面向 RAFT 共识的低能耗无线区块链分片算法

罗皓翔[1]，孙 罡[1*]，雷 波[2]

（1. 电子科技大学 光纤传感与通信教育部重点实验室，成都 611731；2. 中国电信股份有限公司研究院，北京 102209）

摘要 区块链系统由于共识协商需要多轮沟通，会消耗大量的能量。在一些无线网络中，节点电池容量有限，会迅速导致节点能量耗尽和脱机，从而影响共识性能。该文设计了一种面向 RAFT 共识的低能耗的分片算法，算法将无线区块链网络中的节点限制在基于地理区域的分片上，从而避免节点参与全局共识。同时，还提出了一种分片后的能耗估算方法，简化了分片无线区块链网络的能量计算。在太赫兹和毫米波两个信号场景中得到的仿真结果均验证了该算法的有效性，能耗可降低 98.36%，估算方法的最小误差仅为 0.40%。

关键词 无线区块链网络；RAFT 共识；分片；低能耗

中图分类号 TN915 **文献标志码** A DOI 10.12178/1001-0548.2023189

A Low-Energy-Consumption Wireless Blockchain Sharding Algorithm for RAFT Consensus

LUO Haoxiang[1], SUN Gang[1*], and LEI Bo[2]

(1. Key Lab of Optical Fiber Sensing and Communications, University of Electronic Science and Technology of China, Chengdu 611731, China;
2. China Telecom Corporation Limited Research Institute, Beijing 102209, China)

Abstract Blockchain shows great potential in wireless network scenarios due to its security features. It establishes trust and consistency between system nodes without the trusted central authority. However, blockchain systems tend to consume a lot of energy, as many rounds of communication are required for consensus. In some wireless networks, the limited capacity of node batteries can quickly lead to node power depletion and offline, which can affect consensus performance. In addition, when the network is large, the huge energy consumption can also limit the scalability of the blockchain. Therefore, a low-energy-consumption sharding algorithm for RAFT consensus is designed to minimize the energy overhead in this paper. This algorithm restricts nodes to specific shards based on their geographic location, thereby avoiding nodes participating in a global consensus. Meanwhile, this paper also proposes an energy consumption estimation method to simplify the energy calculation of sharded wireless blockchain networks. The simulation results show that the proposed algorithm is effective. The energy consumption can be reduced by 98.36%, and the minimum error of the estimation method is only 0.4%.

Key words wireless blockchain network; RAFT consensus; sharding; low energy consumption

密码学和共识的集成助力了区块链的兴起和发展，这一开创性的分布式系统，具有去中心化的架构和强大的防篡改能力。因此，区块链拥有巨大的潜力彻底革新未来的信息和数据共享方式。此外，区块链技术在信息通信领域的应用也有望增强无线网络的安全性[1-3]。同时，区块链的使用也日益渗透到其他网络领域，如物联网[4]、医疗物联网[5]、车联网[6] 等。

区块链中的共识机制是允许网络中的节点在没有可信第三方的情况下建立信任的基础。主要的共识机制包括工作量证明[7]、权益证明[8]、实用拜占庭容错[9] 等。其中，RAFT 共识[10] 是联盟链和私有链中主要使用的共识算法，能提供网络 1/2 的容错性，即最多允许 $(n-1)/2$ 个故障节点，n 为节点总数。这些特性使它对未来的无线网络很有吸引力。然而，RAFT 中的多轮通信会产生巨大的能量开

收稿日期：2023−07−11；修回日期：2023−08−12
基金项目：四川省自然科学基金（2022NSFSC0913）
作者简介：罗皓翔，博士生，主要从事区块链共识、无线区块链网络方面的研究。
*通信作者 E-mail: gangsun@uestc.edu.cn

销，难以部署在电池容量有限的场景中，如无人机网络和智能安防等。同时，由文献 [11] 的结果可知，RAFT 的能耗随节点数目呈平方增长趋势。因此，能量消耗也会限制 RAFT 共识无线网络的可扩展性。

目前，分片技术是解决区块链可扩展性问题的有效手段[12]。文献 [13] 提出了一种基于节点信任的分片方案，避免了某个分片中出现过多的恶意节点。文献 [14-15] 设计了一种用于跨分片交易的分层分片方案，称为 Pyramid。文献 [16] 分析了 PBFT 的交叉分片和非交叉分片的安全性。文献 [17] 提出了 OmnilLedger，一种新的横向扩展分布式账本，可以在非许可操作的情况下保持区块链的安全性。文献 [18] 设计了一款基于演化博弈的分片算法。然而，现有的大部分分片方案都是针对区块链的共识吞吐量或通信开销而设计的，少有专用的节能分片方案。此外，上述分片方案也不是为无线区块链网络设计的。在无线场景下，通信链路的不稳定性会影响共识时延和吞吐量[1]。因此，无论是从能耗角度还是无线场景来看，现有的分片方案都不能完全适用。此外，无线网络中的节点难以及时获得电源供应，高能耗的区块链功能很容易使节点脱机离线，从而影响共识性能。因此，为了保证无线区块链网络的正常运行，迫切需要设计低能耗的分片方案。

本文设计了一种面向 RAFT 共识的低能耗无线区块链分片算法（Green Chain, GC）。GC 分片根据无线区块链网络中节点的地理位置，将节点限制在某个分片中，避免其参与共识网络的全局通信。此外，该算法在每个分片中选择一个委员会节点以达到全局一致性。

1 系统模型

1.1 GC 分片

本文假设节点位于长为 d_1，宽为 w 的矩形区域中，且节点满足均匀分布。同时，无线区块链网络中节点总数为 n，GC 分片将其分为 y 个分片，每个分片有 x 个节点，那么 x, y, n 满足：

$$xy = n \tag{1}$$

而面向 RAFT 共识的 GC 分片如图 1 所示，可分为以下两步：1）根据矩形的长度将该区域平均划分为 y 个子区域。每个子区域对应一个分片，对每个分片并行执行 RAFT 共识；2）每个分片选择一个领导者作为委员会节点。因此，有 y 个委员会节点被选择出来形成一个分片委员会，并再次执行 RAFT 共识，以达到全局一致性。

