软件学报 ISSN 1000-9825, CODEN RUXUEW
[doi: 10.13328/j.cnki.jos.007571] [CSTR: 32375.14.jos.007571]
©中国科学院软件研究所版权所有.
E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

基于博弈论的可信动态访问控制方案*

周由胜[1,2], 鞠 祯[1], 左祥建[1], 刘媛妮[1]

[1](重庆邮电大学 网络空间安全与信息法学院, 重庆 400065)

[2](重庆邮电大学 计算机科学与技术学院, 重庆 400065)

通信作者: 左祥建, E-mail: zuoxj@cqupt.edu.cn

摘 要: 访问控制技术是一种管理用户对资源访问权限的安全机制, 能有效防止未授权访问和资源泄露. 在数字化时代, 如何通过有效的访问控制技术平衡信息流通与隐私保护之间的关系, 保障数据要素安全有序流动, 已成为当前亟待解决的问题. 然而, 现有访问控制技术在领域数据共享场景研究中仍存在与信任评估融合不足、动态调整能力欠缺以及难以精准授权等问题. 针对上述问题, 提出一个基于博弈论的可信动态访问控制模型方案, 该方案融合“可信评估-动态调整-访问决策”三层协同机制. 首先, 基于属性权重算法, 设计多因素可信预测模型, 计算访问主体的信任概率; 其次, 从长期稳定角度出发, 构建访问主体与客体之间的演化博弈动态调整模型, 周期性地动态调整奖惩激励机制与访问授权阈值, 实现访问控制的适应性优化; 最后, 基于贝叶斯博弈论建立不完全信息实时决策模型, 依据混合策略纳什均衡做出访问控制决策, 并通过均衡状态反馈更新信任度. 仿真实验和敏感性分析的结果表明, 该方案能够有效提高访问控制的准确性, 实现访问控制策略动态调整和精准授权.

关键词: 访问控制; 演化博弈; 贝叶斯博弈; 可信预测; 奖惩激励机制

中图法分类号: TP393

中文引用格式: 周由胜, 鞠祯, 左祥建, 刘媛妮. 基于博弈论的可信动态访问控制方案. 软件学报. http://www.jos.org.cn/1000-9825/7571.htm

英文引用格式: Zhou YS, Ju Z, Zuo XJ, Liu YN. Trustworthy Dynamic Access Control Scheme Based on Game Theory. Ruan Jian Xue Bao/Journal of Software (in Chinese). http://www.jos.org.cn/1000-9825/7571.htm

Trustworthy Dynamic Access Control Scheme Based on Game Theory

ZHOU You-Sheng[1,2], JU Zhen[1], ZUO Xiang-Jian[1], LIU Yuan-Ni[1]

[1](School of Cyber Security and Information Law, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)

[2](School of Computer Science and Technology, Chongqing University of Posts and Telecommunications, Chongqing 400065, China)

Abstract: Access control technology is a security mechanism for managing users’ access to resources, which can effectively prevent unauthorized access and resource leakage. In the digital age, how to balance the relationship between information circulation and privacy protection via effective access control technology and ensure the safe and orderly flow of data elements has become a problem to be urgently addressed at present. However, the existing access control technology still has problems such as insufficient integration with trust evaluation, lack of dynamic adjustment capabilities, and difficulty in precise authorization in the research on domain data sharing scenarios. To this end, a trustworthy dynamic access control model scheme based on game theory is proposed, which integrates a three-layer collaborative mechanism of “trustworthy evaluation, dynamic adjustment, and access decision”. Firstly, based on the attribute weight algorithm, a multi-factor trustworthy prediction model is designed to calculate the trust probability of the access subject. Secondly, from the perspective of long-term stability, an evolutionary game dynamic adjustment model between the access subject and the object is built to periodically and dynamically adjust the reward and punishment incentive mechanism and access authorization threshold, thereby achieving the adaptive optimization of access control. Finally, based on Bayesian game theory, an incomplete information real-time

* 基金项目: 国家重点研发计划 (2023YFF0905300); 国家自然科学基金 (62272076); 重庆市自然科学基金 (CSTB2022NSCQ-MSX0038); 重庆市教委科学技术研究项目 (KJQN202200625)
收稿时间: 2025-05-08; 修改时间: 2025-09-23; 采用时间: 2025-11-03; jos 在线出版时间: 2026-04-29

decision-making model is built, and access control decisions are made based on the mixed strategy Nash equilibrium, with the trust degree updated by the equilibrium state feedback. The results of simulation experiments and sensitivity analysis verify that the proposed scheme can effectively improve the access control accuracy and achieve dynamic adjustment of access control strategies and accurate authorization.
Key words: access control; evolutionary game; Bayesian game; reliable prediction; reward and punishment incentive mechanism

数据作为新时代“五大生产要素”之一, 即是驱动经济增长的新引擎, 也是推动社会进步、提升国家竞争力的关键资源. 我国不断加强数据要素的基础理论研究, 加速构建数据基础制度体系, 充分发挥海量数据和丰富应用场景优势, 促进数字技术与实体经济深度融合. 2022 年, 国务院印发《关于构建数据基础制度更好发挥数据要素作用的意见》[1], 为深化数据要素市场化配置改革, 发挥数据要素价值, 推动数字经济高质量发展提供了政策引导和方向指引. 2024 年, 国家数据局正式发布《可信数据空间发展行动计划 (2024–2028 年)》[2], 明确将促进数据要素合规高效流通使用作为核心目标, 提出构建可信数据空间的战略方向.

在可信数据空间战略框架下, 用户身份与角色边界的模糊性以及多源异构数据的泛在化接入等核心挑战, 显著加剧了数据流通共享系统的复杂性与动态性. 由于数据控制权的分布式特性与开放网络环境的安全脆弱性, 共享数据资产面临双重风险: 一方面, 恶意攻击者可通过身份伪装或权限提升手段进行非授权访问[3]; 另一方面, 数据在跨域传输过程中易遭受中间人攻击引发的篡改威胁, 这将直接破坏数据机密性 (confidentiality) 与完整性 (integrity) 的核心安全属性, 进而导致商业机密泄露、隐私权益侵害等系统性风险[4]. 访问控制技术[5]通过对用户或系统的访问权限进行定义或管理, 确保资源仅能被合法授权实体访问. 该技术在保护数据隐私的同时, 允许数据在授权范围内自由流通和共享. 从而有效平衡信息流通与隐私保护之间的关系. 因此, 有效的访问控制技术能够平衡信息流通与隐私保护之间的关系, 成为保障数据要素安全有序流动的核心技术支撑.

目前, 学术界和工业界已经提出大量解决方案和行业标准来实现共享数据访问控制[6–10], 包括传统访问控制、基于属性的访问控制、基于博弈论的访问控制技术等. 传统访问控制模型[6]通过访问控制列表来定义和管理用户对资源的访问权限. 然而, 传统的静态访问控制技术依赖预先设定的规则和策略, 难以适应快速变化的网络环境, 无法及时调整和优化访问策略, 导致访问权限可能不准确、过时或滥用等问题[7]. 基于属性的访问控制 (attribute-based access control, ABAC)[8]是一种动态、细粒度的访问控制模型, 通过对用户的属性进行动态评估来决定用户对资源的访问权限. 与传统访问控制技术相比, ABAC 具有更精准且灵活的访问控制机制, 但 ABAC 模型通过多种属性评估访问权限, 在属性挖掘和撤销方面仍存在困难[9]. 同时, ABAC 模型难以自主检测和识别用户潜在的恶意访问意图, 也无法有效应对未授权访问和数据泄露等问题. 为此, 有研究者提出将博弈论与访问控制技术相结合[10], 将访问控制视为访问主客体间的一种既有冲突又有合作的互动, 并通过博弈论解决双方的冲突与合作问题, 实现隐私保护与数据共享的动态平衡. 然而, 现有访问控制博弈技术的研究依赖静态参数设置以及固定的授权阈值, 难以根据实时数据动态调节奖惩激励机制和授权阈值, 导致系统无法灵活适应环境变化与用户行为的动态特性, 存在模型动态调整能力不足的问题. 此外, 将信任评估或风险评估与访问控制博弈模型结合[11], 旨在突破单纯依赖身份认证技术的局限, 提高访问控制的精准性. 然而, 现有研究将信任评估简化为静态的过滤条件, 忽略了信任评估结果的动态性和概率性特征, 难以反映访问主体在不同情境下的真实可信度变化, 导致信任评估与访问控制决策之间缺乏深度融合, 无法充分发挥信任评估在访问控制中的潜在效能. 这些问题导致现有访问控制博弈机制灵活性欠缺, 在实际应用中无法有效结合信任评估实现策略动态调整和精准授权, 进而限制了访问控制博弈机制的动态适应性和有效性. 因此, 如何设计基于博弈论的可信动态访问控制方案, 实现访问控制策略动态调整和精准授权, 是当前亟待解决的问题.

因此, 为解决现有访问控制博弈模型在信任评估融合、动态调整能力以及精准授权方面的问题, 本文提出了一种基于博弈论的可信动态访问控制方案. 该方案通过融合“可信评估-动态调整-访问决策”的 3 层协同机制, 实现多层次细粒度的动态访问控制. 本文的主要贡献如下.

首先, 综合考虑访问主体信任评估的多元因素, 提出一种信任度预测模型, 基于最大离散度原则结合信息熵约束的属性权重算法, 计算访问主体的信任概率, 将信任概率值形式化为不完全信息博弈中的类型, 实现信任评估与访问控制博弈模型的深度融合.

其次, 从长期稳定角度出发, 在有限理性假设下构建访问主体和访问客体之间的演化博弈动态调整模型 (game dynamic regulation model, GDRM), 以固定周期更新收益矩阵参数, 通过对奖惩值敏感度分析动态调节系统奖惩激励机制, 并基于演化博弈策略稳定性分析更新授权阈值, 解决了现有模型因静态参数设置而导致的动态性不足问题, 实现访问控制策略动态调整.

最后, 从短期决策角度, 在类型不确定的情况下, 构建访问主体之间的不完全信息博弈决策模型, 将可信预测概率与访问权限对应收益结合, 通过比较纳什均衡与授权阈值做出访问控制决策, 并利用纳什均衡点更新信任度. 此外, 通过数值模拟仿真实验, 验证了本文所提方案在访问控制问题上的准确性和动态适应性.

本文第 1 节综述访问控制技术的相关研究进展. 第 2 节介绍访问控制技术和博弈论的基础知识. 第 3 节阐述动态访问控制博弈模型. 第 4 节构建基于博弈论的可信动态访问控制模型, 详细描述模型架构和模型的执行流程. 第 5 节实现基于博弈论的可信动态访问控制模型, 包括信任预测模型 (trust predict model, TPM)、演化博弈动态调整模型 (GDRM) 和博弈决策模型 (game decision model, GDM). 第 6 节通过仿真实验对演化博弈模型进行敏感性分析. 第 7 节通过实验验证本文方案的稳定性和有效性. 第 8 节对本文进行总结并展望未来工作方向.

1 相关工作

访问控制 (access control, AC) 机制是信息安全体系中的关键组成部分, 是安全领域重点研究方向之一, 其核心目标在于确保资源仅被合法用户以授权方式访问. 传统的访问控制模型在应对日益复杂多变的网络环境时, 逐渐显露出其局限性, 访问控制研究也面临新的挑战与机遇. 为应对这一挑战, He 等人[12]提出通过智能合约实现基于属性的细粒度访问控制的方法. 针对物联网设备在计算能力和系统扩展性方面的局限, Hao 等人[13]提出基于轻量级联盟链的架构, 利用代币积累机制促进访问策略存储, 提供数据访问控制认证服务并评估节点信任度, 实现 IoT (Internet of Things) 设备的智能自主访问控制. Gai 等人[14]提出了基于区块链的访问控制方案, 利用联盟链构建可信环境, 结合多重签名协议与智能合约部署基于角色的访问控制 (role-based access control, RBAC) 模型, 促进不同组织之间的轻量级数据共享. 然而, 现有研究难以有效处理大规模分布式系统中的动态访问需求, 在访问控制的动态适应性和多方协作方面仍存在不足, 面对恶意行为和资源竞争时仍缺乏灵活的策略调整机制. 基于博弈的访问控制技术作为一种创新方法, 通过引入博弈论概念, 使访问控制机制能够有效地适应动态变化的网络环境. 该技术将访问主体与访问客体视为博弈者参与者, 利用纳什均衡等理论来刻画并分析双方的动态博弈关系. 在结合博弈论的访问控制技术研究中, 研究者主要关注访问控制博弈模型的构建、奖惩激励机制以及与信任结合的博弈模型等方面.

在访问控制博弈模型的构建方面, 国内外研究者已有诸多探索. 张伊璇等人[10]提出基于博弈论的隐私保护模型, 通过历史访问数据量化评估访问双方不同策略组合的预期收益, 成功抑制了非授权访问者试图获取敏感信息的行为倾向. 在此基础上, 为满足动态安全需求并提升系统访问效率, 文献 [15] 融合高效授权和动态授权优势, 设计访问控制事后评估机制, 进一步提出了基于纳什均衡的主动式访问控制机制. 然而, 上述模型均基于博弈双方完全理性假设, 忽视了实际场景中因信息不对称或短期利益驱动产生的非理性行为. 针对此问题, 丁红发等人[7]基于有限理性假设并通过 Shannon 自信息理论量化隐私风险, 首次提出多参与者访问控制演化博弈模型. 文献 [16] 在此研究基础上进一步提出了多阶段二人博弈访问控制博弈模型. 尽管这些改进突破了完全理性约束, 但其核心缺陷仍集中于模型的动态适应性不足, 在网络环境变化时, 模型可能无法及时调整和优化策略, 导致其有效性降低. 此外, Gao 等人[17]针对医疗数据共享场景构建了三方博弈演化模型, 分析各方选择策略的演化趋势. Deng 等人[18]在文献 [15] 框架基础上提出了基于区块链的动态信任访问控制博弈机制, 利用区块链智能合约和交易机制, 结合信任评估和博弈评估, 实现动态细粒度的访问控制, 通过双滑动存储窗口和预授权机制提高效率. 然而, 在高并发场景下, 区块链共识验证机制可能增加交易延迟, 限制了方案实际应用效果.

为激励访问者诚信访问行为, 研究者围绕博弈模型的奖惩激励机制展开系列研究. 赵斌等人[19]提出了基于信任的动态访问控制博弈模型, 通过设计奖惩激励约束机制促使参与者基于自身利益理性选择博弈策略. Motepalli

等人[20]进一步构建适用于 PoS 区块链的演化博弈奖励框架, 分析奖励机制演变对参与者行为发展的影响. 然而, 上述模型过度依赖经济理性假设, 即默认参与者始终以利益最大化为目标, 忽视了实际场景中非理性行为的复杂性, 仍存在动态适配与复杂性应对不足的缺陷. 在信任模型优化方向, 张艺等人[21]在博弈收益函数中引入信任等级和动态调节因子, 通过混合策略纳什均衡实现云环境下动态博弈访问决策. Sun 等人[22]结合博弈论和云计算场景, 提出基于贝叶斯信任预测的动态博弈模型, 从短期利益和长期利益两个维度构建均衡分析框架. 尽管上述方案增强了策略连续性, 其信任评估仍然滞后于实时需求, 在信任评估的实时性和精准性上仍需进一步优化. Huang 等人[23]提出了分布式动态可信访问控制模型, 通过动态可信授权, 在动态属性的驱动下, 实现细粒度的访问控制. Jiang 等人[24], 提出融合直觉模糊理论与信任评价方法的访问控制模型, 通过奖惩机制实现对医生访问行为的自适应和动态访问控制. 然而上述方案在处理模糊和不确定信息时仍缺乏足够的鲁棒性.

综上所述, 现有研究在访问控制博弈模型的构建和奖惩激励机制设计方面取得了一定进展, 但访问控制博弈模型在信任评估融合、动态调整能力以及精准授权方面仍存在不足. 尤其是缺乏自适应的动态调整能力, 难以根据环境变化实时优化激励参数与授权阈值, 这导致访问控制策略僵化, 无法在实际应用中实现动态调整和精准授权.

2 基础知识

本文所提方法基于访问控制技术和博弈论, 下面就相关概念和基本知识予以介绍.

2.1 访问控制技术

访问控制技术[5]是主体按照既定访问策略对客体资源进行访问的技术. 其核心组成要素包括访问主体、被访问客体与权限: (1) 访问主体 (subject): 发出访问请求的用户; (2) 访问客体 (object): 被访问的对象; (3) 权限 (permission): 访问主体对客体资源的使用权利.

传统的访问控制模型[6]: (1) 自主访问控制 (discretionary access control, DAC): 访问资源所有者根据双方身份信息, 自主判定并授予访问权限; (2) 强制访问控制 (mandatory access control, MAC): 由系统预先制定安全策略, 据此决定访问权限并强制实施相应的控制措施; (3) 基于角色的访问控制 (RBAC): 通过角色来关联用户与权限, 明确界定不同角色及其关系, 设置相应的权限限制来规范用户的行为[25]. 然而, 传统访问控制模型通常基于预定义的规则和角色, 随着数据加密、人工智能、区块链和网络安全技术的快速发展, 传统模型难以适应动态变化的网络环境和复杂的访问场景, 在应对现代网络威胁和多样化访问需求时, 其局限性逐渐显现.

