一种确定网络安全度量指标体系参考框架的方法

马 锐, 葛 慧, 顾升高, 王克克, 靳 骁, 吴 丹
中国航天系统科学与工程研究院 北京 中国 100048

摘要 评价主体、评价对象和评价尺度组合的多样性决定了评价指标体系的不唯一性, 本文设计了一种网络安全度量指标体系性能评估的理论方法。结合“熵”、“博弈论”的相关思想, 设计了“熵-博弈指标体系优化模型”, 通过对指标区分度的计算以及结合指标重要程度因素的修正, 对指标体系整体区分度进行测算, 比较同一评价对象下不同网络安全度量指标体系的性能差异。通过实例验证了典型网络环境下该理论方法的合理性和可行性。为不同行业、不同业务、不同组成对象甚至同一系统不同时期的网络确定与其相适应的网络安全度量指标体系参考。

关键词 熵; 博弈论; 区分度; 指标体系性能
中图法分类号 TP393 DOI 号 10.19363/J.cnki.cn10-1380/tn.2019.01.06

A Method for Determining the Reference Framework of Network Security Metric Index System

MA Rui, GE Hui, GU Shenggao,WANG Keke, JIN Xiao,WU Dan
China Aerospace Academy of System Science and Engineering, Beijing 100048, China

Abstract The diversity of evaluation subjects, evaluation objects and evaluation scales determines the non-uniqueness of the evaluation index system. In this paper, a theoretical method for evaluating the performance of network security metric index system is designed.Combination of “entropy”, “game theory” related ideas, designs “the index system optimization model of entropy-game theory”, through the calculation of index degree of differentiation and the correction of combining with index importance factor, to measure index system of the overall degree of differentiation, comparing the same evaluation objects under different network security measure index system of performance differences.The rationality and feasibility of the theory and method in typical network environment are verified by an example. For different industries, different services, different components and even the same system in different periods of the network to determine the corresponding network security metrics system reference.

Key words entropy; game theory ; degree of differentiation; the performance of network security metric index system

1 引言

网络安全度量指标体系是网络安全风险评估的工作基础[1], 通常包括了各类信息系统内各种信息资源的各类指标, 指标体系应客观地反映被评价信息系统的安全保障能力。在面对不同评估目标和评估场景时, 应在分析影响信息系统安全性的关键技术和管理因素的基础上, 采用科学的方法进行指标选取, 以最大程度上客观地反映信息系统的安全保障能力。

指标的选取在复杂系统的研究中是一个关键问题。该问题具有较高难度, 指标不足会使信息量不足而影响分析与评价结果, 指标过多则会产生冗余信息, 增加分析和计算的难度[2]。网络安全度量指标体系参考框架的确定是寻找一种能够从大量的指标中消除冗余指标的方法, 选出能够反映系统演化状况的指标最小集合, 并对指标体系的整体区分度进行测算, 以衡量不同情况下网络安全度量指标体系的适用程度。

本文借助于熵理论解决筛选指标的不确定性问题, 将熵理论应用到“指标筛选”的过程中去, 并引用了指标“区分度”的概念[2-3], 同时为兼顾指标的其他特性, 引用博弈论[4]的相关理论, 对指标区分度进行修正。指标区分度是指指标相对于同一层次其他指标对于给定评价对象的区分程度或鉴别能力。区分度高的指标, 对于评价对象评定具有更高的代

通讯作者: 马锐,研究员, Email:mar@spacechina.com。
本课题得到国家重点研发计划项目(No. 2016YFB0800700)资助。
收稿日期: 2018-09-30; 修改日期: 2018-11-23; 定稿日期: 2018-12-14

表性; 区分度低的指标, 对于评价对象评定的意义相对较小。通过测算指标本身对评价对象的区分度, 得知同一层次的评价指标相对于其它指标对于给定评价对象的区分能力的大小, 进而实现指标的合理筛选, 避免因追求指标体系全面性而造成指标冗余。为测算度量指标体系区分能力大小, 本文把“区分度”的测算扩展到整个度量指标体系中去, 根据指标体系的层次结构实现了对度量指标体系整体区分度的测算。指标体系的整体区分度反映了该指标体系对待评价对象的区分能力的大小, 当针对同一组待评价对象构建出了几种不同的度量指标体系时, 通过对指标体系整体区分度的合理测度, 可以帮助识别哪一种指标体系区分能力更好, 进而实现对不同的度量指标体系的合理筛选, 提高了指标体系的可执行性。

2 研究现状

2.1 “指标筛选”相关理论方法的国内外研究现状

构建度量指标体系需要相关评价方法和评价理论的强有力支撑, 只有建立在科学的方法与理论基础上的度量指标体系才具有可靠性和可信度, 指标筛选是指标体系构建的关键一步。

目前, 国内外支撑评价指标筛选的方法有很多, 具体来说可以分为三大类, 即: 定性分析法、定量分析法和定性定量相结合分析法[4-5]。定性分析法主要是从评价的目的和原则出发,由系统分析人员与决策者主观确定有哪些指标组成系统的评价准则体系。以德尔菲法为例, 其依靠专家的经验进行综合评价, 优势是有效利用了专家的知识和经验, 但主观性太强, 时间成本高。定量分析法主要根据指标间的数量关系运用数学方法[6]筛选出所需指标, 其代表有主成分分析法、灰色关联分析法、因子分析法、粗糙集理论分析[7-9]方法等。主成分分析法应用主分量分析的“最佳简化”原则,将一个多变量的高维系统通过降维处理求得最具有代表性的若干主分量来近似表达待评系统的评价指标。灰色关联分析法根据因素之间发展趋势的相似或相异程度来衡量因素间关联程度, 借助于灰色关联度模型来完成计算分析工作。因子分析法研究变量内部相关的依赖关系, 把一些具有错综复杂关系的变量归结为少数几个综合因子。粗糙集理论建立在分类机制的基础上, 将分类理解为特定空间上的等价关系, 主要思想是利用已知的知识库, 将不精确或不确定的知识用已知的知识库中的知识来刻画。定量评价以严谨的数据理论为基础, 克服了人为因素的干扰, 但普遍存在的问题是一些量化的数值没有确切的意义, 常理上不为人们所接受。定性定量相结合评价法是目前指标筛选常用的方法。定性评价采用数学工具进行计算, 定量评价建立在定性预测基础上, 将定量与定性结合起来, 将主观因素应用到目标规划模型的约束条件当中, 实现主观和客观的有机融合是比较理想的指标筛选方法。

国内外许多学者以不同的理论方法对指标筛选这一问题做了大量的研究工作, 也取得了许多研究成果[10,11-13], 但是, 到目前为止大多数研究成果主要集中在指标筛选方面, 极少考虑筛选出来的指标是否具有区分性。指标区分度应作为指标筛选的一个重要考量因素。

