智能系统学报
CAAI TRANSACTIONS ON INTELLIGENT SYSTEMS

基于高维多目标序贯三支决策的恶意代码检测模型

崔志华, 兰卓璇, 张景波, 张文生

引用本文:
崔志华,兰卓璇,张景波,张文生. 基于高维多目标序贯三支决策的恶意代码检测模型[J]. 智能系统学报, 2024, 19(1): 97–105.
CUI Zhihua, LAN Zhuoxuan, ZHANG Jingbo, et al. Malicious code detection model based on high-dimensional multi-objective sequential three-way decision[J]. *CAAI Transactions on Intelligent Systems*, 2024, 19(1): 97–105.

在线阅读 View online: https://dx.doi.org/10.11992/tis.202306013

DOI: 10.11992/tis.202306013
网络出版地址: https://link.cnki.net/urlid/23.1538.TP.20240105.1707.002

基于高维多目标序贯三支决策的恶意代码检测模型

崔志华[1], 兰卓璇[1], 张景波[1], 张文生[2]
（1. 太原科技大学 大数据分析与并行计算山西省重点实验室, 山西 太原 030024; 2. 中国科学院 自动化研究所, 北京 100089）

摘　要: 针对传统基于二支决策的恶意代码检测方法在面对动态环境中的复杂海量数据时, 没有考虑在信息不充足条件下进行决策产生影响的问题, 本文提出了一种基于卷积神经网络的序贯三支决策恶意代码检测模型。通过卷积神经网络对样本数据进行特征提取并构建多粒度特征集, 引入序贯三支决策理论对恶意代码进行检测。为改善检测模型整体性能, 避免阈值选取的主观性, 本文在上述模型的基础上, 同时考虑模型的综合分类性能、决策效率和决策风险代价建立高维多目标序贯三支决策模型, 并采用高维多目标优化算法对模型进行求解。仿真结果表明, 模型在保证检测性能的同时, 有效地提升了决策效率, 降低了决策时产生风险代价, 更好地拟合了真实动态检测环境。

关键词: 恶意代码检测; 序贯三支决策; 卷积神经网络; 高维多目标优化; 基于参考点的高维多目标进化算法; 多粒度; 延迟决策; 决策阈值
中图分类号: TP309　　**文献标志码:** A　　**文章编号:** 1673−4785(2024)01−0097−09

中文引用格式: 崔志华, 兰卓璇, 张景波, 等. 基于高维多目标序贯三支决策的恶意代码检测模型 [J]. 智能系统学报, 2024, 19(1): 97–105.
英文引用格式: CUI Zhihua, LAN Zhuoxuan, ZHANG Jingbo, et al. Malicious code detection model based on high-dimensional multi-objective sequential three-way decision[J]. CAAI transactions on intelligent systems, 2024, 19(1): 97–105.

Malicious code detection model based on high-dimensional multi-objective sequential three-way decision

CUI Zhihua[1], LAN Zhuoxuan[1], ZHANG Jingbo[1], ZHANG Wensheng[2]
(1. Shanxi Key Laboratory of Big Data Analysis and Parallel Computing, Taiyuan University of Science and Technology, Taiyuan 030024, China; 2. Institute of Automation, Chinese Academy of Sciences, Beijing 100089, China)

Abstract: In view of the problem that traditional two-way decision based malicious code detection methods fail to consider the impact of decision making under the condition of insufficient information when facing complex and massive data in a dynamic environment, this paper proposes a sequential three-way decision malware detection model based on convolutional neural network. Firstly, the features of sample data were extracted and multi-granularity feature sets were constructed through convolutional neural networks, and then the sequential three-way decision theory was introduced to detect malicious code. To improve the overall performance of the detection model and eliminate the subjectivity of threshold selection, a high-dimensional multi-objective sequential three-way decision model was built based on the above model, taking account of the comprehensive classification performance, decision efficiency and decision risk cost of the model. In addition, the high-dimensional multi-objective optimization algorithm was used to solve the model. The simulation results show that the model can not only guarantee the detection performance, but also effectively improve the decision efficiency and reduce the decision risk cost. It better fits the real dynamic detection environment.

Keywords: malware detection; sequential three-way decision; convolutional neural network; high-dimensional multi-objective optimization; NSGA-III; multi-granularity; delay decision; decision threshold

收稿日期: 2023−06−07.　**网络出版日期:** 2024−01−08.
基金项目: 国家自然科学基金项目 (61806138); 中央财政指导地方科技发展基金项目 (YDZJSX2021A038); 中国高校产学研创新基金−未来网络创新研究与应用项目 (2021FNA04014); 太原科技大学研究生联合培养示范基地项目 (JD2022003).
通信作者: 崔志华. E-mail: cuizhihua@gmail.com.

恶意代码又称为恶意软件, 是对各种敌对和入侵软件的概括性术语, 指故意编制、具有一定破坏性的、对计算机或网络系统产生威胁的计算机代码或软件。恶意代码随着计算机技术的蓬勃

发展而不断发展，呈现出数量增长快、形式变化多等特点，这对恶意代码的分析和防御工作带来了更大的挑战。

现有的恶意代码检测方法可分为静态分析方法和动态分析方法 2 类。静态分析方法主要是在没有实际运行的情况下对恶意代码的静态特征加以分析，而动态恶意软件分析方法是在受控环境中系统地运行，使用工具来提取其动态特征进行分析。这 2 种检测方式都在一定程度上缓解了恶意代码检测所面临的压力。深度学习和人工智能的快速发展，向恶意代码分析技术提供了新的方向[1]。大量基于深度学习的恶意代码检测模型不断被提出[2-3]，然而现有的基于深度学习的检测模型通常将检测问题视为分类问题，采用二支决策的方式进行分类[4]，将样本分为良性类和恶意类。这意味着，无论分类器学习到的信息是否充分，都会对待分类的样本做出一个确定的决策。而在实际恶意代码检测问题中，由于在做出良性或恶意决定时的基本信息有限，一些样本不能被立即判断或很容易被错误分类，因此，需要在收集更多的可用信息后，再次对这些样本进行确定性决策。