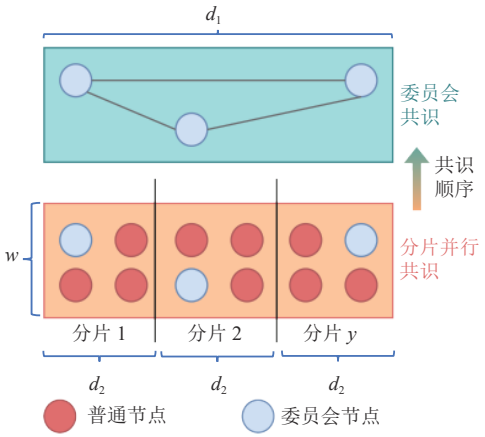

图 1 GC 分片示意图

根据文献 [11] 可知，共识能耗与节点发射功率、共识时延和节点数量密切相关。因此，经过 GC 分片后，共识能耗可以从 3 个方面降低：1）GC 分片可以缩短共识节点的通信距离，以降低发射功率；2）每个分片中用于共识的节点数量较分片前少，可降低通信时延，从而降低能耗；3）GC 分片还可以限制每个分片内的通信开销，以减少通信次数。

当完成分片后，每个分片的最大通信距离为 d_2（当 $d_2>w$）或 w（当 $w>d_2$），这是将矩形对角线长度近似为矩形长的结果。为了简化计算，本文默认 $d_2>w$。而 d_2 和 d_1 之间的关系满足：

$$d_2 = \frac{d_1}{y} \tag{2}$$

为了使分片前和分片后的共识均必然成功，根据文献 [1] 和文献 [11] 可知，d_1 和 d_2 需分别满足式 (3) 和式 (4)：

$$d_1 \leqslant \left(\frac{P_1 h}{z P_N}\right)^{-\alpha} \tag{3}$$

$$d_2 \leqslant \left(\frac{P_2 h}{z P_N}\right)^{-\alpha} \tag{4}$$

式中，P_1、P_2 分别为分片前和分片后的发射功率；h 为瑞利衰落中功率增益的非负随机变量，服从指数为 1 的负指数分布；α 为路径损耗指数；P_N 为干扰噪声功率；z 表示节点可以恢复信号的信噪比（SNR）阈值。

由式 (2)～式 (4) 可得分片前后发射功率之间的关系为：

$$P_2 = P_1 y^{-\alpha} \tag{5}$$

1.2　ECS 估计方法

文献 [11] 提供了一种计算 RAFT 共识能耗的方法，即：

$$E_{\mathrm{R}} = (n-1)(t_1 + t_2)P_T \tag{6}$$

式中，t_1 表示下行链路的时延；t_2 表示上行链路的时延。

那么，对于 GC 分片，能耗等于每个分片的能量消耗之和再加上委员会共识的能耗。由于委员会节点分布在每个分片的任意位置，为了保证委员会共识的必然成功，将传输功率设为 P_1。因此，GC 分片能耗为：

$$E_{\mathrm{GC}} = y(x-1)(t_3 + t_2)P_2 + (y-1)(t_4 + t_2)P_1 \tag{7}$$

式中，t_3 表示每个分片中下行链路的时延；t_4 表示委员会中下行链路的时延。而 t_2 较分片前不会改变，因为上行链路的时延与节点数量无关[11]。

进一步，根据式 (1) 将 x 替换为 n/y，根据式 (5) 将 P_2 替换为 $P_1 y^{-\alpha}$，可得：

$$E_{\mathrm{GC}} = \left[y^{-\alpha} n(t_3 + t_2) - y^{-(\alpha-1)}(t_3 + t_2) + (y-1)(t_4 + t_2)\right] P_1 \tag{8}$$

式 (8) 中参数较多，计算复杂，难以用它来推导 GC 方案的最小能耗。因此，需要简化式 (8)，设计一种面向分片后更简洁的共识能耗估计方法。

根据文献 [11]，时延 t_3 和 t_4 可近似为过零点的线性函数，那么 t_4 可由式 (9) 表示为式 (10)：

$$\frac{x}{y} = \frac{t_3}{t_4} \tag{9}$$

$$t_4 = t_3 \frac{y}{x} = t_3 \frac{y^2}{n} \tag{10}$$

此外，t_2 的值与 t_3 和 t_4 的值相比非常小。当节点数在 0 ～ 70 之间时，t_2 的值比 t_3 和 t_4 的值小两个数量级；当节点数越大，t_2 和 t_3，t_4 之间的差距越大[11]。因此，t_2 的值可以忽略不计。那么，式 (8) 可简化为：

$$E_{\mathrm{GC}} = \left[\frac{y^3}{n} - \frac{y^2}{n} - y^{-(\alpha-1)} + n y^{-\alpha}\right] t_3 P_1 \tag{11}$$

1.3　NG 算法

式 (11) 中提出的分片后能耗的简单估计方法，有助于在 GC 方案中寻求能耗最小的节点分组，即 NG 算法。将式 (11) 看作关于 y 的多项式函数，依次计算其一阶导数和二阶导数，分别得到：

$$\frac{\mathrm{d}E_{\mathrm{GC}}(y)}{\mathrm{d}y} = \left[\frac{3}{n}y^2 - \frac{2}{n}y + (\alpha-1)y^{-\alpha} - \alpha n y^{-(\alpha+1)}\right] t_3 P_1 \tag{12}$$

$$\frac{\mathrm{d}^2 E_{\mathrm{GC}}(y)}{\mathrm{d}y^2} = \left[\frac{6y-2}{n} + \frac{\alpha(\alpha+1)n - (\alpha-1)\alpha y}{y^{\alpha+2}}\right] t_3 P_1 \tag{13}$$

不难发现式 (13) 代表的二阶导数大于 0，因为 $6y > 2$，$\alpha(\alpha+1)n > (\alpha-1)\alpha y$，且其他参数都为正值。因此，一阶导数式 (12) 是一个单调递增的函数。那么，当式 (12) 为 0 时，求出的 y 值可以使式 (11) 代表的能耗最小，即：

$$\frac{3y^2}{n} - \frac{2y}{n} + (\alpha-1)y^{-\alpha} - \alpha n y^{-(\alpha+1)} = 0 \tag{14}$$

