计算机科学
COMPUTER SCIENCE

拟态防御中基于ANP-BP的执行体异构性量化方法

赵嘉, 谷良, 吴瑶, 杜锋

引用本文

赵嘉, 谷良, 吴瑶, 杜锋. 拟态防御中基于ANP-BP的执行体异构性量化方法[J]. 计算机科学, 2024, 51(11A): 231000005-6.

ZHAO Jia, GU Liang, WU Yao, DU Feng. ANP-BP Based Executive Heterogeneity Quantification Method in Mimicry Defense [J]. Computer Science, 2024, 51(11A): 231000005-6.

计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.231000005

拟态防御中基于 ANP-BP 的执行体异构性量化方法

赵 嘉 谷 良 吴 瑶 杜 锋
国网山西省电力公司信息通信分公司 太原 030000
(1009893772@qq.com)

摘 要 基于动态异构冗余框架的拟态防御技术是一种主动防御技术,其利用非相似性、冗余性等特征阻断或扰乱网络攻击,以提高系统的可靠性和安全性,其中最大化执行体之间的异构性是提高拟态防御安全效益的关键。文中提出了一种基于网络层次分析法(ANP)和误差反向传播(BP)的执行体异构性量化方法,该方法通过收集和分析不同的异构性影响因素,建立一个多维度的特征矩阵,利用 ANP 方法综合考虑了各个维度之间的相互依赖关系,对不同维度的特征进行权重分配,同时利用 BP 神经网络解决 ANP 方法带来的主观性过强的问题。通过基于 ANP-BP 的异构性评估模型,能够快速准确有效地筛选出影响异构性最大的因素,为拟态防御执行体异构性评估提供科学依据和技术建议。

关键词:主动防御技术;拟态防御技术;异构性;网络分析方法;BP 神经网络
中图分类号 TP391

ANP-BP Based Executive Heterogeneity Quantification Method in Mimicry Defense

ZHAO Jia,GU Liang,WU Yao and DU Feng
State Grid Shanxi Electric Power Company Information and Communication Branch,Taiyuan 030000,China

Abstract Mimicry defense technology based on dynamic heterogeneous redundancy framework is an active defense technology, which uses characteristics such as non-similarity and redundancy to block or disrupt network attacks to improve system reliability and security. The key to improve the security benefits of mimicry defense is to maximize the heterogeneity among executives. This paper proposes a quantitative method of executive heterogeneity based on network analytic hierarchy process(ANP) and back propagation of error(BP). By collecting and analyzing different influencing factors of heterogeneity, this method establishes a multi-dimensional feature matrix. The ANP method comprehensively considers the interdependence between various dimensions and assigns weights to features of different dimensions. At the same time, BP neural network is used to solve the problem that ANP method is too subjective. The isomerism evaluation model based on ANP-BP can quickly, accurately and effectively screen out the most influential factors of isomerism, and provide scientific basis and technical suggestions for the isomerism evaluation of mimicry defense executive.

Keywords Active defense technique, Mimicry defense technology, Heterogeneity, Analytic network process, BP neural network

1 引言

当前,网络空间安全问题日益成为社会各界关注的焦点,恶意漏洞和后门数量不断增加,各种创新的网络安全技术也层出不穷。为了扭转防御者在网络空间攻防博弈中的弱势地位,邬江兴院士提出了一种创新的广义鲁棒控制架构的网络空间拟态防御技术[1],在该技术理论中,执行体的异构性在网络安全中最为关键,因为它增加系统复杂性,混淆攻击者,使攻击路径多样化,提高攻击成本,减缓攻击速度,从而有效防范针对特定平台或配置的攻击,增强整体网络的安全性。尽管有多种途径可以获得多样化的异构功能等价体,但是对如何度量它们之间的异构性的研究目前相对较少。现有的异构性研究主要集中在构成执行体所需的软硬件资源以及执行体之间公共漏洞的研究上,评估指标相对单一。

本文的主要贡献包括以下几个方面:

1)引入了基于 ANP-BP 的异构性量化方法,通过主客观相结合的方式计算各级指标的权重,从中选取最具影响的因素,建立了一种评估执行体异构性的方法和模型。

2)在已有的异构性评估指标基础上,提出了一套多维度、可解释的拟态防御执行体异构性评价指标体系。

3)通过文献综述和专家评估表的方式为不同准则和影响因素赋予权重,借助 ANP-BP 评估模型对异构性进行了量化评估,评估结果表明,每个因素都会或多或少的影响整体异构性,而服务器构件的选择对整体异构性的影响最大。

