基于禁忌搜索算法的实验室局域网数据安全交换方法

赵 云[1]
ZHAO Yun

摘 要 实验室局域网为提高可靠性大多采用网状拓扑结构，这意味着设备之间存在多条连接链路。在这种情况下，数据交换的路径选择变得更加复杂。现有数据安全交换方法在面临多种路径选择的情况下，会陷入局部最优解。对此，文章引入禁忌搜索算法，开展实验室局域网数据安全交换方法研究。首先，通过强度指标与粒度数据的计算实现室局域网数据特征提取；然后，采用数据安全加密机制，有效防止了数据泄露和非法访问；最后，在此基础上引入禁忌搜索算法，通过设定解空间、目标函数、禁忌表等关键要素，来避免算法陷入局部最优解。以选择最优路径实现实验室局域网数据安全交换传输。通过对比实验证明，该方法不仅能够显著提升实验室局域网数据的安全性和传输效率，还能有效避免无谓的数据交换，为实验室数据的安全管理和高效利用提供了有力支持。

关键词 禁忌搜索算法；局域网；交换；数据安全；实验室

doi：10.3969/j.issn.1672-9528.2025.03.026

0 引言

随着信息技术的快速发展，实验室局域网中的数据交换需求日益增加，数据安全成为了一个亟需解决的问题。传统的数据安全交换方法在面对复杂多变的网络环境时，往往存在诸多不足。例如，程子栋[1]指出，政务信息系统在数据共享开放过程中面临异构系统、权责不清和机制不成熟等问题，导致数据共享缓慢且效率低下。尽管区块链技术在一定程度上可以提高数据共享的安全性和透明度，但在实验室局域网环境中，其复杂的架构和较高的资源消耗限制了其广泛应用。韩路[2]提出了一种基于改进阻塞判别算法的数据安全交换方法，通过调节局域网数据的传输通道参数和加密参数管理，提高了数据转存率和降低了时延。然而，改进阻塞判别算法虽然提高了数据交换的安全性，但在面对大规模数据交换时，其计算复杂度和资源消耗显著增加，可能导致系统性能下降。高勇等人[3]提出基于 XMLSchema 技术的数据交换方法，文章从身份验证、安全密钥、数据传输、接收以及处理等方面提出基于 XML Schema 的数据安全交换机制。然而，在高并发的数据交换场景下，这些多轮交互会累积大量的延迟，降低整体的数据交换性能。童伟等人[4]提出基于区块链技术的数据交换方法，通过数据安全沙箱，按照约定的数据计算模型对加密数据进行沙箱内安全计算，并获取数据安全沙箱发送的计算结果，将计算结果发布到区块链，以供数据需求方通过区块链获取计算结果。然而，区块链的特性之一是数据的分布式存储，每个节点都保存一份完整或部分的账本副本。这意味着数据被多次存储，对于大规模的数据交换，这种冗余存储会占用大量的存储空间。

鉴于上述文献中存在的不足，本文提出了一种基于禁忌搜索算法的数据交换方法。

1 实验室局域网数据特征提取

通过实验室局域网数据特征提取，可以在接收端进行验证，确保接收到的数据与发送的数据在类型、格式和内容上保持一致，从而保证数据的准确性。在实验室局域网环境中，进行数据特征提取时[5]，首先计算强度指标（数据的读写强度）以及粒度数据（数据块的大小）。这些指标对于优化转储策略至关重要，因为能够反应数据的动态变化和存储需求。

强度指标能够揭示数据的读写活动模式，从而帮助识别活跃或静态数据。对于活跃数据，需要更频繁地提取和处理；而对于静态的数据，则可以减少提取频率，以节省资源。则强度指标计算的公式可表示为：

$$I=\frac{R+W}{TG} \tag{1}$$

式中：I 表示强度指标；R 表示读操作次数；W 表示写操作次数；T 表示发送时间。通过合理设置数据块的大小，可以优化数据提取的效率。较小的数据块可能意味着更多的 I/O 操作，而较大的数据块则可以减少 I/O 操作的次数，但可能