2.2 “指标体系性能评价”研究现状

度量指标体系是指可表征评价对象各方面特性及其相互联系的多个指标所构成的具有内在结构的有机整体。评价所建立的指标体系是否合理、科学包括考察指标体系的完整度、区分度、可操作度等多个方面。指标体系性能的评价是指对同类指标体系之间进行比较, 根据指标精简性和普适性要求选出最有效的指标体系。国内学者对指标体系性能评价的研究甚少, 缺少对同类指标体系优选的研究, 更没有对指标体系性能定量评价方法的研究。由于指标体系在完整度、可操作度等方面主观性强, 采用量化分析的可能性和意义不大, 因此本文考虑从指标体系区分度角度度量指标体系的性能。

2.3 熵理论在信息领域的应用[14-15]

熵的概念是由德国物理学家克劳修斯(K.Clausius)于1856年所提出并应用于物理学热力学中, 是用来描述“能量退化”的物质状态参数之一, 最初仅仅是一个可以通过热量改变来测定的物理量, 其本质没有很好的解释。

1877年左右, 奥地利物理学家波尔兹曼(Boltzmann)在研究气体分子运动过程中, 基于把热理解为微观世界分子运动的观点, 对熵作出微观解释。波尔兹曼认为, 在有大量粒子(原子、分子)构成的系统中, 熵就是表示粒子之间的混乱程度的物理量。当一个系统处于平衡时, 系统的微观能量状态个数越多, 熵也越大。如果以Q表示微观能量状态个数, 则它与系统的熵H有如下关系:

$$H = K \ln Q$$

式中K是波尔兹曼常数, 是一个与研究对象有关的常数。从波尔兹曼提出的熵概念可以看出, 熵是研究群

体行为规律的, 而不是研究个体行为的。

1948年, 维纳(N．Wiener)和香农(C.E.Shannon)创立了信息论, 并把熵引用到信息论领域, 香农把通信过程中信息源的信号的不确定性称为信息熵, 把消除了多少不确定性称为信息。信息论针对通信需要两个等概率状态对应的熵定义为1bit(比特)的计值方法不仅在通信中十分有用, 而且在后来兴起的电子计算机技术中的存储量单位中也得到了应用。信息熵成为信息论的一个正统的分支。

香农用“熵”来表征信息的特性, 给出了信息熵公式: $H=-k\sum P_i \log P_i$ (常数 k 仅等于度量单位的选择), 用来表述选择和不确定性与随机事件的连带关系, 一举解决了定量描述信息的难题。他解释道: “量 $H=-k\sum P_i \log P_i$ 在信息论中起着重要的作用, 它作为信息、选择和不确定性的度量, H的公式与统计力学中熵的公式是一样的。式中P表示一个系统处在向量空间中第i个元的概率。因此, 这里的H就是波尔兹曼著名的H定理中的H”。如此熵概念再次得以扩展, “信息量的平均具有熵的各种性质”这一点意味着熵通过信息论, 将会应用于超出自然科学的一些领域。在信息论的带动下, 熵概念首先进入了概率论、通信和计算机领域[16-18]。20世纪后半叶, 以电子计算机为代表的信息革命方兴未艾, 推进了与信息密切相关的熵概念的史无前例的大扩展。纵观熵140多年的历史, 可以说, 熵是对“不确定性”的最佳测度。

目前, 在信息论领域, 熵理论主要应用于指标赋权[19,20]方面的研究。实际上, 根据熵理论中熵权的定义及其性质, 熵权代表该指标在该问题中提供有用信息量的多少, 因此, 熵权的大小并不适合反映指标重要程度特性, 而是适合于反映指标区分度[21]特性。

2.4 本文的研究思路

指标体系是否合理、科学、简明、实用, 决定了评价结果是否真实可行, 而评价主体、评价对象和评价尺度组合的多样性也决定了评价指标不是固定不变的。

本文提出一种针对不同行业不同信息系统确定网络安全度量指标体系参考框架的理论方法: 构建基于熵权区分度的安全度量指标体系优化模型——熵-博弈指标体系优化模型, 实现针对不同评估目标及应用场景[22]的安全度量指标体系优化模型的区分优化, 通过选取信息量大、代表性强的有效指标, 提高安全度量效率、防止指标泛滥, 避免评价结构失真; 基于安全机制有效性评估、系统脆弱性评估以及攻击影响评估[23,24]的通用安全度量指标体系, 建立基于博弈理论的指标区分度-指标重要程度的指标筛选博弈模型, 修正指标区分度, 优化评价结构, 完善熵-博弈指标体系优化模型; 通过对同一类型不同信息系统、以及同一信息系统的不同时间点分别实施安全度量, 对熵-博弈指标体系优化模型进行试验验证。

3 一种确定网络安全度量指标体系参考框架的“熵-博弈指标体系优化模型”

通常在构建一个度量指标体系的事前和事后阶段, 均不考虑评价结果的准确性, 当构建完成后, 即便评价结果不准确也难以修正。虽有部分学者探讨过该问题, 也仅仅局限于主观层面, 缺少理论依据, 如有些是以评价结果是否与实际情况相符为标准, 有些是以评价过程中的方法运用是否合理为标准, 甚至还些是将该度量指标体系的评价结果与其他度量指标体系的评价结果进行对比, 若相近则为合理等等。

本文引用熵理论中“熵”的基本思想, 以评价指标“区分度”和“重要性”为基础, 结合度量指标体系的组织结构, 基于熵理论测算度量指标体系整体区分度, 以确定针对不同评估对象的网络安全度量指标体系参考框架。首先, 将“熵权”应用到指标筛选的过程中, 对指标本身的对评价对象的区分度进行测算, 然后根据指标重要程度, 通过博弈模型对指标区分度进行修正, 进而根据该区分度的大小, 可以在因追求指标体系全面性而造成指标过多时实现指标的合理筛选。最后, 把度量指标体系整体区分度进行测算, 当针对同一组评价对象构建出几种不同的指标体系的时候, 通过对指标体系的整体区分度的合理测度, 确定哪一种指标体系区分度更强, 评价效果更好。

本方法主要有以下几个优点:

(1) 以客观的目标规划对象为主体, 将主观因素寓于到目标规划模型的约束条件当中, 实现了主观和客观的融合。

(2) 以解决不确定性、离散性问题见长的熵理论作为基础, 对指标区分度及指标体系整体性能进行测算。

(3) 将指标重要程度作为合理性影响因子对指标区分度进行修正, 使安全度量指标体系优化模型更具有科学性和合理性。

3.1 指标本身对评价对象的区分度测算

在信息论中, 信息熵表示的是不确定性的量度。

一个系统越是有序, 信息熵就越低; 一个系统越是混乱, 信息熵就越高。所以, 信息熵也可以说是系统有序化程度的一个度量。根据信息熵的定义, 对于某项指标, 可以用熵值来判断某项指标的离散程度, 其熵值越小, 指标的离散程度越大, 该指标对综合评价的影响就越大, 如果某项指标的值全部相等, 则该指标在综合评价中不起作用。