为满足现代网络对动态细粒度访问控制的需求, 解决传统模型的局限性, 有研究者提出基于属性的访问控制 (ABAC) 模型. ABAC 是基于用户、资源、操作以及运行上下文属性的动态细粒度访问控制模型, 以访问主客体属性作为核心决策依据, 结合主客体属性集合和预定义的策略规则, 从而对访问权限进行动态判定, 实现策略管理与权限判定的有效分离. ABAC 采用四元组 (S, O, P, E) 来描述主体、客体、权限及环境属性集合, 支持与加密机制等数据隐私保护技术结合, 实现细粒度访问控制, 在确保用户数据的安全性的同时, 有效防止对未授权数据的分析和泄露. 基于属性的加密技术 (attribute based encryption, ABE) 将解密能力与预定义属性集绑定, 确保只有在用户属性满足特定条件时才能解密和访问数据[26]. 该技术主要包含密钥策略属性基加密 (KP-ABE) 和密文策略属性基加密 (CP-ABE) 两种类型. 在 KP-ABE 中, 通过用户属性控制访问权限; 在 CP-ABE 中, 通过数据属性控制访问权限.

可扩展访问控制标记语言 (extensible access control markup language, XACML)[27]定义一种用于指定访问控制策略、决策以及访问请求和响应格式的方法, 是一种标准化策略管理框架, 采用 XML 来描述策略语言和访问控制决策的请求与响应[28], 主要用于实现基于属性的访问控制模型, 支持在分布式环境中实现对资源的细粒度访问控制. XACML 架构主要由以下 4 个核心组件协同实现: (1) 策略管理点 (policy administration point, PAP): 负责创建、编辑和存储访问控制策略; (2) 策略决策点 (policy decision point, PDP): 做出访问控制决策; (3) 策略执行点 (policy enforcement point, PEP): 执行访问控制决策; (4) 策略信息点 (policy information point, PIP): 提供策略评估额外信息. 传统的 XACML 架构如图 1 所示.

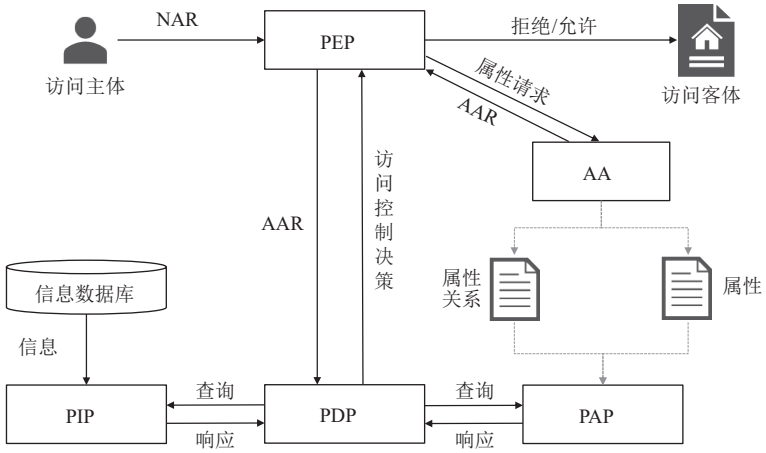


图 1　传统 XACML 架构图

基于属性的访问控制的传统 XACML 架构流程主要涵盖准备和执行两个阶段[29].

● 准备阶段: 属性权威机构 (attribute authority, AA) 负责收集和管理访问主客体的相关属性信息, 并将这些属性及其关联关系发送至策略管理点 PAP. PAP 根据接收到的属性及其关系, 创建、编辑和存储访问控制策略.

● 执行阶段: 当主体发起资源访问时, 主体向客体发送原生访问请求 (native access request, NAR). 策略执行点 PEP 拦截访问请求后先将其转换为 XACML 格式, 然后结合 AA 提供的属性信息构建属性访问请求 (attribute based access request, AAR), 随后将 AAR 转发至策略决策点 PDP. PDP 通过策略信息点 PIP 获取策略评估所需的额外信息对 AAR 进行多维度评估, 最终生成二元授权决策 (允许/拒绝). 决策结果由 PEP 执行相应的访问控制操作.

2.2　博弈论

博弈论是研究策略互动的数学框架, 探讨在相互影响的情况下, 具有决策能力的个体如何做出最优选择的问题[30]. 博弈论主要研究激励结构间的相互作用, 为分析竞争与合作并存的现象提供了数学理论基础和系统的方法体系. 博弈论体系包含 3 大分支[31]: (1) 合作博弈论 (cooperative game theory), 研究联盟的构建与利益分配; (2) 非合作博弈论 (non-cooperative game theory), 分析个体的最优策略选择; (3) 演化博弈论 (evolutionary game theory, EGT), 研究群体策略的动态演化过程.

博弈模型由参与者、策略以及收益函数组成: (1) 参与者: 博弈中的决策主体, 通过选择不同的策略来追求自身利益最大化; (2) 博弈策略: 参与者可选择的行动方案, 不同策略选择会导致不同的博弈结果; (3) 收益函数: 量化在不同策略组合下各参与者的利益得失. 策略型博弈 (strategic game) 可以用以下三元组的数学形式表示: $G = < N, \{S_i\}_{i\in N}, \{u_i\}_{i\in N} >$. 其中,

● $N = \{1, 2, \ldots, n\}$ 表示参与人 (玩家) 的集合;

● S_i 是参与人 i 的策略集合 (所有可能的策略选择);

● $u_i = S_1 \times S_2 \times \ldots \times S_n \to \mathbb{R}$ 是参与人 i 的收益函数, 表示在策略组合 s 下参与人 i 的收益.

策略组合 (strategy profile) 是所有参与者联合选择的策略, 记为: $s = (s_1, s_2, \ldots, s_n)$, 其中 $s_i \in S_i$.

定义 1[32]. 在策略型博弈中, 一个策略组合 $s^* = (s_1^*, s_2^*, \ldots, s_n^*)$ 是纳什均衡的必要条件是: 当且仅当每个参与者策略 s_i^* 对其他参与者的策略 $s_{-i}^* = (s_1^*, \ldots, s_{i-1}^*, s_{i+1}^*, \ldots, s_n^*)$ 而言均是最优反应, 即 $\forall i \in N, \forall s_i \in S_i : u_i(s_i^*, s_{-i}^*) \geqslant u_i(s_i, s_{-i}^*)$. 其中, s_{-i}^* 表示除参与者 i 外其他所有参与者的均衡策略.

定义 2[32]. 参与者以概率分布选择策略, 设 σ_i 是参与人 i 的混合策略 (策略空间 Σ_i 中的元素), 则混合策略纳什均衡满足:

$$\forall i \in N,\ \forall \sigma_i' \in \Sigma_i : \mathbb{E}[u_i(\sigma_i^*, \sigma_{-i}^*)] \geqslant \mathbb{E}[u_i(\sigma_i', \sigma_{-i}^*)] \tag{1}$$

2.2.1 不完全信息博弈论

不完全信息博弈是博弈论中的一类博弈模型, 指参与者在决策时无法完全掌握其他参与者的关键信息, 导致参与者需在不确定条件下进行策略选择, 通常需要借助概率推断或贝叶斯更新来预测对手行为.

定义 3. 不完全信息博弈可以通过以下方式描述.

● 参与者集合: $N = \{1, 2, \ldots, n\}$.

● 策略集合: 每个参与者 i 有一个策略集合 S_i.

● 收益函数: 每个参与者 i 有一个收益函数 $u_i : S \times \Theta \to \mathbb{R}$, 其中 Θ 表示所有可能的类型集合.

● 类型空间: 每个参与者 i 有一个类型空间 Θ_i, 表示参与者 i 可能拥有的所有类型.

● 信念: 每个参与者 i 对其他参与者类型有一个先验信念 $p_i(\theta_{-i} \mid \theta_i)$, 表示在知晓自身类型 θ_i 的前提下, 对其他参与者类型 θ_{-i} 的概率分布的估计.

● 贝叶斯纳什均衡 (Bayesian Nash equilibrium, BNE): 每个参与者 i 的策略 s_i^* 在给定其他参与者的策略和自己的类型信息下, 通过选择策略组合 $(s_1^*, s_2^*, \ldots, s_n^*)$ 最大化自身期望收益. 在不完全信息博弈情境下, 通过贝叶斯纳什均衡进行决策.

2.2.2 演化博弈论

演化博弈是博弈论与生物进化理论的交叉领域, 研究群体中策略的动态演化过程. 演化博弈论放宽了经典博弈中对参与者完全理性的假设, 转而假设参与者具有有限理性. 其核心思想是: 适应性更高的策略通过自然选择或社会学习机制, 能够逐渐在群体中占据主导地位. 参与者在每次博弈中选择的策略不一定是最优策略, 但是通过在演化过程中模仿其他参与者的高收益策略, 在后续博弈中动态调整策略选择, 来提高自身收益. 演化博弈通过演化稳定策略 (ESS) 来分析参与者策略之间的动态平衡.

定义 4. 演化稳定策略 (evolutionarily stable strategy, ESS): 在演化博弈中, 演化稳定策略能被所有个体采用, 且有效抵御其他策略的入侵. 具体而言, 若策略 a_e 满足 $u(a_e, a_e) > u(a_i, a_e), \forall i \neq e$ 或满足 $u(a_e, a_e) = u(a_i, a_e)$ 时, $u(a_e, a_i) > u(a_i, a_i), \forall i \neq e$, 则称策略 a_e 为演化稳定策略, 其中 $u(a_e, a_i)$ 表示当策略 a_e 遇到 a_i 时, a_e 的收益.

3 动态访问控制博弈模型

动态访问控制博弈模型是基于博弈论的可信动态访问控制模型的核心组成部分, 从长期稳定和短期决策两个角度出发, 通过模拟访问主客体的博弈行为, 实现对访问控制的动态调整和博弈决策. 本节将阐述博弈模型的定义、假设和收益函数.

3.1 博弈模型定义

基于博弈论的动态访问控制模型由参与者空间、策略空间、收益函数和类型空间 4 元组 $< P, A, U, \Gamma >$ 定义. 其中, P 是博弈的参与者空间: $P = \{\text{Subject, Object}\}$, 分别是访问主体和访问客体. A 是博弈策略空间, 分别对应访问主体和客体的可选策略, 访问主体的策略空间 $A_S = \{\text{Normal, Malicious}\}$, 包含正常访问 (Normal) 和恶意访问 (Malicious), 访问客体的策略空间 $A_O = \{\text{Allow, Deny}\}$, 包含允许访问 (Allow) 和拒绝访问 (Deny). Γ 是博弈参与者的类型空间: $\Gamma = \{\Gamma_S, \Gamma_O\}$, 类型空间 Γ 的概率分布是公共知识, $\Gamma_S = \{\text{Credible, Incredible}\}$ 是访问主体的类型空间, 包含可信主体 (Credible) 和不可信主体 (Incredible), Γ_O 是访问客体的类型空间. U 是博弈模型的收益函数, 由访问主体和客体的收益 $U = \{u_S, u_O\}$ 组成, $u_S = \{E_S^{C,N,A}, E_S^{C,N,D}, E_S^{C,M,A}, E_S^{C,M,D}, E_S^{I,N,A}, E_S^{I,N,D}, E_S^{I,M,A}, E_S^{I,M,D}\}$ 是访问主体的收益函数, $u_O = \{E_O^{C,N,A}, E_O^{C,N,D}, E_O^{C,M,A}, E_O^{C,M,D}, E_O^{I,N,A}, E_O^{I,N,D} E_O^{I,M,A}, E_O^{I,M,D}\}$ 是访问客体的收益函数, 收益值取决于博弈参与者的类型和策略选择.

在构建的访问控制博弈模型中, 每次博弈的参与者为访问主体和访问客体, 双方均有有限的可选策略. 在每次访问前, 双方策略选择未知, 但已知各方历史访问策略. 此外, 访问客体不知道当前访问主体的具体类型, 但了解其类型空间 Γ_S 概率分布, 因此构成不完美信息静态博弈模型. 从长期稳定角度, 假设参与者有限理性, 将访问主体的

类型概率分布作为已知条件, 构建访问主体与访问客体的演化博弈模型, 通过固定周期更新收益函数矩阵, 结合参数敏感性和系统稳定性分析, 动态调整奖惩激励机制和授权决策阈值; 从短期决策角度, 假设参与者完全理性且了解自身信息, 但不知道对方策略, 依据访问请求权限对应收益值, 构建不完全信息静态博弈模型, 通过混合策略贝叶斯纳什均衡求解, 实现细粒度动态授权决策.

3.2 博弈假设

假设 1: 博弈参与者包括访问主体和访问客体, 主体的可选策略为{正常访问, 恶意访问}, 客体的可选策略为{允许访问, 拒绝访问}. 博弈双方均追求自身利益最大化, 不知道对方当前策略, 但了解彼此的历史策略选择. 在构建博弈收益函数时, 本模型基于相对收益比较原则, 合理简化对博弈结果不产生实质性影响的参数.

假设 2: 访问主体“正常访问”系统可获得的收益 I_1 和系统给予的奖励 R_1; 若“正常访问”请求被拒绝会产生损失 L_1, 访问客体会根据系统惩罚 B_2 和补偿系数 k $(0 \leqslant k \leqslant 1)$ 对访问主体进行补偿; 如果访问主体成功“恶意访问”系统将获得额外收益 I_2, 但“恶意访问”行为会受到系统的惩罚 B_1; 若“恶意访问”行为被客体拒绝, 访问主体会受到惩罚并且需要对客体进行补偿.

假设 3: 访问客体允许“正常访问”可获得收益 I_3 和系统奖励 R_2; 若拒绝“正常访问”请求会受到惩罚 B_2 并根据系统惩罚和补偿系数对访问主体进行补偿; 当客体允许“恶意访问”时会产生损失 L_2 并受到惩罚 B_2; 如果客体拒绝“恶意访问”请求时可获得奖励 R_2 以及访问主体支付的补偿.

假设 4: 假设 2 和假设 3 基于访问主体为诚信用户, 当访问主体是非诚信用户, 访问时需支付额外处理成本 C, 客体也需支付处理成本 C; 同时, 根据系统对访问主体的惩罚 B_1 和信任惩罚因子 γ 对非诚信用户进行惩罚, 其中 $0 \leqslant \gamma \leqslant 1$, γ 会随着主体策略选择概率而动态变化.

假设 5: 主体可信度 T 决定访问主体的诚信类型, 访问主体为诚信用户的概率为 p, 为非诚信用户的概率为 $1-p$; 诚信的访问主体选择“正常访问”策略的概率为 x_1, 选择“恶意访问”策略的概率为 $1-x_1$; 非诚信主体选择“正常访问”策略的概率为 x_2, 选择“恶意访问”策略的概率为 $1-x_2$; 客体“允许访问”策略的概率为 y, 选择“拒绝访问”的概率为 $1-y$. 其中 $p, x_1, x_2, y \in [0,1]$, 均为时间 t 的函数.

假设 6: 通过访问控制收益表记录周期内主客体的收益参数值, 演化博弈动态调整模型根据上一周期收益值进行参数更新, 动态调节奖惩激励机制并更新授权阈值, 实现策略自适应优化. 博弈决策模型基于具体的访问权限对应收益值构建收益矩阵, 通过博弈分析并与授权阈值比较, 生成访问控制决策, 实现细粒度动态授权.

假设成本 C、收益 I、奖励 R、惩罚 B 以及损失 L 均大于 0. 基于博弈论的可信动态访问控制模型的博弈参数设置表 1 所示.

表 1 博弈模型参数表

符号	含义	符号	含义
C	非诚信用户额外的处理成本	B_1	系统设置对访问主体的惩罚值
I_1	访问主体正常访问系统获得的收益	B_2	系统设置对访问客体的惩罚值
I_2	访问主体恶意访问系统获得的额外收益	L_1	访问主体因正常访问被误判的损失
I_3	访问客体允许正常访问的收益	L_2	访问客体允许恶意访问的损失
R_1	系统设置对访问主体的奖励值	k	访问主体和访问客体之间的补偿因子
R_2	系统设置对访问客体的奖励值	γ	非诚信用户的惩罚因子

3.3 博弈收益矩阵

根据上述假设和博弈模型参数, 构建博弈收益矩阵, 用于描述访问主体和访问客体在不同策略组合下的收益情况. 动态访问控制博弈模型的收益矩阵如表 2 所示.

演化博弈动态调整模型通过收益值更新、对奖惩激励机制进行动态调节并更新授权阈值, 实现访问控制策略的自适应优化. 博弈决策模型基于访问权限相应收益值构建收益矩阵, 通过博弈分析并与周期阈值比较, 做出访问控制决策, 实现细粒度动态精准授权.

表 2 博弈模型收益矩阵

访问主体		访问客体	
		允许访问 (y)	拒绝访问 ($1-y$)
可信用户 (p)	正常访问 (x_1)	I_1+R_1 I_3+R_2	$-L_1+R_1+kB_2$ $-(1+k)B_2$
	恶意访问 ($1-x_1$)	$I_1+I_2-B_1$ $-L_2-B_2$	$-(1+k)B_1$ R_2+kB_1
不可信用户 ($1-p$)	正常访问 (x_2)	$-C+I_1+R_1-(1-x_2)\gamma B_1$ I_3+R_2-C	$-C-L_1+R_1+kB_2-(1-x_2)\gamma B_1$ $-(1+k)B_2-C$
	恶意访问 ($1-x_2$)	$-C+I_1+I_2-B_1-(1-x_2)\gamma B_1$ $-L_2-B_2-C$	$-C-(1+k)B_1-(1-x_2)\gamma B_1$ R_2+kB_1-C

4 基于博弈论的可信动态访问控制模型构建

针对传统访问控制模型在领域数据共享场景中策略僵化等问题, 构建基于博弈论的可信动态访问控制模型, 融合基于属性的访问控制技术、博弈论以及信任预测模型. 本节主要构建模型的架构和模型执行流程.

