基于粒子群算法的网络安全评估优化方案设计

曹 卿[1]
CAO Qing

摘 要 为了进一步改善网络安全评估的效果，提出一种基于粒子群算法的网络安全评估优化方案，网络安全评估是保护互联网和信息系统免受恶意攻击的关键任务，因此提高评估效果对于信息安全领域具有重要意义。介绍了一个融合 PSO 算法和贝叶斯网络的网络安全评估方案，目标是提升网络安全评估的准确性和效率。方案的流程包括数据处理、模式构建、关联数据挖掘、粒子群算法和贝叶斯网络训练等步骤。实验证明，所提出的方案比其他方法更准确，并可以识别各种攻击行为，为网络管理员提供决策支持。综上所述，所提出方法的应用将为网络安全领域的决策和应用提供有力的支持，促进信息系统的安全保护，未来的研究可以进一步探索如何应用该方法来解决更复杂的网络安全问题。

关键词 粒子群算法；网络安全；贝叶斯网络；评估优化

doi：10.3969/j.issn.1672-9528.2024.02.038

0 引言

随着科技的发展，网络已经成为人们工作、学习和生活的必备工具。然而，网络的高度互连和共享也伴随着一系列的安全问题，包括隐私泄露、数据篡改、信息窃取和病毒攻击等。尤其是中国的网民数量不断增加，造成了网络犯罪的增加。一些人为了追求暴利，不惜违法盗取网民的个人隐私和重要数据信息。要解决这些问题，需加强网络安全意识，提高技术防控能力，以保护个人和国家信息安全的同时，促进互联网的良性发展[1]。

网络安全在现代社会中扮演着至关重要的角色。传统的防御手段和策略如入侵检测系统、防火墙等方式虽然发挥了一定作用，但仍然存在诸多缺陷。它们无法有效地阻止身份窃取、病毒传播和内部攻击，也难以动态调整以应对不断变化和复杂化的大规模网络环境的安全需求。在频发的网络安全事件面前，必须采用更先进的技术和手段来保障网络安全。

由于网络安全形势的日益严峻，传统的网络安全防御方法已经不能满足当今复杂多变的网络攻击需求。因此，越来越多的学者和企业开始探索网络安全领域的先进技术和手段，如人工智能、大数据分析、区块链等。这些新兴技术和手段在网络安全领域展现出巨大的潜力，能够帮助网络安全人员及时发现异常行为，快速做出反应，并阻止潜在的威胁。可见，当前的网络安全形势需要更加先进和高效的技术手段来进行保障。新一代的网络安全防御方法和策略正在不断涌现，为网络安全领域带来了新的希望和机遇。未来通过不懈努力和不断创新，积极应对网络安全挑战，构建更为安全可靠的网络环境[2]。

论文介绍了一种基于粒子群算法的网络安全评估优化方案设计。通过对大规模网络捕获的安全要素进行数据融合、数据挖掘分析，并利用可视化技术展现结果，能够快速把握当前网络安全环境，识别潜在威胁和脆弱点，及时采取应急响应措施降低风险损失。该方案还能实时评估网络安全态势，提高网络安全性和应急响应能力，并且在效率和精确性上都有所提高。

1 粒子群算法

粒子群算法（particle swarm optimization，PSO）是一种模拟生物群体行为的优化算法[3]。它的灵感来源于鸟群或鱼群等群体的行为，每个个体（粒子）代表一种解决方案，并根据自身经验和群体的协作来更新和改进解决方案，最终找到最优解。

在粒子群算法中，每个粒子都有一个位置和速度。粒子根据自身的当前位置和速度进行移动，并根据目标函数的评价结果来更新最优位置和最优解。粒子在搜索过程中会相互学习和交流，通过共享经验和信息，有助于更好地探索问题空间。粒子群算法的核心思想是“个体最优与群体最优的权衡”，即每个粒子不仅追求自身最优解，还根据群体中的最优解进行适应度调整和参数更新，从而实现全局最优解的搜索。粒子群算法适用于多维、非线性、复杂的优化问题，并

