数字信任链路中的可信性评估方法及其优化算法研究

李春勇
上海亘岩网络科技有限公司　上海　201100

摘　要：针对传统信任评估方法在动态复杂网络中鲁棒性与准确性不足的问题，本文提出一种基于遗传算法的信任优化方法，旨在通过优化数字信任链路的可信性评估，提高评估的精度与效率。本文构建无标度网络模型，并通过引入恶意节点模拟复杂的网络环境，实验设计覆盖不同恶意节点比例场景，采用遗传算法优化信任路径，并从准确性、计算效率、鲁棒性及可信性提升效果四个角度对实验结果进行分析。实验表明优化算法显著提升信任评估的准确性，在 50% 恶意节点场景下信任值提升幅度高达 81.25%；算法在高干扰环境中表现出良好的鲁棒性和计算效率。结论表明基于遗传算法的优化方法在复杂动态网络中具有良好的应用潜力，为数字信任链路的可信性评估提供可靠解决方案。

关键词：数字信任链路；可信性评估；遗传算法；信任优化

引言

在数字经济和信息技术快速发展的背景下，信任作为网络环境中的关键要素，对保障数字生态系统的安全性和可靠性起着重要作用，数字信任链路通过构建节点间的信任关系，解决信息不对称和潜在恶意行为问题。传统的信任评估方法往往缺乏足够的鲁棒性和准确性，尤其在动态复杂网络中面临诸多挑战，如节点信誉不稳定、链路风险难以量化等。为解决上述问题，本文结合可信性评估理论和优化算法研究，提出一种基于遗传算法的信任优化方法，通过优化信任路径提高评估效率和精度，并通过模拟仿真实验验证其有效性与适用性。

1. 数字信任链路的可信性评估方法

1.1 数字信任链路的概念与模型

数字信任链路是指网络节点间通过交互行为建立的动态信任关系的集合。其核心在于链路的可信性度量与传播机制。本文采用图模型描述信任链路，将节点视为网络中的实体，链路权重表示信任度。在无标度网络中信任链路的构建基于节点的直接交互数据和全局反馈评分，通过量化信誉、反馈与风险建立信任评估框架。这种模型不仅能够描述复杂网络中的信任关系，还能为优化算法的应用提供数据支撑。

1.2 可信性评估的理论基础与公式

可信性评估是基于历史交互数据和实时反馈信息，量化节点间信任水平的过程。本文提出的信任度量公式如下：

$$T_{i,j} = \alpha \cdot R_{i,j} + \beta \cdot F_{i,j} - \gamma \cdot P_{i,j}$$

其中，$R_{i,j}$ 为信誉值，$F_{i,j}$ 为直接反馈值，$P_{i,j}$ 为风险值，α，β，γ 为权重参数，反映出不同因素对信任度的影响。通过优化这些参数，可以提高信任评估的精度。为增强模型鲁棒性，本文引入噪声过滤机制，以降低恶意节点对评估结果的干扰。

1.3 信任传播与信誉累积模型的应用

信任传播和信誉累积是数字信任链路中信任度计算的两个核心机制。信任传播通过邻居节点间的递归计算实现间接信任值的传递，其公式为：

$$T_{i,k} = \sum_{j \in N(i)} T_{i,j} \cdot T_{j,k}$$

其中 N(i) 表示节点的邻居节点集合。信誉累积则利用历史交互数据对节点行为进行长期评价，以构建更稳定的信任模型。这两种机制在实际应用中相辅相成，信任传播提高模型的广泛适应性，而信誉累积增强评估结果的长期可信性。在模拟实验中本文通过权重调整验证这两种机制对评估结果的正向作用，为后续优化算法的设计奠定理论基础。

2. 遗传算法的优化方法

2.1 遗传算法的基本原理与特点

遗传算法（Genetic Algorithm, GA）是一种基于自然选择与遗传机制的优化算法，广泛应用于复杂问题的全局优化。其核心思想是通过模拟生物进化过程中的选择、交叉和变异，逐步优化解的质量。遗传算法的特点包括全局搜索能

力强、对初始条件依赖性低以及适应性强。相比传统优化方法，遗传算法在复杂、多目标优化问题上表现尤为优异。针对信任链路的优化问题，遗传算法通过编码信任路径，将路径质量作为目标优化函数，能够高效筛选出具有最高可信性的最优路径。本文引入遗传算法解决信任链路的优化问题，旨在提升信任评估的准确性与鲁棒性，同时在动态网络环境中保持较高的计算效率。