4.1 模型架构

本文提出的基于博弈论的可信动态访问控制模型, 在现有 XACML 架构基础上, 融合基于属性的访问控制技术、信任预测和博弈论, 在领域数据共享场景下实现对访问主体的细粒度动态授权. 本方案通过信任预测评估访问主体的信任度; 从长期角度出发, 通过演化博弈分析, 以固定周期动态调整奖惩激励机制和访问授权阈值; 结合可信预测值与访问行为对应收益, 构建访问主客体之间的不完全信息博弈模型, 通过比较纳什均衡与授权阈值做出访问控制决策, 实现细粒度动态授权; 通过博弈分析结果更新历史记录和主体信任度, 为后续访问提供参考. 本文在传统的 XACML 框架基础上加入信任预测模型 (TPM) 和博弈模型 (game model), 其中博弈模型分为博弈决策模型 (GDM) 和演化博弈动态调整模型 (GDRM). 演化博弈动态调整模型负责动态调节访问控制过程中的奖惩激励机制和授权阈值, 博弈决策模型通过博弈分析做出访问控制决策. 基于博弈论的可信动态访问控制模型架构如图 2 所示.

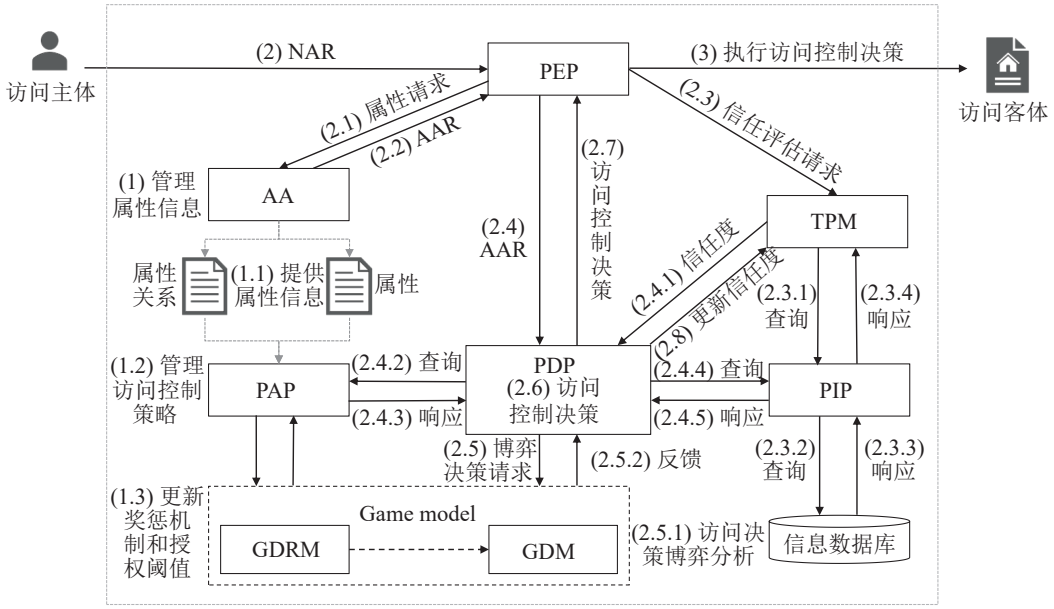


图 2 基于博弈论的可信动态访问控制模型架构

4.2 模型流程

本文提出的基于博弈论的动态访问控制模型通过访问属性资源预配置与实时决策实现动态访问控制, 模型架构主要分为准备阶段和执行阶段.

● 准备阶段

(1) 属性权威 (attribute authority, AA) 机构收集和管理访问控制模型中访问主体和客体的属性信息, 并向策略管理点 (PAP) 发送主客体属性信息及其属性关系.

(2) PAP 根据属性信息管理访问控制策略, 确保策略的合理性和准确性.

(3) 博弈动态调整模型 GDRM 以固定周期更新收益矩阵参数, 动态调整奖惩机制更新授权阈值, 并将更新信息存储在 PAP 中.

● 执行阶段

(1) 访问主体提出原生访问请求 NAR (native access request) 试图访问客体资源, 策略执行点 (PEP) 拦截访问请求并转换为 XACML 格式.

(2) PEP 向 AA 发起属性查询, 获取属性访问请求 AAR 后, 将 AAR 转发至策略决策点 (PDP) 进行授权评估.

(3) PEP 向 TPM 发送信任评估请求, TPM 通过策略信息点 PIP 查询历史信息等信任评估因素, 综合计算并生成实时动态信任度评估值, 并发送至 PDP.

(4) PDP 向 PAP 查询访问控制策略, PAP 将通过 GDRM 更新后的奖惩因子和授权阈值信息回传至 PDP.

(5) PDP 通过 PIP 获取非属性类的访问控制信息.

(6) PDP 将信息发送至 GDM, GDM 根据访问权限对应收益构建收益矩阵, 通过博弈分析计算纳什均衡, 并反馈结果至 PDP.

(7) PDP 比较 GDM 反馈结果和授权阈值, 做出访问控制决策 (允许/拒绝).

(8) PDP 将决策结果反馈给 PEP, PEP 根据结果执行相应访问控制决策.

(9) 系统更新访问主体信任度和访问历史数据.

5 基于博弈论的可信动态访问控制模型实现

本节实现基于博弈论的可信动态访问控制方案, 通过构建可信预测模型、演化博弈动态调整模型和不完全信息博弈决策模型, 形成“可信评估-动态调整-访问决策”三层协同机制, 从而实现领域数据共享场景下细粒度动态自适应访问控制.

5.1 可信预测模型

针对访问控制模型中信任值计算依赖单一维度数据、缺乏动态适应性等问题, 本文提出了一个综合性的信任预测模型来评估访问主体的可信度. 该模型基于最大离散度原则, 采用多因素综合评价方法, 通过信息熵约束的属性权重算法对各因素赋权, 从而计算访问主体的信任概率. 进一步将信任概率作为先验概率, 并结合贝叶斯理论, 将信任概率与访问主体访问行为结合, 从而更新访问主体信任的后验概率.

5.1.1 权重分配

在可信预测模型中, 权重分配直接影响模型的可解释性和预测准确性. 本模型基于最大离散度原则, 并结合信息熵约束的属性权重算法, 综合评估各维度的重要性, 进而为各评估维度权重分配, 计算访问主体的信任概率.

在有序加权平均 (ordered weighted averaging, OWA) 算子中, 权重向量 $W=(\omega_1,\ldots,\omega_n)$ 定义各信任评估维度的权重, 从 ω_1 到 ω_n 权重比例逐渐降低, 表明评估维度的重要性依次递减. Yager[33]提出了两个与 OWA 算子的权重向量 W 的两个相关特征度量. 第 1 个特征度量是对聚合度进行度量的“或度量方法”, 定义为:

$$orness(W)=\frac{1}{n-1}\sum_{i=1}^{n}(n-i)\omega_i \tag{2}$$

其中, $\omega_i\in[0,1]$, 且满足 $\sum_{i=1}^{n}\omega_i=1$. 当权重集 $disp(W)=-\sum_{i=1}^{n}\omega_i\ln\omega_i$ 中在第 1 个元素时, $W=(1,0,\ldots,0)$, 此时

$orness=1$; 当权重集中在最后一个元素时, $W=(0,0,\ldots,1)$, 此时 $orness=0$; 当权重均匀分布时, $W=\left(\frac{1}{n},\frac{1}{n},\ldots,\frac{1}{n}\right)$, 此时 $orness=0.5$. 第 2 个特征度量是利用信息熵模式量化聚合体离散程度, 定义为:

$$disp(W)=-\sum_{i=1}^{n}\omega_i\ln\omega_i \tag{3}$$

其中, $0\leqslant disp(W)\leqslant\ln n$. 当所有权重相等 $(\omega_1=\ldots=\omega_j=\ldots=\omega_n=\frac{1}{n})$ 时, 离散度达到最大, 此时 $disp(W)=\ln n$.

在信息熵约束下, 属性权重的计算转化为在条件 $orness(W)=\frac{1}{n-1}\sum_{i=1}^{n}(n-i)\omega_i=\alpha$ 和 $\sum_{i=1}^{n}\omega_i=1$ 下的离散度最大化 $disp(W)=-\sum_{i=1}^{n}\omega_i\ln\omega_i$ 问题, 通过拉格朗日乘数法求解. 构建拉格朗日函数如下:

$$\mathcal{L}(W,\lambda_1,\lambda_2)=-\sum_{i=1}^{n}\omega_i\ln\omega_i+\lambda_1\left(\frac{1}{n-1}\sum_{i=1}^{n}(n-i)\omega_i-\alpha\right)+\lambda_2\left(\sum_{i=1}^{n}\omega_i-1\right) \tag{4}$$

解得:

$$\ln\omega_j=\frac{n-j}{n-1}\ln\omega_1+\frac{j-1}{n-1}\ln\omega_n\Rightarrow\omega_j=\sqrt[n-1]{\omega_1^{\,n-j}\omega_n^{\,j-1}} \tag{5}$$

$$\omega_1[(n-1)\alpha+1-n\omega_1]^n=((n-1)\alpha)^{n-1}[((n-1)\alpha-n)\omega_1+1] \tag{6}$$

$$\omega_n=\frac{((n-1)\alpha-n)\omega_1+1}{(n-1)\alpha+1-n\omega_1} \tag{7}$$

可以通过公式 (5)–(7) 确定可信预测模型各评估因素的权重, 计算访问主体的信任概率.

5.1.2 信任度计算

TPM 通过多因素信息计算访问主体的信任概率, 综合考虑访问主体的历史访问信息、当前访问请求上下文信息以及他人对访问主体推荐等信息, 并通过信息熵和最大离散度确定各因素权重. TPM 中多因素信息分别由 T_i 表示, 其中 $i=1,2,\ldots,n$. 访问主体的信任度计算公式为 $T=\sum_{i=1}^{n}(\omega_i\cdot t_i)$, 其中 ω_i 为第 i 个因素的权重, t_i 为第 i 个因素的标准化值, $T\in[0,1]$. 所以, 访问主体是诚信主体的概率为 T, 是非诚信主体的概率为 $1-T$. 在本文中考虑影响信任预测计算的核心因素如下.

- 可信概率 T_1: 基于贝叶斯理论, 结合上次访问行为和信任先验概率, 计算得出的可信后验概率.
- 有效访问程度 T_2: 在访问主体的访问历史中, 客体允许“正常访问”的占比. 如果访问主体存在“恶意访问”行为, 或者访问请求被拒绝均不被视为有效访问, 即 T_2 = 允许“正常访问”次数/访问主体发送访问请求次数.
- 声誉度 T_3: 声誉 H 是基于访问行为的系统评价, 在信任预测模型中通过归一化处理将声誉 H 转换为声誉度 T_3, 即 $T_3=H\%$.
- IP 设备的使用频率 T_4: 特定时间内 IP 设备的访问次数占比, T_4 = 该 IP 设备访问次数/总访问次数.
- 他人的推荐信任 T_5: 其他用户或系统对访问主体的信任评价, 通过文献 [34] 的方法构造多级加权方向信任树计算他人的推荐信任值.
- 当前网络环境的安全状态 T_6: 基于网络实时监控数据综合计算网络安全状态, 并通过标准化处理.

5.1.3 信任度更新

在已知访问主体信任度 T 的条件下, 通过博弈混合策略纳什均衡分析, 可以得出不同类型的访问主体选择“正常访问”的概率. 然后, 利用贝叶斯定理, 计算在“正常访问”的条件下访问主体为可信主体的概率 T', 从而更新其信任度. 为清晰地表达计算过程, 假设可信主体事件为 A, “正常访问”事件为 B. 其中, 可信主体的概率 $P(A)=p$, 可信主体条件下“正常访问”的条件概率 $P(\text{正常访问}|\text{可信})=P(B|A)=x_1$, 不可信主体条件下“正常访问”的条件概率 $P(\text{正常访问}|\text{不可信})=P(B|\neg A)=x_2$, 由假设可知访问主体的信任度 $T=P(A)=p$.

“正常访问”的全概率计算如下.

$$P(B)=P(B|A)\times P(A)+P(B|\neg A)\times P(\neg A)=x_1p+x_2(1-p) \tag{8}$$

根据贝叶斯定理, 更新访问主体的后验可信概率 T':

$$P(\text{可信主体}|\text{正常访问}) = P(A|B) = \frac{P(B|A)\times P(A)}{P(B)} = \frac{x_1 p}{x_1 p + x_2(1-p)} \tag{9}$$

通过公式 (9) 计算的概率 P(可信主体|正常访问) 作为访问主体新的信任度 T', 实现信任度的动态更新.

5.2 演化博弈动态调整模型 (GDRM)

演化博弈动态调整模型 (GDRM) 旨在研究访问主客体的授权阈值和奖惩激励机制的动态调整. 该模型基于博弈论, 从长期稳定角度出发, 假设参与者具有有限理性, 将访问主体的类型概率分布作为已知条件与收益函数结合, 构建访问主客体间的访问控制演化博弈模型. 根据访问过程主客体参数历史收益, 模型以固定周期更新收益矩阵, 并通过复制动态方程和演化稳定策略分析, 动态调整授权阈值和奖惩激励机制, 从而实现访问控制策略的适应性优化.

5.2.1 演化博弈模型

在有限理性的假设下, 访问主体策略为{正常访问, 恶意访问}, 其策略选择概率为 $(x, 1-x)$; 访问客体策略为{允许访问, 拒绝访问}, 其策略选择概率为 $(y, 1-y)$. 在不同博弈阶段, 双方的策略选择概率有所不同, 策略概率会根据演化博弈的学习机制不断调整, 促使参与者策略的动态变化. 演化博弈模型的博弈树如图 3 所示, 表示各博弈阶段主体和客体的策略组合.

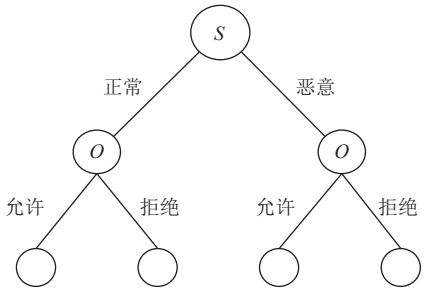


图 3 博弈动态调整模型博弈树

在动态访问控制博弈模型收益矩阵假设基础上, 将访问主体类型概率分布作为已知条件, GDRM 的收益矩阵如表 3 所示.

表 3 演化博弈动态调整模型收益矩阵

访问主体	访问客体	
	允许访问 (y)	拒绝访问 $(1-y)$
正常访问 (x)	$I_1 + R_1 - x_2(1-p)(C + (1-x_2)\gamma B_1)$ $I_3 + R_2 - x_2(1-p)C$	$-L_1 + R_1 + kB_2 - x_2(1-p)(C + (1-x_2)\gamma B_1)$ $-(1+k)B_2 - x_2(1-p)C$
恶意访问 $(1-x)$	$I_1 + I_2 - B_1 - x_2(1-p)(C + (1-x_2)\gamma B_1)$ $-L_2 - B_2 - x_2(1-p)C$	$-(1+k)B_1 - x_2(1-p)(C + (1-x_2)\gamma B_1)$ $R_2 + kB_1 - x_2(1-p)C$

1) 访问主体 S 的平均收益

访问主体 S 选择“正常访问”的收益为:

$$\begin{aligned} U_{S_1} &= y\times[I_1 + R_1 - x_2(1-p)(C + (1-x_2)\gamma B_1)] + (1-y)\times[-L_1 + R_1 + kB_2 - x_2(1-p)(C + (1-x_2)\gamma B_1)] \\ &= -L_1 + R_1 + kB_2 - x_2(1-p)(C + (1-x_2)\gamma B_1) + y\times(I_1 + L_1 - kB_2) \end{aligned} \tag{10}$$

访问主体 S 选择“恶意访问”的收益为:

$$\begin{aligned} U_{S_2} &= y\times[I_1 + I_2 - B_1 - x_2(1-p)(C + (1-x_2)\gamma B_1)] + (1-y)\times[-(1+k)B_1 - x_2(1-p)(C + (1-x_2)\gamma B_1)] \\ &= -(1+k)B_1 - x_2(1-p)(C + (1-x_2)\gamma B_1) + y\times(I_1 + I_2 + kB_1) \end{aligned} \tag{11}$$

则访问主体 S 采取混合策略的平均收益为:

$$\overline{U}_S = xU_{S_1} + (1-x)U_{S_2} \tag{12}$$

2) 访问客体 O 的平均收益

访问客体 O 选择“允许访问”的收益为:

$$U_{O_1} = x\times[I_3 + R_2 - x_2(1-p)C] + (1-x)\times[-L_2 - B_2 - x_2(1-p)C] = -L_2 - B_2 - x_2(1-p)C + x\times(I_3 + R_2 + L_2 + B_2).$$

访问客体 O 选择“拒绝访问”的收益为:

$$U_{O_2} = x\times[-(1+k)B_2 - x_2(1-p)C] + (1-x)\times[R_2 + kB_1 - x_2(1-p)C] = R_2 + kB_1 - x_2(1-p)C + x\times[-kB_1 - (1+k)B_2 - R_2].$$

则访问客体 O 采取混合策略的平均收益为:

$$\overline{U}_O = yU_{O_1} + (1-y)U_{O_2} \tag{13}$$

5.2.2 复制动态方程

根据动态方程原理, 如果参与者选择某策略的个体收益超过群体平均收益, 则该策略选择概率逐渐增长. 由此可得, 访问主体和客体在访问控制演化博弈中的复制动态方程表达式为:

$$\begin{aligned} F_S(x) &= \frac{\mathrm{d}x}{\mathrm{d}t} = x(U_{S_1} - \overline{U_S}) = x(1-x)(U_{S_1} - U_{S_2}) \\ &= x(1-x)\times[-L_1 + R_1 + kB_2 + (1+k)B_1 + y(L_1 - I_2 - k(B_1 + B_2))] \end{aligned} \tag{14}$$

$$\begin{aligned} F_O(y) &= \frac{\mathrm{d}y}{\mathrm{d}t} = y(U_{O_1} - \overline{U_O}) = y(1-y)(U_{O_1} - U_{O_2}) \\ &= y(1-y)\times[-L_2 - R_2 - B_2 - kB_1 + x(I_3 + L_2 + 2R_2 + kB_1 + 2B_2 + kB_2)] \end{aligned} \tag{15}$$

复制动态方程 (14)、(15) 刻画了访问主体 S 和客体 O 在访问控制中的策略动态演化, 令方程组 (14) 和 (15) 为 0, 在平面 $M = \{(x,y)|0 \leqslant x \leqslant 1, 0 \leqslant y \leqslant 1\}$ 演化博弈存在 5 个均衡点, 分别记作 $E_1(0,0)$、$E_2(0,1)$、$E_3(1,0)$、$E_4(1,1)$、$E_5(x^*,y^*)$, 其中 $0 \leqslant x^*, y^* \leqslant 1$, $x^* = \dfrac{L_2 + R_2 + B_2 + kB_1}{I_3 + L_2 + 2R_2 + kB_1 + 2B_2 + kB_2}$, $y^* = \dfrac{-L_1 + R_1 + kB_2 + (1+k)B}{-L_1 + I_2 + k(B_1 + B_2)}$, 表明访问主体以概率 $\left(\dfrac{L_2 + R_2 + B_2 + kB_1}{I_3 + L_2 + 2R_2 + kB_1 + 2B_2 + kB_2}, 1 - \dfrac{L_2 + R_2 + B_2 + kB_1}{I_3 + L_2 + 2R_2 + kB_1 + 2B_2 + kB_2}\right)$ 选取策略{正常访问, 恶意访问}, 访问客体以概率 $\left(\dfrac{-L_1 + R_1 + kB_2 + (1+k)B}{-L_1 + I_2 + k(B_1 + B_2)}, 1 - \dfrac{-L_1 + R_1 + kB_2 + (1+k)B}{-L_1 + I_2 + k(B_1 + B_2)}\right)$ 选取策略{允许访问, 拒绝访问}.