序贯三支决策[5]是一种可以更好地处理此类问题的动态三支决策[6]思想。它在传统二支决策的基础上引入了更加符合人类认知的延迟决策选项。通过构建多粒层结构，从最粗粒度层级到最细粒度层级进行一系列的多阶段三支决策，在决策时允许决策者对信息不充分的对象进行延迟处理。然而，序贯三支决策方法也存在一些问题。在传统的概率粗糙集三支决策模型[7]中，三支决策阈值通常是根据给定的代价函数矩阵来确定，这需要合适的先验知识或专家预先设定损失函数，具有一定的主观随意性，这在一定程度上阻碍了概率粗糙集三支决策模型的实际应用。

为解决上述问题，本文提出了一种基于高维多目标序贯三支决策的恶意代码检测模型（maliciouscode detection model based on many-objective sequential three-way decision，MO-STWD）。序贯三支决策用于构建更适合真实数据环境的恶意代码检测模型。利用高维多目标优化算法获得最优阈值对及参数，可以避免先验知识或专家设定的主观随意性，有效地平衡综合分类性能、决策效率及决策风险损失。本文的主要研究贡献如下：

1) 针对现有检测模型面临信息不足导致的盲目决策问题，将序贯三支决策引入恶意代码检测领域，提出一种序贯三支实时恶意代码检测模型。

2) 为了综合考虑恶意代码检测模型的综合分类性能、决策效率以及决策风险损失，构建了一种高维多目标序贯三支决策模型。

1　恶意代码检测与三支决策模型

随着计算机技术的迅速发展，机器学习和人工智能近年来逐渐在人脸识别[8]、推荐系统[9-10]等多个领域掀起研究热潮。深度学习因其具有从海量数据中学习数据特征的能力，适合处理高维、复杂的恶意代码样本。因此，许多研究者将深度学习方法应用于恶意代码检测领域。Kuo 等[11]将 Android 应用包文件解压缩为 classes.dex 文件，然后利用训练卷积神经网络模型判断输入的 classes.dex 文件是否为恶意代码。Cui 等[12]利用蝙蝠算法降低不平衡数据对恶意代码检测的影响，通过卷积神经网络对图像数据集进行训练，以达到更好的分类效果。Wang 等[13]基于 DenseNet 网络良好的图像分类性能和恶意软件家族在图像上的视觉相似性，将恶意软件转换后的灰度图像输入到模型中，结合 DenseNet 网络和注意力机制进行恶意软件家族分类。Almahmoud 等[14]构建了一个用于恶意软件检测的递归神经网络分类模型，通过静态分析提取了 4 种不同类型的静态特征，利用递归神经网络模型对恶意软件进行分类。Cui 等[15]构建了多目标受限玻尔兹曼机模型，利用评价指标衡量数据分类效果，引入策略池提高数据融合性能，同时为了减轻数据不平衡带来的问题，他们还使用多目标优化算法来处理不平衡的恶意软件家族。然而这些方法都是基于现有的信息进行分类决策，忽略了信息不足带来的影响。

三支决策模型在经典二支决策的理论基础上加入了更加符合人类思维的延迟决策选项，从而使整个决策过程更加完善合理。序贯三支决策是在三支决策基础上的重要延伸和扩展，它将三支决策视为一个中间过程。鉴于序贯三支决策模型更适合实际应用场景，近年来，序贯三支决策模型在很多领域得到了应用。Ye 等[16]考虑到多级推荐信息特征和推荐结果的可解释性，构建了一种基于序贯三支决策的可解释推荐模型。在垃圾邮件过滤领域，袁国鑫等[17]对无法判断类别的邮件进行延迟决策，在获得更多信息后再做出最终

决策。武慧琼等[18]提出了一种基于三支决策的花卉图像分类方法, 有效地提高了花卉图像的分类精度。Dai 等[19]在图像识别领域引入了序贯三支决策思想, 以解决传统支持向量机图像特征提取不完全的问题。孙勇等[20]为了解决目标检测领域中代价不平衡和信息不完全的问题, 设计了一种基于多粒度序贯三支决策和代价敏感学习的目标检测方法。

2　卷积神经网络与智能优化算法

本文所提方法主要基于卷积神经网络、序贯三支决策和高维多目标优化算法,下面就相关概念和基本知识予以介绍。

2.1　卷积神经网络

受人类视觉神经系统的启发, 卷积神经网络广泛应用于图像分类、语义检索和目标检测等领域。它通过对输入图像进行卷积、激活和池化等操作来提取重要的特征信息。因此, 本文模型中使用卷积神经网络来进行特征提取和多粒度特征集的构造。在实验中, 卷积神经网络的损失函数选用分类交叉熵损失, 输入图像大小为 128×128×3, 批处理个数设置为 64, 训练次数设置为 30, 学习率设置为 0.001, 卷积神经网络结构如图 1 所示。