本文通过提出新的量化方法和评价指标,为拟态防御技术的发展提供了更深入的理论支持和实践指导。通过增强网络空间中的异构性,有望提高系统的安全性和可靠性,为决策者提供更多科学的支持和技术建议。

本文第 2 章介绍了相关工作,例举了主要的异构性评估方案以及指出现有研究的不足;第 3 章对网络分析方法(An-

基金项目:国网山西省电力公司科技项目(52051C220006)
This work was supported by the Science and Technology Project of State Grid Shanxi Electric Power Company(52051C220006).
通信作者:杜锋(dfbjt@qq.com)

alytic Network Process, ANP)和反向传播(Back Propagation, BP)神经网络方法在拟态异构性评估背景下的应用进行了介绍;第 4 章讨论了结合上述两种方法对执行体异构性的评估效果;最后对基于 ANP-BP 的执行体异构性评估技术进行了展望并总结全文。

2 相关工作

在拟态防御技术中,系统执行体的异构化差异程度对安全性具有重要影响[2]。以往的研究常常将异构冗余池内的等价体视为彼此独立的个体。然而,实际情况并非如此,因为由于功能等价性的存在,各异构体之间无法完全不同,它们之间的异构性也存在一定程度上的差异。因此,那些异构度较低的等价体之间可能存在漏洞或缺陷的重叠可能性较高。对软件系统中评估软件组件的相异性的工作有很多,本节将概述已有的部分异构性评估工作以及在不同条件下的应用。

关于异构性的研究,Yao 等[3]在挑选组件构造容错软件系统时,提出了两种相异性组件选择算法,分别是最长向异性距离(Maximum Dissimilarity, MD)算法和最佳平均相异距离(Optimal Mean Dissimilarity, OMD)算法。Qiu 等[4]提出了软件相似度度量(Measures of Software Similarity, MOSS)方法,将相似度作为异构性指标,该方法将结构相似性和属性相似性结合到迭代更新过程中计算软件相似性得分。Gao 等[5]基于 MOSS 算法得到执行体间的异构度,提出了基于差异化反馈调度判决算法。Liu 等[6]提出一种更细粒度的相似度量化方法,采用的相似度指标的定义为集合中所有不同元素的相似度之和的归一化。Twu 等[7]提出多系统异构性可通过复杂性、差异性来衡量。文献[8-10]中的异构性采用上述量化方法,其中 Zhang 等[10]结合了二次熵对执行体集的差异性进行量化,最终通过多类构建集的异构性来计算执行体集异构性。Li[11]将拟态的异构性视为多个层次,分为平台架构、操作系统、编译系统、中间件、数据库等的异构性。Wang 等[12]在执行体软件栈各层差异性的基础上,结合了不同软件栈层的漏洞威胁程度作为差异性的度量标准。Wu 等[13]基于执行体共有漏洞采用 Jeccard 距离描述任意两执行体间的异构性。

在前述相关研究中,一些方法因为拟态防御技术的独特性质而难以直接应用这些评估方法,另一些方法则仅关注于执行体的结构差异或共同漏洞。在实际系统的开发和运行过程中,执行体的异构性评估还会受到其他多种因素的影响,而这些因素难以精确量化。鉴于上述情况,本文以拟态防御执行体异构性的相关理论为基础,构建了一个评估指标体系。通过采用 ANP-BP 方法[14]计算各级指标的权重,建立了一种拟态防御执行体异构性评估方法和模型,期望为执行体的选择提供更全面且可解释的评估结果。

3 执行体异构性评估模型

基于 ANP 方法和 BP 神经网络方法各自的优势,创造一种全新的评价方法,称为 ANP-BP 综合评估方法。这一方法的核心理念在于首先运用 ANP 方法计算执行体异构性评价指标的权重,接着对这些指标进行打分,并最终计算它们的综合加权值,将此加权值作为 BP 神经网络的训练数据。ANP 方法的独特之处在于,它通过专家进行两两比较来获取权重,因此能够融合专家的主观经验。这为 BP 神经网络的训练过程提供了宝贵的知识支持。一旦神经网络完成训练,我们就可以保存其参数。在实际评估拟态系统执行体的异构性能力时,只需将相应指标的数据输入到经过训练的 BP 神经网络中,BP 神经网络会根据其学到的经验,输出准确的评估结果。