当 $x = x^*$ 时, 总有 $F_O(y) = 0$, 对任意客体“允许访问”策略的选取概率 y, 模型均达到演化稳定状态. 一旦 x 发生偏移, 模型会发生变化, 当 $x > x^*$ 时, $y = 1$ 为客体的演化稳定策略; 当 $x < x^*$ 时, $y = 0$ 为客体的演化稳定策略, 如图 4 所示. 同理, 当 $y = y^*$ 时, 总有 $F_S(x) = 0$, 对任意主体“正常访问”策略的选取概率 x, 模型均达到演化稳定状态. 一旦 y 发生偏移, 模型会发生变化, 当 $y > y^*$ 时, $x = 1$ 为访问客体的演化稳定策略; 当 $x < x^*$ 时, $x = 0$ 为访问客体的演化稳定策略, 如后文图 5 所示. 因此, 均衡点 $E_5(x^*,y^*)$ 可作为访问控制博弈决策模型中的决策阈值 (th_S, th_O), 当访问主体选择“正常访问”的概率超过阈值 th_S, 且客体选择“允许访问”的概率超过阈值 th_O 时, 博弈决策模型向 PDP 发送“允许访问”的决策响应; 反之, 则发送“拒绝访问”的决策响应.

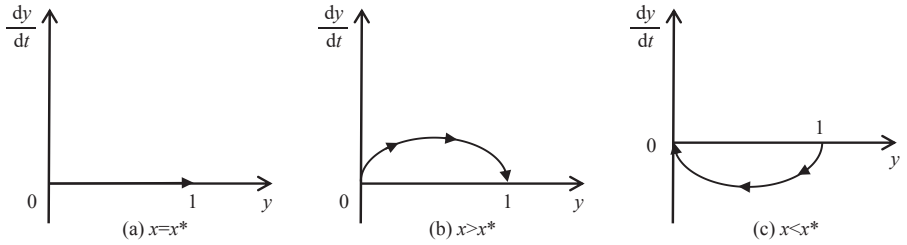


图 4 访问主体策略选取概率的演化路径

5.2.3 稳定策略均衡点演化分析

雅可比矩阵是系统状态方程对状态变量的偏导数矩阵, 用于描述系统在平衡点附近的行为特征. 在复制动态系统中, 通过构建雅可比矩阵来分析系统局部稳定性. 分别计算 $F_S(x)$ 和 $F_O(y)$ 关于 x 和 y 的偏导数, 可得到演化博

弈动态调整模型的雅可比矩阵, 其形式如公式 (16) 所示:

$$J=\begin{bmatrix}\dfrac{\partial F_S(x)}{\partial x} & \dfrac{\partial F_S(x)}{\partial y}\\ \dfrac{\partial F_O(y)}{\partial x} & \dfrac{\partial F_O(y)}{\partial y}\end{bmatrix} \tag{16}$$

其中,

$$\begin{cases}\dfrac{\partial F_S(x)}{\partial x}=(1-2x)\times[-L_1+R_1+kB_2+(1+k)B_1+y(L_1-I_2-k(B_1+B_2))]\\ \dfrac{\partial F_S(x)}{\partial y}=x(1-x)\times(L_1-I_2-k(B_1+B_2))\\ \dfrac{\partial F_O(y)}{\partial x}=y(1-y)\times(I_3+L_2+2R_2+kB_1+2B_2+kB_2)\\ \dfrac{\partial F_O(y)}{\partial y}=(1-2y)\times[-L_2-R_2-B_2-kB_1+x(I_3+L_2+2R_2+kB_1+2B_2+kB_2]\end{cases} \tag{17}$$

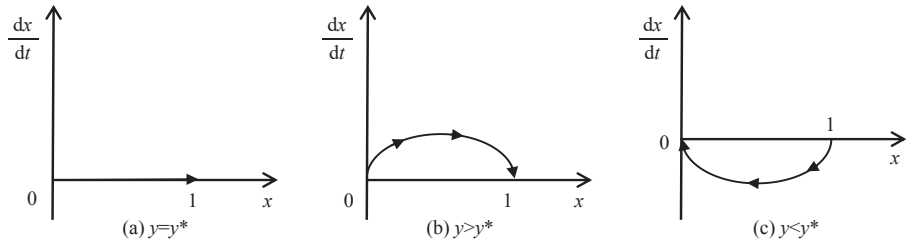


图 5 访问客体策略选取概率的演化路径

利用李雅普诺夫稳定性理论[35], 判断复制动态方程的内部均衡点是否为演化稳定点 (ESS). 具体方法是计算均衡点处的雅可比矩阵, 通过特征值分析评估系统局部稳定性. 若均衡点的雅可比矩阵特征值实部全为负数, 即行列式 $\mathrm{Det}(J)>0$、迹 $\mathrm{Tr}(J)<0$, 此时该均衡点为 ESS; 若所有特征值的实部均为正数, 即行列式 $\mathrm{Det}(J)>0$、迹 $\mathrm{Tr}(J)>0$, 则该均衡点为演化不稳定的内部均衡点; 若特征值的实部有正有负 (或为 0), 即行列式 $\mathrm{Det}(J)<0$、迹 $\mathrm{Tr}(J)=0$ 或不确定, 则该点为系统的鞍点. 根据以上分析, GDRM 的各均衡点的雅可比矩阵行列式 $\mathrm{Det}(J)$ 和迹 $\mathrm{Tr}(J)$ 如表 4 所示.

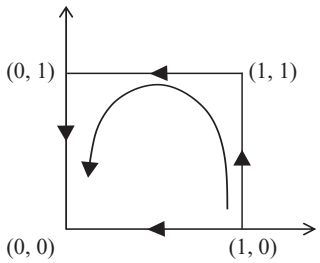
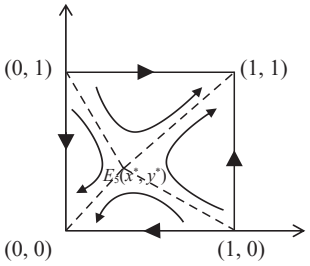
表 4 雅可比矩阵行列式 $\mathrm{Det}(J)$ 和迹 $\mathrm{Tr}(J)$

均衡点	$\mathrm{Det}(J)$	$\mathrm{Tr}(J)$
$E_1(0,0)$	$(-L_1+R_1+kB_2+(1+k)B_1)\times[-(L_2+R_2+B_2+kB_1)]$	$-L_1-L_2+R_1-R_2+(k-1)B_2+B_1$
$E_2(0,1)$	$(R_1+B_1-I_2)\times(L_2+R_2+B_2+kB_1)$	$R_1+R_2+L_2-I_2+B_2+(1+k)B_1$
$E_3(1,0)$	$[-(-L_1+R_1+kB_2+(1+k)B_1)]\times(I_3+R_2+(1+k)B_2)$	$I_3+L_1-R_1+R_2+-B_1-kB_1+B_2$
$E_4(1,1)$	$[-(R_1+B_1-I_2)]\times[-(I_3+R_2+(1+k)B_2)]$	$I_2-I_3-R_1-R_2-B_1-B_2-kB_2$
$E_5(x^*,y^*)$	$-x^*(1-x^*)(L_1-I_2-k(B_1+B_2))\times y^*(1-y^*)(I_3+L_2+2R_2+kB_1+2B_2+kB_2)$	0

因为均衡点 $E_5(x^*,y^*)$ 的迹 $Tr(J)=0$, 所以均衡点 E_5 是系统的鞍点, 此时演化博弈模型无法达到稳定状态. 根据博弈假设, 所有参数均为正数, 因此 $L_2+R_2+B_2+kB_1>0$ 和 $I_3+R+(1+k)B>0$ 恒成立, 所以系统仅可能在均衡点 $E_4(1,1)$ 和均衡点 $E_1(0,0)$ 处达到稳定状态. 在访问控制场景下, 理想稳定状态为访问主体选择“正常访问”而且客体选择“允许访问”, 因此理想情况下系统仅在均衡点 $E_4(1,1)$ 达到演化稳定状态.

当演化博弈系统在均衡点 $E_1(0,0)$ 达到平衡时, 雅可比矩阵满足行列式 $\mathrm{Det}(J)>0$ 且迹 $\mathrm{Tr}(J)<0$, 初始状态满足 $-L_1+R_1+kB_2+(1+k)B_1<0$ 且 $-(L_2+R_2+B_2+kB_1)<0$, 由于 $L_2+R_2+B_2+kB_1>0$ 和 $I_3+R_2+(1+k)B_2>0$ 恒成立, 所以系统中可能的稳定性条件只有 2 种. 此时, 其他均衡点的稳定性如表 5 所示.

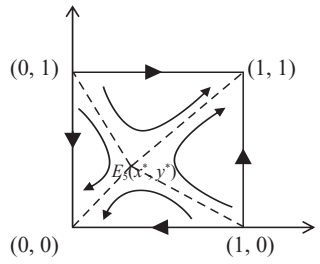
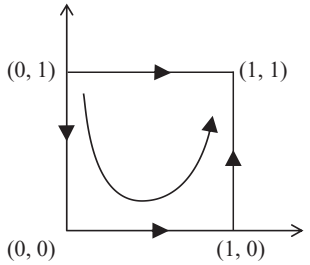
表 5 均衡点 $E_1(0,0)$ 达到平衡时其他均衡点稳定性分析

分析对象		初始状态 ① $R_1+B_1-I_2<0$ $I_3+R_2+(1+k)B_2>0$			初始状态 ② $R_1+B_1-I_2>0$ $I_3+R_2+(1+k)B_2>0$		
		Det(J)	Tr(J)	稳定性	Det(J)	Tr(J)	稳定性
平衡点	$E_1(0,0)$	+	−	ESS	+	−	ESS
	$E_2(0,1)$	−	±	鞍点	+	+	不稳定
	$E_3(1,0)$	+	+	不稳定	+	+	不稳定
	$E_4(1,1)$	−	±	鞍点	+	−	ESS
演化相位图							

注: +表示该值>0, –表示该值<0, ±表示该值正负性不确定

当演化博弈系统在均衡点 $E_4(1,1)$ 达到平衡时, 雅可比矩阵满足行列式 $\mathrm{Det}(J)>0$ 且迹 $\mathrm{Tr}(J)<0$, 此时初始状态满足 $R_1+B_1-I_2>0$ 且 $I_3+R_2+(1+k)B_2>0$, 由于 $L_2+R_2+B_2+kB_1>0$ 和 $I_3+R_2+(1+k)B_2>0$ 恒成立, 所以在系统中只有 2 种可能的稳定性条件. 此时, 其他均衡点的稳定性如表 6 所示.

表 6 均衡点 $E_4(1,1)$ 达到平衡时其他均衡点稳定性分析

分析对象		初始状态 ③ $-L_1+R_1+kB_2+(1+k)B_1<0$ $L_2+R_2+B_2+kB_1>0$			初始状态 ④ $-L_1+R_1+kB_2+(1+k)B_1>0$ $L_2+R_2+B_2+kB_1>0$		
		Det(J)	Tr(J)	稳定性	Det(J)	Tr(J)	稳定性
平衡点	$E_1(0,0)$	+	−	ESS	−	±	鞍点
	$E_2(0,1)$	+	+	不稳定	+	+	不稳定
	$E_3(1,0)$	+	+	不稳定	−	±	鞍点
	$E_4(1,1)$	+	−	ESS	+	−	ESS
演化相位图							

注: +表示该值>0, –表示该值<0, ±表示该值正负性不确定

分析表明, 初始状态②和初始状态③满足相同条件, 属于同一稳定状态, 因此初始状态②与初始状态③等价.

1) 访问主体 S 策略空间演化趋势分析. 对于访问主体而言, 当满足条件 $I_2-B_1<R_1$ 时, 即访问主体采取“恶意访问”时的收益小于系统的奖惩机制时, 访问主体策略向“正常访问”演化. 所以, 提高访问奖惩值、降低“恶意访问”额外收益, 可以有效激励访问主体的“正常访问”行为. 当满足条件 $-L_1+R_1+kB_2>-(1+k)B_1$ 时, 即访问主体因“正常访问”被拒绝的收益大于“恶意访问”被拒绝的收益时, 主体策略将向“正常访问”演化. 所以, 为激励访问主体

的“正常访问”行为, 应增加访问奖惩值和双方的补偿系数.

2) 访问客体 O 策略空间演化趋势分析. 对于访问客体而言, 满足条件 $I_3+R_2>-(1+k)B_2$ 时, 当客体允许主体访问的收益高于拒绝访问的收益时, 客体策略倾向于演化为“允许访问”; 满足条件 $R_2+kB_1>-L_2-B_2$ 时, 即拒绝主体“恶意访问”收益大于允许“恶意访问”的收益, 客体策略向“拒绝访问”演化. 所以, 提高对访问主客体的奖惩值可以有效激励客体允许“正常访问”和拒绝“恶意访问”的行为.

3) 博弈双方策略组合演化趋势分析. 整个演化系统的演化路径从 $(0,1),(1,0)\Rightarrow(0,0)\Rightarrow(1,1)$, 逐步淘汰劣势策略{正常访问, 拒绝访问}和{恶意访问, 允许访问}, 向{恶意访问, 拒绝访问}次优势策略演化, 最终收敛到优势策略{正常访问, 允许访问}. 系统可以通过提高访问控制的奖惩机制, 增加双方的补偿系数, 可有效激励访问主体“正常访问”行为和客体允许主体的“正常访问”和拒绝主体的“恶意访问”行为.

5.2.4 动态调整机制

本文构建的基于博弈论的可信动态访问控制模型, 通过 4 个系统性能指标来评判模型有效性和访问控制决策质量: (1) 合作成功率 (cooperation success rate, *CSR*): 主体成功“正常访问”的比例; (2) 恶意成功率 (malicious success rate, *MSR*): 主体“恶意访问”成功突破的比例; (3) 误判率 (false rejection rate, *FRR*): 客体误判拒绝主体“正常访问”请求的比例; (4) 准确率 (accuracy rate, *AR*): 客体做出正确决策的比例. 演化博弈动态调整模型的动态调整机制基于演化博弈分析和系统性能指标, 根据上一周期的收益参数值和奖惩值计算授权决策阈值 (th_S,th_O), 以引导主客体向理想状态演化为目的动态调整系统的对主客体的奖励值和惩罚值, 具体动态调整包含以下关键步骤.

1) 演化博弈动态调整模型通过博弈收益表记录访问主客体上一周期 τ_{n-1} 内的收益参数值 $\Pi_{i,j}$, 并以固定周期更新收益参数值, 其中 $i\in\{1,2,\ldots,N\}$ 是周期 τ_{n-1} 内访问次序, N 为周期 τ_{n-1} 访问的总次数, j 为博弈参数 $j\in\{C,I_1,I_2,I_3,L_1,L_2\}$. 模型通过权重 σ 更新当前周期 τ_n 参数 j 收益值 Π_j^n, $\Pi_j^n=\sigma\cdot\Pi_j^{n-1}+(1-\sigma)\cdot\overline{\Pi}_j^{n-1}$. 其中, $\overline{\Pi}_j^{n-1}$ 是上一周期 τ_{n-1} 内访问主客体的收益参数 j 均值, $\overline{\Pi}_j^{n-1}=\dfrac{1}{N}\sum_{i=1}^{N}\overline{\Pi}_{i,j}^{n-1}$; Π_j^{n-1} 是在上一周期 τ_{n-1} 参数 j 使用的历史收益值.

2) 根据更新后的收益参数值, 构建 GDRM 收益矩阵, 并通过博弈分析确定 GDRM 的奖惩值约束条件以及授权决策阈值 (th_S,th_O).