某项指标对于不同的评估对象其评价结果是不确定的。不确定性是客观事物本身具有的一种普遍规律, 任何事物的不确定性都是绝对的, 而确定的、规律性的东西是相对的。这在熵的理论中, 被描述为基熵, 即任何事物本身都具有基熵, 无论采用多么有效的降熵措施, 都不可能使其低于基熵。指标区分度大小的意义在于进行网络安全评估时, 指标为评价对象提供有用信息量的多少。评价结果的离散程度越大, 表明指标的区分度越大, 对评估结论影响越大, 反之, 评价结果越接近, 表明指标的区分度越低, 对评估结论的影响越小。这些与熵的思想是一致的, 将熵理论应用于指标区分度测算上, 完全符合指标体系区分度和熵理论的特点。本文运用熵理论来解决某项指标相对于评价对象的其他指标的区分度问题。

假设有 m 个评估指标, n 个评价对象(方案), 按照定性与定量相结合的原则得到如下多对象关于多指标的评价矩阵。

$$R'=\begin{bmatrix} r'_{11} & r'_{12} & \cdots & r'_{1n} \\ r'_{21} & r'_{22} & \cdots & r'_{2n} \\ \vdots & \vdots & & \vdots \\ r'_{m1} & r'_{m2} & \cdots & r'_{mn} \end{bmatrix}$$

由于各指标的计量单位并不统一, 因此在用它们计算综合指标前, 先对它们进行标准化处理, 即把指标的绝对值转化为相对值, 从而解决各项不同质指标值的同质化问题。对 R' 作标准化处理得到

$$R=(r_{ij})_{m\times n}$$

其中: r_{ij} 称为第 j 个评价对象在指标 i 上的值, $r_{ij}\in[0,1]$, 且:

$$r_{ij}=\frac{r'_{ij}-\min\limits_{j}\{r'_{ij}\}}{\max\limits_{j}\{r'_{ij}\}-\min\limits_{j}\{r'_{ij}\}}$$

i=1, 2,⋯,m $\quad$ j=1, 2,⋯, n

评价指标的熵的定义: 在有 m 个评价指标, n 个评价对象的评估问题中, 第 i 个评价指标的熵定义为:

$$H_i=-k\sum_{j=1}^{n}f_{ij}\ln f_{ij} \qquad i=1,2,\cdots,\ m$$

其中: $f_{ij}=\dfrac{r_{ij}}{\sum\limits_{j=1}^{n}r_{ij}}$, $k=\dfrac{1}{\ln n}$

其中, f_{ij} 表示每种可能事件的概率, $-\ln f_{ij}$ 表示每种可能事件包含的信息量的不确定性函数。H_i 的取值范围为 $0\leqslant H_i\leqslant 1$, 在实际情况中, H_i=1 时, 表示该指标对评价对象没有提供任何有价值的信息; H_i=0 时, 意味着只需指标 i 就能涵盖所有的信息量完成评价对象的评估, 这表明剩余的指标没有任何有效信息, 因此在实际情况中 H_i=0 是不合理的, $H_i\neq 0$。

熵权的定义: 在(m, n)评价问题中, 第 i 个指标的熵权 w_i 定义为:

$$w_i=\frac{1-H_i}{m-\sum\limits_{i=1}^{m}H_i}$$

从熵权的定义可以看出: 当评价对象在指标 i 上的值完全相同时, 该指标的熵达到最大值 1, 其熵权为 0。说明该指标未能提供有用信息, 可以考虑去掉。当评价对象在指标 i 上的值相差较大, 熵值较小, 熵权较大。说明该指标向决策者提供了有用信息, 同时还告诉我们在该问题中, 各对象在该指标上有明显差异, 应重点考虑。指标熵越大, 其熵权越小, 且满足:

$$\begin{cases} 0\leqslant w_i\leqslant 1 \\ \sum\limits_{i=1}^{m}w_i=1 \end{cases}$$

评价指标区分度的定义: 在(m, n)评估问题中, 若第 i 个指标的熵值为 H_i, 熵权值为 w_i, 则该指标的区分度 η_i 为:

$$\eta_i=\frac{w_i}{H_i}=\frac{1-H_i}{\left(m-\sum\limits_{i=1}^{m}H_i\right)H_i} \qquad i=1,\ 2,\ \cdots,\ m$$

其中, $H_i=-k\sum\limits_{j=1}^{n}f_{ij}\ln f_{ij}$

3.2 指标区分度与指标重要程度的博弈模型

虽然基于熵理论的指标区分度方法模型能较好地对指标进行筛选, 但其过程中忽略了对指标重要性的考察, 无法避免与指标重要性的矛盾。不可否认的是, 重要性也是信用度量指标体系构建过程中尤

为重要的指标表征量, 指标体系在构建中应均衡指标区分度和指标重要程度二者的关系。

安全是未来信息技术研究中最大挑战之一, 不仅是通过技术、管理等手段解决信息安全问题, 信息安全技术本身的评价也是信息技术安全的重要组成部分。目前, 对信息安全技术的评价有两类: 一是从技术的角度, 评价信息安全技术的有效性和性能, 二是应用数学、经济学、管理学的方法对信息安全技术的价值进行评价。随着信息系统复杂程度的提高, 解决复杂问题的数学、经济学、管理学越来越多地应用于信息安全技术评价中。

博弈论[25,26], 又被称为对策论, 既是现代数学的一个新分支, 也是运筹学的一个重要学科。博弈论是研究决策者在决策主体各方相互作用情况下如何进行决策和分析这种决策均衡性的问题[27]。与其他理论不同, 博弈论强调决策主体各方策略的相互依存性, 即任何一个决策主体必须在考虑其他局中人应对策略的基础上来选择自己最理想的行动方案。参与主体各方的最优策略组合进行博弈, 博弈产生的结果是均衡的。但这个结果可能不是各方主体及整体的利益最大化的一个, 而是在已给定的信息与知识条件下的一种必然产生的结果。因为任何一方改变策略而导致均衡的变化都可能使自己得到一个更差的结果。

从博弈论的观点来看, 典型的信息安全实际上是信息保护者与入侵者之间的博弈, 信息保护者希望信息系统不遭受信息安全事件或最小化信息安全事件的影响, 入侵者希望入侵成功, 获取最大的信息。双方博弈的结果是达到一种平衡。在信息安全领域, 博弈论被广泛应用以描述相互牵制的多因素之间的关系[28,29]。网络安全度量指标的区分度与指标重要程度两个因素在指标筛选过程中相互关联又相互制约, 单纯依赖某种因素构建的指标体系是不恰当的, 应综合考虑两种因素并取得两者的平衡。本文拟采用博弈论的方法构建指标筛选博弈模型[30], 均衡指标区分度和指标重要程度二者的关系, 以根据博弈结果对指标区分度进行修正。

指标筛选博弈模型

定义 指标筛选博弈模型 DISU(Discrimination Importance Strategy Utility)是一个四元组 DISU=(D, I, S, U), 其中

