

改进鲸鱼优化算法的网络入侵预警模型构建

查道贵

宿州职业技术学院 安徽省宿州市 234101

摘 要: 本文聚焦于改进鲸鱼优化算法的网络入侵预警模型构建。研究目的在于提升网络入侵预警模型的性能, 增强对复杂网络入侵行为的检测能力。研究方法上, 提出多项关键策略: 融合多源数据特征提取与鲸鱼优化算法参数自适应调整, 以全面刻画入侵行为并适应不同网络场景; 采用基于动态权重分配的鲸鱼优化算法与深度学习模型融合策略, 发挥两者优势; 引入迁移学习与鲸鱼优化算法结合的跨网络入侵预警策略, 提高模型通用性; 构建基于鲸鱼优化算法的多层次入侵预警模型评估与更新策略, 确保模型持续优化。研究结果表明, 这些策略能有效改进鲸鱼优化算法在网络入侵预警模型中的应用。结论认为, 所提策略可显著提高网络入侵预警模型的准确性和可靠性, 为网络安全提供更有保障。

关键词: 改进鲸鱼算法; 网络入侵; 预警模型

随着网络技术快速发展, 网络入侵事件频繁发生, 给个人、企业以及国家都造成了极大的安全威胁, 构建高效且准确的网络入侵预警模型成了保障网络安全的关键所在, 鲸鱼优化算法作为一种新兴的群体智能优化算法, 有全局搜索能力较强等优点, 不过也存在一些不足之处, 本文对鲸鱼优化算法加以改进, 并将其运用到网络入侵预警模型构建当中, 来提升模型对于复杂网络入侵行为的检测能力, 给网络安全提供更为可靠的保障。

1. 改进鲸鱼优化算法概述

改进鲸鱼优化算法是基于标准鲸鱼优化算法演变而来的一种优化求解手段, 标准鲸鱼优化算法模仿座头鲸的狩猎行为, 借助包围猎物、气泡网攻击等策略来开展全局搜索以及局部寻优, 有结构简单、参数较少等优势, 不过也存在容易陷入局部最优、收敛精度欠缺等问题, 为了提高算法性能, 许多改进策略相继出现。从算法机制本身着手, 引入自适应调整策略, 依据搜索进程动态调节算法参数, 比如在搜索前期增大全局搜索概率, 后期提高局部开发能力, 平衡探索与开发, 或者采用非线性收敛因子, 让算法在不同阶段拥有更合理的收敛速度, 结合其他优化算法思想, 例如把遗传算法的变异操作融入其中, 增加种群多样性, 防止算法过早收敛, 引入模拟退火算法的概率接受准则, 以一定概率接受劣解, 跳出局部最优陷阱。另外以及基于混沌映射初始化种群、引入精英保留策略等改进方式, 这些改进措施切实提升了鲸鱼优化算法的收敛速度、求解精度以及稳定性, 使其在函数优

化、工程实际问题求解等领域呈现出更广阔的应用前景^[1]。

2. 改进鲸鱼优化算法的网络入侵预警模型构建要点

2.1 融合多源数据特征提取与鲸鱼优化算法参数自适应调整策略

构建网络入侵预警模型时数据特征提取是关键环节, 传统网络入侵检测常依赖单一类型数据特征像网络流量特征或者系统日志特征, 这种单一特征提取办法很难全面体现网络入侵行为的复杂状况, 要提升模型预警能力需融合多源数据特征来提取, 多源数据有网络流量数据、主机系统日志、用户行为数据等。网络流量数据能给出网络连接的基础信息比如源 IP、目的 IP、端口号、数据包大小等, 主机系统日志记录系统运行期间的各类事件像进程创建、文件访问等, 用户行为数据反映用户在系统里的操作习惯和行为模式, 融合这些多源数据可从不同角度描绘网络入侵行为, 提升特征的有效性全面性^[2]。

在完成特征提取之后, 鲸鱼优化算法的参数设定对于模型性能有着关键作用, 传统的鲸鱼优化算法参数一般是固定不变的, 很难顺应不同网络环境以及入侵行为的改变, 要达成鲸鱼优化算法参数的自适应调节, 可依据网络流量的动态变动、入侵行为的频率以及类型等要素, 实时对算法里的搜索步长、收敛因子等参数作出调整。比如当网络流量较大同时入侵行为较为频繁的时候, 可以适度增大搜索步长, 以此加快算法的搜索速率, 迅速定位到潜在的入侵行为, 当网络流量较小且入侵行为较为隐蔽时, 那就减小搜索步长, 提