3) 计算系统性能指标在上一周期 τ_{n-1} 的增量: ① 合作成功率增量: $\Delta CSR=CSR_{n-1}-CSR_{n-2}$; ② 恶意成功率增量: $\Delta MSR=MSR_{n-1}-MSR_{n-2}$; ③ 误判率: $\Delta FRR=FRR_{n-1}-FRR_{n-2}$; ④ 准确率增量: $\Delta AR=AR_{n-1}-AR_{n-2}$.

4) 基于系统性能指标以及性能指标的增量, 在满足演化博弈分析的奖惩值约束条件下, 自适应地调整系统对访问主体和客体的奖惩参数配置.

访问主体的奖励值: $R_1=(1+\Delta CSR\times CSR_{n-1}+\Delta AR\times AR_{n-1})\times R_1$.

访问客体的奖励值: $R_2=(1+\Delta CSR\times CSR_{n-1}-\Delta FRR\times FRR_{n-1}+\Delta AR\times AR_{n-1})\times R_2$.

访问主体的惩罚值: $B_1=(1+\Delta MSR\times MSR_{n-1}-\Delta AR\times AR_{n-1})\times B_1$.

访问客体的惩罚值: $B_2=(1+\Delta MSR\times MSR_{n-1}+\Delta FRR\times FRR_{n-1}-\Delta AR\times AR_{n-1})\times B_2$.

5) 验证更新后的奖惩值是否符合约束条件范围内: 若奖惩值超出预设的奖惩边界条件, 则将对应的奖惩值赋值为对应的边界值; 若满足则采纳该奖惩值, 并将更新值作为下一周期访问决策中对主客体的奖惩依据.

5.3 博弈决策模型

博弈决策模型从短期决策角度出发, 结合访问请求权限收益矩阵与可信预测值, 研究信息不对称情况下博弈参与者的策略选择. 基于访问主体不同权限的收益值, 构建不完全信息静态博弈模型, 并通过贝叶斯纳什均衡分析策略, 为访问客体的决策提供依据, 实现领域数据共享场景下对访问主体的细粒度动态授权.

5.3.1 不完全信息博弈模型

在每次访问过程中, 访问主体请求的访问权限与客体资源差异会导致双方在博弈中产生不同的收益与损失. 访问控制博弈决策模型根据 PDP 接收到的访问请求信息、信任评估、访问控制策略及奖惩参数信息, 构建收益矩阵, 通过求解贝叶斯纳什均衡, 比较访问主体和客体选择策略的概率与决策阈值, 并以此做出访问控制决策. 由

于参与者仅了解自身类型信息, 对其他参与者类型和策略选择并不完全了解, 因此访问控制博弈决策模型是一个不完全信息静态博弈模型.

不完全信息环境下, 访问控制博弈决策模型可形式化表示为四元组 $<P,A,U,\Gamma>$, 包括参与者空间、策略空间、收益函数以及类型空间. 为处理不完全信息博弈中信息不对称问题, 海萨尼转换 (Harsanyi transformation)[36]机制引入虚拟的“自然”参与者, 通过概率分布随机选择参与者类型, 从而将不完全信息博弈转换为不完美信息博弈. 转换后“自然”为访问主体和客体随机分配类型, 主体和客体知道自身类型但不了解对方策略, 可视为双方静态博弈. 转换后的博弈树如图 6 所示. 根据博弈假设, “自然”玩家依据信任预测结果选择访问主体类型, 类型空间为 Γ_S = {诚信用户, 非诚信用户}, 其类型空间概率分布为 $(p,1-p)$. 访问主体了解自身类型, 而客体仅知道主体类型概率分布. 访问主体在两种类型下均可选择{正常访问, 恶意访问}策略, 诚信类型下策略选择概率为 $(x_1,1-x_1)$, 非诚信类型下策略选择概率为 $(x_2,1-x_2)$, 访问客体不知道访问主体的具体策略, 并以 $(y,1-y)$ 的概率选择{允许访问, 拒绝访问}策略.

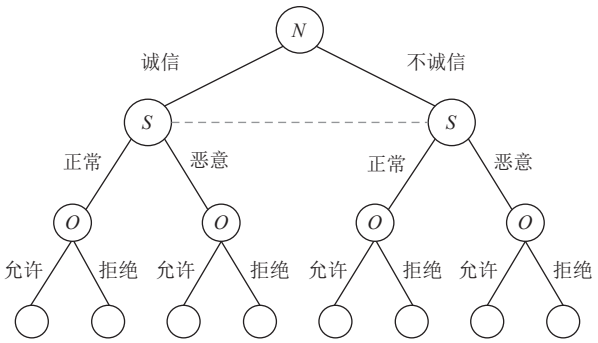


图 6 博弈决策模型博弈树

5.3.2 贝叶斯纳什均衡求解

在博弈决策模型中, 访问主体请求权限与客体资源差异会导致不同收益与损失, 通过海萨尼转换, “自然”根据信任预测结果以 $(p,1-p)$ 的概率选择访问主体的类型, 访问主体和客体知道自身类型信息, 但不了解对方策略选择. 因此, 不完全信息博弈可转换为在各类型下的静态博弈. 通过求解贝叶斯纳什均衡, 根据类型条件概率分布计算各策略的期望收益, 从而确定参与者在给定对方策略和类型分布时的最优反应.

1) 诚信用户纳什均衡

在访问主体的类型是诚信用户时, 博弈决策模型的收益矩阵如表 7 所示.

表 7 诚信用户博弈决策模型收益矩阵

访问主体	访问客体	
	允许访问 (y)	拒绝访问 ($1-y$)
正常访问 (x_1)	I_1+R_1 I_3+R_2	$-L_1+R_1+kB_2$ $-(1+k)B_2$
恶意访问 ($1-x_1$)	$I_1+I_2-B_1$ $-L_2-B_2$	$-(1+k)B_1$ R_2+kB_1

在纯策略角度, 通过画线法分析博弈矩阵. 对访问主体而言, 当客体选择“允许访问”策略时, 若满足 $R_1>I_2-B_1$, 则“正常访问”为最优响应, 反之“恶意访问”为最优响应; 当客体选择“拒绝访问”策略时, 若满足条件 $-L_1+R_1+kB_2>-(1+k)B_1$, 则“正常访问”收益更高, 反之“恶意访问”收益更高. 对于客体而言, 在主体“正常访问”时, 客体“允许访问”的收益高于“拒绝访问”; 当主体“恶意访问”时, 客体“拒绝访问”的收益高于“允许访问”. 因此, 如果主体是诚信用户, 在满足 $R_1>I_2-B_1$ 时, 纯策略纳什均衡为{正常访问, 允许访问}; 满足 $-L_1+R_1+kB_2<-(1+k)B_1$ 时, 纯策略纳什均衡为{恶意访问, 拒绝访问}.

从混合策略角度, 计算博弈的混合策略纳什均衡. 诚信访问主体的收益矩阵为 P_S^1, 此时客体的收益矩阵为 P_O^1.

主体的期望收益为:

$$\begin{aligned}E_{S_1}&=(x_1,1-x_1)P_S^1(y,1-y)^{\mathrm{T}}\\&=-(1+k)B_1+y(I_1+I_2+kB_1)+x_1(-L_1+R_1+(1+k)B_1+kB_2)+x_1y(L_1-I_2-k(B_1+B_2))\end{aligned}\tag{18}$$

客体的期望收益为:

$$\begin{aligned}E_{O_1}&=(x_1,1-x_1)P_O^1(y,1-y)^{\mathrm{T}}\\&=R_2+kB_1+x_1(-R_2-kB_1-(1+k)B_2)+y(-L_2-R_2-B_2-kB_1)+x_1y(I_3+L_2+2R_2+(2+k)B_2+kB_1)\end{aligned}\tag{19}$$

计算访问主体的期望收益关于 x_1 的偏导, 得到:

$$\frac{\partial E_{S_1}}{\partial x_1}=-L_1+R_1+(1+k)B_1+kB_2+y(L_1-I_2-k(B_1+B_2))\tag{20}$$

计算访问客体的期望收益关于 y 的偏导, 得到:

$$\frac{\partial E_{O_1}}{\partial y}=-L_2-R_2-B_2-kB_1+x_1(I_3+L_2+2R_2+(2+k)B_2+kB_1)\tag{21}$$

令 $\dfrac{\partial E_{S_1}}{\partial x_1}=0,\dfrac{\partial E_{O_1}}{\partial y}=0$, 解得:

$$x_1^*=\frac{L_2+R_2+B_2+kB_1}{I_3+L_2+2R_2+(2+k)B_2+kB_1},\ y_1^*=\frac{-L_1+R_1+(1+k)B_1+kB_2}{-L_1+I_2+k(B_1+B_2)}\tag{22}$$

通过公式 (22), 得到诚信访问主体的混合策略纳什均衡如下所示:

$$\begin{bmatrix}\dfrac{L_2+R_2+B_2+kB_1}{I_3+L_2+2R_2+(2+k)B_2+kB_1} & 1-\dfrac{L_2+R_2+B_2+kB_1}{I_3+L_2+2R_2+(2+k)B_2+kB_1}\\ \dfrac{-L_1+R_1+(1+k)B_1+kB_2}{-L_1+I_2+k(B_1+B_2)} & 1-\dfrac{-L_1+R_1+(1+k)B_1+kB_2}{-L_1+I_2+k(B_1+B_2)}\end{bmatrix}\tag{23}$$

博弈决策模型基于混合策略纳什均衡, 计算诚信访问主体“正常访问”以及客体“允许访问”的概率, 将混合策略纳什均衡点 (x_1^*,y_1^*) 与授权阈值 (th_S,th_O) 进行比较. 当访问主体是诚信用户时, 若满足 $x_1^*\geqslant th_S$ 且 $y_1^*\geqslant th_O$, 则访问控制决策为“允许访问”, 反之, 访问控制决策为“拒绝访问”.

2) 非诚信用户纳什均衡

非诚信访问主体惩罚因子 γ 与主体策略选择线性相关, 对非诚信主体的惩罚为 $(1-x_2)\gamma$, 表示非诚信主体“正常访问”的概率越高, 主体所受的惩罚越小; 反之, “恶意访问”的概率与惩罚力度呈正相关. 所以非诚信主体的收益矩阵如表 8 所示.

表 8　非诚信用户博弈决策模型收益矩阵

访问主体	访问客体	
	允许访问 (y)	拒绝访问 ($1-y$)
正常访问 (x_2)	$-C+I_1+R_1-(1-x_2)\gamma B_1$ I_3+R_2-C	$-C-L_1+R_1+kB_2-(1-x_2)\gamma B_1$ $-(1+k)B_2-C$
恶意访问 ($1-x_2$)	$-C+I_1+I_2-B_1-(1-x_2)\gamma B_1$ $-L_2-B_2-C$	$-C-(1+k)B_1-(1-x_2)\gamma B_1$ R_2+kB_1-C

从纯策略角度, 通过画线法分析博弈矩阵. 对访问主体来说, 当客体选择“允许访问”时, 若满足 $R_1>I_2-B_1$, 访问主体选择“正常访问”收益更高, 反之选择“恶意访问”收益更高; 当客体选择“拒绝访问”时, 若满足 $-L_1+R_1+kB_2>-(1+k)B_1$, 主体选择“正常访问”策略收益更高, 反之选择“恶意访问”收益更高. 对客体而言, 访问主体选择“正常访问”时, 客体选择“允许访问”收益更高, 当主体选择“恶意访问”时, 访问客体选择“拒绝访问”收益更高. 所以, 非诚信访问主体若满足 $R_1>I_2-B_1$, 则纯策略纳什均衡为{正常访问, 允许访问}; 若满足 $-L_1+R_1+kB_2<-(1+k)B_1$, 纯策略纳什均衡为{恶意访问, 拒绝访问}.

从混合策略角度, 计算混合策略纳什均衡. 非诚信访问主体的收益矩阵为 P_S^2, 此时客体的收益矩阵为 P_O^2. 主体的期望收益为:

$$E_{S_2} = (x_2, 1-x_2)P_S^2(y, 1-y)^{\mathrm{T}}$$
$$= -C-(1+k+\gamma)B_1 + y(I_1+I_2+kB_1) + x_2(-L_1+R_1+kB_2+(1+k+\gamma)B_1) + x_2y(L_1-I_2-k(B_1+B_2)) \tag{24}$$

客体的期望收益为:

$$E_{O_2} = (x_2, 1-x_2)P_O^2(y, 1-y)^{\mathrm{T}}$$
$$= R_2+kB_1-C + x_2(-R_2-kB_1-(1+k)B_2) + y(-L_2-R_2-B_2-kB_1) + x_2y(I_3+L_2+2R_2+(2+k)B_2+kB_1) \tag{25}$$

计算访问主体的期望收益关于 x_2 的偏导, 得到:

$$\frac{\partial E_{S_2}}{\partial x_2} = -L_1+R_1+kB_2+(1+k+\gamma)B_1+y(L_1-I_2-k(B_1+B_2)) \tag{26}$$

计算访问客体的期望收益关于 y 的偏导, 得到:

$$\frac{\partial E_{O_2}}{\partial y} = -L_2-R_2-B_2-kB_1+x_2(I_3+L_2+2R_2+(2+k)B_2+kB_1) \tag{27}$$

令 $\frac{\partial E_{S_2}}{\partial x_2}=0, \frac{\partial E_{O_2}}{\partial y}=0$, 解得:

$$x_2^* = \frac{L_2+R_2+B_2+kB_1}{I_3+L_2+2R_2+(2+k)B_2+kB_1},\ y_2^* = \frac{-L_1+R_1+kB_2+(1+k+\gamma)B_1}{-L_1+I_2+k(B_1+B_2)} \tag{28}$$

通过公式 (28) 得到非诚信用户的混合策略纳什均衡如下所示:

$$\begin{bmatrix} \frac{L_2+R_2+B_2+kB_1}{I_3+L_2+2R_2+(2+k)B_2+kB_1} & 1-\frac{L_2+R_2+B_2+kB_1}{I_3+L_2+2R_2+(2+k)B_2+kB_1} \\ \frac{-L_1+R_1+kB_2+(1+k+\gamma)B_1}{-L_1+I_2+k(B_1+B_2)} & 1-\frac{-L_1+R_1+kB_2+(1+k+\gamma)B_1}{-L_1+I_2+k(B_1+B_2)} \end{bmatrix} \tag{29}$$

同理, 计算博弈决策模型非诚信访问主体类型的混合策略纳什均衡, 比较混合策略纳什均衡点 (x_2^*, y_2^*) 与授权阈值 (th_S, th_O). 当访问主体是非诚信用户时, 若满足 $x_2^* \geqslant th_S$ 且 $y_2^* \geqslant th_O$, 则访问控制决策为“允许访问”, 相反地, 访问控制决策为“拒绝访问”

6 演化博弈模型仿真分析

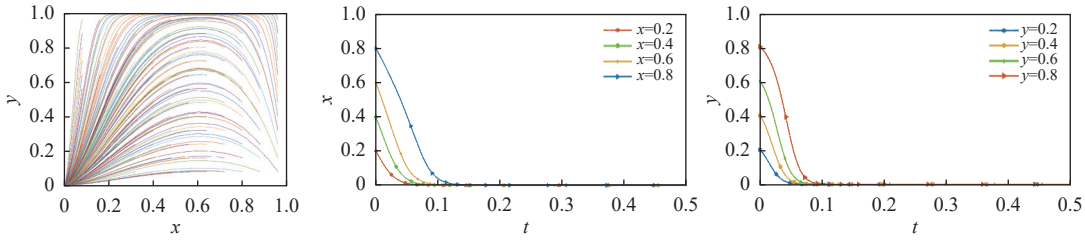
为了更直观地反映访问控制博弈动态演化过程, 验证访问控制演化博弈模型稳定性分析的有效性, 分析初始状态和关键因素对演化过程的敏感性, 根据博弈均衡解的约束条件对模型参数进行赋值, 通过 Matlab R2021b 进行数值仿真, 从而考察各因素对博弈均衡的影响程度.

6.1 初始状态演化分析

在满足初始状态①条件下, 即 $-L_1+R_1+kB_2+(1+k)B_1<0$、$-(L_2+R_2+B_2+kB_1)<0$、$R_1+B_1-I_2<0$ 且 $I_3+R_2+(1+k)B_2>0$, 构建仿真数组 1: $I_2=50$, $I_3=20$, $R_1=20$, $R_2=20$, $B_1=20$, $B_2=20$, $L_1=120$, $L_2=60$, $k=0.5$. 该初始状态下的策略演化仿真结果如图 7(a) 所示, 双方策略选择均收敛于均衡点 (0,0), 所以当“正常访问”被拒时的收益比“恶意访问”的收益小时, 访问主体更倾向于选择“恶意访问”, 客体倾向于选择“拒绝访问”. 访问主体“正常访问”的概率 x 随时间演化如图 7(b) 所示, 如果访问主体初始选择“正常访问”概率降低, 其策略将加速向“恶意访问”演化; 客体“允许访问”的概率 y 随时间演化如图 7(c) 所示, 当客体初始“允许访问”的概率减小时, 其策略会加速向“拒绝访问”演化.