1. 苏州信息职业技术学院 江苏吴江 215200

会增加每次操作的延迟。因此，根据实际情况选择合适的数据块大小。则粒度数据计算公式为：

$$G_d = \frac{D_t}{NI} \tag{2}$$

式中：G_d 表示粒度数据；D_t 表示总数据量；N 表示数据块的数量。

在完成了这两个关键指标的计算后，基于这些信息进行实验室局域网数据特征提取。这一步骤将充分利用强度指标和粒度数据所提供的信息，精准地识别出数据中的关键特征，此过程的数据特征提取遵循公式为：

$$G = e^3 + \sum_{l=1}^{+\infty} \frac{K_{s-l} \times K_l}{K_{s+l} G_d} + \frac{P_l}{IP_s} \tag{3}$$

式中：G 表示最终提取特征数据；K 表示节点阈值取值范围；s 表示进行转储所需的时间；l 表示分类区域区间特征数值；P 表示转储的规则指标。将上述公式作为依据，对实验室局域网数据特征进行提取。从实验室局域网中收集数据，并提取关键特征。这些特征包括数据的大小、类型、冗余度、访问频率等。这一步骤是后续处理的基础，掌握了数据的基本特征。

2 基于禁忌搜索算法的数据安全交换传输

基于上述得到的实验室局域网数据特征，通过一个数据安全加密机制，综合处理并分析从实验室局域网中收集到的各类数据特征 [6-7]，以有效增强数据加密的严谨性与科学性，建立安全加密公式：

$$Q = 1 - G \sum_{v=0}^{i} \frac{L_i^2}{Tv} - \sum_{p=0}^{j} \frac{T_j^2}{Cp} \tag{4}$$

式中：Q 表示安全加密；L_i 表示不同类型的安全特征；T_j 表示交换过程中的不同安全相关因素；C 表示相关交换过程特征参数；v 表示局部数据加密强度值；p 表示处理过滤后的局域网数据特征 [8]。

在实验室局域网内实现了数据安全加密后，引入禁忌搜索算法，以实现高性能的局域网数据交换传输 [9-10]。禁忌搜索算法是一种用于解决组合优化问题的启发式搜索算法，它通过设定解空间、目标函数、禁忌表和禁忌长度等关键要素，来避免算法陷入局部最优解。以选择最优路径实现实验室局域网数据安全交换传输。具体步骤如下：

（1）解空间与目标函数设定

设组合优化问题的解空间为 S，目标函数为 $f(x)$，其中 $x \in S$。目标是找到 $x^* \in S$，使得 $f(x^*)$ 达到最优。对于解 $x \in S$，定义其邻域 $N(x)$。邻域是通过对当前解 x 进行某种局部变换得到的一组解 [11-12]。

（2）禁忌表与禁忌长度设定

设禁忌表为 T，禁忌长度为 $t_{\max}$。禁忌表用于记录最近访问过的解或者移动操作，以避免算法陷入局部最优解的循环搜索。当一个解或者移动操作被加入禁忌表后，在接下来的 $t_{\max}$ 次迭代中，该解或者移动操作将被禁止访问或执行。

（3）算法迭代过程

设 x_k 为第 k 次迭代的当前解，x_{k+1} 为下一次迭代的解。则：

$$x_{k+1} = \arg\min_{x' \in N(x^k)} f(x')Q \tag{5}$$

（4）限制步长交换传输优化

然而，简单的交换策略可能会忽视数据之间的伪效率比（即单位重量所带来的价值）差异，导致低伪效率比的数据被错误地替换掉高伪效率比的数据，进而产生适应度较低的解。对此，本文提出了一种既简洁又高效的限制步长交换策略。该策略的核心思想是尽可能地在伪效率比相近的数据之间进行交换，并设定一个步长限制，以确保交换的合理性。在数据预处理阶段，已经将所有数据的伪效率比进行了降序排列。为了促进同一伪效率比水平数据之间的交换，引入了一个步长参数 L。只有当两个数据在排序中的位置相差不超过 L 时，才允许它们进行交换 [13-14]。设 i 和 j 为两个数据的索引，且 $i < j$，若 $j-i \le L$，则数据 i 和数据 j 被视为可交换的候选。其中，L 为步长限制参数。这一过程的表达式为：

$$N(s) = s \oplus S_w(i,j)x_{k+1} \tag{6}$$

式中：$N(s)$ 表示交换结果；s 表示解决方案的编号；$S_w(i,j)$ 表示在限制步长范围内交换数据和。通过引入限制步长交换策略，能够在保持算法简洁性的同时，并减少了无谓交换的发生。