式 (14) 为一个二次多项式，可以用牛顿迭代法求解，是一种求解多项式方程的高效方法。通过结合式 (14) 和式 (1) 求解得到 x 与 y 的值，即 GC 分片中能耗最小的节点分组。上述 NG 算法可概括为：

初始化：$d_1, d_2, P_1, P_2, \alpha$；
输入：节点数目 n；
根据式 (11) 计算能耗；
寻找式 (11) 的一阶导数式 (12)；
寻找式 (11) 的二阶导数式 (13)；
if 式 (13)>0, then
令式 (12) =0 来解得式 (14)；
输出：能耗最小的节点分组情况。

2　性能分析

除了分片的能耗，共识时延、吞吐量和共识安全性也是 GC 分片中值得关注的重要指标。

2.1　共识时延

GC 分片的时延可分为两部分。第一部分是每个分片达成共识的时延，由于每个分片的共识是并行进行的，因此只需要分析一个分片的时延即可；第二部分是委员会共识的时延。

根据文献 [11] 可知，RAFT 共识的延迟可以用下行链路和上行链路的时延之和来表示。因此，对于第一部分，每个分片的时延可表示为：

$$t_{\mathrm{shard}} = t_3 + t_2 \tag{15}$$

式中，t_3 和 t_2 的值可由式 (16) 求出[6,19]。式 (16) 中

的 f_Q 表示 Q 函数。T 为信道时延，其值与该节点连接的信道数目有关。那么对于 t_3，分片内领导者连接的信道数目为 $x-1$，故有 $t_3=T(x-1)$；同理，对于 t_2，委员会内领导者连接的信道数目为 $y-1$，故有 $t_2=T(y-1)$。N 表示子载波数，在 GC 分片中 $N=1$。B 表示带宽，R 和 C 分别为传输速率和信道容量。P_s 表示无线区块链网络中两个节点之间的传输成功率，可以在文献 [1,11] 得到：

$$1-P_s=f_Q\left(\frac{NTBC-NTBR+\frac{logNTB}{2}}{(\log_2 e)\sqrt{NTB}}\right) \tag{16}$$

此外，对于第二部分的时延，委员会的共识与每个分片的共识一致，均为 RAFT 共识。因此该部分的时延也可以用式 (15) 表示，其中 t_4 的解与 t_3 的解方法类似，均可由式 (16) 解得。因此可得：

$$t_{\text{committee}}=3t_4+t_2 \tag{17}$$

综上，GC 分片的总时延为：

$$t_{\text{total}}=t_{\text{shard}}+t_{\text{committee}} \tag{18}$$

2.2 吞吐量

吞吐量的定义是每秒生成的事务数（Throughput Per Second, TPS）。事务的产生与共识的达成有关，因此，TPS 可以由共识时间的倒数表示：

$$\text{TPS}=\frac{1}{t_{\text{total}}} \tag{19}$$

2.3 共识安全性

共识安全性在区块链共识和分片中往往指共识成功率[12-13]。由于文献 [11] 已经将基于通信链路故障的 RAFT 共识成功率研究得较为透彻，因此本文主要关注于基于节点故障的共识安全性。根据 RAFT 共识 50% 的容错能力，分片前网络中的故障节点数目 f 应当满足：

$$f\leqslant\left\lfloor\frac{n-1}{2}\right\rfloor \tag{20}$$

只要故障节点数目满足上式，RAFT 共识的活性即可得到满足，即节点总数大于 $2f+1$ 后，RAFT 网络的性能也不会得到提升，相反还会拖累共识性能，延长共识时延[11]。因此，本文假设 $n=2f+1$。进一步假设节点的可靠性，即没有发生故障的概率为 P_R，那么 RAFT 网络共识成功的概率 P_C 可表示为：

$$P_C=\sum_{i=0}^{f}C_{n-1}^{i}(1-P_R)^i P_R{}^{(n-1-i)} \tag{21}$$

对于经过 GC 分片后的 RAFT 网络，共识成功需要两件事件同时发生，命名为事件 A 和事件 B。事件 A 代表超过 50% 的分片成功达成共识，事件 B 代表超过 50% 的委员会节点在委员会共识中保持活性。

事件 A 的概率为：

$$P(A)=\sum_{i=0}^{\left\lfloor\frac{y-1}{2}\right\rfloor}C_{y-1}^{i}(1-P_{\text{shard}})^i P_{\text{shard}}{}^{(y-1-i)} \tag{22}$$

式中，P_{shard} 表示每个分片达成共识的概率，为：

$$P_{\text{shard}}=\sum_{j=0}^{\left\lfloor\frac{x-1}{2}\right\rfloor}C_{x-1}^{j}(1-P_R)^j P_R{}^{(x-1-j)} \tag{23}$$

若事件 A 成功发生，那么事件 B 发生的概率为：

$$P(B|A)=\sum_{k=0}^{\left\lfloor\frac{y-1}{2}\right\rfloor-i}C_{y-1}^{k}(1-P_R)^k P_R{}^{(y-1-i-k)} \tag{24}$$

由此，GC 分片后，能顺利达成共识的概率为式 (22) 和式 (24) 的乘积，表示为：

$$P_{GC-N}=\sum_{i=0}^{\left\lfloor\frac{y-1}{2}\right\rfloor}C_{y-1}^{i}(1-P_{\text{shard}})^i P_{\text{shard}}{}^{(y-1-i)}\times \sum_{k=0}^{\left\lfloor\frac{y-1}{2}\right\rfloor-i}C_{y-1}^{k}(1-P_R)^k P_R^{(y-1-i-k)} \tag{25}$$

3 委员会节点选择优化算法

上文所述的委员会节点选择，是简单地随机在每个分片内选取一个领导者作为委员会节点，导致委员会节点随机分布在每个分片内，使得委员会共识时的通信距离难以确定。为了保障委员会共识尽可能地成功，GC 分片选取矩形的长 d_1 作为通信距离从而确定委员会节点的传输功率，即式 (3)。因此，委员会节点的选择存在优化的可能，可以使这类节点的通信总距离最小，从而最小化传输功率，以达到进一步降低能耗的目的。