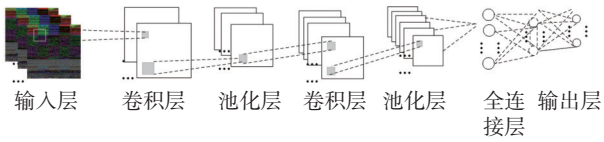

图 1　卷积神经网络结构

Fig. 1　Structure of convolutional neural network

2.2　序贯三支决策

在研究粗糙集模型时, Yao 等[6]提出了三支决策理论。该理论以决策粗糙集理论和贝叶斯定理为核心, 其中决策粗糙集理论通过状态集和决策集展开。

给定状态集 $\Omega=\{X, \neg X\}$, 决策集 $D=\{D_P, D_B, D_N\}$, 其中 D_P、D_B、D_N 分别表示将状态集中的样本划分入, 执行不同的决策行为可能会产生不同的风险代价。风险代价函数如表 1 所示, 表 1 中 λ_{PP}、λ_{BP}、λ_{NP} 分别表示当前样本 x 属于状态 X 时, 执行 D_P、D_B、D_N 操作时的损失; λ_{PN}、λ_{BN}、λ_{NN} 分别表示当前样本 x 属于状态 X 时, 执行 D_P、D_B、D_N 操作时的损失。其中 D 代表正域 POS(x), B 代表边界域 BND(x), N 代表负域 NEG(x)。假设 $0\leqslant\lambda_{PP}\leqslant\lambda_{BP}\leqslant\lambda_{NP}$, $0\leqslant\lambda_{NN}\leqslant\lambda_{BN}\leqslant\lambda_{PN}$, 根据文献 [21] 的计算方式, 可以得到:

$$\alpha=\frac{(\lambda_{PN}-\lambda_{BN})}{(\lambda_{PN}-\lambda_{BN})+(\lambda_{BP}-\lambda_{PP})} \tag{1}$$

$$\beta=\frac{(\lambda_{BN}-\lambda_{NN})}{(\lambda_{BN}-\lambda_{NN})+(\lambda_{NP}-\lambda_{BP})} \tag{2}$$

$$\gamma=\frac{(\lambda_{PN}-\lambda_{NN})}{(\lambda_{PN}-\lambda_{NN})+(\lambda_{NP}-\lambda_{PP})} \tag{3}$$

式中: $0<\beta<\gamma<\alpha<1$。令 $P(X|[x])$ 表示样本 x 被分为状态 X 的概率, 可以得到如下 3 条规则:

1) 如果 $P(X|[x])\geqslant\alpha, x\in\text{POS}(x)$;

2) 如果 $\beta<P(X|[x])<\alpha, x\in\text{BNN}(x)$;

3) 如果 $P(X|[x])\leqslant\beta, x\in\text{NEG}(x)$。

序贯三支决策结合粒计算, 将三支决策视为中间过程, 构建具有不同粒度特征的多粒度层次空间。假设论域U由n层粒度构成, 即$\{g_1, g_2, \cdots, g_n\}$, 在每个粒层$g_i(1\leqslant i\leqslant n-1)$ 上, 存在样本 x 被分为状态 X 的概率$P^i(X|[x]]\ (1\leqslant i\leqslant n-1)$ 及该粒层相应的阈值对$(\alpha_i,\beta_i)(1\leqslant i\leqslant n-1)$, 根据三支决策的划分规则可将待分类样本集划分为$\text{POS}^i(x)$、$\text{BND}^i(x)$和$\text{NEG}^i(x)$, $(1\leqslant i\leqslant n-1)$。对于处于$\text{BND}^i(x)$中的样本, 在更细粒度将被重新评估, 得到更精确的分类。随着粒度层的增加, 边界域将越来越小。当在第n粒度需要终止该序贯过程时, 可采取二支决策的方案, 通过γ_n将所有待分类样本分入$\text{POS}^n(x)$和$\text{BND}^n(x)$中。

表 1　三支决策风险代价函数表

Table 1　The three-way decision risk cost function table

损失决策集	P	N
D_P	λ_{PP}	λ_{PN}
D_B	λ_{BP}	λ_{BN}
D_N	λ_{NP}	λ_{NN}

2.3　NSGA-III 算法

高维多目标优化问题由$n(n>3)$个目标函数和相关约束条件组成。其中需要被优化的目标通常具有一定的冲突或者没有直接的关联, 需要决策者根据实际应用需求从候选解集中选择所需要的解。高维多目标优化问题定义为

$$\begin{cases}\min F(x)=(f_1(x), f_2(x), \cdots, f_m(x))\\ \text{s.t. } h_i(x)\geqslant 0, i=1,2,\cdots,r\\ g_j(x)=0, j=1,2,\cdots,t\end{cases} \tag{4}$$

式中: $f_m(x)$ 为第m个目标函数; $x=(x_1, x_2, \cdots, x_i)$, x_i为第 i 个决策变量; $h_i(x)\geqslant 0$, $i=1,2,\cdots,r$定义了不等式约束; $g_j(x)=0$, $j=1,2,\cdots,t$表示等式约束。

常见的多目标优化算法 (如 NSGA-II[22]) 在面对目标函数大于 3 个时, 由于维数增多选择压力下降, 不能很好地平衡多样性和收敛性。针对这

一问题, Deb 等[23] 提出了基于参考点和非支配排序的高维多目标进化算法 (many-objective optimization algorithm using reference-point-based nondominated sorting approach, NSGA-III)。NSGA-III 算法以基于快速非支配排序的多目标优化算法 (multi-objective optimization algorithm using nondominated sorting-based approach, NSGA-II) 的框架为基础, 使用参考点策略代替了 NSGA-II 算法中的拥挤度排序策略, 以解决在高维空间中非支配解集分布不均匀的问题。非支配排序策略和参考点策略是 NSGA-III 算法的核心。算法通过非支配排序策略按照个体之间的支配关系对种群进行分层, 将种群中收敛性较好的解选择出来, 而参考点策略通过计算种群中个体与参考点、理想点连接构成的参考向量之间的距离来保持算法的多样性。

3　序贯三支决策恶意代码检测模型

为了提高恶意代码检测性能, 避免因信息不充分而导致的误报漏报, 本文提出了基于序贯三支决策的恶意代码检测模型。在此基础上, 构建了高维多目标序贯三支决策模型, 并采用 NSGA-III 算法对该模型进行求解, 可以同时优化模型的综合检测性能、决策风险代价和决策效率, 从而获得恶意代码检测过程中的最优模型。