1. 闽南理工学院信息管理学院 福建石狮 362700
[基金项目] 福建省中青年教师教育科研项目（JAT220424）

且具有收敛速度快、易于实现等优点。它已经在许多领域得到了广泛应用，包括机器学习、数据挖掘、图像处理、路线规划等。同时，粒子群算法也有一些改进版本，如改进的粒子群算法、多目标粒子群算法等，以满足应对不同问题的需求 [4-5]。

随着研究的深入，PSO 在多个领域得到广泛应用，成为一种随机的种群优化技术。PSO 将鸟类个体抽象为没有质量的粒子，在多维空间中寻找全局最优解 [6-7]。

论文研究了基于非线性变化的PSO算法中的惯性权重 w。在算法的初始阶段，由于迭代次数较少，w 与最大权重 w_{max} 相近，PSO 算法展现出了很强的全局寻优能力。随着迭代次数的增加，算法的局部寻优能力得到保证，同时惯性权重 w 的减少幅度呈逐渐增加的非线性趋势。这进一步加快了算法的收敛速度，并提高了其在全局寻优方面的效果。

2 网络安全评估优化方案设计

2.1 方法建立

此部分采用了 PSO 算法来进行全局寻优，这是一种模拟鸟群或鱼群等自然群体行为的算法。通过将粒子的位置和速度作为搜索空间的探索，PSO 算法不断调整参数以寻找最优解。将 PSO 算法应用于网络安全评估中，将粒子的位置表示为不同的关联数据组合，将速度视为关联数据组之间的变化趋势。通过不断更新粒子的位置和速度，PSO 算法能够不断优化关联数据组的组合方式，进而提高网络安全评估的准确性和效率。

同时，还引入了贝叶斯网络来进行训练和生成评估模型。贝叶斯网络是一种概率图模型，用于模拟随机变量之间的依赖关系 [8]。在网络安全评估中，将各种攻击行为以及相关的关联数据作为随机变量，通过训练贝叶斯网络来建立攻击行为与关联数据之间的条件概率分布。生成的评估模型将能够根据当前网络的状态和行为数据，通过概率推理来判断网络的安全态势，并生成相应的评估结果。

通过在实际网络环境中进行实验和评估，发现采用 PSO 算法和贝叶斯网络的优化方法能够显著提高网络安全评估的准确性和效率。这种方法不仅能够识别各种攻击行为及其关联数据，还能够判断网络的安全态势和预测潜在攻击的可能性。PSO 算法是一种启发式优化算法，模拟鸟群觅食过程的数学模型，通过迭代更新粒子位置以找到最优解。结合 PSO 算法和贝叶斯网络的优化方法，可以更精确地捕捉网络中复杂的攻击行为和关联性，从而提高了网络安全评估的准确性和效率。基于生成的评估结果，网络管理员能够及时采取相应的安全措施以应对潜在威胁，保障网络的安全稳定运行。这种方法为网络安全领域带来了更多的决策参考，有助于提前发现和应对各种潜在的网络安全威胁，从而降低网络遭受攻击的可能性，保护用户数据和网络系统的安全。在未来的研究中，将不断优化和改进这种方法，以适应网络安全形势的快速变化，为网络安全领域的研究和实践提供更有力的支持。