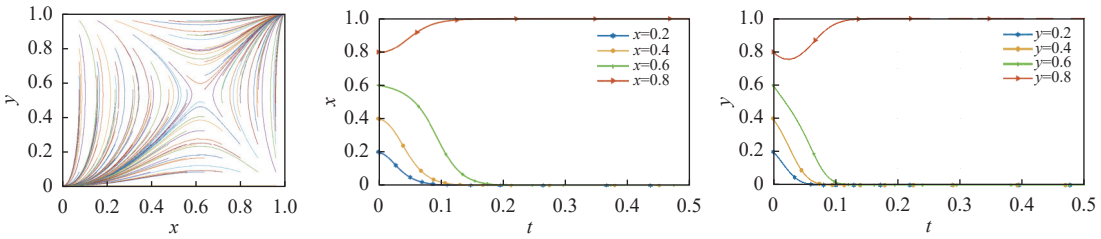
满足初始状态②/③时, 即 $-L_1+R_1+kB_2+(1+k)B_1<0$、$-(L_2+R_2+B_2+kB_1)<0$、$R_1+B_1-I_2>0$ 且 $I_3+R_2+(1+k)B_2>0$, 构建仿真数组 2: $I_2=20$, $I_3=20$, $R_1=20$, $R_2=20$, $B_1=20$, $B_2=20$, $L_1=120$, $L_2=60$, $k=0.5$. 该初始状态下的策略演化仿真结果如图 8(a) 所示, 双方策略选择收敛于均衡点 (0,0) 和均衡点 (1,1). 如果访问客体选择拒绝, 主体“正常访问”的损失大于“恶意访问”需要接受的惩罚; 如果访问客体允许, 主体“恶意访问”收益低于“正常访问”. 此时, 访问主体可能选择“正常访问”, 也可能选择“恶意访问”; 访问客体可能选择“允许访问”, 也可能选择“拒绝访问”. 访问主体“正常访问”概率 x 随时间演化如图 8(b) 所示, 访问主体初始选择“正常访问”概率越高越可能向“正常访问”策略演化, 如果初始概率降低会加速向“恶意访问”演化; 访问客体“允许访问”概率 y 随时间演化如

图 8(c) 所示, 访问客体初始选择“允许访问”的概率越高越可能向“允许访问”演化, 随着初始概率降低, 客体会加速向“拒绝访问”演化.



(a) 数组1条件下演化结果 (b) x初始值不同时的演化路径 (c) y初始值不同时的演化路径

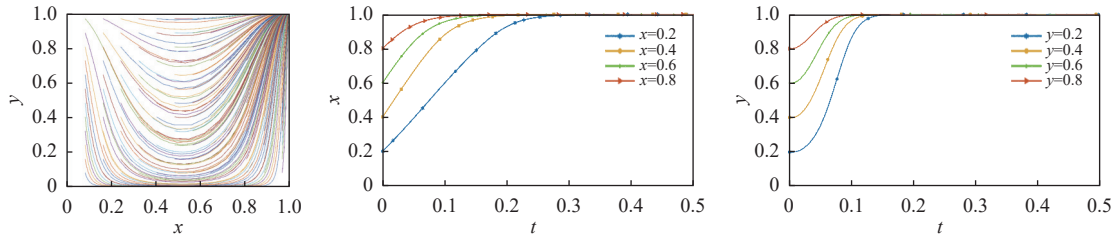
图 7 初始状态①的演化路径图



(a) 数组2条件下演化结果 (b) x初始值不同时随时间t的演化路径 (c) y初始值不同时随时间t的演化路径

图 8 初始状态②/③的演化路径图

满足初始状态④条件下, 即 $-L_1+R_1+kB_2+(1+k)B_1>0$、$-(L_2+R_2+B_2+kB_1)<0$、$R_1+B_1-I_2>0$ 且 $I_3+R_2+(1+k)B_2>0$, 构建仿真数组 3: $I_2=30$, $I_3=30$, $R_1=30$, $R_2=20$, $B_1=30$, $B_2=20$, $L_1=60$, $L_2=30$, $k=0.5$. 该初始状态下策略演化仿真结果如图 9(a) 所示, 双方的策略收敛于均衡点 $(1,1)$, 当主体“正常访问”被拒损失和“恶意访问”收益都较小、对主客体的奖惩值较大时, 主体更愿意选择“正常访问”, 客体也更愿意选择“允许访问”. 访问主体“正常访问”的概率 x 随时间演化如图 9(b) 所示, 访问主体初始选择“正常访问”概率增加, 会加速向“正常访问”演化; 访问客体“允许访问”的概率 y 随时间演化如图 9(c) 所示, 访问客体初始选择“允许访问”概率增加, 会加速向“允许访问”演化.



(a) 数组3条件下演化结果 (b) x初始值不同时随时间t的演化路径 (c) y初始值不同时随时间t的演化路径

图 9 初始状态④的演化路径图

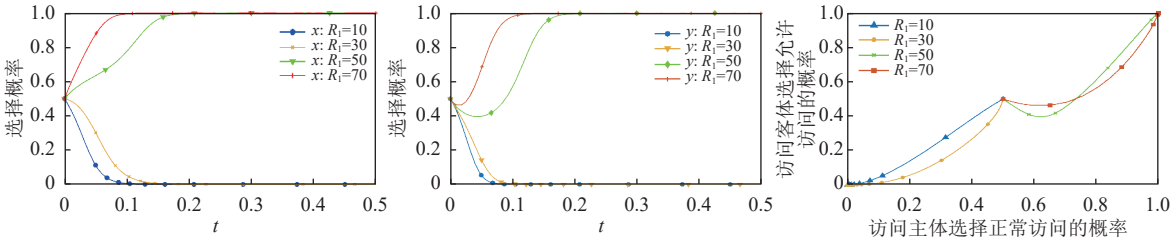
6.2 参数敏感度分析

演化博弈动态调整模型优化模型参数的途径是对访问主体和访问客体的奖惩值进行动态调整, 以引导模型向理想状态演化. 在初始状态②/③的条件下, 双方策略选择收敛于均衡点 $(0,0)$ 和均衡点 $(1,1)$, 所以以数组 2 作为演化过程敏感性分析的基础数组能够更好地观察参数对演化过程的影响. 假设访问主体选择“正常访问”和客体选择“允许访问”的初始概率均为 0.5.

6.2.1 主体奖励敏感度分析

在数组 2 其他参数不变基础上, 通过修改主体奖励值 R_1 的取值, 分析主体奖励值对博弈模型演化的敏感度.

主体的奖励值 R_1 取值从 10 增至 70 时, 访问主体和客体的策略演化路径如图 10(a) 和 (b) 所示, 主体的奖励值 R_1 的敏感度分析如图 10(c) 所示. 当奖励值 R_1 的取值满足 $R_1 < L_1 - kB_2 - B_1 - kB_1$ 时, 随着 R_1 减小会加速主体向“恶意访问”演化和客体向“拒绝访问”演化的速度, 而且主客体的演化速度相近, 这表明 $R_1 < L_1 - kB_2 - B_1 - kB_1$ 时主客体都对主体的奖励值 R_1 敏感; 当奖励值 R_1 的取值满足 $R_1 > L_1 - kB_2 - B_1 - kB_1$ 时, 随着 R_1 增大会加速主客体向{正常访问, 允许访问}演化的速度, 而且主体演化速度>客体演化速度, 表明 $R_1 > L_1 - kB_2 - B_1 - kB_1$ 时访问主体对主体的奖励值 R_1 更敏感. 因此, 增加主体的奖励值 R_1 可有效激励访问主客体向{正常访问, 允许访问}演化.

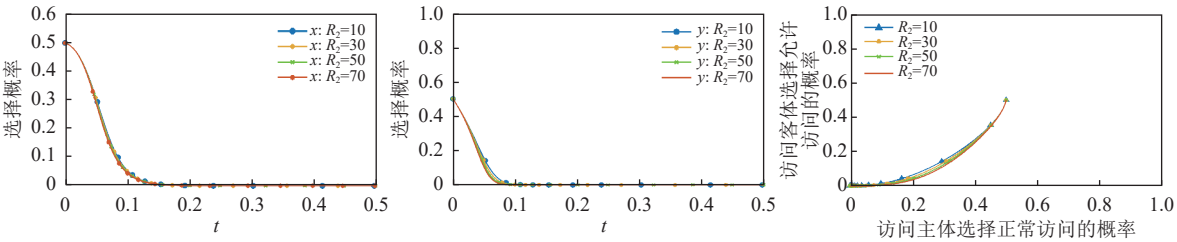


(a) 系统对访问主体的奖励R_1对x的影响 (b) 系统对访问主体的奖励R_1对y的影响 (c) 访问主体奖励R_1敏感度分析

图 10 主体奖励值分析图

6.2.2 客体奖励敏感度分析

在数组 2 其他参数不变基础上, 通过修改客体奖励值 R_2 的取值, 分析客体奖励值对博弈模型演化的敏感度. 客体奖励值 R_2 取值从 10 增至 70 时, 访问主体和客体的策略演化路径如图 11(a) 和 (b) 所示, 客体奖励值 R_2 的敏感度分析如图 11(c) 所示. 由图可知, 客体的奖励值 R_2 的取值并不会影响模型的演化方向, 仅对演化的速度产生细微影响, 可以忽略不计. 所以, 访问控制 GDRM 不受客体奖励值 R_2 的影响.



(a) 系统对访问客体的奖励R_2对x的影响 (b) 系统对访问客体的奖励R_2对y的影响 (c) 访问客体奖励R_2敏感度分析

图 11 客体奖励值分析图

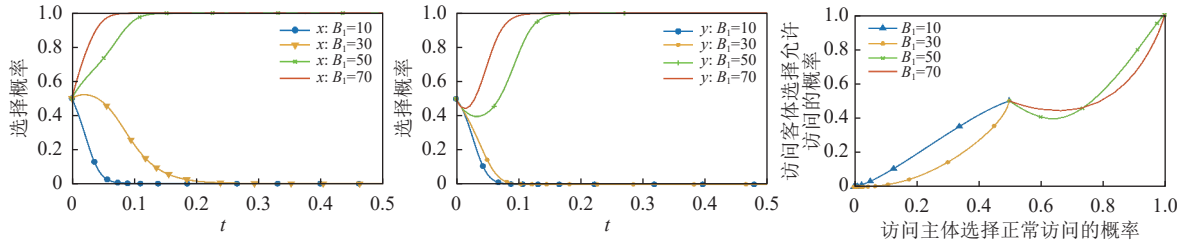
6.2.3 主体惩罚敏感度分析

在数组 2 其他参数均保持不变的基础上, 通过修改主体惩罚值 B_1 的取值, 分析主体奖励值对博弈模型演化的敏感度. 主体的惩罚值 B_1 取值从 10 增至 70 时, 访问主体和客体的策略演化路径如后文图 12(a) 和 (b) 所示, 主体的惩罚值 B_1 的敏感度分析如图 12(c) 所示. 当惩罚值 B_1 的取值满足 $B_1 < \dfrac{L_1 - kB_2 - R_1}{1+k}$ 时, 随着 B_1 减小会加速主体向“恶意访问”演化和客体向“拒绝访问”演化的速度, 主客体的演化速度相近, 这表明在满足 $B_1 < \dfrac{L_1 - kB_2 - R_1}{1+k}$ 时, 主客体对主体的惩罚值 B_1 同等敏感; 当惩罚值 B_1 的取值满足 $B_1 > \dfrac{L_1 - kB_2 - R_1}{1+k}$ 时, 随着 B_1 增大会加速主客体向{正常访问, 允许访问}演化的速度, 而且主体演化速度>客体演化速度, 表明满足 $B_1 > \dfrac{L_1 - kB_2 - R_1}{1+k}$ 时, 访问主体对主体的惩罚值 B_1 更敏感. 因此, 增加主体的惩罚值 B_1 可有效激励访问主客体向{正常访问, 允许访问}演化.

6.2.4 客体惩罚敏感度分析

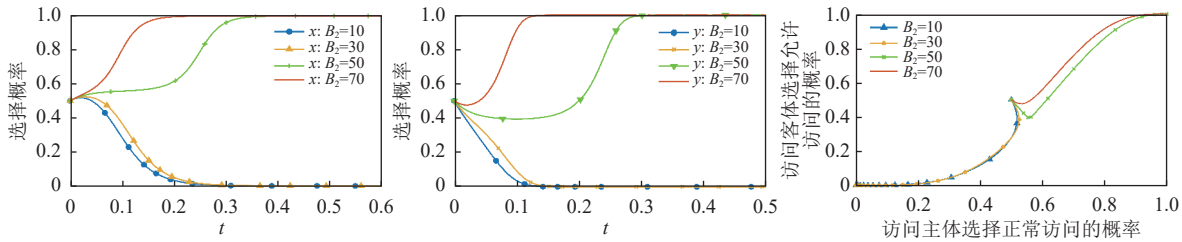
保持数组 2 其他参数不变的基础上, 通过修改客体惩罚值 B_2 的取值, 分析主体奖励值对博弈模型演化的敏感度. 客体的惩罚值 B_2 取值从 10 增至 70 时, 访问主体和客体的策略演化路径如图 13(a) 和 (b) 所示, 客体的惩罚值 B_2 的敏感度分析如图 13(c) 所示. 当惩罚值 B_2 的取值满足 $B_2 < \dfrac{L_1 - (1+k)B_1 - R_1}{k}$ 时, 随着 B_2 减小会加速

主体向“恶意访问”演化和客体向“拒绝访问”演化的速度, 而且客体演化速度>主体演化速度, 这表明在满足 $B_2 < \frac{L_1-(1+k)B_1-R_1}{k}$ 时, 访问客体对客体的惩罚值 B_2 更敏感; 当惩罚值 B_2 的取值满足 $B_2 > \frac{L_1-(1+k)B_1-R_1}{k}$ 时, 随着 B_2 增大会加速主客体向{正常访问, 允许访问}演化的速度, 而且客体演化速度>主体演化速度, 这表明在满足 $B_2 > \frac{L_1-(1+k)B_1-R_1}{k}$ 时, 访问客体对客体的惩罚值 B_2 更敏感. 因此, 增加客体的惩罚值 B_2 有效激励访问主客体尤其是访问客体向{正常访问, 允许访问}演化.



(a) 系统对访问主体的惩罚B_1对x的影响　(b) 系统对访问主体的惩罚B_1对y的影响　(c) 访问主体惩罚B_1敏感度分析

图 12　主体惩罚值分析图

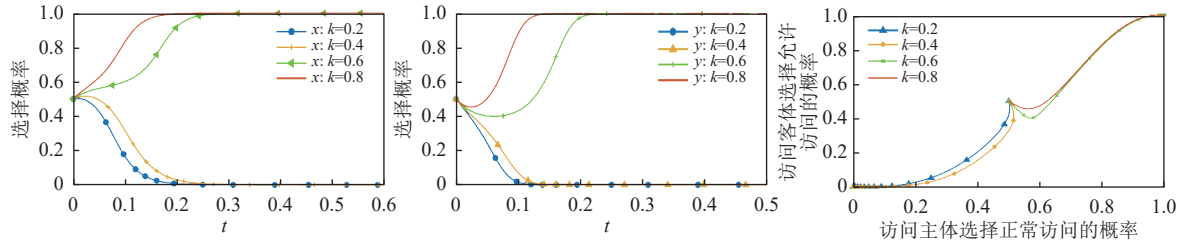


(a) 系统对访问客体的惩罚B_2对x的影响　(b) 系统对访问客体的惩罚B_2对y的影响　(c) 访问客体惩罚B_2敏感度分析

图 13　客体惩罚值分析图

6.2.5　主客体补偿系数敏感度分析

在数组 2 中其他参数均不变的基础上, 通过修改主客体补偿系数 k 的取值, 分析主客体之间的补偿系数对博弈模型演化的敏感度. 主客体补偿系数 k 取值从 0.2 增至 0.8 时, 访问主体和客体的策略演化路径如图 14(a) 和 (b) 所示, 主客体补偿系数 k 的敏感度分析如图 14(c) 所示. 当补偿系数 k 的取值满足 $k < \frac{L_1-B_1-R_1}{B_1+B_2}$ 时, 随着 k 减小会加速主体向“恶意访问”演化和客体向“拒绝访问”演化的速度, 而且客体演化速度>主体演化速度, 这表明在满足 $k < \frac{L_1-B_1-R_1}{B_1+B_2}$ 时, 访问客体对主客体补偿系数 k 更敏感; 当惩罚值 k 的取值满足 $k > \frac{L_1-B_1-R_1}{B_1+B_2}$ 时, 随着 k 增大会加速主客体向{正常访问, 允许访问}演化的速度, 而且客体演化速度>主体演化速度, 这表明在满足 $k > \frac{L_1-B_1-R_1}{B_1+B_2}$ 时, 访问客体对主客体补偿系数 k 更敏感. 因此, 增加主客体补偿系数 k 更敏感有效激励访问主客体, 尤其是访问客体向{正常访问, 允许访问}演化.

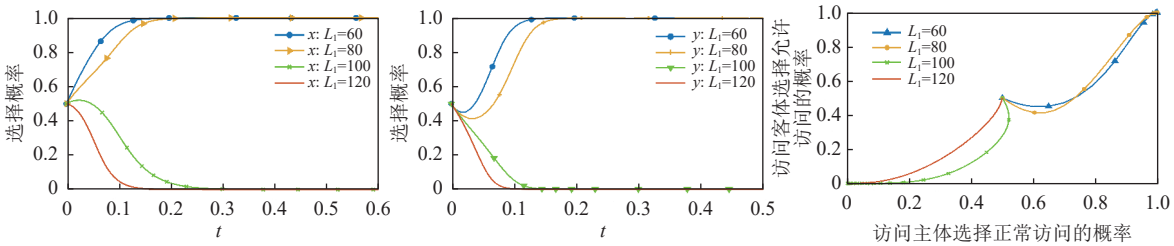


(a) 主客体的补偿系数k对x的影响　(b) 主客体的补偿系数k对y的影响　(c) 主客体的补偿系数k的敏感性分析

图 14　主客体补偿系数分析图

6.2.6 主体损失敏感度分析

在数组 2 其他参数不变的基础上, 通过修改主体损失 L_1 的取值, 分析主体被误判产生的损失对博弈模型演化的敏感度. 主体损失 L_1 取值从 60 增至 120 时, 访问主体和客体的策略演化路径如图 15(a) 和 (b) 所示, 主体损失 L_1 的敏感度分析如图 15(c) 所示. 当主体损失 L_1 满足 $L_1 < R_1 + kB_2 + B_1 + kB_1$ 时, 随着 L_1 减小会加速主客体向{正常访问, 允许访问}演化, 而且主体演化速度>客体演化速度, 这表明在满足 $L_1 < R_1 + kB_2 + B_1 + kB_1$ 时, 主体对损失 L_1 更敏感; 当主体损失 L_1 的取值满足 $L_1 > R_1 + kB_2 + B_1 + kB_1$ 时, 随着 L_1 增大会加速主体向“恶意访问”演化和客体向“拒绝访问”演化的速度, 而且客体演化速度>主体演化速度, 这表明在满足 $L_1 > R_1 + kB_2 + B_1 + kB_1$ 时, 访问主体对主体损失 L_1 没有客体敏感. 因此, 只有在主体“正常访问”被误判的损失 L_1 很大时才会选择“恶意访问”, 间接证明增加奖惩机制能够有效激励访问主客体向{正常访问, 允许访问}演化.