3.1　序贯三支决策恶意代码检测模型基础框架

鉴于序贯三支决策能够动态地处理不确定性决策问题, 本文提出了序贯三支决策恶意代码检测模型。该模型的详细框架如图 2 所示, 主要由 2 部分组成: 采用卷积神经网络 (convolutional neural network, CNN) 模型来构建多粒度特征集并估计待分类样本条件概率; 在决策时采用序贯三支决策理论对待分类样本做出决策。

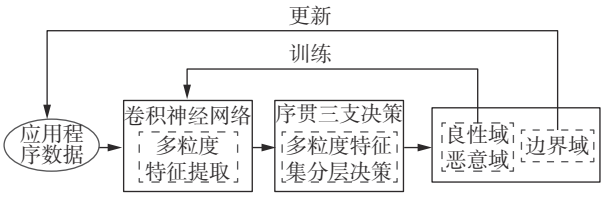

图 2　恶意代码检测模型框架

Fig. 2　Diagram of malicious code detection model

基于序贯三支决策的恶意代码检测模型的具体步骤如下:

使用现有的标记样本集训练初始 CNN 模型, 将所有待分类样本输入到 CNN模型与 SoftMax 函数中, 评估每个应用行为属于正域的条件概率值 $P(X|[x])$。

随后, 将 $P(X|[x])$ 与当前粒层的阈值对(α_i,β_i)进行比较, 根据三支决策规则, 将所有样本划分到相应的正域$\mathrm{POS}^i(x)$、边界域$\mathrm{BND}^i(x)$和负域$\mathrm{NEG}^i(x)$中。由于三支决策独特的延迟决策理论, 边界域$\mathrm{BND}^i(x)$中的样本需要在最初的判定条件中不断地加入新的信息来进行下一步决策, 所以 CNN 模型在每次分类完成之后会把已经划分入正域$\mathrm{POS}^i(x)$和负域$\mathrm{NEG}^i(x)$中的样本作为新的训练集进行训练, 得到下一粒度的决策模型。在每一粒度层, 将上一粒度的边界域样本及当前粒度的待分类样本合并构成新的待检测样本集, 并依据三支决策规则对其进行分类决策。循环上述步骤即形成了一个序贯三支决策恶意代码检测模型的过程。序贯三支决策多粒度决策过程具体如图 3 所示。

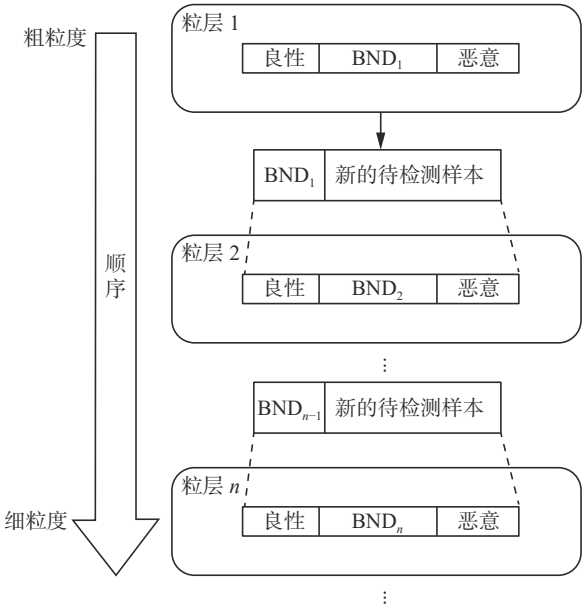

图 3　序贯三支决策多粒度决策过程

Fig. 3　Sequential three-way multi-granularity decision

3.2　高维多目标模型

在恶意代码检测的实际应用场景中, 序贯三支决策模型为用户提供了求解信息不充分、不确定问题的一个新的方向。为了能在提升检测模型的综合分类性能的同时, 尽可能地提升决策效率、降低决策风险代价, 在上述模型的基础上, 构建了高维多目标序贯三支决策模型。

3.2.1　目标函数

检测模型的综合分类性能可通过分类问题中常见的评价指标来衡量, 本文利用这些评价指标作为目标函数, 多个评价标准可以从各个方面衡量检测模型的综合分类性能。因此, 综合分类性能可通过召回率 (true positive rate,TPR) 和假阳性率 (false positive rate, FPR) 2 个目标来衡量。

目标 1: 最大化 TPR。TPR 表示在实际为正

的样本中被预测为正样本的比例, 其定义为

$$T_{\mathrm{PR}}=\frac{\left|X_{\mathrm{pos}(\alpha,\beta)}(x)\cap X\right|}{\left|X_{\mathrm{pos}(\alpha,\beta)}(x)\cap X\right|+\left|X_{\mathrm{neg}(\alpha,\beta)}(x)\cap X\right|} \tag{5}$$

式中: $\mathrm{POS}_{(\alpha,\beta)}(x)$和$\mathrm{NEG}_{(\alpha,\beta)}(x)$分别为划分到正域和负域中的样本, X为实际为正的样本, $\left|\mathrm{POS}_{(\alpha,\beta)}(x)\cap X\right|$为实际为正被预测为正的样本数量, $\left|\mathrm{NEG}_{(\alpha,\beta)}(x)\cap X\right|$为实际为正被预测为负的样本数量。

目标 2: 最小化 FPR。FPR 表示在实际为负的样本中被预测为正样本的比例, 其定义为

$$F_{\mathrm{PR}}=\frac{\left|X_{\mathrm{pos}(\alpha,\beta)}(x)\cap \neg X\right|}{\left|X_{\mathrm{pos}(\alpha,\beta)}(x)\cap \neg X\right|+\left|X_{\mathrm{neg}(\alpha,\beta)}(x)\cap \neg X\right|} \tag{6}$$

