Modeling and Simulation 建模与仿真, 2024, 13(1), 576-587
Published Online January 2024 in Hans. https://www.hanspub.org/journal/mos
https://doi.org/10.12677/mos.2024.131056

Hans汉斯

区块链系统L-顽固策略的安全问题研究

黄　超[1]，刘　亚[1]，唐伟明[1]，任艳丽[2]

[1]上海理工大学光电信息与计算机工程学院，上海
[2]上海大学通信与信息工程学院，上海

收稿日期：2023年11月30日；录用日期：2023年12月25日；发布日期：2024年1月24日

摘　要

随着数字货币的诞生，区块链技术被广泛的运用在金融、物联网等各个领域。但同时也暴露出各种安全性问题，如数据层的碰撞攻击、网络层的日蚀攻击、共识层的贿赂攻击、应用层的顽固攻击等。为了保障区块链技术在实际应用系统中能安全运行，研究者针对不同威胁策略，提前分析以提高系统的安全强度。本文发现基于日蚀攻击的L-顽固策略在特定情况下存在更大的安全问题。为了进一步分析这种组合式策略对区块链系统的威胁，建立了L-贿赂顽固策略(LBSM)模型。该模型在原L-顽固策略中，再考虑贿赂策略，将部分挖矿收益当作贿款吸引其他节点在私链上工作，提高私链在分支竞争中的胜率，诚实节点将会遭受更多的损失。仿真实验表明：LBSM模型造成的损失高出原L-顽固策略3.76%。最后，针对LBSM策略安全问题，提出了一些相关检测和防御措施，以提高区块链系统整体安全性。

关键词

区块链，数字货币，顽固策略，安全问题，工作量证明

Researches on Security Issues of L-Stubborn Strategies in the Blockchain System

Chao Huang[1], Ya Liu[1], Weiming Tang[1], Yanli Ren[2]

[1]School of Computer Science and Engineering, University of Shanghai for Science and Technology, Shanghai
[2]School of Communication and Information Engineering, Shanghai University, Shanghai

Received: Nov. 30th, 2023; accepted: Dec. 25th, 2023; published: Jan. 24th, 2024

Abstract

Since the digital currency was proposed, blockchain technology has been widely used in various fields such as finance and the Internet of Things. At the same time, various security issues have been exposed, such as collision attacks at the data layer, eclipse attacks at the network layer, bri-

文章引用: 黄超, 刘亚, 唐伟明, 任艳丽. 区块链系统 L-顽固策略的安全问题研究[J]. 建模与仿真, 2024, 13(1): 576-587. DOI: 10.12677/mos.2024.131056

bery attacks at the consensus layer, and stubborn attacks at the application layer. In order to ensure the safe operation of blockchain technology in practical application systems, researchers analyze different threat strategies to improve the security of the system. In this paper, it is found that the L-stubborn strategy based on eclipse attacks has greater security risks in certain situations. In order to further analyze the threat of this combined strategy to the blockchain system, an L-bribery-stubborn strategy (LBSM) model was established. Under the original L-stubborn strategy, if the malicious nodes consider the bribery strategy again, using part of the mining revenue as a bribe to attract other nodes to work on the private chain and increase the winning rate of the private chain in the fork competition, honest nodes will suffer even greater damage. Simulation experiments show that the loss is 3.76% higher than the original L-stubborn strategy. Finally, for the security issues of the LBSM strategy, some relevant detection and defense measures have been proposed to improve the overall security of the blockchain system.

Keywords

Blockchain, Digital Currency, Security Issues, Stubborn Strategy, Proof of Work

1. 引言

随着区块链技术的日益发展，去中心化的加密货币受到广泛关注[1]。这些加密货币基于区块链技术[2]来保证其安全性，同时采用工作量证明共识机制(PoW, proof of work) [3]来实现双方交易的一致性与不可篡改性。节点通过消耗自身拥有的算力来解决特定的密码学问题，以此来发现新区块。当工作节点发现一个新区块后，会将其立刻广播至网络，由网络中其他节点来验证该区块的合法性，如果超过一定比例的节点验证通过，然后将该区块添加至主链的末端，再开启新的一轮工作。发现该合法区块的矿工将获得一定数额的奖励作为报酬。

区块链系统在设计之初，就考虑了安全性。该系统要求大多数节点需遵守诚实工作原则[4]，即发现新区块之后立刻公布至网络；只要节点拥有算力不超过全网一半，即不发动“51%攻击”[5]，那么整个网络就是安全的。但相关研究者表明恶意节点如果采取自私策略(selfish strategy) [6]、扣块策略(block withholding strategy) [7]、顽固策略(stubborn strategy) [8]等威胁策略，以获取不公平份额奖励，会较大地影响诚实节点的收益，严重地会导致整个区块链系统有效哈希能力降低，从而暴露在较大的安全威胁下。

贿赂策略(bribery strategy) [9]正是一种能够通过贿赂或租赁的方式让恶意节点在短期内拥有大量的哈希能力，并完成特定操作的攻击。目前相关策略的研究，只局限在贿赂策略与自私策略相结合，还未有贿赂策略与顽固策略相关分析，因此贿赂策略与顽固策略组合的模型存在潜在的安全问题。L-顽固策略中恶意节点的私链与诚实节点公链之间的竞争更加激烈。随着技术的不断改进，恶意节点可能将考虑多种威胁策略组合使用，破坏区块链系统的安全，因此研究者需要提前研究组合式威胁策略，对进一步评估区块链系统的安全性具有重要意义，并为区块链技术在实际系统中的安全应用提供强有力的保障。

本文旨在将贿赂策略与 L-顽固策略相结合，分析其中存在的安全问题，对诚实节点造成的影响，建立 L-贿赂顽固策略(LBSM, lead bribery selfish mining)相关模型，并对此威胁策略提出有效的检测和防御措施。主要工作内容如下：