此外，GC 分片算法是为了保障无线链路的稳定，进而在无线通信层面保障共识的必然成功，由此设定节点传输功耗，即式 (3) 和式 (4)。但在某些实际应用场景中，对共识成功率的要求并未如此严格，如在车联网中达到 99% 的成功率即可[20]。因此，GC 分片也可以根据实际应用场景所需的共识

成功率，降低节点的传输功率，从而进一步优化能耗指标。

令 s_i 代表第 i 个分片内所有节点的集合，$i\in1, 2, 3,\cdots, y$；令 n_i^j 为第 i 个分片中第 j 个节点，$j\in1, 2, 3,\cdots, x$；每个分片内委员会节点表示为 n_i^c，其对应的传输功率设为 P_i；变量 $\delta_c[n_i^j]$ 是一个指标变量，当其等于 1 时，代表把第 j 个节点定为第 i 个分片的委员会节点。由此，约束基于通信链路故障的共识成功率 P_{GC-L} 大于可以接受的值 $P_{\min}$，降低委员会节点的传输功率，并且在每个分片内选择使通信总距离最小的委员会节点，使得共识能耗最小。该优化问题可表示为：

$$\begin{aligned}&\min_{P_i,n_i^c} E_{\mathrm{GC}}\\ &\text{s.t.}C1: n_i^c\in s_i \quad i\in1, 2, 3,\cdots, y\\ &C2: \sum_{j=1}^{x}\delta_c[n_i^j]=1 \quad \delta_c[n_i^j]\in0,1\\ &C3: P_{\mathrm{GC-link}}\geqslant P_{\min}\end{aligned}\tag{26}$$

式中，$C1$ 代表所有的委员会节点存在于每个对应的分片内；$C2$ 说明每个分片只能存在一个委员会节点；$C3$ 表示基于通信链路故障的共识成功率需大于实际的应用需求。

由于式 (26) 中 E_{GC} 包含多个变量的乘积，因此拟采用结合拉格朗日乘子法的次梯度下降算法来获得能耗最小化策略。

若目标问题的拉格朗日松弛函数为乘子集合为 U 的 $L(\delta_c,P_i,U)$，原问题的拉格朗日对偶问题可以表示为：

$$\max_{U} g(U)=\max_{U}\inf_{\{\delta_c,P_i\}} L(\delta_c,P_i,U)\tag{27}$$

通过对 $L(\delta_c,P_i,U)$ 关于 δ_c 和 P_i 求导，并令其等于零，对给定的 U，可以得到内部极小化问题的可行解。然后通过次梯度算法更新 U，可根据解得的可行解求出外部极大化问题的解。重复上述步骤，直到乘数收敛到预设的阈值，便可得到目标函数的最优解。

委员会节点选择算法 CNS 的主要步骤如下。

初始化：拉格朗日松弛函数的乘子集合 $U(t)$；

for 迭代次数 $t\in[0, 1, 2,\cdots,t_{\max}]$；do

根据 $U(t)$ 计算 $\begin{cases}\dfrac{\mathrm{d}L(\delta_c,P_i,U)}{\mathrm{d}\delta_c\left[n_i^j\right]}=\dfrac{\mathrm{d}L(\delta_c,P_i,U)}{\mathrm{d}P_i}=0\\ \sum\limits_{j=1}^{x}\delta_c\left[n_i^j\right]=1,\delta_c\left[n_i^j\right]\in\{0,1\}\end{cases}$ 寻找可行解；

根据次梯度算法更新乘子集合 $U(t+1)$；

if $U(t+1)-U(t)\leqslant\varepsilon$, then 返回可行解；

else 继续迭代；

end if

end for

4　性能仿真

本节首先验证 ECS 方法和 NG 算法的正确性和准确性；其次，与其他 RAFT 方案对比，仿真结果证明了 GC 分片在能耗方面的优越性；此外，验证了第 2 节中推导的共识时延、吞吐量和共识安全性；最后给出了第 3 节优化算法的仿真结果。在仿真之前，需要设置必要的参数。本文考虑在未来 6G 通信中部署面向无线区块链网络的 GC 分片，因此这些参数包含太赫兹信号和毫米波信号两个场景[1,11]，如表 1 所示。其中路径损耗指数 α 在太赫兹和毫米波信号环境中的值来自文献 [21-22]。

表 1　仿真参数

参数	值	
	太赫兹信号	毫米波信号
P_N/W	0.2	0.2
P_1/W	1	1
B/GHz	20	800
C/GHz	80	8
R/GHz	40	4
α	2.229	1.7

4.1　能耗估计与节点分组

令 n=20, 30, 40，并将分片数量 y 依次设置为 2, 3, ⋯, 7，以验证 ECS 方法和 NG 算法的准确性。

由式 (6) 可知，当节点数为 20、30 和 40 时，对于尚未分片的无线 RAFT 网络，在太赫兹信号下其共识能耗分别为 14.78、32.78、59.20 aJ (1 aJ= 10^{-18} J)；而在毫米波信号下，其共识能耗分别为 1 577 、3 561、6 499 aJ。上述能耗值较低，是因为部署了高频太赫兹和毫米波信号的无线区块链网络具有较低的时延，该仿真结果在 4.3 节中展示。然而，随着区块链系统的不断发展，目前最快的区块链系统可以实现超过 50 000 次共识/s[23]，后文的仿真也证明了本算法吞吐量极高。而大量的共识将导致大量的能耗，因此，降低共识能耗非常迫切且必要。

图 2a、图 b 和图 2c 展示了在太赫兹信号下，

分片数目 2, 3,…, 7 时，节点数目分别为 20、30 和 40 的实际和估计能耗。图 3a、图 3b 和图 3c 则代表毫米波情况下，不同分片数目时，3 种节点数目的实际和估计能耗。从两类信号场景的仿真结果来看，实际能耗和估计能耗的差异很小，最小误差仅为 0.4%，平均误差小于 2%，证明了 ECS 方法的准确性。同时，两类信号的对比实验还说明了毫米波下的能耗较太赫兹下的能耗大两个数量级。