①D=(D_1, D_2, …, D_n)是参加指标筛选博弈的指标区分度集合(discrimination set), 局中人是博弈的决策主体和策略制定者。在不同的博弈中局中人的含义是不同的, 既可以是个人也可以是具有共同的目标和利益的团体或者集团。

②I=(I_1, I_2, …, I_n)是参加指标筛选博弈的指标重要程度集合(importance set), 局中人是博弈的决策主体和策略制定者。在不同的博弈中局中人的含义是不同的, 既可以是个人也可以是具有共同的目标和利益的团体或者集团。

③S=(S_1, S_2, …, S_n)是局中人的策略集合(strategy set), $i\in n$, S_i=(s_i^d; s_i^i)是指标区分度和指标重要程度(策略)二元组, $S_i=(s_1^d,s_2^d,\cdots,s_n^d;s_1^i,s_2^i,\cdots,s_n^i)$ 表示局中人的策略集合, 是局中人进行博弈的工具和手段, 每个策略集合至少应该有两个不同的策略, 即 n> 2。

④U=(U_1, U_2, …, U_n)是局中人的效用函数集合(utility function set)。$i\in n$, U_i 是效用值。效用值表达了指标区分度、指标重要程度双方从博弈中能够得到的收益水平, 它是所有局中人策略的函数。不同的策略可能得到不同收益, 它是每个局中人真正关心的参数。

图 1 给出了指标筛选博弈模型的示意图, 该模型是博弈模型的通用模型。指标筛选博弈模型四元组为: DISU=(D, I, S_i, U_i), 其中 D 表示指标区分度, I 表示指标重要程度。$S_i=(s_1^d,s_2^d,\cdots,s_n^d;s_1^i,s_2^i,\cdots,s_n^i)$ 表示指标区分度、指标重要程度策略集合。U_i 表示指标区分度、指标重要程度的指标收益。指标筛选博弈模型可以用一个矩阵描述, 见图 2, 矩阵中的列表示指标重要程度, 矩阵中的行表示指标区分度。矩阵中的数值表示指标区分度、指标重要程度的收益值。

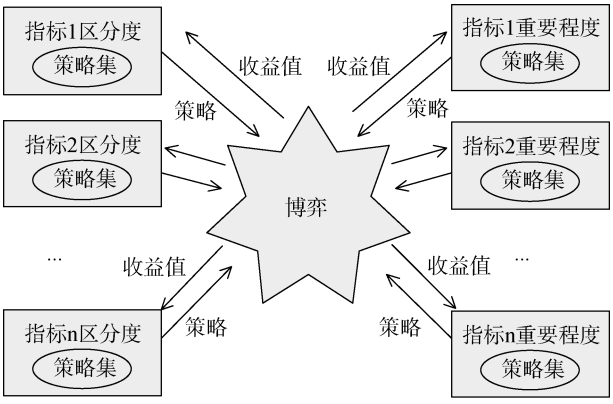


图 1 指标筛选博弈模型示意图

Figure 1 Index selection game theory model

$$\begin{array}{c} \\ S_1^d \\ S_2^d \\ S_3^d \end{array}\begin{array}{c} \begin{array}{cccccc} S_1^i & & S_2^i & & S_3^i & \end{array} \\ \begin{bmatrix} (U_{d11} & U_{i11}) & (U_{d12} & U_{i12}) & (U_{d13} & U_{i13}) \\ (U_{d21} & U_{i21}) & (U_{d22} & U_{i22}) & (U_{d23} & U_{i23}) \\ (U_{d31} & U_{i31}) & (U_{d32} & U_{i32}) & (U_{d32} & U_{i33}) \end{bmatrix} \end{array}$$

图 2 指标区分度-重要程度指标筛选博弈矩阵

Figure 2 Game theory matrix of Index differentiation- importance degree selection

本文将指标区分度、指标重要程度的收益值之比作为指标区分度的修正参数 k, 指标区分度修正参数与指标区分度成反比, 指标区分度调整参数越大表示指标重要程度相对于指标区分度越不重要, 指标区分度需要进行较大调整; 指标区分度调整参数越小表示指标重要程度相对于指标区分度越重要, 指标区分度只需要进行较小的调整。

3.3 指标体系整体区分度测算方法

假设待评价对象的整体区分度为 $\eta_{整体}$, 待评价对象的一级指标权熵为 $(w_1,w_2,\cdots,w_n)$, 该一级指标对应的区分度大小为 $(\eta_1,\eta_2,\cdots,\eta_n)$, 指标区分度修正参数为 $(k_1,k_2,\cdots,k_n)$。一级指标 1 对应的二级指标的权熵为 $(w_{11},w_{12},\cdots,w_{1k})$, 对应的区分度为 $(\eta_{11},\eta_{12},\cdots,\eta_{1k})$, 指标区分度修正参数为 $(k_{11},k_{12},\cdots,k_{1k})$, 一级指标 n 对应的二级指标的权熵为 $(w_{n1},w_{n2},\cdots,w_{nj})$, 对应的区分度为 $(\eta_{n1},\eta_{n2},\cdots,\eta_{nj})$, 指标区分度修正参数为 $(k_{n1},k_{n2},\cdots,k_{nj})$。

其中, $(w_1,w_2,\cdots,w_n)$, $(w_{11},w_{12},\cdots,w_{1k})$, $(w_{n1},w_{n2},\cdots,w_{nj})$, $(\eta_{11},\eta_{12},\cdots,\eta_{1k})$, $(\eta_{n1},\eta_{n2},\cdots,\eta_{nj})$ 都是已知的, 则可以构建该度量指标体系的整体区分度 $\eta_{整体}$。其计算过程如下:

计算一级指标区分度 $(\eta_1,\eta_2,\cdots,\eta_n)$

$$\eta_1=\sum_{i=1}^{k}w_{1i}\eta_{1i}k_{1i}$$

$$\cdots\cdots$$

$$\eta_n=\sum_{i=1}^{j}w_{ni}\eta_{ni}k_{ni}$$

求解该度量指标体系的整体区分度 $\eta_{整体}$

$$\eta_{整体}=\sum_{i=1}^{n}w_i\eta_i k_i$$

由上述计算过程可以总结出度量指标体系的整体区分度 $\eta_{整体}$ 的测算模型如下:

$$\eta_{整体}=w_1k_1\sum_{i=1}^{k}w_{1i}\eta_{1i}k_{1i}+\cdots\cdots+w_nk_n\sum_{i=1}^{j}w_{ni}\eta_{ni}k_{ni}$$

其中: $(\eta_{11},\eta_{12},\cdots,\eta_{1k})$, ……, $(\eta_{n1},\eta_{n2},\cdots,\eta_{nj})$ 是底层指标的“区分度”;

$(w_{11},w_{12},\cdots,w_{1k})$, ……, $(w_{n1},w_{n2},\cdots,w_{nj})$ 为底层指标对其上层指标的权熵;