1) L-顽固策略将私链上最后一个私有块公布时引入贿赂策略，建立 LBSM 状态机模型，作为理性的

节点，会选择对自己最优的分支进行工作，从而提高私链在此轮分支竞争中获胜的概率。

2) 从理论角度分析了 LBSM 策略相较于 L-顽固策略、LT-顽固策略、LF-顽固策略和贿赂自私策略(BSM, bribery selfish mining)的影响；然后通过仿真实验，将 LBSM 策略与这些策略等进行综合对比。实验结果表明：恶意节点的哈希算力(记为 α)在 0.27~0.3 之间且网络影响能力(记为 γ)大于 0.4 时，采取 LBSM 策略使诚实节点的损失比 L-顽固策略、LT-顽固策略、LF-顽固策略中最高时还多出 3.76%，比 BSM 策略最高时多出 1.81%。

3) 研究分析 LBSM 威胁策略的特点以及恶意节点需要触发的前提条件，提出一些检测、预防 LBSM 威胁策略的方案，提高区块链系统的安全性，为相关应用提供技术屏障，并展望区块链未来的安全工作。

2. 相关工作

近几年，许多国内外学者就攻击策略分析其对诚实节点安全问题的研究剧增。Nayak 等人[8]对顽固策略进行了详细划分并将多种威胁策略相结合，将其与网络层的日蚀策略[10]相结合，利用日蚀策略阻碍双方节点之间通信，进一步提高恶意节点的相对收益。在 Nayak 等人[8]研究的基础上，Zhang 等人[11]通过建立具体的模型表示出其中相关策略的收益，更加详细的计算出 Nayak 等人[8]研究中各种策略的获利比；Liu 等人[12]研究了以太坊中顽固策略对于叔块(uncle block)的影响，相较于前者，考虑了网络的拥塞率，降低了获利更多时所需算力的阈值。Wang 等人[13]将顽固策略的思想应用在以太坊系统上，得出恶意节点在以太坊上采取顽固策略获得的收益比诚实节点最高多出 46.9%。Bonneau 等人[9]首次研究贿赂策略的几种贿赂方式以及分析了通过贿赂策略可能会带来潜在的问题；在 Bonneau 等人研究[9]的基础上，Sun 等人[14]通过对贿赂模型采取定量分析方法，引入利润方式计算得出新模型可以降低贿赂策略的成本并增加其获得相对收益；Gao 等人[15]将贿赂策略适用于自私策略上，在降低恶意节点所需最低算力的基础，进一步提高其相对收益；Yang 等人[16]进一步与强化学习相结合，利用马尔科夫决策过程(MDP, Markov decision process)，得出每一种状态的最优选择，使获得的最终收益最大。

2.1. L-顽固策略

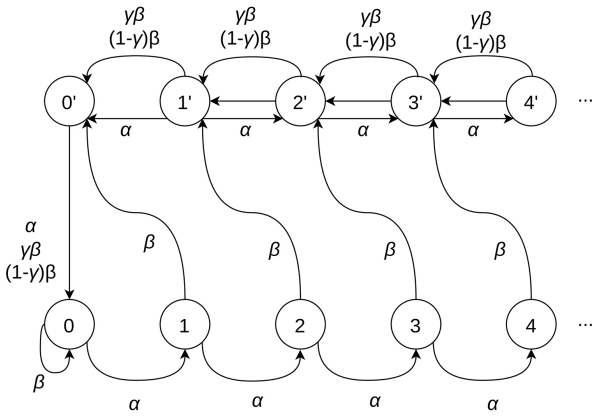

Figure 1. Diagram of L-stubborn strategy state transition
图 1. L-顽固策略状态转换关系图

L-顽固策略由自私策略衍变而来，为了追求更多的最终收益，攻击者在 L-顽固策略中，频繁且有意造成区块链分叉，与诚实节点之间的竞争更加激烈。例如，在自私策略中，如果恶意节点的私链上存有两个尚未公布的区块，此时诚实节点发现了下一个新区块，恶意节点将私链上两个隐藏的区块全部公布至网络，成为新的主链，获得相应奖励；然而相同情况下，恶意节点采取 L-顽固策略，每次只将私链上

第一个尚未公布的区块公布，继续造成区块链分叉，诚实节点陷入下一轮竞争，由于此时私链上还存有一个尚未公布的区块，只有诚实节点在本轮竞争中率先挖到下一个新区块，恶意节点才会将私链完全揭露，但区块链仍然处于分叉状态，诚实节点也依旧处于竞争状态。可见，相比于自私策略，L-顽固策略中，恶意节点与诚实节点之间的竞争更加频繁，恶意节点私链上存有多少个尚未公布的区块，就会导致区块链出现多少次分叉，出现分叉次数越多，对诚实节点造成的影响越大。L-顽固策略具体的状态转换关系如图 1 所示。

2.2. BSM 策略

在自私策略中，恶意节点的私链上仅存有一个隐藏的区块，此时诚实节点率先发现新区块，随后恶意节点将私链上隐藏区块公布至网络，网络中出现两条等长分支，此时率先延伸的分支将会被选为主链。将贿赂策略应用在这种情形，恶意节点将一部分的收益当作贿款发动贿赂攻击，吸引更多节点到自己所属分支上工作，增大私链上的总算力，提高在竞争中获胜概率。假定这部分接受贿款的节点为理性节点，理性节点始终采取获利最多的策略。因此在上述情况中，理性节点选择在恶意节点所属分支上工作，如果率先发现新区块，除了系统给予的区块奖励，还会获得额外的贿款，而理性节点在当前公链上工作并且率先发现新区块，只能够得到系统给予的区块奖励，因此理性矿工更愿意选择在私链上工作。