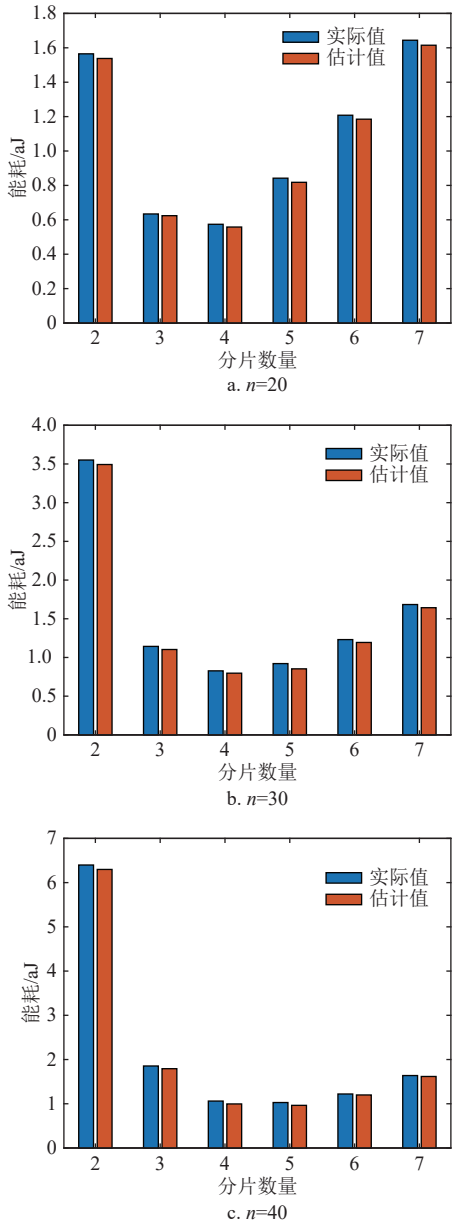

图 2　太赫兹信号下 GC 分片的能耗

此外，通过仿真发现，无论节点数目为多少，总存在一个节点分组情况使得能耗最小。在太赫兹和毫米波信号下，上述节点数目的最小能耗对应的分片数量为 4 或 5。这一结果与 NG 算法可相互验证，证明了该算法的正确性。

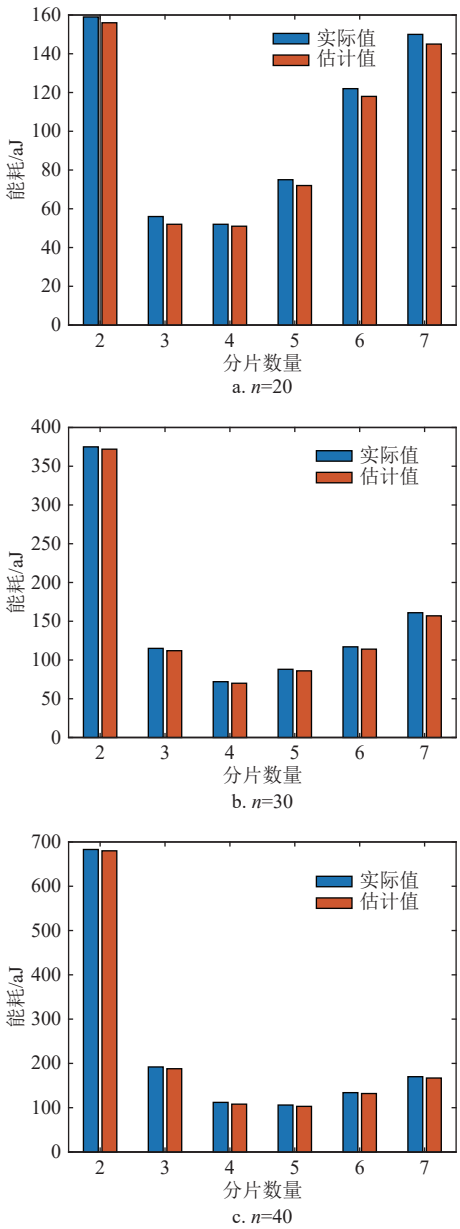

图 3　毫米波信号下 GC 分片的能耗

最后，通过比较未分片的共识能耗和分片后的最小能耗，GC 分片节能效果可以达到 98.36%，且节能效果随节点数目增加而增加。这一结果表明，GC 分片在无线区块链网络中具有巨大的节能潜力，对能量受限的无线网络场景具有极大的吸引力。

4.2　能耗对比

选取最小化能耗的节点分组情况的 GC 分片与其他 RAFT 方案的能耗进行对比。比较对象来自文献 [20] 中的 Two-hop RAFT 方案。为了不失一般性，与 4.1 类似，本部分也比较了 n=20, 30, 40 时在太赫兹和毫米波信号下的能耗。太赫兹下的仿真结果

如图 4a～图 4c 所示，毫米波下的仿真结果如图 5a～图 5c 所示。其中 Two-hop 方案 1 和 2 分别代表不同的一跳和两跳的节点数目。当 n=20 时，方案 1 代表有 5 个一跳节点，其中 3 个一跳节点分别连接 5 个两跳节点；方案 2 代表有 5 个一跳节点，每个一跳节点分别连接 3 个两跳节点；当 n=30 时，方案 1 代表有 5 个一跳节点，每个一跳节点分别连接 5 个两跳节点；方案 2 代表有 6 个一跳节点，其中 4 个一跳节点分别连接 6 个两跳节点；当 n=40 时，方案 1 代表有 4 个一跳节点，每个一跳节点分别连接 9 个两跳节点；方案 2 代表有 5 个一跳节点，每个一跳节点分别连接 7 个两跳节点。