$(w_1,w_2,\cdots,w_n)$ 为一级指标的权熵。

当一个指标体系构建起来以后, 将各级指标的重要程度确定下来, 并用一个相对值表示出来后, 这时只需要底层指标的“区分度”的值便可以计算出指标体系的整体区分度的大小, 而底层指标的区分度可以使用“区分度”的计算公式获得。经过层层计算, 最终可以得到整个度量指标体系的“区分度”数值。

3.4 指标体系合理性分析

分别对构建的指标体系进行区分度测算, 根据指标体系整体区分度, 可以对所选取的指标体系的合理性进行判断, 以选择合适的指标体系。

不同行业的业务特征不同, 信息系统也各不相同, 面对同一种安全风险所产生的安全影响也不同, 因此, 安全度量的尺度也应有所区别, 适合所有行业的指标体系是不存在的。在构建的各种指标体系中, 经过对不同的评估对象不断的评估实践, 对指标体系的性能进行分析和计算, 找出最适合本行业的指标体系是网络安全度量科学研究应予解决的问题。

4 应用实例与分析

下面应用第 3 章的熵-博弈指标体系优化模型, 以实例验证上述指标体系区分度测算方法的可用性和可操作性。假设有一套评价虚拟化信息系统安全的度量指标体系 T, 该指标体系中包含的指标是针对混合型网络(而非纯虚拟化信息系统)的安全度量指标, 即既包含适用于虚拟化信息系统的指标, 又包含适用于传统信息系统的指标。使用这套指标体系对 4 个同类评价项目(对象)S001、S002、S003、S004 进行评价, 为突出实验效果, 选取一种临界的条件: 假设这 4 个评价对象均为纯虚拟化信息系统, 显然, 用这套适用于混合型信息系统的指标体系去评价纯虚拟化信息系统是不合适的。通过实例计算在引用不恰当的指标体系的情况下指标体系的整体区分度与消除不恰当指标后产生的新指标体系的整体区分度比较, 能够区分出指标体系的适用性, 体现出指标区分度测算的价值: 对评判指标体系性能进行评估, 分析对该类评价项目的适应性, 从而选择适用的指标体系。

4.1 指标体系 T 区分度计算

指标体系 T 包括一级指标 3 个, 二级指标 15 个。一级指标包括: 安全域划分、身份鉴别、访问控制。二级指标包括: 虚拟系统与传统系统之间的安全域划分、不同等级的虚拟系统之间的安全域划分、同一个虚拟系统内部的安全域划分、传统系统的安全域划分, 虚拟机的身份鉴别、TC 的身份鉴别、管理控制台的身份鉴别、服务器的身份鉴别、

普通用户终端的身份鉴别、虚拟系统与传统系统之间的访问控制、虚拟机的访问控制、TC 的访问控制、管理控制台的访问控制、服务器的访问控制、普通用户终端的访问控制。内容及代码如表 1 所示。

表 1 指标体系 T

Table 1 The evaluation index system T

一级指标	二级指标
安全域划分(T1)	虚拟系统与传统系统之间的安全域划分(T11)
	不同等级的虚拟系统之间的安全域划分(T12)
	同一个虚拟系统内部的安全域划分(T13)
	传统系统的安全域划分(T14)
身份鉴别(T2)	虚拟机的身份鉴别(T21)
	TC 的身份鉴别(T22)
	管理控制台的身份鉴别(T23)
	服务器的身份鉴别(T24)
	普通用户终端的身份鉴别(T25)
访问控制(T3)	虚拟系统与传统系统之间的访问控制(T31)
	虚拟机的访问控制(T32)
	TC 的访问控制(T33)
	管理控制台的访问控制(T34)
	服务器的访问控制(T35)
	普通用户终端的访问控制(T36)

以一级指标 T1“安全域划分”为例, 根据某项目现场真实检测数据, 二级指标 T11、T12、T13、T14 得分如表 2 所示。计算各二级指标的熵值、熵权值及区分度。具体如下:

表 2 一级指标“安全域划分 T1”得分表

Table 2 The first level evaluation index “Security Domain Divide T1” Score Chart

项目 / 指标	S001	S002	S003	S004
T11	80	60	100	75
T12	60	77	73	68
T13	70	67	66	57
T14	90	73	80	81

构建评价矩阵 $\boldsymbol{R}'$

$$\boldsymbol{R}'=\begin{bmatrix}80 & 60 & 100 & 75\\ 60 & 77 & 73 & 68\\ 70 & 67 & 66 & 57\\ 90 & 73 & 80 & 81\end{bmatrix}$$

对矩阵进行归一化处理后, 得到矩阵 $\boldsymbol{R}$

$$\boldsymbol{R}=\begin{bmatrix}0.500 & 0.000 & 1.000 & 0.375\\ 0.000 & 1.000 & 0.765 & 0.471\\ 1.000 & 0.769 & 0.692 & 0.000\\ 1.000 & 0.000 & 0.412 & 0.471\end{bmatrix}$$

采用第 3 章的方法计算指标的熵值、熵权值及区分度, 结果如下:

计算指标的熵值

$$H_i=(0.728,0.761,0.784,1)^{\mathrm{T}}$$

计算指标的熵权值

$$w_i=(0.374,0.329,0.298,0)^{\mathrm{T}}$$

计算指标的区分度 $\eta_i=(0.513,0.432,0.380,0)^{\mathrm{T}}$

采用与一级指标 T1“安全域划分”同样的某项目现场真实检测数据, 取得另外两个一级指标“身份鉴别”、“访问控制”下的二级指标 T21、T22、T23、T24、T25, T31、T32、T33、T34、T35、T36 的得分, 分别如表 3、4 所示, 构造评价矩阵, 并采用以上方法计算各二级指标的熵值、熵权值、区分度。计算结果如表 5 所示。

表 3 一级指标“身份鉴别 T2”得分表

Table 3 The first level evaluation index “Identity Authentication T2” Score Chart

项目 / 指标	S001	S002	S003	S004
T21	80	70	85	73
T22	75	65	79	66
T23	90	87	67	85
T24	70	74	69	68
T25	85	69	80	82

表 4 一级指标“访问控制 T3”得分表

Table 4 The first level evaluation index “Access Control T3” Score Chart

项目 / 指标	S001	S002	S003	S004
T31	77	80	92	87
T32	75	72	78	76
T33	78	76	82	73
T34	85	72	70	80
T35	80	78	75	79
T36	73	69	71	80

4.2 指标体系 T′的区分度计算

不适用的指标显然是没有价值的, 在选用指标体系时应首先考虑到这个因素。但在实际的网络安全评估中, 通常是使用同一套国家标准, 指标体系

表 5 指标体系 T 熵值、熵权值、区分度表

Table 5 The Entropy, entropy value, degree of differentiation table of evaluation index system T