式中: $\neg X$为实际为负的样本, $\left|\mathrm{POS}_{(\alpha,\beta)}(x)\cap \neg X\right|$为实际为负被预测为正的样本数量, $\left|\mathrm{NEG}_{(\alpha,\beta)}(x)\cap \neg X\right|$为实际为负被预测为负的样本数量。

目标 3: 最大化决策效率。在恶意代码检测模型的序贯过程中, 模型的检测效率是通过承诺率 (commitment rate, CMR) 来度量的。承诺率是指在当前三支决策下, 在当前所有检测的样本中被划分到确定性域的比例, 其计算公式为

$$C_{\mathrm{MR}_{(\alpha,\beta)}}=\frac{1}{U}\left(\left|X_{\mathrm{pos}(\alpha,\beta)}(x)\right|+\left|X_{\mathrm{neg}(\alpha,\beta)}(x)\right|\right) \tag{7}$$

承诺率越大, 意味着被划分到正域和负域的样本数量越多, 其边界域不确定性越低, 表明决策效率越高。

目标 4: 最小化风险代价。使用三支决策进行分类时, 每种决策行为都应该承担相应的风险代价, 其风险代价函数如表 1 所示。假设样本X属于正域的条件概率为p_i, 则将样本X划分到 3 个域的风险代价可定义为

$$\begin{cases}\text{正域风险代价：}\lambda_{\mathrm{PP}}p_i+\lambda_{\mathrm{PN}}(1-p_i)\\ \text{边界域风险代价：}\lambda_{\mathrm{BP}}p_i+\lambda_{\mathrm{BN}}(1-p_i)\\ \text{负域风险代价：}\lambda_{\mathrm{NP}}p_i+\lambda_{\mathrm{NN}}(1-p_i)\end{cases}$$

假设将样本正确分类所需承担的风险代价为 0, 即$\lambda_{\mathrm{PP}}=\lambda_{\mathrm{NN}}=0$。则所有待分类样本做出决策时需要承担的风险代价总和为

$$\begin{aligned}R_{\mathrm{isk}}=&\sum_{x_i\in X_{\mathrm{pos}(\alpha,\beta)}(x)}\lambda_{\mathrm{PN}}(1-p_i)+\sum_{x_j\in X_{\mathrm{neg}(\alpha,\beta)}(x)}\lambda_{\mathrm{NP}}p_j+\\&\sum_{x_k\in X_{\mathrm{bnd}(\alpha,\beta)}(x)}\lambda_{\mathrm{BP}}p_k+\lambda_{\mathrm{BN}}(1-p_k)\end{aligned} \tag{8}$$

依据式 (1)~(3), 可将λ_{PN}、λ_{NP}、λ_{BP}和λ_{BN}与α、β、γ之间的关系反推出, 将其代入式 (8) 可得:

$$\begin{aligned}R_{\mathrm{isk}}=&\sum_{p_i\geqslant\alpha}(1-p_i)+\sum_{p_j\leqslant\beta}\frac{1-\gamma}{\gamma}p_j+\\&\sum_{\beta<p_k<\alpha}\left(\frac{(1-\alpha)\cdot(\gamma-\beta)}{\gamma\cdot(\alpha-\beta)}p_k+\frac{\beta\cdot(\alpha-\gamma)}{\gamma\cdot(\alpha-\beta)}(1-p_k)\right)\end{aligned} \tag{9}$$

综上所述, 本文构建的高维多目标模型为

$$\begin{cases}\max f_1=T_{\mathrm{PR}}\\ \min f_2=F_{\mathrm{PR}}\\ \max f_3=C_{\mathrm{MR}(\alpha,\beta)}\\ \min f_4=R_{\mathrm{isk}}\\ \text{s.t. } 0<\beta<\gamma<\alpha<1\end{cases} \tag{10}$$

3.2.2 决策变量

在序贯三支决策恶意代码检测模型中, 卷积神经网络的超参数选择及三支决策阈值对的变化是影响模型性能的关键参数。因此, 本文将卷积神经网络的超参数及三支决策阈值α、β、γ作为优化上述目标的决策变量。决策变量的设计为

$$P_i=\{p_1,p_2,p_3,\alpha,\beta,\gamma\} \tag{11}$$

式中: p_1、p_2、p_3分别为卷积神经网络的超参数: 学习率l_r、dropout 参数以及优化器的类型。

3.2.3 模型求解

本文采用 NSGA-III 算法对所提出的高维多目标模型进行求解。NSGA-III 求解步骤如下:

1) 初始化包含 N 个个体的种群$P_t=\{I_1,I_2,\cdots,I_N\}$, 并令算法代数 $t=0$;

2) 根据种群中的个体生成不同的卷积神经网络训练构建多粒度特征集, 并进行三支决策;

3) 根据式 (10), 计算种群中每个个体的召回率、假阳性率、承诺率以及决策风险代价;

4) 生成理想点, 并通过交叉变异操作生成 N 个子代个体组成的$Q_t=\{Q_1,Q_2,\cdots,Q_N\}$, 将父代与子代组合生成大小为 $2N$ 的新种群$P'_t=P_t\cup Q_t$;

5) 按照非支配排序策略和参考点策略, 在新种群P'_t中选取 N 个优秀的个体组成新的父代种群P_{t+1}, 并令算法代数$t=t+1$;

6) 判断是否满足最大迭代次数, 满足则算法结束, 不满足则返回 2)。

4 MO-STWD 模型实验分析

4.1 实验设计

实验环境为 Intel core Xeon® E5-2620CPU (2.10 GHz)、Nvidia GeForce RTX 2080Ti GPU、128 GB RAM、windows 10 操作系统, 软件平台使用 pycharm 和 Matlab2019b。其中恶意代码模型基本框架在 pycharm 环境下基于 keras 框架下完成, 高维多目标优化算法及其对比算法在 Matlab2019b 版本下优化算法平台 (evolutionary multi-objective optimization platform, PlatEMO) 上进行。为了证明本文所提模型的有效性, 本文在 2 个数据集上进行了实验。第 1 个数据集是由 Kaggle 平台提供的, 简称 Kaggle 数据集。该数据集中包含 12 015 张图像, 其中恶意软件图像 6 006 张、良性软件图