3. LBSM 模型设计与研究

3.1. 模型与假设

由最初自私策略到顽固策略中多种情形，再到自私策略与贿赂策略相结合，最后到顽固策略与贿赂策略相结合，共同目的都是为恶意节点带来更多的期望收益。而其中 BSM 策略是将自私策略与贿赂策略相结合，而 L-顽固策略是在自私策略的基础上改进得到的攻击策略，因此基于 BSM 策略的思想，将 L-顽固策略与贿赂策略相结合使用，进而提出 LBSM 策略。

在 LBSM 策略中，恶意节点提前在私链上隐藏挖到的区块，待诚实节点公布发现的区块时，仅将私链上第一个隐藏区块公布至网络，有意造成区块链分叉，致使恶意节点私链与诚实节点竞争成为新的主链。倘若恶意节点私链上还有隐藏的区块且其在当前竞争中落败诚实节点，继续将私链上第一个隐藏公布，区块链继续分叉，直到恶意节点将私链完全公布，双方依旧处于竞争状态，此时恶意节点发动贿赂策略，拿出一部分的收益当作贿款，吸引更多矿工到其私链上工作，从而增加恶意节点在最后一次竞争中获胜的概率。

由于 LBSM 策略结合了贿赂策略，需要考虑如下几个问题：1) 在考虑贿赂策略的时候，恶意节点需预设多少贿款；2) 当恶意节点自身的算力为多少时，触发攻击最为合理，倘若自身拥有的算力过小，虽然贿赂策略能够从一定程度上帮助恶意节点在竞争中取胜，但是最终获胜概率还是过小，效果适得其反；反之，如果自身拥有的算力过大，贸然实施贿赂策略将会导致最终收益相对减少。

为便于研究 LBSM 策略，首先确定模型中的角色以及前提假设。在 LBSM 策略中，一共定义了三种角色，即恶意节点、诚实节点与理性节点。恶意节点为了追求更多的最终收益，在 L-顽固策略中合适的时机考虑贿赂策略；诚实节点始终都采取诚实工作的策略，当区块链还未发生分叉时，始终选择在当前的主链上工作，一旦区块链发生分叉，由于诚实节点不能确定分叉中哪条分支能够最终成为主链，因此每条分支上都会出现部分的诚实节点；理性节点为了获得更多的收益，在恶意节点考虑贿赂策略之后，选择到私链上工作，在追求更多收益的同时增加了恶意节点在竞争中取胜的概率。如表 1 所示，为当前模型下的系统参数。

为了确保后续仿真实验结果的准确性，下面给出几个不失一般性的攻击假设：

1) 恶意节点和理性节点均取收益最优的策略；

2) 不考虑区块链系统中出现自然分叉的情况；

3) 在 LBSM 策略中，区块链分叉的情况仅由恶意节点与诚实节点之间竞争造成，不考虑理性节点造成区块链分叉；

4) 为了方便计算，将网络中的总哈希算力标准化为 1。

Table 1. System parameter
表 1. 系统参数

参数	含义
α	恶意节点拥有的总算力
β	诚实节点拥有的总算力
$\beta 1$	理性节点拥有的总算力，且 $\alpha + \beta + \beta^1 = 1$
ε	将部分的收益当作贿款发动贿赂攻击
$State = i$	私链领先公链 i 个区块，且未发生分叉
$State = i'$	私链领先公链 i 个区块，且发生分叉
γ	恶意节点的网络影响因子，即区块链分叉时，选择在其分支上工作的诚实节点的算力占比

3.2. 模型分析

首先给出 LBSM 策略中具体状态转换关系，如图 2 所示。图中数字表示恶意节点私链领先当前诚实节点主链区块个数，数字加上单引号表示区块链发生分叉时，恶意节点私链上隐藏区块的个数，两种状态之间的转换用单箭头表示，并且计算出对应的转换概率。

从图 2 可见，状态 0’到状态 0 之间的转换与恶意节点能否获得更多最终收益密切相关，且二者之间的转换有如下四种情形：(1) 恶意节点与诚实节点最后一次竞争成为主链时，恶意节点自身率先挖到下一个区块，并且马上公布至网络，此时私链成为新的主链，此种情况如图 3(a)所示；(2) 区块链发生了分叉，诚实节点不能够确定哪一条链将会在竞争中取胜，因此部分诚实节点选择到恶意节点私链上工作，且这部分诚实节点率先发现下一个区块，帮助恶意节点的私链在分支竞争中取胜，由于私链仍率先扩展，成为新的主链，此种情况如图 3(b)所示；(3) 与情况(2)相似，但不同的是，由选择在当前主链上工作的诚实节点率先发现下一个区块，当前主链在竞争中率先拓展，成为下一轮主链，且恶意节点在竞争中失败，不会获得奖励，此种情况如图 3(c)所示；(4) 恶意节点为了增大自身在竞争中取胜的概率，选择考虑贿赂策略，吸引更多矿工到私链上工作，增大私链上的总算力。由于这部分接受贿款的节点只选择到私链上工作，这部分节点能否获得更多收益与私链能否在此轮竞争中成为新的主链密切相关。此时由这部分节点率先发现下一个区块，私链率先延伸，成为新的主链[17]，此种情况如图 3(d)所示。在上述的四种情况中，第(1)、(2)、(4)三种情况均为恶意节点能够获得更多收益。四种情况中最后一次竞争结果如图 3 所示。

同时，针对图 2 中其他情况，也给出相应的解释说明。诸如从 $State = 2'$到 $State = 1'$的转换情况，由于此时并未到达最终竞争时刻，恶意节点不会考虑贿赂攻击，理性节点将会选择诚实工作策略，因此会出现如下两种情况：

情况 1：此轮竞争中，部分诚实节点率先在私链上发现新区块，由于此时私链上存有两个尚未公布的区块，恶意节点将私链上第一个尚未公布的区块公布，这将导致区块链继续分叉且私链上仍存有一个尚未公布的区块，此种情况的概率为 $\gamma(1-\alpha)$。