通过采用 ANP-BP 综合评估方法,我们能够充分发挥 ANP 方法的专家知识融合和 BP 神经网络的数据处理能力,以更精确、全面地评价拟态系统执行体的异构性能力。这一方法的优势在于充分整合了两种方法的长处,为执行体性能评估提供了更为可靠的基础。

3.1 评价指标体系构建

在使用 ANP 方法对拟态防御系统中的执行体异构性进行评估时,首要步骤是构建执行体异构性评价指标体系[15]。这一过程旨在科学地反映执行体的异构性,综合考虑各种影响因素[16],并与实际系统运行等相关需求相符。

其中目标层为执行体异构性评估指标体系,拟态防御执行体异构性影响因素包括组织结构、安全控制、经济效益 3 个一级指标,囊括执行体自身结构到防御能力再到拟态系统执行效率。同时将 3 个一级指标作为子目标构建 9 个二级指标,分别是服务器、操作系统、数据库、鲁棒性、抗攻击性、可靠性、执行效率、可组合性、经济成本,更全面更深入地对执行体异构性进行评估,具体的指标说明如表 1 所列。为了使指标体系具有可操作性、合理性以及可解释性,采用"是否式""频率式"等 5 种量化方法对每一个基础指标进行了定量化分析和分级。为此,遵循指标体系构建原则,根据层次分析理论,系统地构建了拟态防御执行体异构性评估指标体系,如图 1 所示。

表 1 异构评价指标体系

Table 1 Heterogeneous evaluation index system

Primary Index	Secondary Index	Indicator Specification
Organizational StructureM_1	Server N_1	Different types or versions of servers affect the heterogeneity
	Operating system N_2	Different types or versions of operating systems affect the heterogeneity
	Archive N_3	Different types or versions of databases will affect the heterogeneity
Secure Control M_2	Robustness N_4	The ability of the executor to adapt to various internal and external changes and disturbances
	Anti-aggression N_5	The executor's resistance to various attack types and attack strategies
	Reliability N_6	The ability of the executing body to maintain stable operation for a certain period of time
Economy Benefit M_3	Execution efficiency N_7	The time and resources required by the executing body to complete a specific task or operation
	Compatibility N_8	Whether the introduction of executants requires modification of existing systems, environments, and related components
	Economic cost N_9	The implementation cost and resource input required by the implementation body introduction

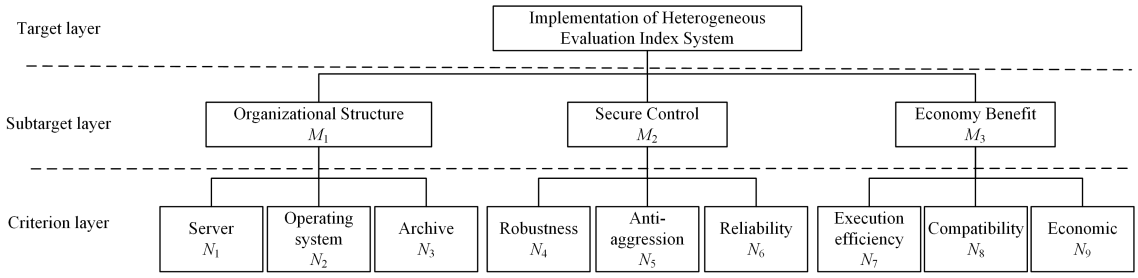

图 1　异构性评估指标体系

Fig. 1　Heterogeneous evaluation index system

3.2　基于 ANP 法的权重确定

网络分析法[17]（ANP）是一种多因素决策分析方法，用于处理复杂的决策问题。该方法是在层次分析法（AHP）的基础上考虑多层结构、多个指标之间的相互耦合关系并进行改进的一种多准则决策方法。它通过构建层次结构来表示决策因素之间的依赖关系，然后使用专家判断或实证数据来确定这些关系的相对权重。该方法基于网络结构，将问题转化为一个有向图，表示各指标内部和外部的关系。在执行体异构性评估中，ANP 可用于综合考虑不同执行体的关键特征，如操作系统类型、数据库软件等，并确定它们对整体异构性的贡献度。