像 6 009 张。第 2 个数据集采用公开的工业物联网数据集 Leopard Mobile, 共包含 14 733 个恶意软件样本和 2 486 个良性样本。为了模拟实际恶意代码检测的动态过程，本文将测试集随机分成 5 个部分来模拟时间动态过程，并在第 5 个粒度进行二支决策，以便与其他模型进行比较。卷积神经网络及优化算法相关参数设置如表 2 所示。

表 2　实验参数设置

Table 2　Experimental parameter settings

参数	数值
输入图像大小	128×128×3
Batchsize	64
损失函数	Categorical Cross Entropy
Epoch	30
种群大小	30
最大迭代次数	30
交叉概率P_{rc}	1
变异概率P_{rm}	1/6

4.2　评价指标

恶意代码检测通常被视为二分类问题。因此，可以采用分类问题中常见的评价指标对模型进行评价。本文使用准确率 (accuracy)、精确率 (precision)、召回率 (recall, TPR) 和假阳性率 (false positive rate, FPR) 以对模型提供全面的评估。评价指标计算方式为

$$A_{\mathrm{ccuracy}} = \frac{T_P + T_N}{T_P + F_N + F_P + T_N} \tag{12}$$

$$P_{\mathrm{recision}} = \frac{T_P}{T_P + F_P} \tag{13}$$

$$T_{\mathrm{PR}} = \frac{T_P}{T_P + F_N} \tag{14}$$

$$F_{\mathrm{PR}} = \frac{F_P}{T_N + F_P} \tag{15}$$

式中：T_P 和 F_P 分别表示正确和错误地被分类为恶意的样本数量，T_N 和 F_N 表示被正确地和错误地归类为良性的样本数量。

4.3　实验结果与分析

4.3.1　三支决策分类器与传统二支决策分类器的性能对比

为了验证基于序贯三支决策的恶意代码检测模型的有效性，本节在保证使用同样的卷积神经网络进行特征提取的情况下，将序贯三支决策分类器与传统的二支决策分类器进行比较。实验使用支持向量机 (support vector machine, SVM)、Softmax 分类器和 K-最近邻 (K-nearest neighbor, KNN) 与序贯三支决策分类器进行对比试验。在 Kaggle 数据集上的实验结果见表 3。

表 3　不同分类器的实验对比

Table 3　Experimental comparison of different classifiers　%

分类方法	准确率	精确率	召回率	假阳性率
SoftMax	93.14	88.34	**99.47**	13.24
SVM	96.69	95.43	98.07	4.70
KNN	94.52	92.62	96.74	7.71
MO-STWD	**98.06**	**97.43**	98.87	**2.61**

表 3 中展示了卷积神经网络与不同分类器结合后，在准确率、精确率、TPR 和 FPR 上的分类结果.表 3 中可以看出，本文提出的基于高维多目标序贯三支决策的恶意代码检测模型（malicious code detection model based on many-objective sequential three-way decision, MO-STWD）在卷积神经网络下的准确率达到 98.06%，精确率和 TPR 指标均超过 97%，而 FPR 为 2.61%，与其他分类模型相比，该模型在大多数指标上都表现出更好的结果。对于第 1 个指标 Accuracy，三支决策分类器比 SoftMax 分类器高出 0.049 2，与 SVM 和 KNN 相比，该指标分别高出 0.013 7 和 0.035 4。在 FPR 中，其他分类模型的指标值分别比三支决策分类模型高 0.106 3、0.020 9 和 0.051 0。此外，对于 Precision，本文方法也表现出最好的结果。但在 Recall 中，虽然没有达到最大值 0.994 7，也仅低于最大值 0.006 0。这些数据表明，序贯三支决策分类模型在综合性能上要优于其他分类模型。在引入延迟决策后，避免了一些不确定样本被错误分类的风险，提升了整体模型的检测性能。因此，基于序贯三支决策的恶意代码检测方法优于传统的基于二支决策的方法。

4.3.2　不同算法在求解高维多目标序贯三支决策模型上的对比

在该实验中，使用不同的优化算法，分别为 NSGA-III、参考向量引导多目标优化进化算法（reference vector guided evolutionary algorithm, RVEA）[24]、基于网格的多目标优化进化算 (grid-based evolutionary algorithm, GrEA) [25] 和基于指标的约束多目标进化算 (indicator-based constrained multi-objective evolutionary algorithms, HyPE)[26]，对本文构建的高维多目标序贯三支决策模型在 Kaggle 数据集上进行求解，以验证 NSGA-III 算法的可取性。其中对比优化算法对应的参数是默认设置的。为了直观地比较具有相同目标函数的每种算法的性能，在表 4 中给出了在不定义终点的情况下，各个算法第 5 个粒度时在 TPR、FPR、CMR 和 Risk 上的结果比较。不同优化算法的每个目标值是所有个体的平均值。从表 4 中可以看出，NSGA-III

算法在 FPR 和 Risk 上取得了最优, 分别为 2.19% 和 91.802 4。在召回率 (TPR) 上, HyPE 算法的结果更好。GrEA 算法在承诺率 (CMR) 上的结果较好。从求解目标上来看, 与其他算法相比, NSGA-III 算法在该模型的优化性能有更好的效果。

表 4　不同优化算法在求解 4 个目标上的性能

Table 4　Performance of different optimization algorithms in solving the four objectives

优化方法	召回率/%	假阳性率/%	CMR/%	Risk
RVEA	95.43	2.42	94.73	124.720 2
HyPE	**99.45**	4.05	92.58	185.424 7
GrEA	97.29	3.27	**95.20**	115.587 4
NSGA-III	98.31	**2.19**	94.97	**91.802 4**

