心.2013 年中国互联网网络安全报告.2014–06.
2 国家计算机网络应急技术处理协调中心.2013 年我国互联网网络安全态势综述.2014–03.
3 GB/T 20984–2007.信息安全技术信息安全风险评估规范.中华人民共和国国家标准,2007.
4 Saaty TL. Decision making — the analytic hierarchy and network processes (AHP/ANP). Journal of Systems Science and Systems Engineering, 2004.
5 陈治宏,卢国明,吴晓华,郝玉洁,李建平.基于 AHP 的群决策风险评估方法.计算机应用,2009,S1:125–127,145.
6 杨雅婷,马博,苏国平,蒋同海,李晓.区域信息化水平评价方法研究.计算机工程,2010,13:272–275.
7 付国庆,龚军,吕小毅.基于 AHP 与模糊数学的信息安全风险评估模型.信息安全与通信保密,2014,10:100–103.
8 Stinson DR. Cryptography: Theory and Practice. CRC Press, 2005.
9 王犇,周兴社,杨亚磊.基于多属性熵权合成的软件可信等级评估方法.微电子学与计算机,2014,6:21–24.