情形 2：此时部分诚实节点率先在公链上发现新区块，恶意节点将私链上第一个尚未公布的区块发布，在区块链分叉的同时，私链上仍旧保留一个未公布的区块，此种情况的概率为$(1-\gamma)(1-\alpha)$。

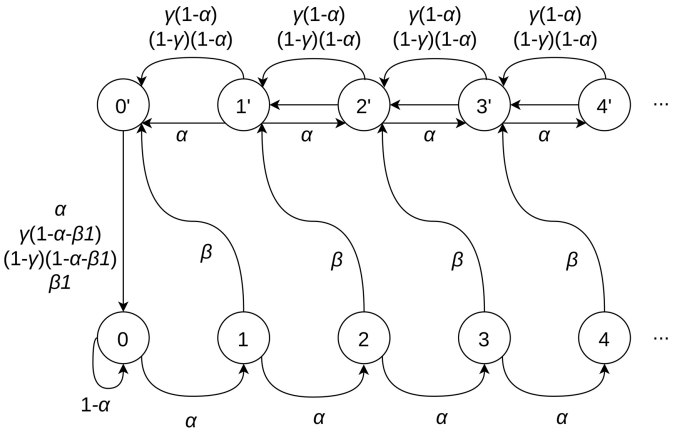

Figure 2. Diagram of LBSM strategy state transition
图 2. LBSM 策略状态转换关系图

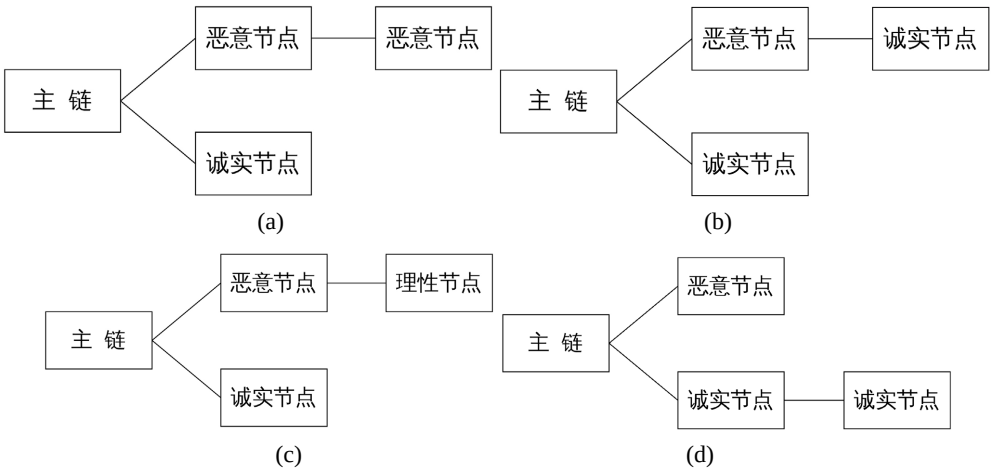

Figure 3. Transition from State = 0’ to State = 0 in LBSM strategy
图 3. LBSM 策略中从 State = 0’转换到 State = 0

无论出现情况 1 还是情况 2，此时区块链处于分叉状态且私链上还存有一个尚未公布的区块。图 4 表示上述两种情形，图中诚实节点率先在恶意节点私链上扩展为情形 1，率先在公链上扩展为情形 2。其中，实线矩阵表示为已公布区块，虚线矩阵表示为私链上还未公布的区块。

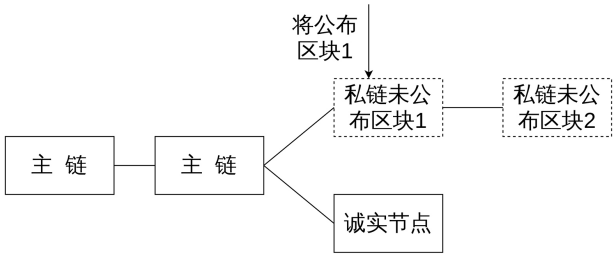

Figure 4. Transition from State = 2’ to State = 1’ in LBSM strategy
图 4. LBSM 策略中从 State = 2’转换到 State = 1’

4. 仿真实验

为得到恶意节点采取 LBSM 策略获益最多的区域空间，本文按照上图 2 中的逻辑关系编写了相应代码来实现，实验环境部署在 pycharm2021 以及 IntelliJ IDEA 2021 (Java)上，从恶意节点拥有的算力、恶意节点的网络影响因子，及贿赂策略能够吸引的理性节点的算力三个主要参数来进行实验操作。

本文选定攻击者拥有算力 $\alpha = 0.3$ 以及 $\varepsilon = 0.02$ 这两个特殊参数值(结合本文实验结果以及大量相关文献，选定 $\varepsilon = 0.02$ 最合适)。首先验证得到：确实存有某种特殊的情况，相较于其他攻击策略，恶意节点采取 LBSM 策略能够获得最多收益；然后综合研究多种参数值，最终得到符合条件的特定区域。

4.1. LBSM 策略与 L-顽固策略对比

由于 LBSM 策略是在 L-顽固策略的基础上结合贿赂策略，因此首先从理论上对比分析 LBSM 和 L-顽固策略。从前文图 1 以及图 2 中的状态转换关系可以得到，L-顽固策略中从状态 0’转换到状态 0 有三种可能情况，且发生的概率分别为 α，$\gamma\beta$，$(1-\gamma)\beta$；而 LSBM 策略中有四种转换关系，且发生的概率分别为 α，$\gamma(1-\alpha-\beta^1)$，$(1-\gamma)(1-\alpha-\beta^1)$，$\beta^1$。相比于 L-顽固策略，在 LBSM 策略中，恶意节点考虑贿赂攻击，增加其分叉竞争中的胜率。