3.2.1　构建网络结构

ANP 首先将系统元素分为两个主要部分。

控制元素层：这一部分包括问题目标和决策准则。所有的决策准则都被视为是相互独立的，并且它们只受问题目标的支配。

网络层：网络层由所有在控制元素层下受支配的元素组成。在这个层面，元素之间相互依存和相互支配，不存在内部独立性，每个准则在递阶层次结构中不再支配一个简单的独立元素，而是一个相互依存且具有反馈关系的网络结构。根据表 1 构建的执行体异构性评估指标体系确定其网络结构，如图 2 所示。

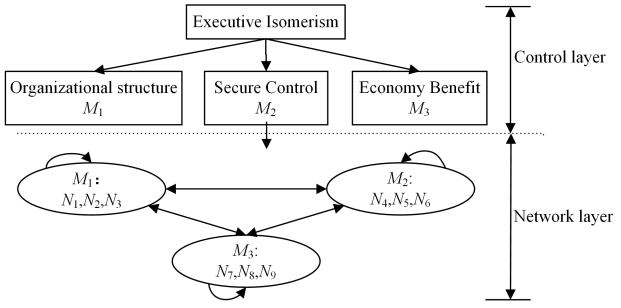

图 2　异构性 ANP 结构

Fig. 2　ANP structure of heterogeneous

3.2.2　重要度打分

根据各指标之间的相互关系，通过重要度相对尺度表 2 对各层级和各评估指标之间的重要度比值进行两两比较。

表 2　重要度相对尺度

Table 2　Relative scale of importance

Implication	Relative Importance
Equally important	1
Slightly important	3
Obvious importance	5
Strongly important	7
Vita limportant	9
The median of the above importance levels	2,4,6,8
The opposite expression of the above leves	1/3,1/5,…

3.2.3　权重计算

1）建立未加权超矩阵。假设 $P_1,P_2,\cdots,P_m$ 为 ANP 控制层各准则元素，$R_1,R_2,\cdots,R_i$ 为网络层中各元素组，$R_{i1},R_{i2},\cdots,R_{in}$ 表示每个元素组中的内部元素，其中 n 代表 R_i 中包含的内部元素数量。在 ANP 中的间接优势度的比较过程中，将控制层元素 P_s 和网络层元素组 R_j 中的元素 R_{j_1} 分别视为准则和次准则，在比较 R_i 中的元素时构建判断矩阵，以得到归一化特征向量 $\boldsymbol{w}_{in}$。接下来，对构建的判断矩阵进行一致性检验，若一致性比率（CR）小于 0.1，则认为具有一致性，表明 $\boldsymbol{w}_{in}$ 是网络元素的排序向量。同时，与其他元素有关的排序向量也可以通过相同的原理获得，从而形成矩阵 $\boldsymbol{W}_{ij}$，如式（1）所示。

$$\boldsymbol{W}_{ij}=\begin{bmatrix} w_{i1}^{(j1)} & w_{i1}^{(j2)} & \cdots & w_{i1}^{(jnj)} \\ w_{i2}^{(j1)} & w_{i2}^{(j2)} & \cdots & w_{i2}^{(jnj)} \\ \vdots & \vdots & \ddots & \vdots \\ w_{ini}^{(j1)} & w_{ini}^{(j2)} & \cdots & w_{ini}^{(jnj)} \end{bmatrix} \tag{1}$$

同理，可对各个元素间的关系进行一一比较计算，则可以求得各子矩阵，将所有的子矩阵组合可构成未加权超矩阵 $\boldsymbol{W}$，如式（2）所示：

$$\boldsymbol{W}=\begin{bmatrix} W_{11} & W_{12} & \cdots & W_{1n} \\ W_{21} & W_{22} & \cdots & W_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ W_{m1} & W_{m2} & \cdots & W_{mm} \end{bmatrix} \tag{2}$$

2）构造加权超矩阵。以 P_s 为计算准则，以元素组 R_β（$\beta=1,2,\cdots,i$）为计算次准则，构建 $R_1,R_2,\cdots,R_i$ 关于 R_β 的判断矩阵，并求得相关的权重向量。将判断矩阵对应的权重向量排序组合构成矩阵 $\boldsymbol{M}$，利用矩阵 $\boldsymbol{M}$ 对矩阵 $\boldsymbol{W}$ 加权后可得加权超矩阵 $\bar{\boldsymbol{W}}$，如式（3）所示：

$$\bar{\boldsymbol{W}}=\boldsymbol{W}\cdot\boldsymbol{M} \tag{3}$$

3）构造极限超矩阵，形成指标权重，使用幂法对加权超矩阵进行稳定处理，即求加权超矩阵的 n 次方至矩阵乘积收敛且唯一，可得到极限超矩阵，其每一行的值为每个评估指标的权重值。