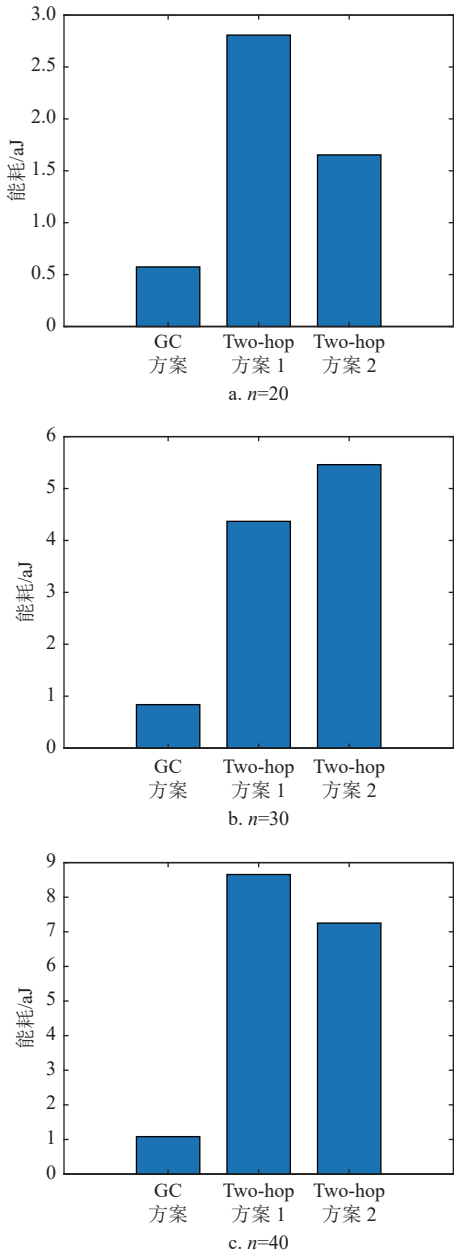

图 4　太赫兹信号下的能耗对比

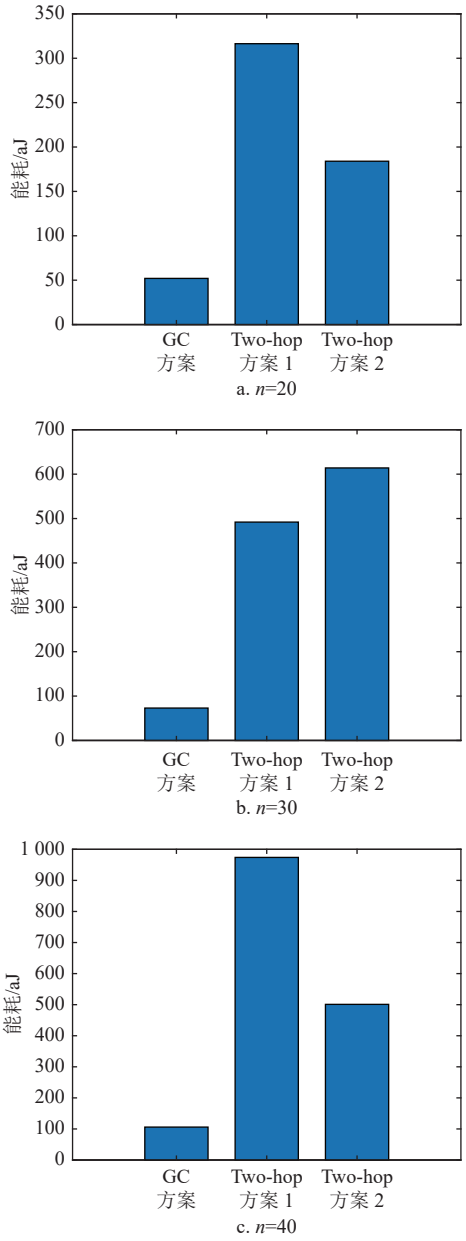

图 5　毫米波信号下的能耗对比

无论是太赫兹还是毫米波信号，3 种方案的能耗均具有以下规律：当 n=20 时，GC 分片能耗最小，Two-hop 方案 1 能耗最大；当 n=30 时，能耗最小方案仍为 GS 分片，能耗最大方案为 Two-hop 方案 2；当节点数目为 40 时，结果与节点数目为 20 时相同。由于 Two-hop 方案的一跳和两跳节点数目会发生变化，因此不同 Two-hop 方案的能耗也会发生变化。但无论在何种情况下，能耗最小的始终是本文提出的 GC 分片。结果表明，GC 分片在能耗方面具有明显优势，证明了该算法的优越性。

4.3 共识时延、吞吐量和共识安全性

首先，对比了太赫兹和毫米波两类信号情况下，GC 分片与上述 Two-hop 两种方案的共识时延，结果如图 6a 和图 6b 所示。3 种方案在太赫兹信号情况下的时延均处于 as (1as=10^{-18} s) 数量级，但毫米波信号的时延较太赫兹信号大两个数量级。此外，无论是何种信号条件，当 n=20 时，GC 分片与 Two-hop 方案 2 的时延一致小于 Two-hop 方案 1；当 n=30 时，GC 分片与 Two-hop 方案 1 的时延一致小于 Two-hop 方案 2；当节点数目为 40 时，GC 分片大致与 Two-hop 方案 2 的时延一致小于 Two-hop 方案 1。这一结果表明了 GC 分片在时延上具有优越性。

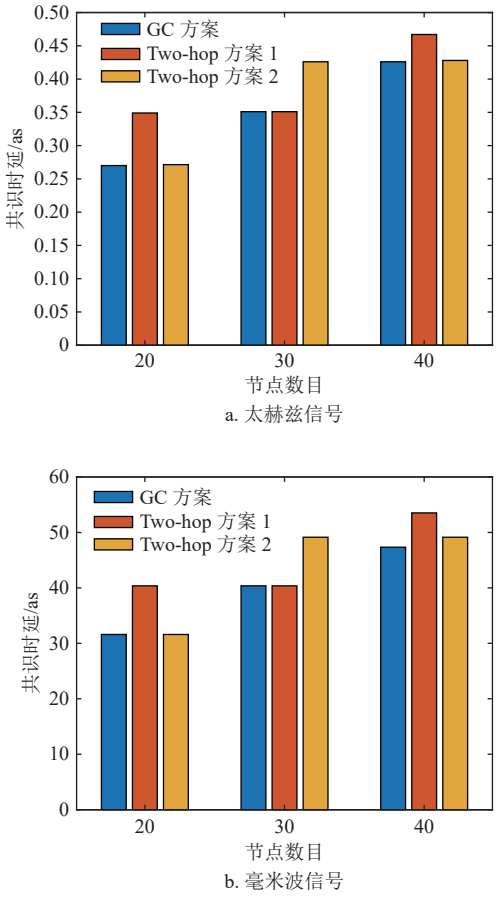

图 6 时延对比

其次，本部分对比了在太赫兹和毫米波两类信号情况下，GC 分片与上述 Two-hop 两种方案的吞吐量，结果如图 7a 和图 7b 所示。与时延类似，GC 分片在吞吐量上也比 Two-hop 方案具有优势。同时，3 种方案的吞吐量随节点数目的变化以及原因也与时延一致，故在此不再赘述。