一级指标	二级指标	熵值(H)	熵权值(w)	区分度(η)
安全域划分(T1)	虚拟系统与传统系统之间的安全域划分(T11)	0.728	0.374	0.513
	不同等级的虚拟系统之间的安全域划分(T12)	0.761	0.329	0.432
	同一个虚拟系统内部的安全域划分(T13)	0.784	0.298	0.380
	传统系统的安全域划分(T14)	1	0	0
身份鉴别(T2)	虚拟机的身份鉴别(T21)	0.679	0.242	0.356
	TC 的身份鉴别(T22)	0.591	0.308	0.520
	管理控制台的身份鉴别(T23)	0.789	0.159	0.202
	服务器的身份鉴别(T24)	0.612	0.292	0.477
	普通用户终端的身份鉴别(T25)	1	0	0
访问控制(T3)	虚拟系统与传统系统之间的访问控制(T31)	0.679	0.226	0.333
	虚拟机的访问控制(T32)	0.763	0.167	0.219
	TC 的访问控制(T33)	0.723	0.195	0.270
	管理控制台的访问控制(T34)	0.640	0.254	0.397
	服务器的访问控制(T35)	0.777	0.157	0.202
	普通用户终端的访问控制(T36)	1	0	0

是固定不变的, 这就意味着对任何的评价对象都使用同一套指标体系。对于不适用的指标项, 如没有相对应的测评对象, 目前的大部分做法是人为地为评估指标设置一个固定的评估值。如一个单位的信息系统只是一个大系统的分支节点, 只有终端设备, 没有机房, 那么对于机房类的评估指标设置一个固定的评估值, 只要是没有机房这类评估对象的信息系统, 机房类评估项的得到的评估值是一样的, 没有任何区分度。第 3 章的方法能够从理论上验证出指标体系区分度问题。

根据第 3 章指标区分度的计算方法, 得到部分指标的区分度为 0, 在熵值理论中, 区分度为 0 的指标意味着没有价值的指标。事实上, 在指标体系 T 中, T14、T25、T36 均为适用于传统信息系统的指标, 对于 S001、S002、S003、S004 这 4 个纯虚拟化信息系统并无价值。由此得到的理论结果和事实结论是一致的。将这些不合理指标删除后, 重新构成新的指标体系 T′。

同样的评估人员使用指标体系 T'对同样的评价项目(对象)S1、S2、S3、S4 进行评价, 采用第 3 章所述的方法计算指标的熵值、熵权值、区分度, 结果如表 6 所示。

表 6 指标体系 T'熵值、熵权值、区分度表

Table 6 The Entropy, entropy value, degree of differentiation table of evaluation index system T′

一级指标	二级指标	熵值(H')	熵权值(w')	区分度(η')
安全域划分(T′1)	虚拟系统与传统系统之间的安全域划分(T′11)	0.919	0.613	0.667
	不同等级的虚拟系统之间的安全域划分(T′12)	0.960	0.302	0.314
	同一个虚拟系统内部的安全域划分(T′13)	0.989	0.086	0.086
身份鉴别(T′2)	虚拟机的身份鉴别(T′21)	0.679	0.242	0.356
	TC 的身份鉴别(T′22)	0.591	0.308	0.520
	管理控制台的身份鉴别(T′23)	0.789	0.159	0.202
	服务器的身份鉴别(T′24)	0.612	0.292	0.477
访问控制(T′3)	虚拟系统与传统系统之间的访问控制(T′31)	0.679	0.226	0.333
	虚拟机的访问控制(T′32)	0.763	0.167	0.219
	TC 的访问控制(T′33)	0.723	0.195	0.270
	管理控制台的访问控制(T′34)	0.640	0.254	0.397
	服务器的访问控制(T′35)	0.777	0.157	0.202

4.3 指标区分度及重要程度博弈矩阵

在指标筛选的过程中, 为了筛选出更具代表性且尽可能少的指标, 较多考虑了指标区分度的因素, 但实际上存在这样一种指标: 指标区分度很低, 但重要程度很高, 比如在指标体系 T'中, T'23“管理控制台的身份鉴别”指标的区分度很低, 但相对于其他指标, 它是一条很重要的评价指标, 因此有必要对指标区分度进行修正, 以增加录用几率。如果指标区分度低, 但重要程度高, 则应提高指标的录用机率, 调高指标区分度修正参数; 如果指标区分度高, 但重要程度低, 则应降低指标录用机率, 调低指标区分度修正参数; 如果指标区分度、重要程度相当, 则无需修正指标区分度参数。

将 m 个评估指标的指标区分度、指标重要程度策略分别分为 m 个等级, 取值为 1, 2,…, m。当指标区分度策略的等级大于指标重要程度策略的等级时, 说明指标不是特别重要, 指标入选机率可以调低, 指标区分度需要调低, 即修正参数<1; 当指标区分度策略的等级小于指标重要程度策略的等级时, 说明指标比较重要, 需要增加其入选机率, 因此指标区分度需要调高, 即修正参数>1; 当指标区分度策略的等级与指标重要程度策略的等级相等时, 指标区分度无需调整, 即修订参数为 1。

在指标区分度一定的情况下, 当指标重要程度达到最小, 即指标重要程度策略等级为 1 时, 指标重要程度策略等级对修正参数负向影响最大; 当重要程度达到最大, 即指标重要程度策略等级为 m 时, 指标重要程度策略等级对修正参数正向影响最大, 两者越趋近时, 影响越小。

对于指标区分度、指标重要程度博弈达到的效用值难以用函数方式描述出来, 本文使用专家法对指标区分度、指标重要程度的指标收益值进行打分。

以横坐标代表指标重要程度, 纵坐标代表指标区分度, 把指标区分度的等级看作一个区分度策略, 把指标重要程度的等级看作一个重要程度策略。同级同类指标数量最多为 6, 使用专家法, 得到指标收益值如如图 3 指标筛选博弈矩阵所示。以指标区分度等级 6 为例, 当指标重要程度等级为 1 时, 指标区分度收益为 0.1, 指标重要程度收益为 1; 当指标重要程度为 2 时, 指标区分度收益为 0.3, 指标重要程度收益为 1; 当指标重要程度为 3 时, 指标区分度收益为 0.5, 指标重要程度收益为 1; 当指标重要程度为 4 时, 指标区分度收益为 0.7, 指标重要程度收益为 1; 当指标重要程度为 5 时, 指标区分度收益为 0.9, 指标重要程度收益为 1; 当指标重要程度为 6 时, 指标区分度收益为 1, 指标重要程度收益为 1。

	1	2	3	4	5	6
1	(1,1)	(1,0.9)	(1,0.7)	(1,0.5)	(1,0.3)	(1,0.1)
2	(0.9,1)	(1,1)	(1,0.9)	(1,0.7)	(1,0.5)	(1,0.3)
3	(0.7,1)	(0.9,1)	(1,1)	(1,0.9)	(1,0.7)	(1,0.5)
4	(0.5,1)	(0.7,1)	(0.9,1)	(1,1)	(1,0.9)	(1,0.7)
5	(0.3,1)	(0.5,1)	(0.7,1)	(0.9,1)	(1,1)	(1,0.9)
6	(0.1,1)	(0.3,1)	(0.5,1)	(0.7,1)	(0.9,1)	(1,1)