3.3　基于 BP 神经网络的权重确定

BP 神经网络是一种监督学习算法，用于模式识别和预测。在执行体异构性评估中，BP 网络负责学习和预测执行体的异构性，输入层接收各异构性因素评分，隐藏层学习它们之间的复杂关系，输出层提供异构性的量化结果。

3.3.1　网络层次确定

BP 神经网络的结构通常包括输入层、隐含层和输出层，每一层都包含多个人工神经元。由于任何连续函数都可以通过包含一个隐含层的神经网络来准确逼近，对于非线性函数映射，只需要一个隐含层就足够。因此，在建立执行体异构性

的 BP 评价模型时，我们选择了经典的三层神经网络结构[18]，其包括一个输入层、一个隐含层和一个输出层。

3.3.2 输入层设计

根据执行体异构性评价指标体系，我们将输入层神经元的数量与评价体系的 9 个二级评价指标一一对应，并根据网络输入层与隐含层之间传递函数对输入范围的要求，对这 9 个指标数据进行了归一化处理，确保它们的数值位于[0,1]的范围内。

3.3.3 隐含层神经元数目确定

隐含层神经元数目目前没有统一标准进行准确计算，因此依据黄金分割法来定义隐含层节点的数量，具体表达式如下：

$$\frac{p+t}{2}\leqslant m\leqslant(p+t)+10 \tag{4}$$

其中，p 为输入层神经元个数，t 为输出层神经元个数，m 为隐含层神经元个数。由式(4)确定 m 的初始范围定义为[5,20]，通过训练比较不同隐含层神经元个数时网络的误差，来确定隐含层神经元数目为 8。

3.3.4 输出层设计

鉴于异构性评价旨在衡量拟态防御系统执行体的整体异构性水平，并输出唯一的期望值，我们将输出层的神经元数量设定为 1。结合 BP 神经网络的基本原理，最终形成了一个 9-8-1 的 BP 神经网络结构，如图 3 所示。在这个网络中，我们将 9 个二级指标对应的输入值输入到输入层，然后通过 8 个节点构成的隐含层，最终传递到只包含 1 个节点的输出层。

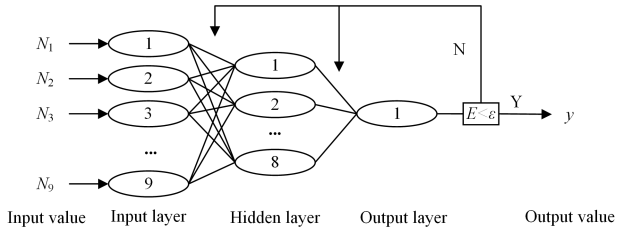

图 3 BP 神经网络结构

Fig. 3 BP neural network structure

3.4 基于 ANP-BP 的评估方法

在拟态防御背景下执行体异构性评估指标体系构建完全的情况下，可用 ANP-BP 的方法对异构性进行评估[19]。本文的评估步骤如下：

1)根据指标之间的直接重要度进行比较，将控制层元素作为准则层 P_i 进行判断矩阵的构造，利用特征根法求得准则层 P_i 的权重，并检验矩阵的一致性。

2)在评价的总体目标下，通过元素的两两比较来判断元素的重要性，并构造未加权超矩阵 $\boldsymbol{W}$。

3)比较它们之间的间接重要性，确定网络层之间的判断矩阵，并根据它们之间的相互关系形成超级矩阵子块。通过构造超矩阵 $\boldsymbol{W}$ 以进一步得到加权超矩阵 $\bar{\boldsymbol{W}}$。

4)计算极限排序向量，求加权超矩阵的 n 次方，当其收敛时，得到网络层的指标权值。

5)邀请行业专家对二级指标进行打分，并进行规范化，计算主指标的得分值。

6)根据专家的评分表以及 ANP 方法计算出的期望值用于训练 BP 神经网络，再通过多次迭代优化 BP 网络隐藏层的权重值，训练完成的神经网络即可用于拟态防御执行体异构性评估。