接下来，利用仿真实验对比分析两种攻击策略的收益情况。首先研究恶意节点自身网络影响因子 γ 值对最终收益的影响，在设定 $\beta^1 = 0.1$，$\varepsilon = 0.02$ 的前提下，图 5 展示了恶意节点算力 $\alpha = 0.3$ 时，其能够获得的最终收益值。实验结果表明：当恶意节点网络影响因子 γ 小于 0.4 时，此时其采取 LBSM 策略获得的挖矿收益高于 L-顽固策略。

此外，研究理性节点总算力 β^1 取值对恶意节点最终收益的影响。在设定 $\alpha = 0.3$，$\varepsilon = 0.02$ 前提下，图 6 展示了 $\beta^1 = 0.05$ 以及 $\beta^1 = 0.15$ 时，恶意节点能获得的最终收益值。实验结果表明：当 γ 小于 0.4 时，恶意节点考虑贿赂策略吸引的理性节点算力越大，得到的最终收益就越多；当 γ 超过 0.4 时，由于恶意节点在竞争中取胜概率相对较大，此时再考虑贿赂策略，需将一部分的收益当作贿款给予理性节点，虽然能够从一定程度上增加最终取胜概率，但导致获得最终收益值减少。

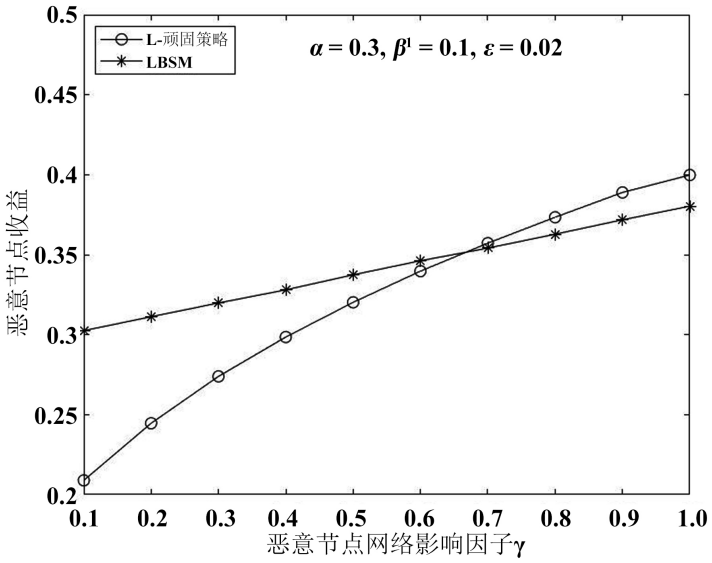

Figure 5. The impact of malicious node computing power on its revenue in LBSM strategy
图 5. LBSM 策略中恶意节点算力对其收益的影响

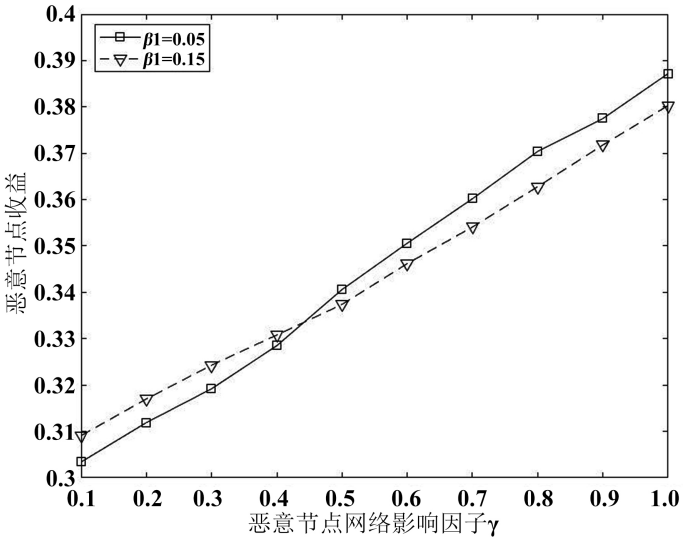

Figure 6. The impact of rational node computing power on its revenue in LBSM strategy
图 6. LBSM 策略中理性节点算力对其收益的影响

Table 2. Whenα = 0.3, β^1 = 0.1, ε = 0.02, the revenue of malicious nodes
表 2. 当 α = 0.3，β^1 = 0.1，ε = 0.02 时，恶意节点的收益

γ	LBSM 策略	L/LF/LT-顽固策略中最大收益
0.4	0.3280	0.3161
0.5	0.3374	0.3269
0.6	0.3462	0.3422
0.7	0.3541	0.3676
0.8	0.3628	0.3900
0.9	0.3718	0.4103
1.0	0.3793	0.4289

4.2. LBSM 策略与 LF/LT-顽固策略对比

在顽固策略中，L-顽固策略不仅能够单独使用而且还能结合 F-顽固策略形成 LF-顽固策略或 T-顽固策略形成 LT-顽固策略一同使用。接下来，将 LBSM 策略与 LF-顽固策略以及 LT-顽固策略进行比较。在设定 α = 0.3，β^1 = 0.1，ε = 0.02 的前提下，表 2 展现了不同恶意节点自身网络影响因子 γ 值对最终收益的影响。由表 2 可知：在上述设定参数的前提下，当 $0.4 \le \gamma \le 0.6$ 时，恶意节点采取 LBSM 策略获得更多的收益，且比相同情况下 L/LF/LT-顽固策略中最多收益值还要高出 3.76%；但是一旦 γ 取值超过 0.6，此时恶意节点采取 LBSM 策略获得的收益少于 L-顽固策略或其结合策略。

4.3. LBSM 策略与 BSM 策略对比

BSM 策略结合了自私策略与贿赂策略，同时 LBSM 策略结合了 L-顽固策略与贿赂策略；二者都结合了贿赂策略且 L-顽固策略是自私策略衍生的一种攻击策略。基于上述这几点，对于 LBSM 与 BSM 策略进行全面的比较。