(a) 主体被误判的损失值对x的影响 (b) 主体被误判的损失值对y的影响 (c) 主体被误判损失值的敏感度分析

图 15 主体误判损失值分析图

在访问控制场景下, 系统的理想稳定状态为访问主体“正常访问”且客体“允许访问”, 即仅在均衡点 $E_4(1,1)$ 达到演化稳定状态. 为激励博弈调整模型向理想稳定状态演化, 在动态调整访问控制奖惩激励参数时应尽量满足初始状态④条件, 通过奖惩机制设计, 使系统在{正常访问, 允许访问}策略下实现长期稳定. 根据参数敏感度分析结果, 演化博弈动态调整模型对访问主体的奖惩值以及对访问客体的惩罚值都对演化结果有显著影响, 加大对参与者的奖惩力度可以加速系统向稳定策略演化. 同时, 可以增加主客体之间的补偿系数, 增加访问主体“恶意访问”行为和访问客体“拒绝访问”行为对对方的补偿, 从而减少主体“恶意访问”和客体“拒绝访问”的行为. 通过以上措施, 可以有效促进系统的稳定性和安全性.

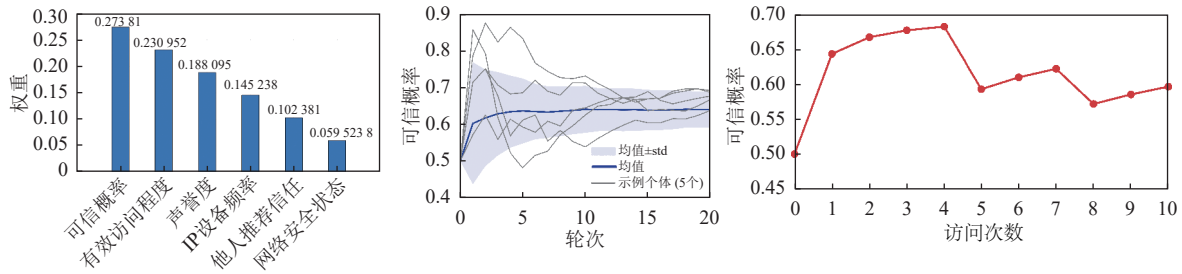
7 方案性能分析

为了更直观地反映基于博弈的可信动态访问控制模型的性能, 借助 Matlab R2021b 对信任预测模型和博弈决策模型进行数值仿真, 并与现有文献中的其他方案进行对比分析, 以验证该模型的有效性.

7.1 信任预测模型性能分析

信任预测模型通过模拟访问主体的多次访问行为, 综合考虑影响信任预测的多个核心因素, 并通过贝叶斯理论动态更新访问主体的信任概率. 本方案通过模拟信任预测模块的功能验证信任预测模型的可行性. 根据信息熵约束的属性权重算法对本文中提到的影响信任预测的因素进行权重分配, 在 *orness* 取值 0.65 时, 各因素的权重分配值如图 16(a) 所示, 满足从 ω_1 到 ω_n 权重比例逐渐降低的条件, 并且满足所有权重之和等于 1. 实验模拟了 100 个访问主体 20 次的访问行为, 统计每个主体的信任概率, 并计算每次的均值和标准差, 并从 100 个样本中随机挑选 5 个访问主体作为信任概率计算示例, 多主体信任预测变化如图 16(b) 所示, 图像表明对同一个访问主体的信任预测是不断变化的, 但是随着主体的访问次数增加, 模型对访问主体的信任预测的离散度逐渐收敛, 这表明访问主体访问的次数越多, 模型对该主体的信任预测越准确. 为验证模型能根据主体访问行为动态更新信任概率, 实验设计单个访问主体连续 10 次访问系统的场景, 其中设定第 4 次和第 7 次是“恶意访问”, 访问主体信任概率随着访问次数增加的变化曲线如图 16(c) 所示, 访问主体的信任度会随着访问次数而动态调整, 并且能够在产生“恶意访问”的行为后迅速降低信任概率值, 表明该模型能够准确合理地根据信任预测的多因素以及访问主体的历史行为

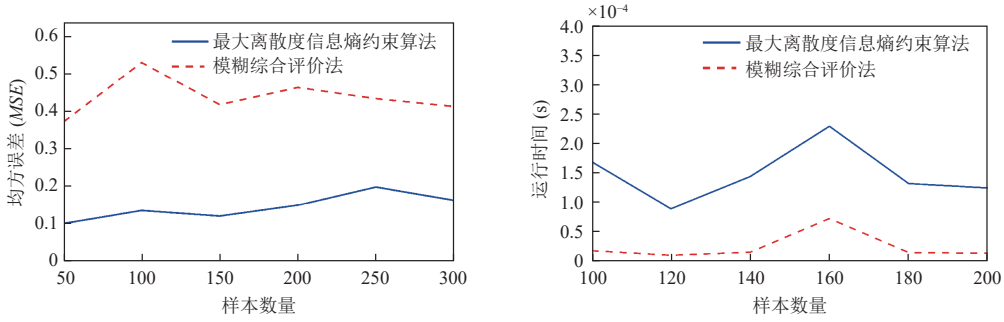
预测其信任度, 从而验证基于贝叶斯理论的信任预测模型的有效性.



(a) 影响信任预测因素权重分配 *orness*=0.65的OWA权重　(b) 100个主体访问20次信任值变化　(c) 访问主体10次访问信任概率变化

图 16　信任预测模型功能测试

本文采用最大离散度信息熵约束算法预测访问主体的信任度, 文献 [24] 通过模糊综合评价法量化信任度为进一步评估这两种方法的性能, 将两种信任度量化方法在准确性和运行时间方面进行对比分析. 实验中模拟对 300 个访问主体进行信任预测, 采用均方误差 $MSE = \frac{1}{n}\sum_{i=1}^{n}(y_i - \hat{y}_i)^2$ 来量化信任预测的准确性. 其中, 样本数量 $n = 300$, y_i 为真实值, $\hat{y}_i$ 为预测值. 实验结果如图 17 所示, 在图 17(a) 中, 本文采用的最大离散度信息熵约束算法的均方误差值约为 0.158, 而文献 [24] 方法均方误差平均值约为 0.439. 由此可见, 最大离散度信息熵约束算法的均方误差低于模糊综合评价法, 表明本文采用方法在信任预测的准确性方面表现更优. 在图 17(b) 中, 最大离散度信息熵约束方法的计算时间约为 0.147 ms, 而模糊综合评价法的计算时间约为 0.023 ms. 这表明, 本文方法的信任度计算运行速度较慢. 由于信任预测模型的预测结果将直接影响主体类型判断, 因此在本文构建的访问控制博弈模型中应优先确保信任预测的准确性. 未来研究可在确保信任预测准确性的基础上, 进一步探索提高计算效率的方法.



(a) 不同样本数量下信任预测准确性对比　(b) 不同样本数量下的运行时间对比

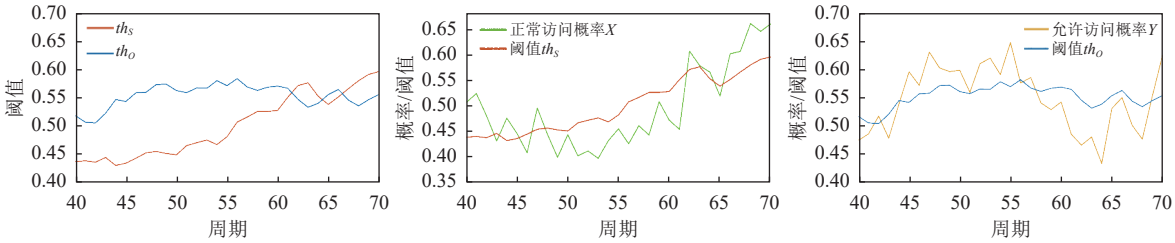
图 17　信任预测不同算法性能对比

7.2　博弈决策模型性能分析

博弈决策模型通过动态调整访问主体与访问客体的收益矩阵参数, 以混合策略贝叶斯纳什均衡作为决策依据, 并利用均衡点动态更新阈值和信任度. 为验证博弈决策模型的动态性和有效性, 模拟主体 100 个周期的访问行为以及客体的相应决策, 并记录访问控制决策过程中主体“正常访问”和客体“允许访问”的概率以及周期的授权阈值.

演化博弈动态调整模型的授权阈值和概率的关系变化如图 18 所示. 主客体的授权阈值变化趋势如图 18(a) 所示, 主体阈值在 0.4–0.6 之间动态变化, 客体阈值在 0.5–0.6 之间动态变化, 这反映了模型授权阈值能够通过演化博弈动态调整模型动态调整的特性. 访问主体授权阈值与“正常访问”概率关系和访问客体授权阈值与“允许访问”概率关系如图 18(b) 和图 18(c) 所示. 访问主体授权阈值的变化趋势与访问主体“正常访问”概率的变化趋势一致, 客体授权阈值的变化趋势与访问客体“允许访问”概率的变化趋势一致. 这表明主客体的授权阈值会随着访问次序的

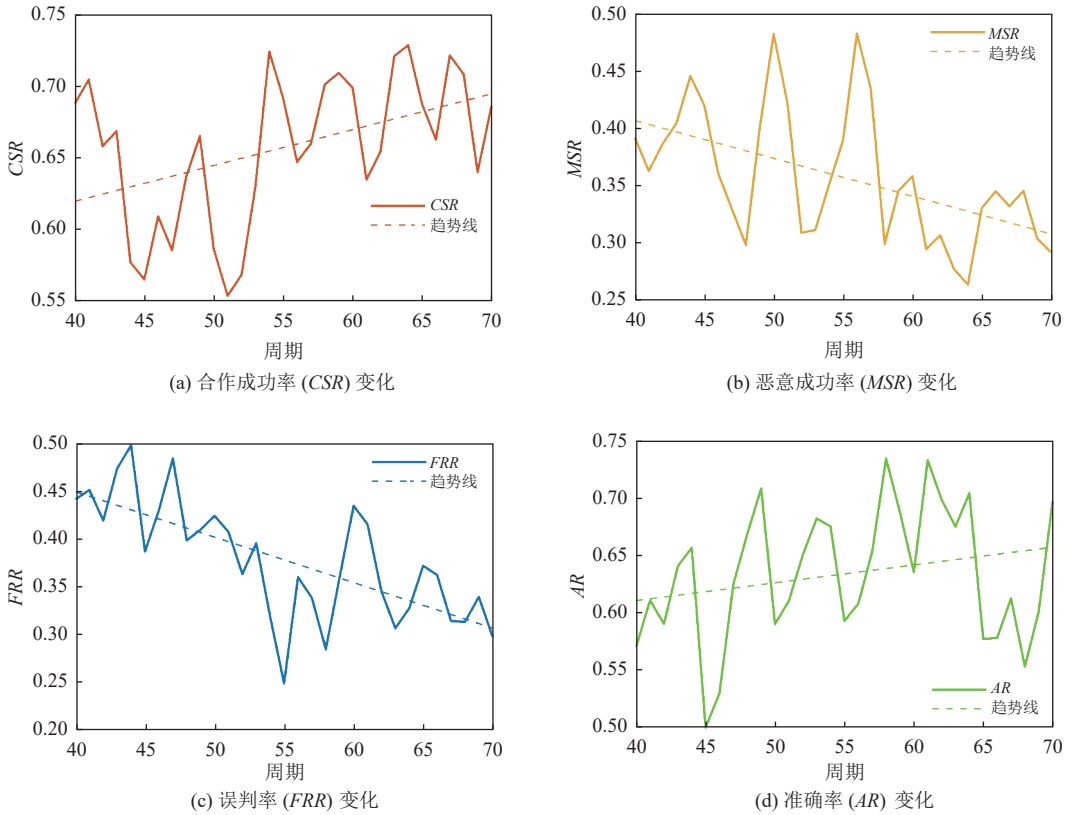
增加而动态调整, 并且与“正常访问”概率和“允许访问”概率的变化紧密相关. 以上结果验证了基于博弈的可信动态访问控制模型能够根据实际访问情况动态调整奖惩值和阈值, 从而实现更精准的访问控制决策.



(a) 主客体授权阀值的变化趋势 (b) 正常访问概率X与阈值th_S的关系 (c) 允许访问概率Y与阈值th_O的关系

图 18 演化博弈模型动态变化图

系统的性能指标变化如图 19 所示, 图中分别展示了系统的性能指标: 合作成功率 (*CSR*)、恶意成功率 (*MSR*)、误判率 (*FRR*) 以及准确率 (*AR*) 的变化情况, 其中合作成功率和准确率均大于 0.5, 恶意成功率和误判率均小于 0.5, 合作成功率和准确率越高且恶意成功率和误判率越低的系统性能更好. 如图 19 所示, 合作成功率和准确率有一定的上升趋势, 恶意成功率和误判率有下降趋势, 这表明通过合理地调整对主客体奖惩力度以及定期更新授权阈值能够有效地提高系统性能, 降低恶意事件和误判事件的发生概率.



(a) 合作成功率 (*CSR*) 变化 (b) 恶意成功率 (*MSR*) 变化

(c) 误判率 (*FRR*) 变化 (d) 准确率 (*AR*) 变化

图 19 系统性能指标变化趋势

7.3 功能对比

本方案与方案 [7,15,18,19,21,23] 在功能上进行了对比, 结果如表 9 所示, 表中“—”表示方案中没有涉及, “√”

表示方案具有此特性或功能, “×”表示方案不具有此特性或功能. 所有方案均为动态访问控制方案, 实现了对动态网络环境的适应性. 其中, 本方案与方案 [18,23] 将基于属性访问控制模型作为基础模型, 而方案 [7] 则以基于风险的访问控制模型作为基础模型. 此外, 本方案与方案 [7,18,23] 均采用 XACML 框架作为基础流程框架, 确保了访问控制策略的标准化和可扩展性.

表 9　各方案功能性对比

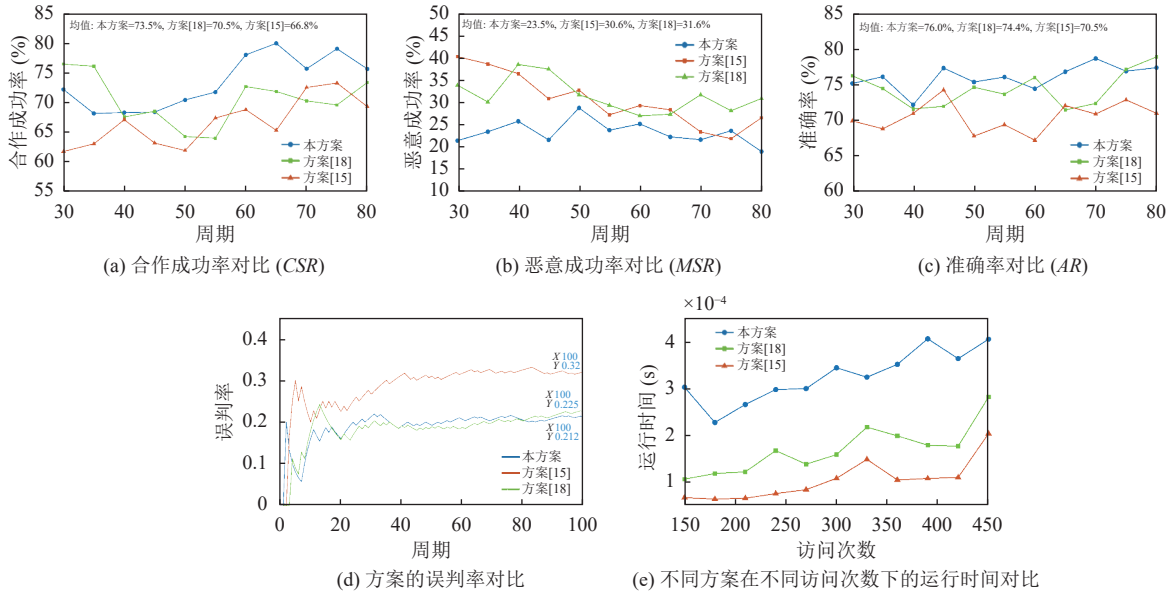
方案	基础模型	博弈论	主动性	动态性	评价标准	奖惩机制	动态阈值
本文方案	ABAC	演化博弈+不完全信息静态博弈	√	√	信任概率	√	√
方案[7]	RBACM	演化博弈	√	√	风险度量	×	×
方案[15]	—	完全信息静态博弈	√	√	评估值	×	×
方案[18]	ABAC	完全信息静态博弈	√	√	信任值	×	×
方案[19]	—	不完全信息动态博弈	√	√	评估值	√	×
方案[21]	—	完全信息静态博弈	√	√	信任值	×	×
方案[23]	ABAC	—	×	√	信任值	—	—

在访问控制技术与博弈论结合方面, 现有的多数文献 (如文献 [18,21]) 均基于文献 [10,15] 中所提出的访问控制博弈技术框架, 将完全信息静态博弈与访问控制结合以确定授权阈值, 而方案 [7] 则考虑参与者有限理性的情况下, 采用演化博弈论与访问控制技术结合确定授权阈值, 方案 [19] 采取不完全信息动态博弈来实现基于博弈的访问控制. 而本方案创新性地融合“可信评估-动态调整-访问决策”的三层协同机制, 从长期稳定和短期决策双重角度, 基于演化博弈和不完全信息静态博弈论, 实现主动且动态的访问控制框架. 具体而言, 将演化博弈论视为从长期稳定角度对有限理性的访问主体和客体进行分析的理论依据, 通过动态调节对主客体的奖惩值, 引导模型向理想状态演化, 并且根据演化博弈分析结果周期性地更新对访问主体进行授权的阈值; 将信任预测概率值作为不完全信息结合贝叶斯静态博弈模型, 从短期决策角度刻画访问主体与访问客体之间的策略博弈, 实现对访问主体的精准授权. 本方案和方案 [19] 均在访问控制博弈模型中引入了奖惩激励机制, 不同之处在于, 方案 [19] 通过实时评估节点的信任状态来驱动奖惩机制的动态更新, 而本方案从长期稳定角度出发, 通过演化博弈分析动态调整奖惩激励机制, 实现授权阈值的动态调整, 并利用纳什均衡反馈更新访问主体的信任概率. 总体而言, 本方案在功能上更为全面, 能够通过长期演化和短期博弈实现动态更新信任概率、调整奖惩机制和授权阈值, 实现了细粒度的动态精准授权.