升算法的搜索精准度,防止出现漏报情况,借助这种参数自适应调整策略,可让鲸鱼优化算法更出色地适应不同的网络场景,提升网络入侵预警模型的性能^[3]。

为达成参数的自适应调整,要构建一套有效的参数评估机制,借助评估模型在不同参数设置时的预警准确率、召回率、F1 值等指标,依据评估结果动态调整参数,还可借助机器学习方法,如强化学习,使算法在持续训练中自动学习最优参数设置策略,融合多源数据特征提取与鲸鱼优化算法参数自适应调整策略,可构建更准确高效的入侵预警模型,有效应对复杂多变的网络入侵威胁。

2.2 基于动态权重分配的鲸鱼优化算法与深度学习模型融合策略

深度学习模型于网络入侵检测领域收获了颇为可观的成果,其有的强大特征学习以及分类能力,可切实有效地识别各类网络入侵行为,不过深度学习模型也存有一些欠缺之处,像训练过程繁杂、对数据量需求较高、容易陷入局部最优状态等,鲸鱼优化算法作为一种群体智能优化算法,拥有全局搜索能力较强、收敛速度较快等优势,可与深度学习模型展开有效的融合,以此弥补彼此的不足^[4]。

在融合进程之中,可运用动态权重分配的策略,在模型开展训练的初期阶段,鉴于深度学习模型尚未充分获取到数据的特征,这个时候可赋予鲸鱼优化算法较大的权重,借助其全局搜索能力迅速寻觅到模型参数的较优解决方案,随着训练的持续推进,深度学习模型逐步学习到数据的特征,其分类能力持续提高,此时可以适度降低鲸鱼优化算法的权重,提升深度学习模型的权重,使得模型更注重对数据特征的精细学习与分类。这种动态权重分配策略可依据模型训练的不同阶段,自动调节鲸鱼优化算法和深度学习模型在融合模型里的贡献,充分呈现两者的优势。

要达成动态权重分配,就得设计出一套恰当合理的权重计算办法,可依据模型于不同训练阶段的性能指标,像损失函数值、准确率等,去计算鲸鱼优化算法以及深度学习模型的权重,举例来讲,要是模型的损失函数值下降速度较快,那就说明深度学习模型的学习成效较好,这时可增加深度学习模型的权重,要是模型陷入局部最优状态,便可增大鲸鱼优化算法的权重,帮助模型跳出局部最优。另外还可引入一些启发式规则,依照网络入侵行为的特点以及变化趋势,动态调整权重,借助基于动态权重分配的鲸鱼优化算法和深度

学习模型融合策略,可构建出更为鲁棒且高效的入侵预警模型,提升对未知入侵行为的检测能力^[5]。

2.3 引入迁移学习与鲸鱼优化算法结合的跨网络入侵预警策略

在实际的网络环境中,不同网络之间的入侵行为具有一定的相似性和差异性。传统的入侵预警模型往往是在单一网络环境下进行训练和测试,当将其应用到其他网络环境时,可能会出现性能下降的问题。为了解决这一问题,可以引入迁移学习与鲸鱼优化算法结合的跨网络入侵预警策略。

迁移学习可把在某一网络环境中所学到的知识与经验,转移到另外一个网络环境里,以此来减少在新网络环境下的训练用时以及数据需求,当构建跨网络入侵预警模型之际,一开始可借助源网络环境下的数据训练出一个基础的入侵预警模型,接着运用迁移学习的方式,把源网络模型里的部分参数或者特征提取器迁移至目标网络模型当中。在目标网络环境中,借助鲸鱼优化算法对迁移之后的模型做的优化与调整,鲸鱼优化算法可搜寻到目标网络环境下最优的模型参数,让模型更适配目标网络的入侵行为特征^[6]。

迁移学习与鲸鱼优化算法相结合时,要留意源网络和目标网络间的差别,可运用特征选择以及特征转换的方式,削减源网络与目标网络间的特征差异,比如挑选在两个网络环境里都有较好区分度的特征来实施迁移,或者对源网络的特征加以转换,让其更契合目标网络的特征分布,另外也可借助鲸鱼优化算法对迁移学习进程中的参数给予优化,像迁移的比例、特征选择的阈值等。引入迁移学习与鲸鱼优化算法结合的跨网络入侵预警策略,能提升入侵预警模型在不同网络环境下的通用性与适应性,降低模型构建的成本和难度。在实际应用当中,不同网络环境下的入侵行为模式以及特征分布,有可能会因为网络架构、用户群体、业务类型等诸多因素而呈现出很大的差异,借助特征选择与转换,以及鲸鱼优化算法对迁移参数加以优化,可提高跨网络入侵预警的效能,比如说,在企业网络和校园网络之间进行迁移的时候,企业网络或许更关注数据泄露方面的入侵特征,而校园网络则可能遭遇更多恶意软件传播带来的威胁。借助上述策略,模型能精准筛选并转换关键特征,同时优化迁移比例等参数,使得从企业网络学习到的知识能有效迁移至校园网络场景。这不仅避免了为每个新网络环境重新构建模型的高昂成本与复杂流程,还能快速适应新环境中的入侵变化,为跨