3 对比实验

3.1 实验环境

为验证本文提出的基于禁忌搜索算法的交换方法在实际应用中的可行性和有效性，选定一个实验室局域网作为实验环境和对象，并在该网络环境中实施了数据交换测试。为确保实验的可对比性，设立两组对照实验：对照 A 组采用基于区块链的交换方法，对照 B 组则采用基于改进阻塞判别算法的交换方法。通过对比这 3 种方法的交换结果，全面检验了其应用性能。实验的具体参数包括：物联网区域覆盖 3 000 km×3 000 km，整个实验在 15 h 内完成，存

储节点的密度为每平方公里 150 个，每次数据交互的周期为 800 s，最低传输速率设定为 1 024 kbit/s。实验中所涉及的数据局域网拓扑结构如图 1 所示。按照图 1 所示完成对实验环境的建立。

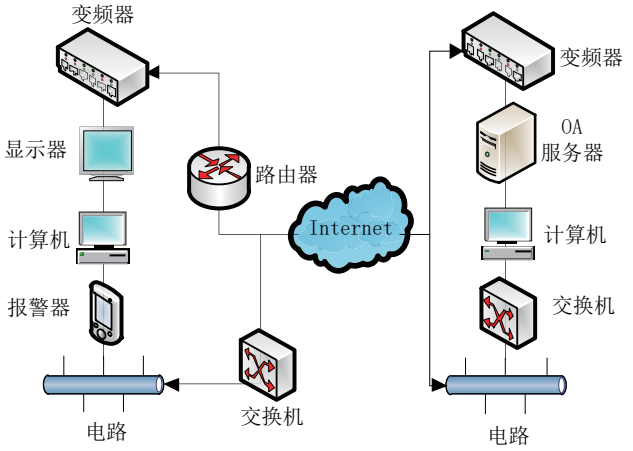

图 1 实验环境拓扑结构图

3.2 实验指标

在该实验环境中，关注并记录在各个不同节点上数据的转存率这一关键指标。转存率作为衡量数据安全交换效率与效果的重要参数，其高低直接反映了数据在传输过程中的完整性和稳定性。

$$R_i = \frac{S_i}{T_i} \times 100\% \tag{7}$$

式中：R_i 表示节点 i 的转存率；S_i 表示成功转存的数据量；T_i 表示转存的总数据量。转存率越高，表示数据安全交换的效果越为理想，数据丢失的风险越小，传输的准确性和可靠性也就越高。

除此之外，为了更加深入地分析 3 种数据安全交换方法在实际应用中的安全性表现，决定进一步记录并比较在不同节点数量下数据的丢包情况。丢包率是衡量数据交换过程中数据丢失程度的重要指标，它直接关系到数据交换的可靠性和完整性。

$$D_i = \frac{L_i}{P_i} \times 100\% \tag{8}$$

式中：D_i 表示节点 i 的丢包率；L_i 表示丢失的数据包数量；P_i 表示传输的总数据包数量。

3.3 实验结果

（1）数据特征提取

利用上述第 1 小节步骤，进行实验室局域网数据特征提取，结果如图 2 所示。本文方法能够有效区分不同特征，这意味着数据特征提取方法成功地识别出了数据中的各种关键属性。对后续的数据安全交换传输具有重大意义。