图 3 指标区分度-重要程度指标筛选博弈矩阵例图

Figure 3 Game theory matrix example of Index differentiation- importance degree selection

综合以上策略, 把指标区分度收益与指标重要程度收益之比作为指标区分度修正参数。

以指标体系 T′中的 T′11,T′12,T′13 为例, 假设其重要程度等级值分别为(2, 1, 3), 由于区分度等级值分别为 (3, 2, 1), 因此 k'_{11} =0.9/1, k'_{12} =0.9/1, k'_{13} =1/0.7。

采用同样的方法计算指标体系 T、T'的指标区分度修正参数。指标体系 T 的指标区分度修正参数如下:

$$k=(k_{1i},\ k_{2i},\ k_{3i})^{\mathrm{T}}$$

其中, k_{1i}=(0.9, 0.9, 1/0.7, 1)$^{\mathrm{T}}$; k_{2i}=(1/0.7, 0.7, 1/0.7, 0.5, 1)$^{\mathrm{T}}$; k_{3i}=(1/0.9, 1/0.7, 1, 0.5, 1, 1)$^{\mathrm{T}}$。

指标体系 T'的指标区分度修正参数如下:

$$k'=(k'_{1i},\ k'_{2i},\ k'_{3i})^{\mathrm{T}}$$

其中, k'_{1i} =(0.9/1, 0.9/1, 1/0.7)$^{\mathrm{T}}$; k'_{2i}=(1/0.7, 0.7, 1/0.7, 0.7)$^{\mathrm{T}}$; k'_{3i} =(1/0.9, 1/0.7, 1, 0.5, 1)$^{\mathrm{T}}$。

4.4 指标体系整体区分度测算结果

为简化一级指标的熵权值的计算, 假设在指标体系 T 中, 3 个一级指标的熵权值相同, 为 w= (1/3,1/3,1/3)$^{\mathrm{T}}$, 指标的重要程度也相同, 为 k=(1,1,1)$^{\mathrm{T}}$, 则指标体系 T 的整体区分度为:

$$\eta_{整体}=\sum_{i=1}^{n}w_i\eta_i k_i=w_1k_1\sum_{i=1}^{k}w_{1i}\eta_{1i}k_{1i}+\cdots\cdots+w_nk_n\sum_{i=1}^{j}w_{ni}\eta_{ni}k_{ni}=0.361$$

同样, 假设指标体系 T'中, w'= (1/3,1/3,1/3)$^{\mathrm{T}}$, k'=(1,1,1)$^{\mathrm{T}}$, 指标体系 T'的整体区分度为:

$$\eta_{整体}=\sum_{i=1}^{n}w_i\eta_i k_i=w_1k_1\sum_{i=1}^{k}w_{1i}\eta_{1i}k_{1i}+\cdots\cdots+w_nk_n\sum_{i=1}^{j}w_{ni}\eta_{ni}k_{ni}=0.371$$

$\eta'_{整体}>\eta_{整体}$, 说明指标体系 T'的整体区分度优于指标体系 T, 从而在理论上证明了通过指标体系整体区分度是能够区分出指标体系性能的, 从而证明指标体系整体区分度测算理论及方法是合理的、可行的。

本文为了直观验证指标体系区分度测算理论及

方法的合理性和可行性, 选取了一种临界状态作为条件, 同样地, 在非临界条件下, 通过指标体系整体区分度的计算, 能够比较出不同指标体系区分度的差异, 依此对指标体系性能进行评价, 可以作为一种确定网络安全度量指标体系参考框架的方法。

5 总结

本文应用熵理论、博弈理论为基础对指标整体区分度进行计算, 研究了指标筛选和指标性能评价的方法, 并以虚拟化网络安全度量指标体系的筛选为例, 使用熵-博弈论方法解决实际应用问题, 结果与实际情况相符, 确定该方法可用于指标筛选和指标体系性能的评价, 通过该方法可以确定不同对象, 不同应用条件下的网络安全度量指标体系。

根据本文提出的指标筛选和指标性能评价的方法, 可以对不同的信息系统或者相同信息系统的不同时间点构建不同的度量指标体系, 通过比较计算出的整体区分度数值, 不仅可以对指标体系的性能进行评价, 还可以在其他性能相近的情况下实现对这些度量指标体系的有效选取, 因此具有一定的现实意义。

参考文献

[1] D.G.Feng, Y. Zhang, and Y.Q. Zhang, "Survey of information security risk assessment", *Journal of China Institute of Communications*, vol.25, no. 7, pp.10-18 (in Chinese), 2004.
(冯登国, 张阳, 张玉清, "信息安全风险评估综述", *通信学报*, 2004, 25 (7): 10-18.)

[2] Y.N.Li, "Research on Distinguish Degree & Weight Designing of Evaluation System based on Entropy Theory n[M.S. dissertation]", Nanjing University of Aeronautics and Astronautics(in Chinese), Nanjing, 2008.
(李元年. "基于熵理论的指标体系区分度测算与权重设计"[硕士学位论文]. 南京:南京航空航天大学, 2008.)

[3] Y.R.Zhang, M.Xian, and G.Y.Wang, "A Quantitative Evaluation Technique of Attack Effect of Computer Network Based on Network Entropy", *Journal of China Institute of Communications*, vol.25, no. 11, pp.158-165 (in Chinese), 2004.
(张义荣, 鲜明, 王国玉, "一种基于网络熵的计算机网络攻击效果定量评估方法", *通信学报*, 2004, 25(11): 158-165.)

[4] C.Lin, Y.Wang, and Q.L.Li, "Stochastic modeling and evaluation for network security", *Chinese Journal of Computer*, vol.28, no. 12, pp.1944-1956 (in Chinese), 2005.
(林闯, 汪洋, 李泉林, "网络安全的随机模型方法与评价技术", *计算机学报*, 2005, 28(12): 1944-1956.)

[5] Abdou, Samir, Savoy,and Jacques, "Statistical and comparative evaluation of various indexing and search models". *Lecture Notes in Computer Science*, pp.362-373, 2006.

[6] G.A.Shafer, "Mathematical theory of evidence", Princeton University Press,1976.

[7] Y.F.Lu, L.L.Li, and Z.Zhang, "Research on Approach of Evaluation Index Screening Based on Grey Rough Set", *Fire Control & Command Control*, 43(1): 37-42 (in Chinese), 2018.
(路云飞, 李琳琳, 张壮, "基于灰色粗糙集的指标筛选方法", *火力与指挥控制*, 2018, 43(1): 37-42.)

[8] X.Guo and R.M.Hu, "The effectiveness evaluation for security system based on risk entropy model and Bayesian network theory", in *IEEE International Camahan Conference on Security Technology (ICCST)*, pp. 57-65, 2010.

[9] S.B.Chen and X.F.Wang, "Feature Selection Algorithm for Incomplete Data Based on Information Entropy", *PR & AI*, 27(12): 1131- 1137 (in Chinese), 2014.
(陈圣兵, 王晓峰, "基于信息熵的不完备数据特征选择算法", *模式识别与人工智能*, 2014, 27(12): 1131-1137.)