Nayak 等人[8]中的实验结果已经验证了恶意节点采取 L-顽固策略获得的收益始终多于自私策略的特

定区域。下面将验证存在 LBSM 策略始终胜于 BSM 策略的特定区域。首先研究恶意节点自身网络影响因子 γ 值对这两种结合策略最终收益的影响。在设 $\beta^1 = 0.1$，$\varepsilon = 0.02$ 的前提下，图 7 分别展示了恶意节点拥有的算力 $\alpha = 0.31$、$\alpha = 0.32$ 以及 $\alpha = 0.33$ 时，γ 值对其最终收益的影响。

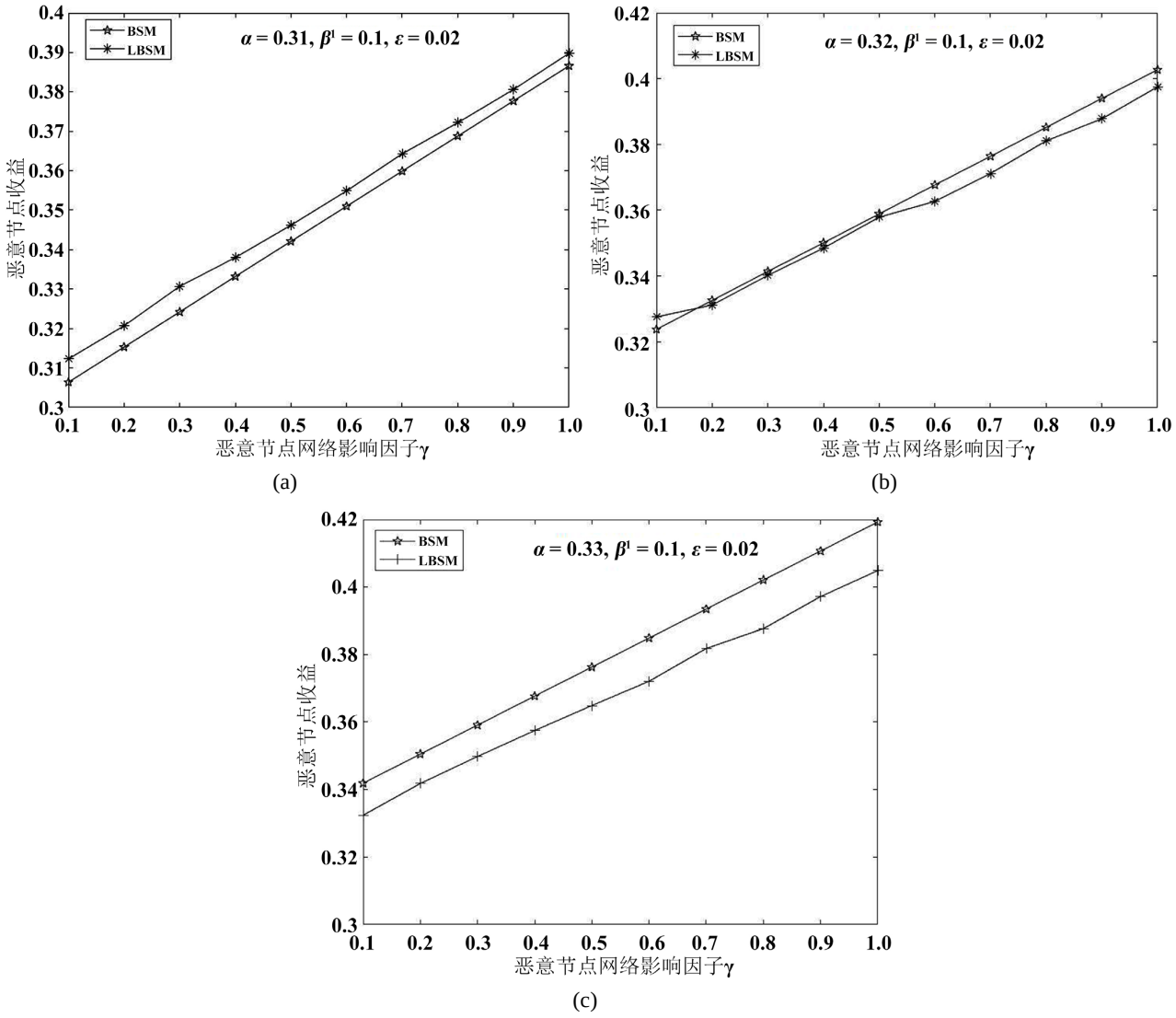

Figure 7. The impact of γ on the revenue of malicious nodes in LBSM and BSM strategies
图 7. LBSM 和 BSM 策略中 γ 对恶意节点收益的影响

实验结果表明：当 $\alpha = 0.31$ 时，无论 γ 取值，LBSM 策略始终都优于 BSM 策略；而当 $\alpha = 0.32$ 时，当且仅当 $\gamma < 0.2$ 时，LBSM 策略能为恶意节点带来更多收益；而当 $\alpha = 0.33$ 时，此时恶意节点采取 BSM 策略获得收益值更多。由此可见，在设定合理参数的前提下，存在特定区域使得恶意节点采取 LBSM 策略获得最终收益高于贿赂自私策略。

接下来，研究理性节点总算力 β^1 值对这两种结合策略最终收益的影响。表 3 和表 4 分别表示 $\beta^1 = 0.1$ 以及 $\beta^1 = 0.15$ 时，这两种策略的最终收益情况。从两表中可知，当 $\alpha = 0.31$ 且 $\gamma < 0.5$ 时，无论 $\beta^1 = 0.1$ 或 $\beta^1 = 0.15$，LBSM 策略几乎始终胜于 BSM 策略；而一旦 $\alpha = 0.32$ 且 $\gamma < 0.5$ 时，结果却恰恰相反，此时恶意节点采取 BSM 策略始终获得更多收益值。