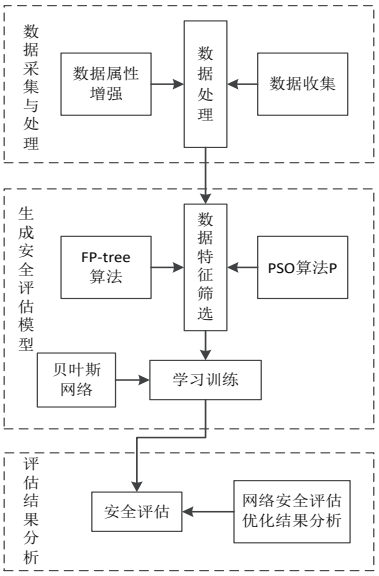

图 1 基于粒子群算法的网络安全评估优化方案

2.2 算法流程

该算法综合了数值属性增强处理、频繁模式树构建和关联数据挖掘、粒子群算法和贝叶斯网络训练等步骤，形成了一个复杂的网络安全评估系统。

首先，通过对数值属性的增强处理，将数据中的零值进行属性增强，选择适用的前缀来表达零值所代表的含义。对于其他相同数字数据，采用相同的增强方法，这可以有效地将数据中的零值转化为可用的信息，并避免其对网络安全评估产生干扰。接下来，算法通过初始化频繁模式树，确定相关参数并确定最小支持度。

其次，对数据进行特征筛选，建立频繁模式树，并剔除小于最小支持度的数据，从而生成关联数据组。这些步骤旨在提取有效的数据特征，为后续的网络安全评估提供可靠的数据基础。

然后，将关联数据组输入到改进的粒子群算法中，通过迭代推进，寻找多维解空间内的全局最优解。粒子群算法的引入有助于优化参数搜索过程，提高了网络安全评估的准确性和效率。同时，将处理后的网络流量数据输入到贝叶斯网络中进行训练，利用优化的贝叶斯网络提升网络安全态势评估的性能。贝叶斯网络在这里的作用是通过学习数据分布和概率关系，为网络管理员提供对网络安全态势的准确判断和预测能力。

最后，将测试集数据输入训练好的模型中，得出输出结

果，即态势评估值。选择最大的态势值作为当前网络的态势值，并结合网络安全态势评估等级表来分析当前的网络安全状况，得出当前网络安全状态结果值。通过处理和优化数据特征，该算法提高了网络安全评估的准确度和性能。最终的网络安全态势评估结果可以帮助判断当前网络的安全状况，并提供必要的支持来处理网络安全问题。

这套算法体系完整、结构合理，可应用于网络安全领域，并对提高网络安全性具有重要意义。通过融合多种计算方法和技术，该算法综合利用了数据处理、特征提取和优化算法等领域的知识，为网络安全评估提供了全面而准确的分析。在实际应用中，这套算法可以帮助网络管理员及时发现网络安全问题，并采取有效的措施，从而保障网络的安全稳定运行。在未来的研究和实践中，将继续改进和完善该算法，以应对不断变化的网络安全威胁，为网络安全领域的发展贡献更多的力量。

算法如下：

Step 1：数值属性增强处理

for each data in dataset do

if data contains repeated "0" then

replace "0" with first three initials of the meaning in English

else if data contains repeated same digit then

replace digit with first three initials of the meaning in English + digit

end for

Step 2：初始化频繁模式树

set minimum support threshold based on dataset

Step 3：特征筛选

build frequent pattern tree using dataset and minimum support threshold

mine frequent patterns from frequent pattern tree

filter out factors with smaller support than minimum support threshold

Step 4：粒子群联合贝叶斯网络

input filtered frequent pattern data into improved particle swarm algorithm

update particles' positions and velocities to converge to global optimal solution

input processed network traffic data into Bayesian network for training

Step 5：态势评估

input test dataset into trained model

calculate and select maximum situation evaluation value

analyze network security situation based on network security situation evaluation table

output current network security status result

End

3 实验分析

3.1 数据预处理

实验使用 KDD99 数据集，这个数据集是一个经典的用于网络入侵检测的数据集，由 MIT 林肯实验室创建。它模拟了 1998 年至 1999 年期间模拟的一组网络流量，来模拟实际电信网络中的非法活动。该数据集包含了 41 种不同的网络攻击类型，分为 4 个主要类别：DoS（拒绝服务攻击）、R2L（远程到本地攻击）、U2R（用户到根攻击）和 Probing（侦查攻击）。