[10] Z.Liu, J.S.Duanmu, Q.Wang,and C.L.Wang, "An Evaluation Method of Scheme Based on Entropy Weight Multi-objection Decision-making", *Mathematics in Practiceand Theory*, vol.35, no. 10, pp. 114-119 (in Chinese), 2005.
(刘智, 端木京顺, 王强, 王成林, "基于熵权多目标决策的方案评估方法研究", *数学的实践与认识*, 2005, 35(10): 114-119.)

[11] Gautam, Sunil Kumar, Om,and Hari, "Comparative analysis of classicication techniques in network based intrusion detection system", in *1st International Conference on Intelligent Computing and Communication(ICIC2'2016)*, pp. 591-601, 2016.

[12] Christian Callegari, Stefano Giordano, and Michele Pagano, "Entropy-based network anomaly Detection", in *2017 International Conference on Computing, Networking and Communications (ICNC'2017)*, 2017.

[13] Z.M.Lu and Y.P.Feng, "Information entropy and cross information entropy based attacking methods for complex nerworks", *Journal of Information Hiding and Mutimedia Signal Processing*, 7(6): 1243-1253, 2016.

[14] Y.H.Qiu, "Management Decision Making and Application Entropy", China Machine Press, 2001.
(邱菀华, 管理决策与应用熵学, 机械工业出版社, 2001.)

[15] C.E.Shannon, "A note on the concept of entropy", *Bell System Technical Journal*, 27(3): 379-423, 1948.

[16] H.W.Liu, "A Study on Feature Selection Algorithms Using Information Entropy[Ph.D.dissertation]", Jilin University(in Chinese), Changchun, 2010.
(刘华文, "基于信息熵的特征选择算法研究"[博士学位论文], 长春: 吉林大学, 2010.)

[17] J.C.Xu, "Knowledge Entropy and Feature Selection in Incomplete Decision System", *Applied Mathematics and Information Sciences*, 7(2): 829-837, 2013.

[18] L.Sun, J.C.Xu,and S.Q.Li, "New Approach for Feature Selection by Using Information Entropy", *Journal of Information and Computational Sciences*, 8(12): 2259-2268, 2011.

[19] Shamilov and Aladdin, "A Development of entropy optimization methods", *WSEAS Transactions on Mathematics*, pp. 568-575, May 2006.

[20] J.Ma, Z.P.Fan,and L.H.Huang, "A subjective and objective integrated approach to determine attribute weight",*European Journal of*

Operational Research, 112(2): 397-404, 1999.

[21] X.G.Zhu, "The research about the degree of different and its countermeasure in credit evaluation[M.S.dissertation]", Beijing University of Chemical Technology (in Chinese), Beijing, 2014.
(朱晓刚. "信用评价中区分度问题与对策研究"[硕士学位论文]. 北京: 北京化工大学, 2014.)

[22] L.Demetrius,T.Manke, "Robustness and network evalution-an entropic principle", *Physica A:Statistical Mechanics and its Applications*, 346(3): 682-696,2005.

[23] C.Z.Hu, "Calculation of the Behavior Utility of a Network System: Conception and Principle", *Engineer*, 4(2018): 78-84,2018.

[24] K.M.Carter, J.F.Riordan, and H. Okhravi, "A game theoretic approach to strategy determination for dynamic platform defense", in *Proceedings of the First ACM Workshop on Moving Target Defense(ACM-MTD'1)* , pp. 21-30, 2014.

[25] W.Jiang,B.X.Fang, Z.H.Tian,and H.L.Zhang, "Evaluating Network Security and Optimal Active Defense Based on Attack-Defense Game Model", *Chinese Journal of Computers*, vol.32, no. 4, pp. 817- 827(in Chinese), 2009.
(姜伟, 方滨兴, 田志宏, 张宏莉, "基于攻防博弈模型的网络安全测评和最优主动防御", *计算机学报*, 2009, 32(4): 817-827.)

[26] J.Q.Cai, "The research of network vulnerability assessment based on game theory model[M.S.dissertation]", North China Electric Power University (in Chinese), Baoding, 2010.
(蔡建强. "基于博弈模型的网络脆弱性评估的研究"[硕士学位论文]. 保定: 华北电力大学, 2010.)

[27] S.Roy, C.Ellis,S.Shiva, et al. "A survey of game theory as applied to network security", in *Proceedings of the 43rd Hawaii International Conference on System Sciences(HICSS'43)*, pp.1-10, 2010.

[28] B.Y.Zhang, Zh.G.Chen, W.Sh.Tang, et al, "Network security situation assessment based on stochastic game model", in *ICIC'11 Proceedings of the 7th International Conference on Advanced Intelligent Computing(ICAIC'7)*. , pp. 517-525, 2011.

[29] Y.Z.Wang, M.Yun, J.Y.Li,et al, "Stochastic game net and applications in security analysis for enterprise network", *International Journal of Information Security*,11(1): 41-52, 2012.

[30] G.Liu, H.Zhang, and Q.M.Li, "Network security optimal attack and defense decision-making method based on game model", *Journal of Nanjing University of Science and Technology*, 38(1): 12-21 (in Chinese), 2014.
(刘刚, 张宏, 李千目, "基于博弈模型的网络安全最优决策方法", *南京理工大学学报*, 2014, 38(1): 12-21.)

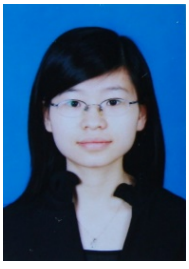
马锐 于 2003 年在重庆邮电大学计算机应用专业获得硕士学位。现任中国航天系统科学与工程研究院信息工程研究所研究员。研究领域为信息安全、计算机网络。Email: mar@spacechina.com

葛慧 于 2011 年在南京理工大学计算机应用技术专业获得硕士学位。现任中国航天系统科学与工程研究院信息工程研究所研究员。研究领域为信息安全、计算机软件。Email: shmily_ ge@qq.com

顾升高 于 2004 年在中国地质大学(武汉)计算机科学与技术专业获得学士学位, 现任中国航天系统科学与工程研究院信息工程研究所所长、高级工程师。研究领域为信息化总体设计、计算机网络。Email: gushg@ spacechina.com

王克克 于 2014 年在哈尔滨工业大学计算机应用专业获得硕士学位。现任中国航天系统科学与工程研究院信息工程研究所工程师。研究领域为信息安全、计算机软件。Email: wangkeke126@126.com

靳骁 于 2018 年在中国航天系统科学与工程研究院计算机应用专业获得硕士学位。现任中国航天系统科学与工程研究院信息工程研究所工程师。研究领域为信息安全、计算机软件。Email: deprajin@163.com



吴丹 于 2004 年在北京交通大学交通信息与控制工程专业获得硕士学位。现任中国航天系统科学与工程研究院高级工程师。研究领域为软件安全、复杂系统设计。Email: wdan511@sina.com