通过对这两个参数进行定性以及定量的对比可知，当 $\alpha < 0.31$ 且 γ 取值为 0.5 左右时，LBSM 策略为恶意节点带来的最终收益始终高于 BSM 策略。

Table 3. When $\beta^1 = 0.1$, the revenue of malicious nodesadopting BSM and LBSM strategies
表 3. 当 $\beta^1 = 0.1$ 时，恶意节点采取 BSM 和 LBSM 策略的收益

α	γ	BSM 策略	LBSM 策略
0.31	0.1	0.3064	0.3123
0.31	0.3	0.3242	0.3307
0.31	0.5	0.3421	0.3462
0.32	0.1	0.3419	0.3324
0.32	0.3	0.3591	0.3498
0.32	0.5	0.3763	0.3649

Table 4. When $\beta^1 = 0.15$, the revenue of malicious nodes adopting BSM and LBSM strategies
表 4. 当 $\beta^1 = 0.15$ 时，恶意节点采取 BSM 和 LBSM 策略的收益

α	γ	BSM 策略	LBSM 策略
0.31	0.1	0.3105	0.3249
0.31	0.3	0.3268	0.3272
0.31	0.5	0.3431	0.3428
0.32	0.1	0.3279	0.3348
0.32	0.3	0.3439	0.3383
0.32	0.5	0.3599	0.3538

4.4. 多种策略对比

为了能够直观的表达出 LBSM 策略能够为恶意节点提供最多收益的特定区域，将上述所有实验结果统一整合，如图 8 所示。图中不同颜色分别代表了不同的挖矿策略，相同颜色构成的区域表示攻击者的 α 以及 γ 取值在该区域中时，能够获得最多的挖矿收益。由图 8 可得，当恶意节点的算力取值为 0.3 附近且自身网络影响因子取值为 0.5 附近时，其采取 LBSM 策略能够获得最多收益。

4.5. 检测与防御

恶意节点利用组合式的攻击策略获取更多额外奖励的方式显然破坏了系统的公平性，为保证系统中每个节点的合法的利益，同时降低甚至杜绝恶意节点不公平行为的发生。下面给出一些检测以及防御 LBSM 策略的方法，具体如下：

1) 记录节点的哈希算力：由图 8 可知，恶意节点采取 LBSM 策略获得更多收益时，所需算力至少为全网算力的 27%。因此，节点在进入矿池挖矿前，由该矿池管理者记录所有节点拥有的其是否存在恶意行为，一旦发现作恶行为即可将其驱逐出矿池。

2) 对比分叉率：由于在区块链系统中，发生自然分叉的概率微乎其微，因此当系统出现分叉时，计算出此时分叉率，对比当前系统能够容忍的最大分叉率，一旦超过最大分叉率，则对该分支上所有的节点进行逐一排除，直到将恶意节点排除出矿池。

3) 设立奖惩机制[18]：系统中的节点根据智能合约[19] [20] [21]采用积分信誉机制。节点们之间相互

监督，例如节点 A 发现节点 B 的恶意行为，节点 A 立刻告知系统，然后系统检查节点 B 的行为，如确实存在恶意行为，则惩罚节点 B，扣除相应的积分，同时增加节点 A 的相应积分；一段时间后，系统将积分低于某个阈值的节点驱逐，禁止该节点参与工作。

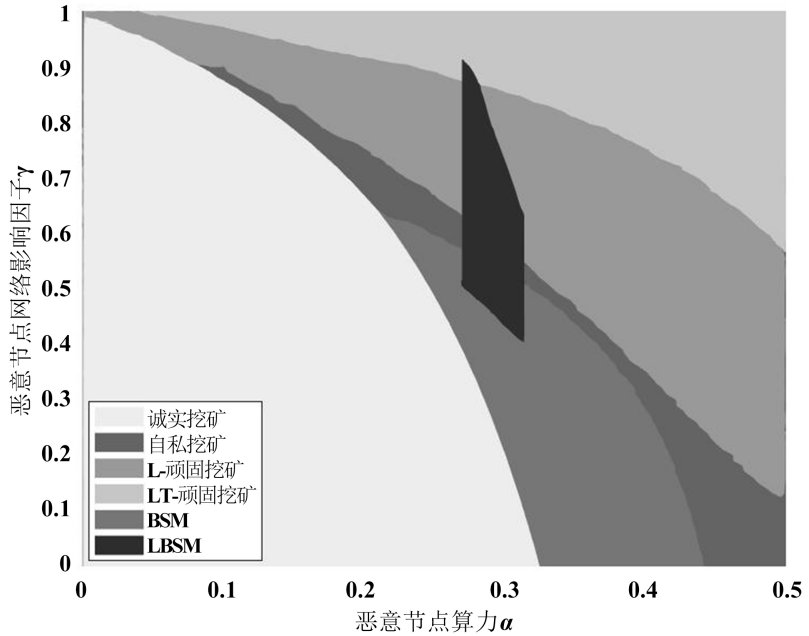

Figure 8. Comparison of multiple strategies
图 8. 多种策略对比

5. 总结与展望

本文发现基于日蚀攻击的 L-顽固策略在特定情况下存在更大的安全问题。恶意节点在原 L-顽固策略的基础上，再结合贿赂策略，短期内提高其在私链分支上竞争的优势，从而能造成诚实节点更大的损失，最高可超过原 L-顽固策略的 3.76%。本文将此类组合式策略称为 LBSM 威胁策略，并通过理论和实践与其它威胁策略综合对比，证明存在上述安全问题。为维护区块链系统的安全性以及稳定性，本文还提出了 3 种检测和防御手段，即，通过记录并检查哈希算力超过全网 27%的节点的行为、检测分叉率异常等手段剔除恶意节点，并根据智能合约设置奖惩机制鼓励所有节点正常工作。最后，在未来的工作中，为防止此类安全问题的发生，将进一步研究有效的防护方案，构建更完善、稳定的区块链系统。