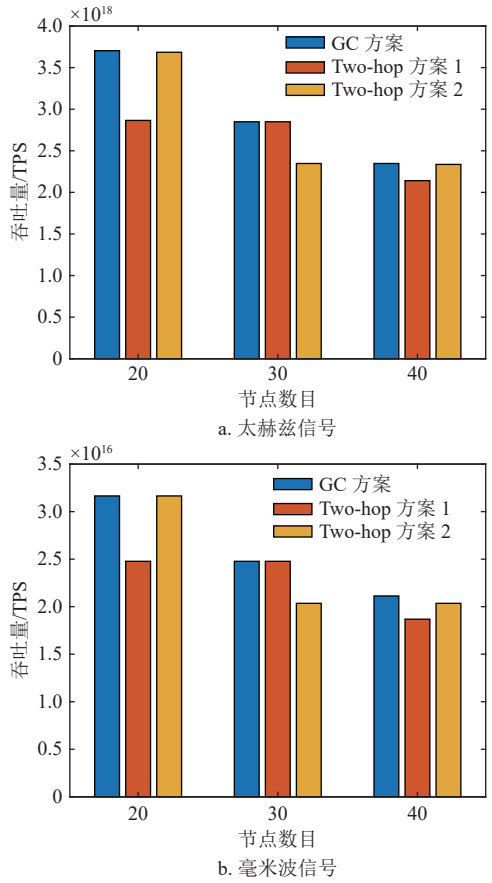

图 7 吞吐量对比

最后，仿真了 GC 分片基于节点故障的共识安全性。根据文献 [24] 的启示，在这部分仿真中，该共识成功率以其对数值进行表示，并与未分片的 RAFT 共识的共识成功率对数值进行对比。对数值代表了对无线 RAFT 网络关于节点数量的可靠性度量，能够为共识网络配置提供有用的指导。与上文类似，本部分仿真也考虑了节点数目分别为 20、30 和 40 时的情况。但因为太赫兹和毫米波信号只会对通信链路产生影响，不会对节点故障产生影响，因此此处不再分信号类型进行仿真。仿真结果如图 8 所示，其展示了上述情况在不同节点可靠性时共识成功率的对数值变化趋势。

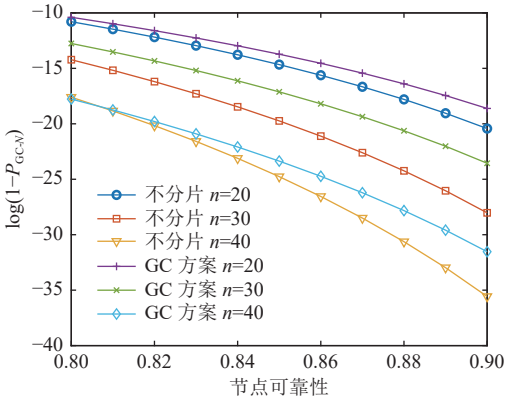

图 8 基于节点故障的共识安全性

4.4　CNS 优化算法

节点数目分别为 20、30 和 40 的 3 种情况下，在太赫兹和毫米波两类信号下进行仿真。在优化算法中，设约束基于通信链路故障的共识成功率 $P_{\mathrm{GC}\text{-}L}$ 大于可以接受的最小共识成功率 $P_{\min}$ 的值分别为 0.9 和 0.99。CNS 优化算法在两类信号条件下的仿真结果分别如图 9a 和图 9b 所示。

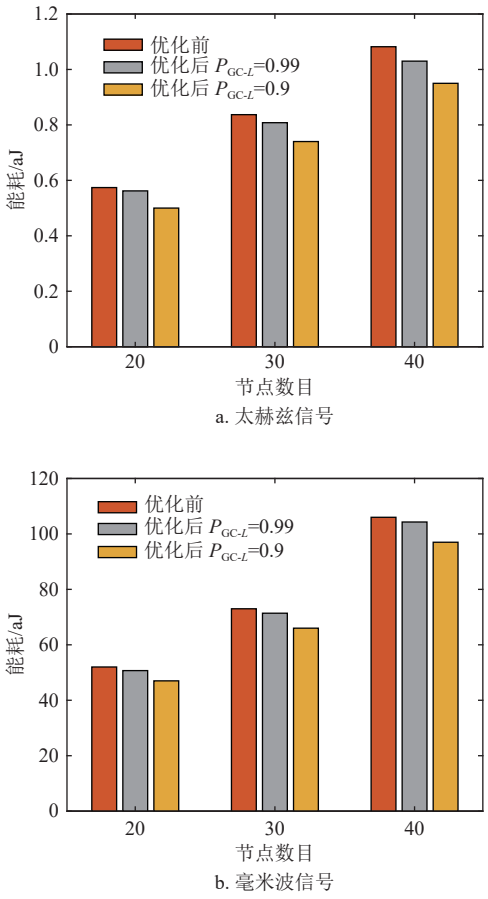

图 9　CNS 优化算法

根据仿真结果，不难发现，无论是太赫兹还是毫米波信号环境，CNS 算法均能取得一定的优化效果。一方面，节点数目越多，优化效果越好。这是因为节点数目增加，可能会使分片数目也随之增加，那么对委员会节点选取的优化空间就越大；而另一方面，可接受的最小共识成功率越低，优化效果也会越明显。这是因为更低的共识成功率代表系统对节点发射功率的需求也就越低，从而进一步降低能耗。

5　结束语

本文设计了一种面向 RAFT 共识的低能耗无线区块链分片 GC。为了更方便地计算分片后的共识能耗，提出了一种简单的能耗估算方法 ECS。此外，为了最小化 GC 分片的能量消耗，研究了能耗最小的节点分组问题，并提出了针对该问题的 NG 算法。同时，从理论上分析了 GC 分片算法的共识时延、吞吐量和基于节点故障的共识成功率。最后，还给出了委员会节点选取的优化算法 CNS，以进一步优化能耗。仿真结果表明 GC 分片在能量受限的无线区块链网络中有着良好的应用场景。

参 考 文 献

[1] LUO H X, YANG X Y, YU H F, et al. Performance analysis of non-ideal wireless PBFT networks with mmWave and terahertz signals[C]//Proceedings of the IEEE International Conference on Metaverse Computing, Networking and Applications. New York: IEEE, 2023: 104-108.