KDD99 数据集中的连续特征属性需要进行标准化和归一化处理，以消除度量单位和属性差异对聚类结果的影响。标准化调整属性值分布为均值为 0、标准差为 1 的正态分布，而归一化将属性值缩放到 [0,1] 范围内。这些步骤提升了聚类分析的准确性和稳定性。

论文利用了关联规则分析方法对 KDD99 数据集进行处理，以构建优化的贝叶斯网络模型，从而提高训练模型的精确度和速度。特别针对 KDD-99 数据集的 4 类攻击类型，在 FP-tree 算法的特性下，针对多维属性稀疏性的数据，提出了在第七维到第四十一维数据中增强重复出现的数值型数据属性，其中包括含有“0”或“1”的数据。

这些方法和步骤的应用旨在增进对网络安全的理解和防范，提高对非法活动的检测能力，进而保护网络系统和用户的安全。通过对 KDD99 数据集的深入研究和分析，可以为网络安全领域的研究和实践贡献宝贵的经验和见解，为构建更加健壮和可靠的网络安全防护机制提供有力的支持。

3.2 实验验证与分析

本次实验使用 Windows 11 操作系统的计算机。CPU 是 Intel core i7-9750H，主频为 2.60 GHz，内存容量为 16 GB，图形处理器为 NVIDIA Geforce GTX 1650。实验所使用的编程语言为 Python 3.9。

基于关联规则的安全评估方案（ATA-OM）实验，首先对数据进行预处理，标准化和归一化处理数值。然后替换处理好的数值以适应频繁模式树算法，对频繁模式树算法初始化，设定相关参数，如最小支持度和选取依据。最后，数据经处理后，维度下降，加上表示当前数据支持度的维度。算法根据设置的最小支持度，提取关联数据组，关联数据组保留网络安全影响较大的因子。将四个关联数据组输入贝叶斯网络进行训练，得到完整的贝叶斯网络模型。将测试数据输入训练好的贝叶斯网络，得到四大类攻击的态势值，选取最大的态势值作为当前网络的最终态势值。结合网络安全态势评估等级分类表分析当前网络安全状况，并与基于传统贝叶

斯的网络安全态势模型进行对比。

基于粒子群联合贝叶斯的网络安全评估优化模型（PSO-OM）的验证实验。与前一个实验相同，首先对数据进行预处理和替换处理，对频繁模式树进行初始化操作，设置最小支持度，通过频繁模式树处理数据，提取四个关联数据组。其次，将关联数据在粒子群算法中进行进一步处理，通过迭代寻找全局最优解，保留对网络安全影响较大的因子。然后，根据处理后的数据构建优化的贝叶斯网络，优化贝叶斯网络的学习结构，提升复杂贝叶斯网络结构的计算能力，加快评估速度，将之前的数据集输入贝叶斯网络中，训练模型。最后将测试集输入训练完的模型，输出关于四类攻击的态势评估值，选取最大值作为当前网络安全态势的评估值，确定当前网络最可能的攻击类型。

将两组实验结果进行整合，进行误差率分析，通过对比 PSO-OM、ATA-OM 和经典的 BN 对 DOS、R2L、Probing 的准确率和误差率进行评估。由于 U2R 在数据集中的样本过低，不计入实验结果。

在图 2 和图 3 的实验中，对论文提出的基于粒子群的网络安全评估优化方案进行了准确率和误差率的比较。结果显示，该优化方案在准确性和误差方面均优于基于关联规则分析的网络安全评估优化方法以及传统的贝叶斯网络的网络安全评估优化方法。具体来说，论文提出的优化方法表现出更高的准确性和更低的误差率，这表明该方法在提高网络安全评估的准确性和可靠性方面具有较大的潜力。