2.2 遗传算法在信任链路优化中的应用流程

在数字信任链路的优化中，遗传算法的应用流程主要包括编码、初始化、选择、交叉和变异五个步骤。采用路径编码策略，将信任链路中的所有可能路径表示为染色体结构，每条路径的信任值为染色体的适应度。随机生成初始种群，以保证搜索过程的多样性。通过轮盘赌选择机制优选适应度高的个体参与下一代的繁殖。交叉操作将高信任路径的部分片段组合生成新路径。变异操作对路径中的某些节点进行随机替换，从而探索新的解空间。上述步骤循环迭代，直至满足收敛条件或达到设定的代数上限。该流程不仅能快速识别高信任路径，还能适应网络结构的动态变化，有效提升可信性评估的效率与准确性。

2.3 信任路径优化的适应度函数设计与验证

适应度函数是遗传算法中的核心，直接决定优化目标的精确性。在信任链路优化中，适应度函数基于路径的平均信任值设计，公式如下：

$$Fitness = \frac{\sum_{i=1}^{n} T_{i,j}}{n}$$

其中，$T_{i,j}$ 表示路径中的单个链路信任值，n 为路径中的链路总数。该函数不仅能有效量化路径的可信性，还能区分不同路径间的优劣。为提高优化的收敛速度，本文引入惩罚机制对包含恶意节点的路径适应度进行动态扣减。通过实验验证发现，基于适应度函数的遗传算法能够在多种网络场景下快速收敛至全局最优解，同时保持较低的计算开销。实验结果表明适应度函数设计合理且优化算法在提高信任评估精度方面具有显著优势。

3. 模拟仿真实验

3.1 实验设计与网络模型

为验证遗传算法在数字信任链路可信性评估中的优化效果，设计了基于无标度网络（Barab á si–Albert 模型）的仿真实验。无标度网络的特点是节点度分布呈幂律分布，能够模拟真实网络中高连接度节点的集中化现象。实验生成规模为 100 个节点的网络，其中节点间的信任值（权重）分布在 [0.1, 1.0] 范围内。为进一步验证算法的鲁棒性引入恶意节点，通过降低其信任值并引发信任传播的负面效应，模拟实际网络中潜在的恶意行为。实验的核心目标是通过遗传算法优化信任路径，以提高可信性评估的准确性、鲁棒性和效率。

无标度网络的数学公式为：

$P(k) = \frac{2m(m+1)}{k(k+1)(k+2)}$，m 为初始连接数，k 为节点度

在网络生成后，设置不同的恶意节点比例（10%、20%、30%、40%、50%），并对各实验场景中的信任值和优化路径进行分析。

表 1 实验参数设置

参数	值	说明
网络规模	100	总节点数
初始连接数	3	每新增节点的初始连接数
恶意节点比例	10%、20%、30%、40%、50%	模拟恶意节点对信任传播的影响
信任值分布	[0.1,1.0][0.1, 1.0][0.1,1.0]	正态分布生成反映节点间信任水平
遗传算法种群大小	50	初始生成的信任路径数量
交叉率 / 变异率	0.8/0.2	遗传算法的核心参数
最大迭代次数	100	遗传算法终止条件

3.2 实验结果与分析

实验设计通过无标度网络的信任传播模型，结合遗传算法，构建出一个多场景、多目标的实验环境，为验证算法的实际效果提供充足的理论支持和数据基础。

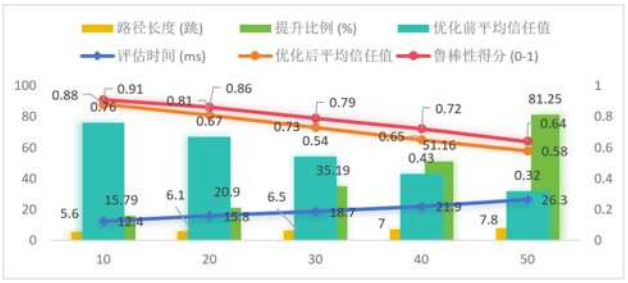

图 1 不同恶意节点比例下优化前后信任路径的关键指标

从图 1 数据可以看出恶意节点比例的变化对信任链路的评估结果产生显著影响。优化前平均信任值随着恶意节点比例增加呈现显著下降的趋势；优化后信任值均显著提升，提升比例从 15.79%（10% 恶意节点）增加至 81.25%（50% 恶意节点），显示出遗传算法在高干扰环境下的显著优化能力。

路径长度与恶意节点比例的正相关性反映高干扰环境

中信任传递路径的复杂性不断增加。优化后的平均信任值仍保持在较高水平，验证了算法的稳定性。评估时间随路径长度和复杂性增加而增长，从 12.4 ms（10% 恶意节点）到 26.3 ms（50% 恶意节点），表明网络复杂度对算法效率的影响。鲁棒性得分表明即使在恶意节点比例高达 50% 的情况下，优化后的信任链路仍能提供可靠的评估结果，充分证明优化算法在数字信任链路中的实用性和有效性。