为了比较整体模型检测性能, 本文以 5 个粒度为例, 并在最后一个粒度中使用二支决策进行分类, 这与之前的实验类似。

表 5 给出了使用各种算法优化高维多目标模型的准确度、精确度、TPR 和 FPR 的分类结果。显然, 从表 5 中可以看出, 对于精确率而言, NSGA-III 比最低值高出 0.42%。对于准确率而言, NSGA-III 与 HyPE 算法均取得最优。对于 Recall 而言, NSGA-III 的性能不是最优的, 但也仅比最优的 HyPE 低 0.5%。但对于 FPR 而言。NSGA-III 算法的结果是最优的。从整体上来看, NSGA-III 算法在该模型的求解性能较为突出, 因此, 本文采用 NSGA-III 算法对高维多目标序贯三支决策模型进行求解。

表 5　不同优化算法的实验对比结果

Table 5　Experimental comparison results of different optimization algorithms　%

优化方法	准确率	精确率	召回率	假阳性率
RVEA	96.53	97.25	95.76	2.77
HyPE	**98.06**	96.84	**99.37**	3.23
GrEA	97.89	97.29	98.50	2.73
NSGA-III	**98.06**	**97.43**	98.87	**2.61**

4.3.3　不同恶意代码检测模型的对比

为了进一步衡量基于高维多目标序贯三支决策的恶意代码检测模型的性能, 将本文模型与其他恶意软件检测模型在 Kaggle 数据集上进行了比较实验。该实验选取的对比模型包括基于蝙蝠优化算法的动态采样模型 (dynamic resampling method based on the bat algorithm, DRBA)[12], 多目标 CNN[27], 及多目标受限玻尔兹曼机 (restricted boltzmann machine, RBM) 模型[15]。这些模型都是基于二支决策的检测模型, 通过深度学习模型从恶意代码图像中提取特征, 直接对样本进行二支分类决策。

表 6 给出了在实验环境不变的情况下, 本文模型和其他恶意代码检测模型的对比结果。可以看出, 本文提出的检测方法在 4 个评价指标上都表现出最好的结果。与其他恶意代码检测模型相比, 本文所提模型的 Accuracy 值提升了 0.018 3~0.031 0, 假阳性率降低了 0.012 5~0.038 0。本文模型相较于其他模型在综合性能上表现更好的优势在于该模型将延迟决策引入, 将基于当前信息无法分类的样本先划入边界域中, 避免因特征不足或数据不充分而导致样本被错误分类的风险; 使用卷积神经网络进行特征提取, 结合动态检测过程构建多粒度特征空间, 将边界域中的样本在更细粒度的特征空间中进行分类, 可提升模型的准确率。

表 6　不同恶意代码检测模型在 Kaggle 数据集上的实验对比结果

Table 6　Experimental comparison results of different malicious code detection models in Kaggle dataset　%

分类方法	准确率	精确率	召回率	假阳性率
DRBA	94.96	96.06	93.76	3.85
多目标CNN	96.23	93.91	98.86	6.41
多目标RBM	95.90	95.65	96.18	4.38
MO-STWD	**98.06**	**97.43**	**98.87**	**2.61**

为了验证本文所提模型的泛化性, 将 Kaggle 数据集替换成 Leopard Mobile 数据集, 表 7 给出了在保持实验环境不变的情况下, 本文模型与其他模型的对比结果。从表 7 中可以看出, 本文所提的基于高维多目标序贯三支决策的恶意代码检测模型在准确率、精确率及假阳性率方面优于其他 3 个对比模型。这表明本文模型适用于不同的恶意代码数据集, 具有一定的泛化性。

表 7　不同恶意代码检测模型在 Leopard Mobile 数据集的实验对比结果

Table 7　Experimental comparison results of different malicious code detection models in Leopard Mobile dataset　%

分类方法	准确率	精确率	召回率	假阳性率
DRBA	94.53	92.62	96.85	7.83
多目标CNN	95.56	94.14	**97.01**	6.16
多目标RBM	96.17	96.09	96.11	3.78
MO-STWD	**96.88**	**96.74**	95.57	**2.17**

5　结束语

本文综合考虑了恶意代码检测问题的分类性能、决策效率及决策风险损失, 提出了一种基于

高维多目标序贯三支决策的恶意代码检测模型。该模型结合了卷积神经网络和序贯三支决策的特点对恶意代码样本进行分类检测，此外，本文在两个真实数据集上对模型进行了测试，数值结果表明，本文所提的方法不仅能够提升恶意代码的检测性能和决策效率，而且还能控制模型的决策风险代价。在未来的工作中，可以对高维多目标模型进行改进，并探寻更优的算法进行求解，进一步降低模型的复杂度，提升恶意代码检测性能。

参考文献：

[1] YANG Yanming, XIA Xin, LO D, et al. A survey on deep learning for software engineering[EB/OL]. (2020−11−30)[2023−06−07]. https://arxiv.org/abs/2011.14597.pdf.

[2] YUAN Baoguo, WANG Junfeng, WU Peng, et al. IoT malware classification based on lightweight convolutional neural networks[J]. IEEE Internet of things journal, 2022, 9(5): 3770–3783.

[3] LIU Yue, TANTITHAMTHAVORN C, LI Li, et al. Deep learning for android malware defenses: a systematic literature review[J]. ACM computing surveys, 2021, 55(8): 153.

[4] ZHANG Yongchao, LIU Zhe, JIANG Yu. The classification and detection of malware using soft relevance evaluation[J]. IEEE transactions on reliability, 2022, 71(1): 309–320.

[5] YAO Yiyu. Granular computing and sequential three-way decisions[C]//International Conference on Rough Sets and Knowledge Technology. Berlin, Heidelberg: Springer, 2013: 16−27.