本文方案和方案 [15,18] 均基于文献 [10] 中所提出的访问控制博弈技术框架, 结合博弈论和访问控制技术, 实现访问客体对访问主体的访问控制决策. 方案 [7] 通过风险度量作为评价标准与本文采用度量方法不同, 方案 [19,21] 不是以基于属性的访问控制模型作为基础模型, 方案 [23] 没有将博弈论引入的访问控制模型中, 所以方案 [15,18] 与本文方案在研究方法和技术路线上更为相似, 因此选择方案 [15,18] 作为对比方案, 能更准确地评估本文方案的性能.

将本文方案与方案 [15,18] 在系统性能指标以及运行时间方面进行对比. 仿真实验涵盖了 100 个连续实验周期 (每个周期 10 次访问行为), 通过计算各周期的合作成功率 (*CSR*)、恶意成功率 (*MSR*) 以及准确率 (*AR*) 来评估系统的性能. 为清晰展示趋势, 实验数据取第 30–80 周期, 并将每 5 个周期的指标均值作为一个数据点进行绘图. 本文方案与方案 [15,18] 的合作成功率如图 20(a) 所示, 3 个方案的 *CSR* 均呈上升趋势, 本方案的 CSR 均值为 73.5%, 方案 [18] 的 *CSR* 均值为 70.5%, 方案 [15] 的 *CSR* 均值为 66.8%, 这一优势主要源于本方案能够根据群体行为的历史演化, 自适应地调整激励力度与授权阈值, 相较于对比方案中相对静态的参数设置本方案能更有效地促进主客体之间的合作. 本文方案与方案 [15,18] 的恶意成功率如图 20(b) 所示. 总体而言, 3 个方案的 *MSR* 均有下降趋势, 这反映出博弈论方法在抑制恶意访问行为方面的普遍有效性. 在图 20(b) 中, 本方案的 *MSR* 均值为 23.5%, 方案 [18] 的 *MSR* 均值为 31.6%, 方案 [15] 的 *MSR* 均值为 30.6%, 说明动态调整奖惩机制和授权阈值能有效减少和拦截恶意访问, 增强了系统的自适应能力. 本文方案与方案 [15,18] 的准确率如图 20(c) 所示, 3 个方案的 *AR* 均有上升趋势, 这表明结合博弈的访问控制技术能够有效减少访问客体允许“恶意访问”和拒绝“正常访

问”的比例. 在图 20(c) 中, 本方案的 *AR* 均值为 76.0%, 方案 [18] 的 *AR* 均值为 74.4%, 方案 [15] 的 *AR* 均值为 70.5%. 本方案准确率较高的原因是通过将演化博弈与贝叶斯博弈的结合, 能实现自适应调整策略的同时又根据信任状态进行精准授权. 模拟 100 个周期一个主体的访问行为, 通过计算周期内的误判率来评判系统决策的准确性. 不同方案的 FRR 对比如图 20(d) 所示, 3 个方案的 *FRR* 都是短期内增加但后期趋于稳定, 本文方案的 FRR 收敛于 21.2%, 方案 [15] 的 *FRR* 收敛于 32%, 方案 [18] 的 *FRR* 收敛于 22.5%. 这说明在访问控制博弈模型中通过动态调整奖惩机制和授权阈值可有效降低访问客体拒绝正常访问的概率.



(a) 合作成功率对比 (*CSR*) (b) 恶意成功率对比 (*MSR*) (c) 准确率对比 (*AR*)

(d) 方案的误判率对比 (e) 不同方案在不同访问次数下的运行时间对比

图 20 方案功能对比

各方案运行时间对比如图 20(e) 所示, 随着访问次数的增加 3 个方案的运行时间均有增加, 本文方案运行时间在 0.343 ms 左右, 方案 [15] 运行时间约在 0.115 ms 左右, 方案 [18] 运行时间在 0.19 ms 左右. 相较于其他方案本方案运行时间较长, 但本方案能实现访问控制模型的可信预测、动态调整以及精准授权的功能. 总体而言, 本文方案在系统性能指标方面优势明显, 但在运行效率上还需进一步优化. 未来研究可在确保模型动态调整奖惩机制和授权阈值基础上, 进一步探索提高访问控制效率的方法.

8 总 结

本文提出了基于博弈论的可信动态访问控制模型, 融合“可信评估-动态优化-访问决策”三层协同机制, 通过信任度预测模型计算访问主体的信任概率; 构建访问主客体之间的博弈动态调整模型, 通过定期更新收益函数, 结合演化博弈分析动态调整奖惩机制和授权阈值; 采用贝叶斯博弈建立实时决策模型, 以混合策略纳什均衡做出访问控制决策, 并通过均衡状态反馈更新信任度; 通过仿真实验和参数敏感性分析, 验证了模型参数的合理性及敏感参数的影响; 将本文方案与其他方案对比, 结果表明本文方案能够动态调整访问控制奖惩机制和授权阈值, 从而实现精准授权. 未来研究可以进一步探索如何提升模型的计算效率和资源利用率, 并在更多实际应用场景中验证其性能和可行性.

References

[1] The Central People’s Government of the People’s Republic of China. The Central Committee of the Communist Party of China and the State Council about building data base system better advice give play to the role of data elements. 2022 (in Chinese). https://www.gov.cn/zhengce/2022-12/19/content_5732695.htm

[2] National Data Administration. National data bureau about print and distribute “credible data space development action plan (2024–2028)”. 2024 (in Chinese). https://www.gov.cn/zhengce/zhengceku/202411/content_6996363.htm

[3] Halgamuge MN. Estimation of the success probability of a malicious attacker on blockchain-based edge network. Computer Networks, 2022, 219: 109402. [doi: 10.1016/j.comnet.2022.109402]

[4] He BZ, Feng T, Liu CY, Su CH. CD-BISHAC: Cross-domain scheme for blockchain-based industrial Internet of Things security hybrid access control. IEEE Internet of Things Journal, 2025, 12(6): 7164–7179. [doi: 10.1109/JIOT.2024.3492279]

[5] Aboukadri S, Ouaddah A, Mezrioui A. Machine learning in identity and access management systems: Survey and deep dive. Computers & Security, 2024, 139: 103729. [doi: 10.1016/j.cose.2024.103729]

[6] Aftab MU, Hamza A, Oluwasanmi A, Nie XY, Sarfraz MS, Shehzad D, Qin ZG, Rafiq A. Traditional and hybrid access control models: A detailed survey. Security and Communication Networks, 2022, 2022(1): 1560885. [doi: 10.1155/2022/1560885]

[7] Ding HF, Peng CG, Tian YL, Xiang SW. Privacy risk adaptive access control model via evolutionary game. Journal on Communications, 2019, 40(12): 9–20 (in Chinese with English abstract). [doi: 10.11959/j.issn.1000−436x.2019240]

[8] Shahraki AS, Rudolph C, Alavizadeh H, Kayes ASM, Rahayu W, Tari Z. Securing cross-domain data access with decentralized attribute-based access control. Ad Hoc Networks, 2025, 173: 103807. [doi: 10.1016/j.adhoc.2025.103807]

[9] Servos D, Osborn SL. Current research and open problems in attribute-based access control. ACM Computing Surveys (CSUR), 2017, 49(4): 1–45. [doi: 10.1145/3007204]

[10] Zhang YX, He JS, Zhao B, Zhu NF. A privacy protection model base on game theory. Chinese Journal of Computers, 2016, 39(3): 615–627 (in Chinese with English abstract). [doi: 10.11897/SP.J.1016.2016.00615]

[11] Zhang XM, Deng HT, Xiong ZG, Liu YC, Rao Y, Lyu Y, Li Y, Hou DL, Li YF. Secure routing strategy based on attribute-based trust access control in social-aware networks. Journal of Signal Processing Systems, 2024, 96(2): 153–168. [doi: 10.1007/s11265-023-01908-1]

[12] He GX, Li CL, Shu Y, Luo YL. Fine-grained access control policy in blockchain-enabled edge computing. Journal of Network and Computer Applications, 2024, 221: 103706. [doi: 10.1016/j.jnca.2023.103706]

[13] Hao XH, Ren W, Fei YY, Zhu TQ, Choo KKR. A blockchain-based cross-domain and autonomous access control scheme for Internet of Things. IEEE Trans. on Services Computing, 2023, 16(2): 773–786. [doi: 10.1109/TSC.2022.3179727]

[14] Gai KK, She YF, Zhu LH, Choo KKR, Wan ZG. A blockchain-based access control scheme for zero trust cross-organizational data sharing. ACM Trans. on Internet Technology, 2023, 23(3): 38. [doi: 10.1145/3511899]

[15] Zhang YX. Research on the key technology of the proactive access control based on game theory [Ph.D. Thesis]. Beijing: Beijing University of Technology, 2017 (in Chinese with English abstract).

[16] Ding HF, Peng CG, Tian YL, Xiang SW. A game theoretical analysis of risk adaptive access control for privacy preserving. In: Proc. of the 2019 Int’l Conf. on Networking and Network Applications (NaNA). Daegu: IEEE, 2019. 253–258. [doi: 10.1109/NaNA.2019.00052]

[17] Gao Y, Zhu ZL, Yang J. An evolutionary game analysis of stakeholders’ decision-making behavior in medical data sharing. Mathematics, 2023, 11(13): 2921. [doi: 10.3390/math11132921]

[18] Deng XH, Li BY, Zhang SW, Deng LM. Blockchain-based dynamic trust access control game mechanism. Journal of King Saud University-Computer and Information Sciences, 2023, 35(2): 702–725. [doi: 10.1016/j.jksuci.2023.01.010]

[19] Zhao B, Xiao CB, Zhang WY, Gu X. Incentive and restraint mechanism of rewards and punishment in access control based on game theory. Journal of Electronics & Information Technology, 2019, 41(4): 1002–1009 (in Chinese with English abstract). [doi: 10.11999/JEIT180406]

[20] Motepalli S, Jacobsen HA. Reward mechanism for blockchains using evolutionary game theory. In: Proc. of the 3rd Conf. on Blockchain Research & Applications for Innovative Networks and Services (BRAINS). Paris: IEEE, 2021. 217–224. [doi: 10.1109/BRAINS52497.2021.9569791]

[21] Zhang Y, Tian LQ, Wu ZN, Wu WX. Trust oriented dynamic access control game mechanism in cloud services. Journal of Chinese Computer Systems, 2021, 42(8): 1774–1779 (in Chinese with English abstract). [doi: 10.3969/j.issn.1000-1220.2021.08.032]

[22] Sun PJ. A tripartite game model of trust cooperation in cloud service. Computers & Security, 2021, 106: 102272. [doi: 10.1016/j.cose.2021.102272]

[23] Huang HX, Zhang JB, Hu J, Fu YF, Qin CG. Research on distributed dynamic trusted access control based on security subsystem. IEEE Trans. on Information Forensics and Security, 2022, 17: 3306–3320. [doi: 10.1109/TIFS.2022.3206423]

[24] Jiang R, Liu R, Zhang T, Ding WP, Tian SH. An electronic medical record access control model based on intuitionistic fuzzy trust. Information Sciences, 2024, 658: 120054. [doi: 10.1016/j.ins.2023.120054]

[25] Saxena UR, Alam T. Provisioning trust-oriented role-based access control for maintaining data integrity in cloud. Int’l Journal of System Assurance Engineering and Management, 2023, 14(6): 2559–2578. [doi: 10.1007/s13198-023-02112-x]

[26] Zhang YH, Deng RH, Xu SM, Sun JF, Li Q, Zheng D. Attribute-based encryption for cloud computing access control: A survey. ACM Computing Surveys (CSUR), 2020, 53(4): 83. [doi: 10.1145/3398036]

[27] Hasel Mehri G, Le TD, Cappers B, Hartog JD, Zannone N. WiP: Enhancing the comprehension of XACML policies. In: Proc. of the 29th ACM Symp. on Access Control Models and Technologies. San Antonio: ACM, 2024. 41–46. [doi: 10.1145/3649158.3657052]

[28] Ardagna CA, Bena N. XML-based access control languages. In: Jajodia S, Samarati P, Yung M, eds. Encyclopedia of Cryptography, Security and Privacy. Cham: Springer, 2025. 2803–2808. [doi: 10.1007/978-3-030-71522-9_833]

[29] Liu AD, Du XH, Wang N, Li SZ. Blockchain-based access control mechanism for big data. Ruan Jian Xue Bao/Journal of Software, 2019, 30(9): 2636–2654 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/5771.htm [doi: 10.13328/j.cnki.jos.005771]

[30] Barron EN. Game Theory: An Introduction. 3rd ed. Hoboken: John Wiley & Sons, 2024.

[31] Ahmad F, Shah Z, Al-Fagih L. Applications of evolutionary game theory in urban road transport network: A state of the art review. Sustainable Cities and Society, 2023, 98: 104791. [doi: 10.1016/j.scs.2023.104791]

[32] Osborne MJ, Rubinstein A. A Course in Game Theory. Cambridge: MIT Press, 1994.

[33] Yager RR. On ordered weighted averaging aggregation operators in multicriteria decisionmaking. IEEE Trans. on systems, Man, and Cybernetics, 1988, 18(1): 183–190. [doi: 10.1109/21.87068]

[34] Pan Jun S. A trust-game-based access control model for cloud service. Mobile Information Systems, 2020, 2020(1): 4651205. [doi: 10.1155/2020/4651205]

[35] Khalil HK. Lyapunov's stability theory. In: Baillieul J, Samad T, eds. Encyclopedia of Systems and Control. Cham: Springer, 2021. 1170–1174. [doi: 10.1007/978-3-030-44184-5_77]

[36] Hu H, Stuart Jr HW. An epistemic analysis of the Harsanyi transformation. Int'l Journal of Game Theory, 2002, 30(4): 517–525. [doi: 10.1007/s001820200095]

附中文参考文献

[1] 中共中央国务院关于构建数据基础制度更好发挥数据要素作用的意见. 2022. https://www.gov.cn/zhengce/2022-12/19/content_5732695.htm

[2] 国家数据局. 国家数据局关于印发《可信数据空间发展行动计划 (2024–2028 年)》的通知. 2024. https://www.gov.cn/zhengce/zhengceku/202411/content_6996363.htm

[7] 丁红发, 彭长根, 田有亮, 向淑文. 基于演化博弈的隐私风险自适应访问控制模型. 通信学报, 2019, 40(12): 9–20. [doi: 10.11959/j.issn.1000−436x.2019240]

[10] 张伊璇, 何泾沙, 赵斌, 朱娜斐. 一个基于博弈论的隐私保护模型. 计算机学报, 2016, 39(3): 615–627. [doi: 10.11897/SP.J.1016.2016.00615]

[15] 张伊璇. 基于博弈论的主动式访问控制关键技术研究 [博士学位论文]. 北京: 北京工业大学, 2017.

[19] 赵斌, 肖创柏, 张问银, 古雪. 基于博弈论的访问控制奖惩激励约束机制. 电子与信息学报, 2019, 41(4): 1002–1009. [doi: 10.11999/JEIT180406]

[21] 张艺, 田立勤, 毋泽南, 武文星. 云服务中面向信任的动态访问控制博弈机制. 小型微型计算机系统, 2021, 42(8): 1774–1779. [doi: 10.3969/j.issn.1000-1220.2021.08.032]

[29] 刘敖迪, 杜学绘, 王娜, 李少卓. 基于区块链的大数据访问控制机制. 软件学报, 2019, 30(9): 2636–2654. http://www.jos.org.cn/1000-9825/5771.htm [doi: 10.13328/j.cnki.jos.005771]

作者简介

周由胜, 博士, 教授, 博士生导师, CCF 专业会员, 主要研究领域为车载网络安全, 隐私计算, 人工智能安全, 网络攻击与防御.

鞠祯, 硕士生, 主要研究领域为访问控制, 博弈论.

左祥建, 博士, 讲师, CCF 专业会员, 主要研究领域为安全多方计算, 数据安全, 隐私保护.

刘媛妮, 博士, 教授, CCF 专业会员, 主要研究领域为移动人群感知, 物联网安全, IP 路由技术.