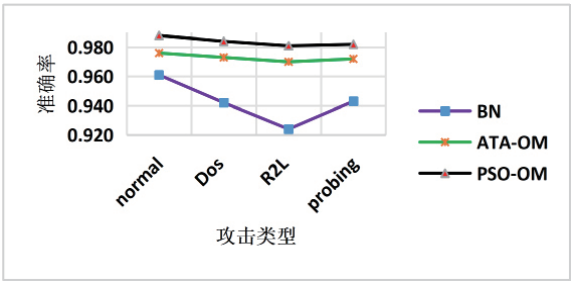

图 2 准确率实验分析图

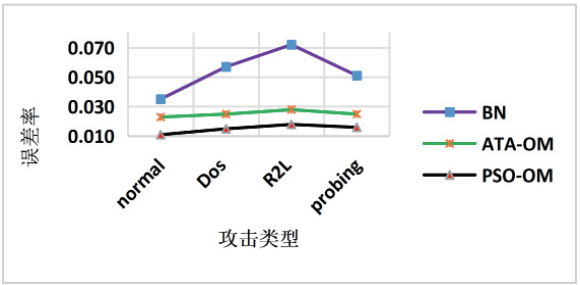

图 3 误差率实验分析图

通过对实验结果的分析，可以得出结论，基于粒子群的网络安全评估优化方案相较于其他方法，在评估网络安全方面具有更好的性能表现，为网络安全领域的研究和实践提供了有力的支持和指导。这一发现为网络安全技术的改进提供了有益的思路和方向，有望在实际应用中取得更好的效果。

综上所述，论文提出的基于粒子群的网络安全评估优化方案在准确性和误差率方面的优势得到了实验证实，为网络安全领域的研究和应用带来了新的启示和机遇。这一研究成果为网络安全技术的发展贡献了重要的理论和实践价值，对于提升网络安全保障和风险管理具有重要意义。

4 总结

为了进一步提高网络安全评估的效果，论文在研究中首先在粒子群算法中引入了适应度函数的改进方法，以提高搜索过程的效率和准确性。其次，在贝叶斯网络的优化过程中，考虑了特征选择的问题，通过选择最相关的特征子集，进一步提高了模型的性能。然后，本文还对优化方法的时间复杂度进行了详细分析，并提出了相应的优化策略，以确保方法的实用性和可行性。最后，通过大量的实验数据和验证实验的结果，充分证明了该优化方法在网络安全评估中的有效性和可靠性。综上所述，论文所提出的基于粒子群联合贝叶斯的网络安全评估优化方法是一种有效和可行的方法，可为网络安全领域的决策和应用提供有力的支持。这一优化方法在理论和实践上均取得了显著的成果，为网络安全领域的技术发展和应用提供了重要的借鉴和参考。

参考文献：

[1] 劳雪松 . 基于漏洞检测技术的网络安全评估系统设计 [J]. 信息与电脑 (理论版), 2023,35(14):226-228.

[2] 周经辉 . 基于网络安全评估的信息安全保护算法研究 [J]. 长江信息通信 ,2022,35(12):152-154.

[3] KENNED J, EBERHART R. Particle swarm optimization [C]// Proceedings of ICNN95-international Con-ference on Neural Networks. Piscataway: IEEE, 1995,4: 1942-1948.

[4] 解羽 . 基于神经网络的互联网安全态势预测技术研究 [D]. 沈阳 : 沈阳理工大学 ,2021.

[5] 李娜娜 . 基于改进粒子群算法的多目标优化问题研究 [D]. 贵阳 : 贵州民族大学 ,2022.

[6] 仝兆景 , 李金香 , 乔征瑞 . 一种具有结构先验的贝叶斯网络结构学习算法 [J]. 电子科技 ,2023,36(11):1-7.

[7] 郭任 . 基于改进粒子群算法的网络安全姿态自动预测方法 [J]. 网络安全技术与应用 ,2023(9):33-35.

[8] 宋伟伟 . 基于贝叶斯网络的网络安全态势感知和预测方法研究 [D]. 哈尔滨 : 哈尔滨理工大学 ,2023.

【作者简介】

曹卿（1986—），女，福建晋江人，硕士，讲师，研究方向：数据库、数据挖掘。

（收稿日期：2023-11-30）