[6] YAO Yiyu. The superiority of three-way decisions in probabilistic rough set models[J]. Information sciences, 2011, 181(6): 1080–1096.

[7] YAO Yiyu. Probabilistic rough set approximations[J]. International journal of approximate reasoning, 2008, 49(2): 255–271.

[8] GOEL R, MEHMOOD I, UGAIL H. A study of deep learning-based face recognition models for sibling identification[J]. Sensors, 2021, 21(15): 5068.

[9] CUI Zhihua, ZHAO Peng, HU Zhaoming, et al. An improved matrix factorization based model for many-objective optimization recommendation[J]. Information sciences, 2021, 579: 1–14.

[10] XIE Lijie, HU Zhaoming, CAI Xingjuan, et al. Explainable recommendation based on knowledge graph and multi-objective optimization[J]. Complex & intelligent systems, 2021, 7(3): 1241–1252.

[11] KUO W C, LIN Yupin. Malware detection method based on CNN[C]// International Computer Symposium. Singapore: Springer, 2019: 608−617.

[12] CUI Zhihua, XUE Fei, CAI Xingjuan, et al. Detection of malicious code variants based on deep learning[J]. IEEE transactions on industrial informatics, 2018, 14(7): 3187–3196.

[13] WANG Changguang, ZHAO Ziqiu, WANG Fangwei, et al. A novel malware detection and family classification scheme for IoT based on DEAM and DenseNet[J]. Security and communication networks, 2021, 2021: 1–16.

[14] ALMAHMOUD M, ALZU'BI D, YASEEN Q. ReDroidDet: android malware detection based on recurrent neural network[J]. Procedia computer science, 2021, 184: 841–846.

[15] CUI Zhihua, ZHAO Yaru, CAO Yang, et al. Malicious code detection under 5G HetNets based on a multi-objective RBM model[J]. IEEE network, 2021, 35(2): 82–87.

[16] YE Xiaoqing, LIU Dun. An interpretable sequential three-way recommendation based on collaborative topic regression[J]. Expert systems with applications, 2021, 168: 114454.

[17] 袁国鑫, 于洪. 一种基于邮件头信息的三支决策邮件过滤方法 [J]. 计算机科学, 2017, 44(9): 74–77,114.
YUAN Guoxin, YU Hong. Method of three-way decision spam filtering based on head information of E-mail[J]. Computer science, 2017, 44(9): 74–77,114.

[18] 武慧琼, 张素兰, 张继福, 等. 一种基于三支决策的花卉图像分类 [J]. 小型微型计算机系统, 2019, 40(7): 1558–1563.
WU Huiqiong, ZHANG Sulan, ZHANG Jifu, et al. Classification method of flower images based on three-way decisions[J]. Journal of Chinese computer systems, 2019, 40(7): 1558–1563.

[19] DAI Jin, SHAO Shuai, WANG Zu, et al. An novel image recognition method based on three-way decision[J]. MATEC web of conferences, 2018, 176: 01035.

[20] 孙勇, 李华雄. 基于多粒度序贯三支决策的代价敏感目标检测方法 [J]. 山西大学学报(自然科学版), 2020, 43(4): 914–926.
SUN Yong, LI Huaxiong. Cost-sensitive multi-granularity sequential three-way decision for object detection[J]. Journal of Shanxi University (natural science edition), 2020, 43(4): 914–926.

[21] 于洪, 王国胤, 姚一豫. 决策粗糙集理论研究现状与展

望 [J]. 计算机学报, 2015, 38(8): 1628–1639.
YU Hong, WANG Guoyin, YAO Yiyu. Current research and future perspectives on decision-theoretic rough sets[J]. Chinese journal of computers, 2015, 38(8): 1628–1639.

[22] DEB K, PRATAP A, AGARWAL S, et al. A fast and elitist multiobjective genetic algorithm: NSGA-II[J]. IEEE transactions on evolutionary computation, 2002, 6(2): 182–197.

[23] DEB K, JAIN H. An evolutionary many-objective optimization algorithm using reference-point-based nondominated sorting approach, part I: solving problems with box constraints[J]. IEEE transactions on evolutionary computation, 2014, 18(4): 577–601.

[24] CHENG Ran, JIN Yaochu, OLHOFER M, et al. A reference vector guided evolutionary algorithm for many-objective optimization[J]. IEEE transactions on evolutionary computation, 2016, 20(5): 773–791.

[25] YANG Shengxiang, LI Miqing, LIU Xiaohui, et al. A grid-based evolutionary algorithm for many-objective optimization[J]. IEEE transactions on evolutionary computation, 2013, 17(5): 721–736.

[26] BADER J, ZITZLER E. HypE: an algorithm for fast hypervolume-based many-objective optimization[J]. Evolutionary computation, 2011, 19(1): 45–76.

[27] CUI Zhihua, DU Lei, WANG Penghong, et al. Malicious code detection based on CNNs and multi-objective algorithm[J]. Journal of parallel and distributed computing, 2019, 129: 50–58.

作者简介:

崔志华, 教授, 博士生导师, 太原科技大学计算机科学与技术学院院长, 主要研究方向为大数据建模与优化、网络安全。主持国家自然科学基金项目、教育部科学技术研究重点项目、山西省重点研发项目等 10 余项。发表学术论文 100 余篇, 出版专著 4 部。E-mail: cuizhihua@gmail.com。

兰卓璇, 硕士研究生, 主要研究方向为大数据建模与优化、网络安全。E-mail: 1285839182@qq.com。

张文生, 教授, 博士生导师, 主要研究方向为人工智能、跨模态数据标注、医疗数据分析推理。主持国家自然科学基金重点与面上项目 6 项、国家科技部 863 项目、支撑计划项目和 973 计划课题 9 项, 授权发明专利 40 余项。发表学术论文 160 余篇。E-mail: wensheng.zhang@ia.ac.cn。