由以上步骤可归纳出本文的异构性评估流程，评估流程如图 4 所示。

ANP-BP 评价方法融合了 ANP 方法和 BP 神经网络的优点，兼具以下特点。首先，它继承了 ANP 方法的系统化特征，使得复杂问题能够被更好地组织和处理。此外，ANP-BP 方法还解决了某些难以量化的指标问题，为评价提供了更全面的视角。其次，ANP-BP 方法汲取了 BP 神经网络的自学习和自处理能力，使得模型能够不断适应新的数据和情境，提高评价的灵活性。通过 BP 神经网络，还能够减少人为主观因素对评价结果的影响，有效提升了评价的客观性和可靠性。

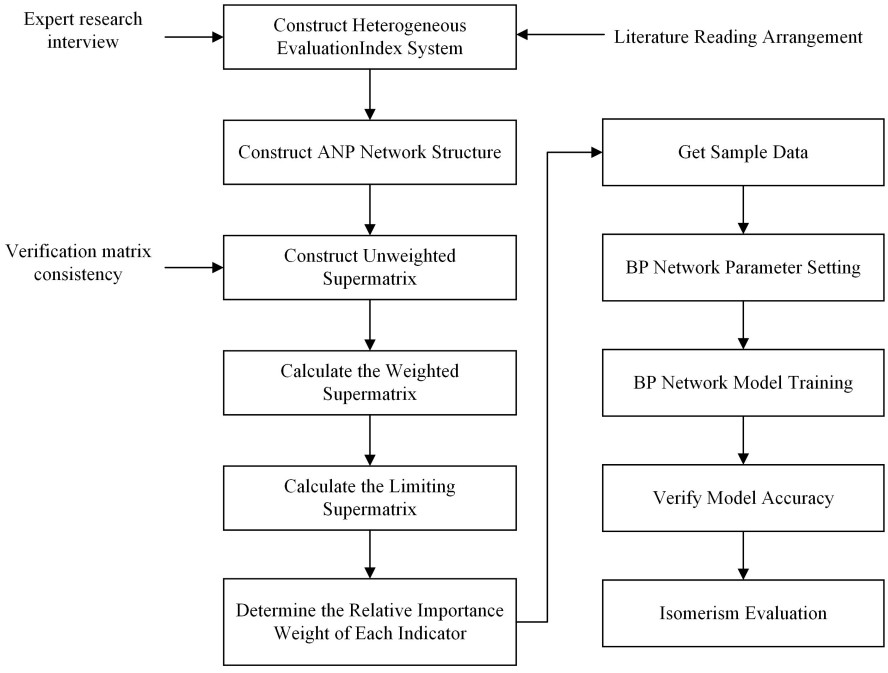

图 4 异构性评估流程

Fig. 4 Heterogeneous evaluation process

4　实验分析

4.1　指标权重计算

在确定异构型评估指标体系与创建 ANP 网络结构之后，通过上述 ANP 方法原理构造未加权超矩阵、加权超矩阵、极限超矩阵，借助 SD 软件，在确保一致性的前提下，计算各指标权重，各指标权重如表 3 所列。

表 3　评价指标权重

Table 3　Evaluation index weight

M	First-order Index	N	Secondary Index	Comprehensive Weight
Organizational Structure M_1	0.52784	N_1	0.62670	0.267633
		N_2	0.27969	0.191751
		N_3	0.093610	0.068453
Secure Control M_2	0.33251	N_4	0.07543	0.033984
		N_5	0.69552	0.193864
		N_6	0.22905	0.104667
Economy Benefit M_3	0.13965	N_7	0.64422	0.082506
		N_8	0.27056	0.043626
		N_9	0.08522	0.013515

4.2　BP 神经网络的构建与训练

对于拟态防御系统，依据已构建的异构性评估指标体系按照百分制邀请专家对该拟态系统中的执行体所对应的异构性评价指标进行评分，并将评分结果作为 BP 网络的样本数据。其中样本中的期望值为 9 个二级指标的数值与 ANP 方法求得的各自的权重值相乘所得的结果。

将 100 组样本数据分为两部分，前 95 组作为训练样本，后 5 组作为检验样本。本文通过使用多次迭代优化的预训练 BP 神经网络来验证本文所提网络模型的有效性，当实验结果中的误差非常小时，表明 BP 神经网络评估方法可以较为精确地得到拟态防御系统中执行体的异构性评估值。对数据样本进行分析计算，设置学习率为 0.0005，目标误差为 10^{-4}，将样本数据归一化后输入至网络，经过 2717 次迭代训练后误差将被优化至目标范围内，训练误差曲线如图 5 所示，此时保存网络参数。