[2] NGUYEN V L, LIN P C, CHENG B C, et al. Security and privacy for 6G: A survey on prospective technologies and challenges[J]. IEEE Communications Surveys & Tutorials, 2021, 23(4): 2384-2428.

[3] LUO H X, YU H F, LUO J. PRAFT and RPBFT: A class of blockchain consensus algorithm and their applications in electric vehicles charging scenarios for V2G networks[J]. Internet of Things and Cyber-Physical Systems, 2023, 3: 61-70.

[4] XU X Q, SUN G, YU H F. An efficient blockchain PBFT consensus protocol in energy constrained IoT applications[C]//Proceedings of the International Conference on UK-China Emerging Technologies. New York: IEEE, 2021: 152-157.

[5] CHEN Y C, LUO H X, BIAN Q. A privacy protection method based on key encapsulation mechanism in medical blockchain[C]//Proceedings of the IEEE 21st International Conference on Communication Technology. New York: IEEE, 2021: 295-300.

[6] YANG X Y, LUO H X, DUAN J S, et al. Ultra reliable and low latency authentication scheme for Internet of vehicles based on blockchain[C]//Proceedings of the IEEE INFOCOM 2022 - IEEE Conference on Computer Communications Workshops. New York: IEEE, 2022: 1-5.

[7] NAKAMOTO S. Bitcoin: A peer-to-peer electronic cash system[EB/OL]. [2023-03-21]. https://bitcoin.org/bitcoin.pdf.

[8] VASIN P. Blackcoin's proof-of-stake protocol v2[EB/OL]. [2023-05-21]. https://www.dailyblackcoin.com/blackcoin-pos-protocol-v2-whitepaper.pdf.

[9] CASTRO M, LISKOV B. Practical Byzantine fault tolerance[C]//Proceedings of the 1999 USENIX Symposium on Operating Systems Design and Implementation. [S.l.]: USENIX OSDI, 1999: 173-186.

[10] ONGARO D, OUSTERHOUT J. In search of an understandable consensus algorithm[J]. Proceedings of the

2014 USENIX Annual Technical Conference, USENIX ATC 2014, 2014: 305-319.
[11] LUO H X, YANG X Y, YU H F, et al. Performance analysis and comparison of nonideal wireless PBFT and RAFT consensus networks in 6G communications[J]. IEEE Internet of Things Journal, 2024, 11(6): 9752-9765.
[12] LI W Y, FENG C L, ZHANG L, et al. A scalable multi-layer PBFT consensus for blockchain[J]. IEEE Transactions on Parallel and Distributed Systems, 2021, 32(5): 1146-1160.
[13] ZHANG P Y, GUO W F, LIU Z J, et al. Optimized blockchain sharding model based on node trust and allocation[J]. IEEE Transactions on Network and Service Management, 2023, 20(3): 2804-2816.
[14] HONG Z C, GUO S, LI P. Scaling blockchain via layered sharding[J]. IEEE Journal on Selected Areas in Communications, 2022, 40(12): 3575-3588.
[15] HONG Z C, GUO S, LI P, et al. Pyramid: A layered sharding blockchain system[C]//Proceedings of the IEEE INFOCOM 2021 - IEEE Conference on Computer Communications. New York: IEEE, 2021: 1-10.
[16] LI X L, LUO H X, DUAN J S. Security analysis of sharding in blockchain with PBFT consensus[C]// Proceedings of the ICBCT'22: The 2022 4th International Conference on Blockchain Technology. New York: ACM, 2022: 9-14.
[17] KOKORIS-KOGIAS E, JOVANOVIC P, GASSER L, et al. OmniLedger: A secure, scale-out, decentralized ledger via sharding[C]//Proceedings of the IEEE Symposium on Security and Privacy. New York: IEEE, 2018: 583-598.
[18] 徐小琼, 孙罡, 罗龙. 物联网区块链中基于演化博弈的分片算法[J]. 电子科技大学学报, 2022, 51(3): 363-370.
XU X Q, SUN G, LUO L. Sharding algorithm based on evolutionary game in the IoT-blockchain[J]. Journal of University of Electronic Science and Technology of China, 2022, 51(3): 363-370.
[19] CHANG B, ZHANG L, LI L Y, et al. Optimizing resource allocation in URLLC for real-time wireless control systems[J]. IEEE Transactions on Vehicular Technology, 2019, 68(9): 8916-8927.
[20] CAO J Y, LENG S P, ZHANG L, et al. A V2V empowered consensus framework for cooperative autonomous driving[C]//Proceedings of the GLOBECOM 2022 - 2022 IEEE Global Communications Conference. New York: IEEE, 2022: 5729-5734.
[21] ABBASI N A, HARIHARAN A, NAIR A M, et al. Channel measurements and path loss modeling for indoor THz communication[C]//Proceedings of the 2020 14th European Conference on Antennas and Propagation (EuCAP). New York: IEEE, 2020: 1-5.
[22] GUAN Y C, ZHANG J H, TIAN L, et al. A comparative study for indoor factory environments at 4.9 and 28 GHz[C]//Proceedings of the 2020 14th European Conference on Antennas and Propagation (EuCAP). New York: IEEE, 2020: 1-5.
[23] PHILLIPS D. What is Solana? What is Solana? A Scalable, decentralized network for dapps-decrypt [EB/OL]. [2023-05-21]. https://decrypt.co/resources/what-is-solana-a-scalable-decentralized-network-for-dapps, 2023.
[24] LI Y T, FAN Y X, ZHANG L, et al. RAFT consensus reliability in wireless networks: Probabilistic analysis[J]. IEEE Internet of Things Journal, 2023, 10(14): 12839-12853.

编 辑 税 红