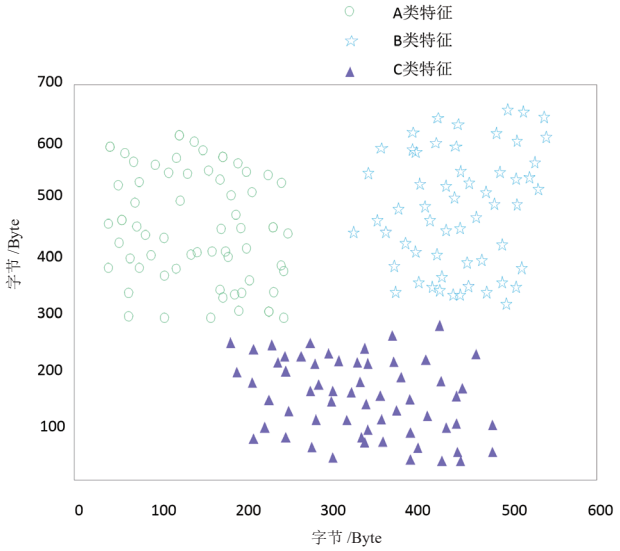

图 2 特征提取效果

（2）转存率对比

通过转存率实验设计，能够客观地比较基于禁忌搜索算法的交换方法与对照 A 组和对照 B 组在数据安全交换方面的实际表现，从而为选择最适合实验室局域网环境的数据交换策略提供科学依据。将 3 种方法完成交换任务后的转存率绘制成图 3 所示。

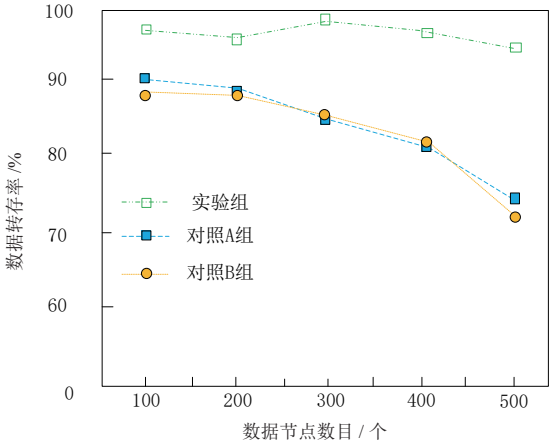

图 3 三种方法交换后转存率对比图

观察图 3 所展示的 3 条曲线，可以清晰地得出以下结论：在实验组所采用的交换方法作用下，数据的转存率始终保持在 90% 以上的高水平。相比之下，对照 A 组和对照 B 组的数据转存率则未能达到这一标准。更为显著的是，随着数据节点数量的不断增多，对照 A 组和对照 B 组的数据转存率呈现出一种明显的下降趋势，而实验组的数据转存率则相对稳定。这一对比结果有力地证明了实验组交换方法在实际应用中的优越性和有效性。

（3）数据丢包率对比

在实验过程中，将逐步增加网络中的节点数量，以模拟不同规模和复杂度的网络环境。对于每一种数据安全交换方法，将在每个节点数量级别上记录其丢包率，结果如图 4 所示。

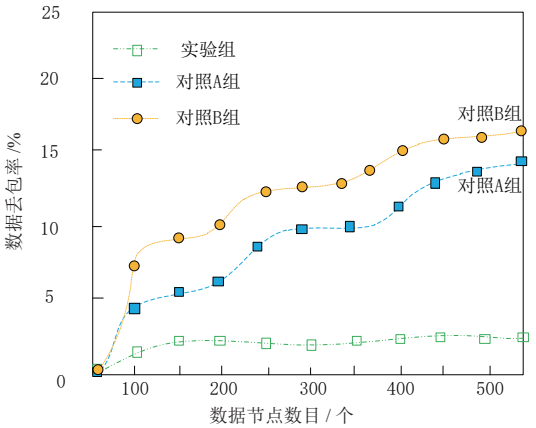

图 4 三种方法交换过程中数据丢包率对比图

对比图 4 中 3 条曲线，可以观察到随着数据节点数量的增多，3 种数据安全交换方法的数据丢包率均呈现出一种递增的趋势。然而，值得注意的是，实验组所采用的方法在数据丢包率方面表现出色，其数据丢包率始终维持在 5% 以下的较低水平。相比之下，对照 A 组和对照 B 组的数据丢包率则相对较高，其中对照 A 组的数据丢包率超过了 10%，而对照 B 组更是高达 15% 以上。