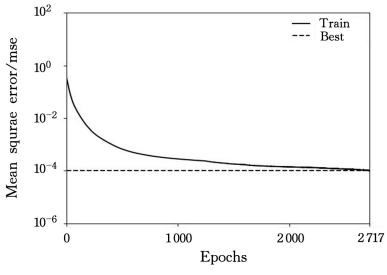

图 5　训练误差曲线

Fig. 5　Training error curve

将作为检验样本的第 96～100 组数据输入网络进行仿真验证，并对其输出值与期望值进行比较，结果如表 4 所列。

表 4　检验样本结果误差分析

Table 4　Error analysis of test sample results

Sample Number	Actual Output	Expected Output	Relative Error/%
96	0.5182	0.5188	−0.0963
97	0.5733	0.5724	0.1572
98	0.4280	0.4273	0.1638
99	0.4581	0.4587	−0.1308
100	0.6479	0.6422	0.9032

由 BP 神经网络计算出的评价结果与期望值相比，二者数值非常接近，其中 5 个检验样本中最大的相对误差为 0.90%，进一步表明了 ANP-BP 方法适用于拟态防御执行体异构性评估。

4.3　异构性对比

选取 8 组不同的异构执行体集，服务器、操作系统和数据库均采用不同的软件，如表 5 所列。

表 5　执行体集

Table 5　Executive set

Number	Hardware/Software Combination
1	Windows Server 2012＋IIS 7.5＋MySQL 5.7 FreeBSD 11.3＋Nginx1.16.1＋PostgreSQL 11 Ubuntu 18.04＋Apache 2.4＋Oracle 11g
2	Windows Server 2016＋IIS 7.5＋MySQL 5.7 FreeBSD 11.3＋Nginx1.16.1＋MySQL 8.0 Ubuntu 18.04＋Apache 2.4＋Oracle 11g
3	Windows Server 2012＋IIS 7.5＋MySQL 5.7 Windows Server 2016＋Nginx1.16.1＋ MySQL 8.0 CentOS 7＋Apache 2.4＋Oracle 11g
4	Debian 10.3＋IIS 7.5＋MySQL 5.7 CentOS 7＋Nginx1.16.1＋ MySQL 8.0 Ubuntu 18.04＋Apache 2.4＋Oracle 11g
5	Windows Server 2012＋ Nginx1.16.1＋MySQL 5.7 FreeBSD 11.3＋Nginx1.16.1＋ MySQL 8.0 Ubuntu 18.04＋Apache 2.4＋Oracle 11g
6	Windows Server 2012＋ Nginx1.16.1＋MySQL 5.7 Windows Server 2016＋Nginx1.16.1＋ MySQL 8.0 Ubuntu 18.04＋Apache 2.4＋Oracle 11g
7	Windows Server 2012＋IIS 7.5＋MySQL 5.7 Windows Server 2016＋Nginx1.16.1＋ MySQL 8.0 Windows Server 2019＋ IIS 7.5＋Oracle 11g
8	Windows Server 2012＋ Nginx1.16.1＋MySQL 5.7 FreeBSD 12.1＋Nginx1.16.1＋ MySQL 8.0 Ubuntu 18.04＋ Nginx1.16.1＋Oracle 11g

将通过 ANP-BP 模型得到的评估结果与 Margalef 指数、Shannon-Wiener 指数、Simpson 指数与 Tree-Level 指数对比，异构性量化结果如图 6 所示。

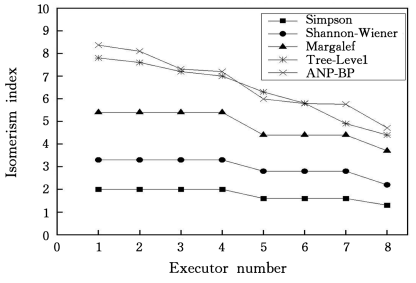

图 6　异构性量化对比

Fig. 6　Quantitative comparison of heterogeneity

综合以上分析，可以得出基于 ANP-BP 的评估模型能够准确客观地评价执行体的异构性，有效地衡量异构性并制定相应的调度策略，同时也可以为类似的异构性评估提供一定的参考价值。