参考文献

[1] Nakamoto, S. (2008) Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

[2] Nofer, M., Gomber, P., Hinz, O. and Schiereck, D. (2017) Blockchain. *Business & Information Systems Engineering*, **59**, 183-187. https://doi.org/10.1007/s12599-017-0467-3

[3] Kiayias, A. and Zindros, D. (2020) Proof-of-Work Sidechains. In: Bracciali, A., Clark, J., Pintore, F., Rønne, P. and Sala, M., Eds., *FC* 2019: *Financial Cryptography and Data Security*, Springer, Cham, 21-34. https://doi.org/10.1007/978-3-030-43725-1_3

[4] Jiang, N., Xu, D., Zhou, J., *et al*. (2020) Toward Optimal Participant Decisions with Voting-Based Incentive Model for Crowd Sensing. *Information Sciences*, **512**, 1-17. https://doi.org/10.1016/j.ins.2019.09.068

[5] Ye, C., Li, G., Cai, H., *et al*. (2018) Analysis of Security in Blockchain: Case Study in 51%-Attack Detecting. 2018 5*th International Conference on Dependable Systems and Their Applications* (*DSA*), Dalian, 22-23 September 2018, 15-24. https://doi.org/10.1109/DSA.2018.00015

[6] Eyal, I. and Sirer, E.G. (2014) Majority Is Not Enough: Bitcoin Mining Is Vulnerable. In: Christin, N. and Safavi-Naini, R., Eds., *FC* 2014: *Financial Cryptography and Data Security*, Springer, Berlin, 436-454. https://doi.org/10.1007/978-3-662-45472-5_28

[7] Bag, S., Ruj, S. and Sakurai, K. (2016) Bitcoin Block Withholding Attack: Analysis and Mitigation. *IEEE Transactions on Information Forensics and Security*, **12**, 1967-1978. https://doi.org/10.1109/TIFS.2016.2623588

[8] Nayak, K., Kumar, S., Miller, A. and Shi, E. (2016) Stubborn Mining: Generalizing Selfish Mining and Combining with an Eclipse Attack. 2016 *IEEE European Symposium on Security and Privacy* (*EuroS&P*), Saarbruecken, 21-24 March 2016, 305-320. https://doi.org/10.1109/EuroSP.2016.32

[9] Bonneau, J. (2016) Why Buy When You Can Rent? In: Clark, J., Meiklejohn, S., Ryan, P., Wallach, D., Brenner, M. and Rohloff, K., Eds., *FC* 2016: *Financial Cryptography and Data Security*, Springer, Berlin, 19-26. https://doi.org/10.1007/978-3-662-53357-4_2

[10] Marcus, Y., Heilman, E. and Goldberg, S. (2018) Low-Resource Eclipse Attacks on Ethereum's Peer-to-Peer Network. https://eprint.iacr.org/2018/236

[11] Zhang, Y., Zhao, M., Li, T., *et al*. (2023) Achieving Optimal Rewards in Cryptocurrency Stubborn Mining with State Transition Analysis. *Information Sciences*, **625**, 299-313. https://doi.org/10.1016/j.ins.2022.12.093

[12] Liu, Y., Hei, Y., Xu, T. and Liu, J.W. (2020) An Evaluation of Uncle Block Mechanism Effect on Ethereum Selfish and Stubborn Mining Combined with an Eclipse Attack. *IEEE Access*, **8**, 17489-17499. https://doi.org/10.1109/ACCESS.2020.2967861

[13] Wang, Z., Liu, J., Wu, Q., *et al*. (2019) An Analytic Evaluation for the Impact of Uncle Blocks by Selfish and Stubborn Mining in an Imperfect Ethereum Network. *Computers & Security*, **87**, Article ID: 101581. https://doi.org/10.1016/j.cose.2019.101581

[14] Sun, H., Ruan, N. and Su, C. (2020) How to Model the Bribery Attack: A Practical Quantification Method in Blockchain. In: Chen, L., Li, N., Liang, K. and Schneider, S., Eds., *Computer Security—ESORICS* 2020, Springer, Cham, 569-589. https://doi.org/10.1007/978-3-030-59013-0_28

[15] Gao, S., Li, Z., Peng, Z. and Xiao, B. (2019) Power Adjusting and Bribery Racing: Novel Mining Attacks in the Bitcoin System. *Proceedings of the* 2019 *ACM SIGSAC Conference on Computer and Communications Security*, London, 11-15 November 2019, 833-850. https://doi.org/10.1145/3319535.3354203

[16] Yang, G., Wang, Y., Wang, Z., *et al*. (2020) IPBSM: An Optimal Bribery Selfish Mining in the Presence of Intelligent and Pure Attackers. *International Journal of Intelligent Systems*, **35**, 1735-1748. https://doi.org/10.1002/int.22270

[17] 曾诗钦, 霍如, 黄韬, 等. 区块链技术研究综述: 原理, 进展与应用[J]. 通信学报, 2020, 41(1): 134-151.

[18] 田国华, 胡云瀚, 陈晓峰. 区块链系统攻击与防御技术研究进展[J]. 软件学报, 2021, 32(5): 1495-1525.

[19] 贺海武, 延安, 陈泽华. 基于区块链的智能合约技术与应用综述[J]. 计算机研究与发展, 2018, 55(11): 2452-2466.

[20] 钱鹏, 刘振广, 何钦铭, 等. 智能合约安全漏洞检测技术研究综述[J]. 软件学报, 2022, 33(8): 3059-3085.

[21] 江沛佩, 王骞, 陈艳姣, 等. 区块链网络安全保障: 攻击与防御[J]. 通信学报, 2021, 42(1): 151-162.