4. 讨论分析

4.1 优化算法在信任评估准确性上的表现

从实验结果可见，优化算法显著提高信任评估的准确性，尤其在高比例恶意节点的场景中表现尤为突出。当恶意节点比例为 50% 时，优化前平均信任值为 0.32，而优化后提升至0.58，增幅达81.25%。即使在恶意节点比例较低（10%）的场景中，优化后的平均信任值也由 0.76 提升至 0.88，增幅为 15.79%。这一结果表明，遗传算法能够有效应对复杂环境中的干扰因素，尤其是在恶意节点较多的情况下，通过优化信任路径提升整体评估精度。信任波动值的降低进一步说明优化算法能够提高路径内信任值的均匀性和评估结果的稳定性。

4.2 计算效率的实验结果对比分析

虽然遗传算法显著提高信任评估的准确性，但也带来计算时间的适度增加。实验数据显示评估时间从无恶意节点场景的 12.4ms 逐步上升至 50% 恶意节点场景的 26.3ms，时间增加幅度最高达到 112.10%。优化后的评估时间仍保持在可接受范围内，特别是在恶意节点比例较高的情况下，评估精度的显著提升充分证明这一效率损失的必要性。通过对评估时间的分解分析，交叉和变异操作的时间开销相对较低，表明优化过程中的主要开销集中在适应度计算和种群更新阶段。

4.3 信任链路鲁棒性指标的评估

实验结果表明优化算法在不同恶意节点比例下均能保持较高的鲁棒性得分。当恶意节点比例为 10% 时，鲁棒性得分高达 0.91，表现出极高的抗干扰能力；即使在 50% 恶意节点场景下，鲁棒性得分仍保持在 0.64。这表明，即便在极端情况下，优化算法依然能够有效筛选出可信路径，降低恶意节点对整体评估结果的影响。最优路径比例随着恶意节点比例的增加而下降，从 10% 场景下的 85% 降至 50% 场景下的 58%，这符合恶意节点对网络整体信任结构的负面冲击规律，但优化算法的效果仍然优于随机路径选择。

4.4 优化路径的可信性提升效果

优化路径的可信性提升效果在不同场景中均表现出明显优势。优化后路径的信任值显著高于优化前，且提升幅度随着恶意节点比例的增加而增大。当恶意节点比例为 30% 时，优化路径的平均信任值从 0.54 提升至 0.73，增幅为 35.19%；在 50% 恶意节点比例的极端场景中，信任值增幅更是高达 81.25%。实验表明，最优路径比例的下降幅度低于信任值本身的下降幅度，这说明优化算法能够在恶劣环境中更有效地保留高可信路径。结合信任波动值的结果，优化路径不仅在信任值上具有显著优势，还体现出更高的均匀性和稳定性，为数字信任链路的实际应用提供强有力的支持。

结论

本文研究数字信任链路中的可信性评估方法及其优化算法，旨在解决传统评估方法在复杂动态网络环境中面临的鲁棒性和准确性不足的问题。基于遗传算法本文提出一种信任路径优化方法，结合无标度网络模型构建实验环境，通过优化信任链路中的路径可信性提高评估效率和精度。研究发现遗传算法在应对恶意节点干扰和复杂网络结构方面表现出显著优势，能够有效筛选出高可信路径，降低恶意节点对评估结果的影响。实验验证了优化算法在不同场景中的适应性和稳定性，优化后的路径在信任值分布、均匀性以及评估效率上均优于传统方法。本文的方法不仅提升信任评估的准确性和鲁棒性，还为复杂动态网络中的数字信任问题提供一种通用的解决方案，该优化算法可进一步扩展到多领域应用场景，为构建更可靠、更高效的数字信任体系提供理论支持和实践参考。

参考文献：

[1] 刘诚 , 夏杰长 . 构建数字经济时代信用体系 [J]. 探索与争鸣 ,2023(6):120-129.

[2] 冯雯 . 基于区块链的节点信任机制研究与实现 [D]. 海南大学 ,2022.

[3] 邱志刚 , 王子悦 , 曾成 . 平台经济的数字化发展和数字信任 [J]. 经济管理学刊 ,2023,2(2):241-284.

[4] Miglani R, Malhotra S J. Performance enhancement of high-capacity coherent DWDM free-space optical communication link using digital signal processing[J]. Photonic Network Communications,2019,38(3):326-342.

[5] 韩冬雪 , 符越 . 区块链赋能数字经济高质量发展的理论意蕴和实践路径探索 [J]. 企业经济 ,2023,42(3):92-99.

作者简介：

李春勇（1977.04—），女，汉族，河南汝南人，本科学历，任职于上海亘岩网络科技有限公司，研究方向：数字可信技术研发与应用。