结束语　本文基于 ANP 与 BP 神经网络构建了一个拟态防御执行体异构性评价模型。通过 ANP 方法，考虑了指标之间的相互影响关系，并识别了对异构性影响最大的关键指标。在为异构性评估提供了基础的同时，还为 BP 神经网络提供了训练数据。通过 BP 神经网络结合了专家经验，避免了过多的主观因素影响，从而得出更准确的评估结果。证

明了 ANP-BP 评估模型在拟态防御执行体异构性评价中的适用性，并为与此相关的研究工作提供了一定的参考。

参 考 文 献

[1] WU J X. Research on mimicry defense in Cyberspace[J]. Journal of Information Security, 2016(4): 1-10.

[2] TONG Q, ZHANG Z, WU J X. Active defense technology based on software and hardware diversity[J]. Journal of Information Security, 2017, 2(1): 1-12.

[3] YAO W B, YANG X Z. Different software component selection algorithm design[J]. Journal of Harbin Institute of Technology, 2003(3): 261-264.

[4] QIU D H, LI H, SUN J L. Measuring software similarity based on structure and property of class diagram[C]// Sixth International Conference on Advanced Computational Intelligence. IEEE, 2013: 75-80.

[5] GAO M, LUO J, ZHOU H Y, et al. A differential feedback scheduling decision algorithm based on mimicry defense[J]. Telecommunication Science, 2019, 36(5): 73-82.

[6] LIU Q R, LIN S J, GU Z Y. Heterogeneous functional-equivalent block scheduling algorithm for mimicry security defense [J]. Journal of Communications, 2018, 39(7): 188-198.

[7] TWU P, MOSTOFI Y, EGERSTEDT M. A measure of heterogeneity in multi-agent systems[C]// 2014 American Control Conference. IEEE, 2014: 3972-3977.

[8] YUE Y Y, FU X, DENG S. Multi-access edge Computing Server heterogeneity quantification Method based on mimicry defense [J]. Computer Applications and Software, 2019, 40(6): 276-281, 349.

[9] ZHANG J X, PANG J M, ZHANG Z, et al. A quantization method for heterogeneity of network security systems based on dissimilar redundancy architecture[J]. Journal of Electronics and Information Technology, 2019, 41(7): 1594-1600.

[10] ZHANG J X, PANG J M, ZHANG Z. A quantitative method for heterogeneity of Web servers based on mimicry construction [J]. Journal of Software, 2019, 31(2): 564-577.

[11] LI J J. Research on Evaluation Method and Technology of mimicry security information System[J]. Information Technology and Network Security, 2019, 38(4): 33-36.

[12] WANG X M, YANG W H, ZHANG W, et al. Research on Scheduling strategy of mimicry Web server based on BSG[J]. Journal of Communications, 2018, 39(S2): 112-120.

[13] WU Z Q, WEI J. Heterogeneous executors scheduling algorithm for mimic defense systems[C]// 2019 IEEE 2nd International Conference on Computer and Communication Engineering. Piscataway: IEEE Press, 2019: 279-284.

[14] ZHANG Y J, YANG Y P, ZHOU Y, et al. State assessment of urban security development based on ANP-BP neural network [J]. Journal of Xi 'an University of Science and Technology, 2022, 42(6): 1104-1113.

[15] LIU H. Research on Heterogeneous Software Deployment Strategy for mimicry Defense System[D]. Information Engineering University of Strategic Support Forces, 2020.

[16] WANG M, FU W H, WANG B T, et al. Optimization of mimicry defense strategy based on Evolutionary game [J]. Application Research of Computers, 2024, 41(2): 576-581.

[17] JIANG D M, DING L. ANP-BP highway tunnel fire risk assessment model and its application[J]. Journal of Qingdao University of Technology, 2018, 39(5): 111-116.

[18] WANG L F. Theory and Algorithm of Network Analysis Method (ANP)[J]. Systems Engineering Theory & Practice, 2001(3): 44-50.

[19] HUANG Y T, HUANG X B. BP neural network optimization based on ANP and Sparrow search algorithm for prefabricated building schedule risk assessment[J]. Journal of Engineering Management, 2019, 36(6): 36-41.

ZHAO Jia, born in 1995, master. His main research interest is network security.

DU Feng, born in 1992, master. His main research interests include data management and blockchain technology.