网络环境下的网络安全提供坚实保障^[7]。

2.4 构建基于鲸鱼优化算法的多层次入侵预警模型评估与更新策略

网络入侵行为处于持续变化与演进的状态，相应地入侵预警模型也得持续评估与更新，保证其性能始终维持在最佳水准，传统的模型评估办法一般仅聚焦于模型在特定数据集上的性能指标，像准确率、召回率等，缺少对模型在实际应用里的全面评估，要构建更为完善的入侵预警模型，需借助鲸鱼优化算法来构建多层次入侵预警模型评估及更新策略。

对于模型评估而言，可从多个不同层次着手来开展评估工作，首先是针对数据层展开评估，针对用于训练以及测试模型的数据开展质量评估，这其中囊括了数据的完整性、准确性以及多样性等多个方面，要是数据出现质量方面的问题，那么说不定会对模型的性能产生影响，此时就需要及时去进行数据清洗以及预处理工作。其次是关于模型层的评估，借助鲸鱼优化算法来对模型的参数实施优化，运用交叉验证等一系列方法去评估模型在不同数据集上所呈现出的性能，凭借鲸鱼优化算法所有的搜索能力，可找寻到模型在不同评估指标情形下的最优参数组合，最后是应用层评估，把模型部署到实际的网络环境当中，针对模型在实际应用过程里的预警效果进行评估，如预警的及时性、准确性以及对网络性能所造成的影响等。

在模型更新环节，依据评估得出的结果，借助鲸鱼优化算法来实现对模型的更新操作，一旦模型在某一层次的评估结果不尽如人意，便可有针对性地对模型展开调整工作，举例来说，要是在数据层评估时察觉到数据存在偏差情况，那么就需要重新进行数据的收集以及标注，要是在模型层评估中发现模型出现过拟合或者欠拟合问题，那么可以运用鲸鱼优化算法来调整模型的复杂度或者正则化参数，要是在应用层评估时发现模型针对某些新型入侵行为的检测能力有所欠缺，那么可引入新的特征或者算法来对模型加以改进。凭借构建一套基于鲸鱼优化算法的多层次入侵预警模型评估与更新策略，可促使模型持续适应网络入侵行为的变化，提升入侵预警的准确性以及可靠性^[8]。

结束语：

本文对鲸鱼优化算法给予改进并应用于网络入侵预警

模型构建工作，提出了一系列有创新性的策略，这些策略涉及多源数据特征提取与算法参数自适应调整的融合，基于动态权重分配的算法与深度学习模型的融合，引入迁移学习并结合算法来达成跨网络预警，以及构建多层次评估与更新策略。上述策略相互协作，切实提升了模型的性能，未来随着网络技术持续发展以及入侵手段变得日益复杂，我们会持续开展研究，完善并优化模型，应对网络安全挑战，为构建安全可靠的网络环境贡献一份力量。

参考文献：

- [1] 邓俊,陈杰,李怡然,等.基于改进鲸鱼优化算法的双馈风电机组控制参数辨识[J].太阳能学报,2025,46(05):496-505.
 - [2] 陈皓宇,罗璟,杨灏泉,等.优化装箱填充率的改进鲸鱼模拟退火算法[J].科学技术与工程,2025,25(15):6477-6485.
 - [3] 胡俊,李小龙,张喻,等.基于改进鲸鱼算法优化支持向量机的电压暂降源识别[J].东北电力技术,2025,46(05):18-22+57.
 - [4] 曾钰翔,张栓.基于IWOA算法的区间二型TSK FLS方法在超声波流量计故障诊断中的应用[J].化工自动化及仪表,2025,52(03):432-440.
 - [5] 苏林王,赵一鸣,王雪刚,等.非支配排序鲸鱼优化算法在深圳沿江沉管隧道管节长度优化中的应用[J].隧道建设(中英文),2025,45(05):964-974.
 - [6] 杨丽荣,周俊,曹冲.改进鲸鱼遗传算法优化的液压机械臂轨迹跟踪[J].传感器与微系统,2025,44(05):94-98.
 - [7] 胡鑫宇,向慧明.基于多策略改进鲸鱼算法的无人机三维路径规划[J].现代电子技术,2025,48(09):79-85.
 - [8] 李宣伯,王雪怡,关朝.基于改进鲸鱼算法的新能源微网能量调度优化方法[J].电气技术与经济,2025,(04):25-27.
- 作者简介：**查道贵（1975.9—），男，汉，安徽安庆人，硕士，宿州职业技术学院计算机信息系副教授，研究方向计算机网络安全、数据安全
- 基金项目：**2022年安徽省教育厅自然科学重点项目《基于鲸鱼优化算法的网络入侵检测研究》（编号：2022AH052765）