这一实验结果有力证明了实验组所采用的基于禁忌搜索算法的交换方法，在数据安全性方面具有显著的优势。即使在节点数量增加、网络负载加重的情况下，该方法依然能够保持较低的数据丢包率，从而确保了数据交换的可靠性和完整性。因此，可以得出结论，基于禁忌搜索算法的交换方法在实际应用中具有更高的可行性和有效性，特别是在对数据安全性要求较高的场景下，其优势更加明显。

4 结语

本文提出的基于禁忌搜索算法的实验室局域网数据安全交换方法，通过引入禁忌搜索算法的智能记忆机制，实现了对数据交换过程的优化。禁忌搜索算法能够灵活应对网络环境的动态变化，实现数据交换策略的快速调整，提高了数据交换的安全性和可靠性。然而，随着网络技术的不断发展，新的安全威胁和攻击手段层出不穷，本文提出的方法需要不断更新和完善，以应对各种新的安全挑战。

参考文献：

[1] 程子栋 . 基于区块链的政务信息系统数据安全共享交换研究 [J]. 软件 , 2024, 45 (6): 86-88.

[2] 韩路 . 基于改进阻塞判别算法的局域网数据安全交换方法 [J]. 现代电子技术 , 2022, 45 (17): 90-94.

[3] 高勇 , 李国强 , 李鹏飞 . 基于 XMLSchema 技术的跨网数据安全交换处理机制与研究 [J]. 信息通信 ,2020(12):181-183.

[4] 童伟 , 解欢 , 徐丹萍 . 基于区块链技术和安全沙箱机制实现数据安全交换的研究 [J]. 信息与电脑 (理论版), 2023, 35 (8): 185-188.

[5] 郭柯 , 师晓敏 . 基于区块链的交通数据共享交换模型及经济效益分析 [J]. 中国交通信息化 , 2024 (4): 90-93.

[6] 李国民 , 许继恒 , 袁媛 , 等 . 基于人工智能与物联网设备的市政废物管理数据汇聚与交换研究 [J]. 中国设备工程 , 2024 (4): 32-34.

[7] 鲁战利 , 孙贤雯 , 蔡亮 , 等 . "RPA+ 移动存储介质 " 解决政府数据安全跨网交换的方法与实践 [J]. 信息安全研究 , 2024, 10 (1): 81-87.

[8] 黄瀚 . 多模态数据融合处理对数据中心效率提升的影响研究 : 以浙江省民政数据共享交换中心为例 [J]. 办公自动化 , 2024, 29 (11): 93-96.

[9] 厉香蕴 , 陈春晖 . 基础地理信息数据安全交换关键技术及应用 [J]. 测绘与空间地理信息 , 2022, 45 (12): 88-90.

[10] 陈纯子 , 李楠 , 王允达 . 网闸在气象数据跨网安全交换中的应用测试 [J]. 信息系统工程 , 2022 (1): 73-76.

[11] 杨芝 , 宗欣 , 徐晓东 , 等 . 基于国密算法的跨网数据安全交换技术研究 [J]. 中国标准化 ,2025(1):41-45.

[12] 郭敬东 , 刘文亮 , 吴飞 , 等 . 数字孪生技术下物联网智能终端数据安全交换方法 [J]. 自动化技术与应用 , 2025, 44(2): 71-74.

[13] 郁晓庆 , 高洁 , 姚晓蓉 . 基于信创产品的数据安全交换系统研究 [J]. 中国新通信 ,2025,27(1):33-35.

[14] 刘娟娟 . 大数据背景下高校教育数据开放共享安全体系研究 [J]. 计算机应用文摘 , 2025,41(5):188-190.

【作者简介】

赵云（1981—），男，江苏句容人，硕士，实验师，研究方向：计算机科学与技术。

（收稿日期：2024-11-15）