

基于区块链的多层卫星互联网络安全管理技术

朱睿杰¹, 张玉东¹, 魏雅婷¹, 席超²

(1. 郑州大学信息工程学院, 河南 郑州 450001 ;

2. 航天恒星科技有限公司, 北京 100086)

摘要: 卫星互联网具有覆盖范围广、通信时延低、传输容量大、地域影响小等优势, 能为全球用户提供无处不在的互联网接入服务。但是卫星网络与地面网络的异构性, 卫星网络的信道开放、节点暴露等特点会对网络接入和资源管理造成安全威胁。针对卫星互联网的安全问题, 提出基于区块链的多层卫星互联网安全管理架构。区块链作为一种分布式账本技术, 以区块链式数据结构来验证和存储数据, 通过密码学方法保证数据块的不可篡改, 能实现网络安全接入和资源可信管理, 为卫星互联网提供信息安全防护。通过将区块链技术与卫星互联网融合, 提高卫星互联网的安全性。

关键词: 卫星互联网; 区块链; 安全管理

中图分类号: TP393

文献标识码: A

doi: 10.11959/j.issn.2096-8930.2022011

Security Management Technology of Multilayer Satellite Internet Based on Blockchain

ZHU Ruijie¹, ZHANG Yudong¹, WEI Yating¹, XI Chao²

1. School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China

2. Space Star Technology Co. Ltd, Beijing 100086, China

Abstract: Satellite internet have the advantages of wide coverage, low latency, large transmission capacity and no geographical influence. It can provide ubiquitous internet access services for users all over the world. However, the heterogeneity of satellite internet and ground network, the channel opening and node exposure of satellite internet will pose a security threat to network access and resource management. Aiming at the security problem of satellite internet, a multilayer satellite internet security management architecture based on blockchain was proposed. As a distributed ledger technology, blockchain uses chain data structure to verify and store data, and adopts encryption methods to maintain that data blocks cannot be tampered. Blockchain can realize network security access, trusted resource management, and provide information security protection for satellite internet. This paper improved the security of satellite internet by integrating blockchain technology with satellite internet.

Keywords: satellite internet, blockchain, security management

0 引言

卫星互联网是基于卫星通信系统, 以IP为网络服务平台, 以互联网应用为服务对象, 能够成为互联网的一个组成部分, 也能够独立运行的网络系统^[1]。卫星互联网具有覆盖范围广、通信时延低、信道容量大、地域影响

小等优势, 能够为全球用户提供互联网服务。根据“互联网世界”2021年第一季度统计数据^[2], 全球互联网用户数量已经突破51亿人, 占世界人口总数的65.6%, 但是在相对落后的一些地区, 互联网的普及率却只有43.2%。在全球范围内, 地理环境复杂地带面积占比高, 其铺设地

收稿日期: 2022-01-07; **修回日期:** 2022-03-03

基金项目: 国家自然科学基金资助项目 (No.62001422); 国家博士后科学基金特别资助项目 (No.2021T140622); 河南省教育厅科技创新人才 (No.22HASTIT016); 信息光子学与光通信国家重点实验室开放课题 (北京邮电大学) (No.IPOC2019A008)

Foundation Items: The National Natural Science Foundation of China (No.62001422), The China Postdoctoral Science Foundation (No. 2021T140622), The Henan Scientific and Technology Innovation Talents (No.22HASTIT016), The Open Fund of IPOC (BUPT) (No. IPOC2019A008)

面通信基础设施难度大、时间长、成本高、运维难,这导致互联网资源分配不均。卫星互联网作为目前行业的热点,不受地域影响,能提供无处不在的互联网服务,这对互联网全球覆盖意义重大。另外,卫星互联网不受灾害的影响,能作为灾害地区的通信手段。国家发展和改革委员会在2020年4月20日正式将卫星互联网与5G、物联网、工业互联网一起列入新型基础设施建设范围。这标志着我国卫星互联网建设作为国家级重大工程正式提上议程^[9]。

卫星网络与地面网络是异构网络,卫星互联网接入存在安全风险。卫星网络的信道开放、节点暴露等特点也对卫星互联网的资源管理造成安全威胁。区块链作为一种去中心化技术,非常适合解决卫星互联网的安全性和可靠性问题。2008年NAKAMOTO^[4]提出区块链的概念,并将其用于数字货币。区块链具有分布式、可验证和不可篡改的特点。由于区块链的分布式特性,攻击者无法篡改存储在区块链上的数据。目前,除了金融领域,区块链还被广泛应用于其他各行各业,如医疗^[5]、物流^[6]、物联网^[7]等。共识机制作为区块链系统的核心,起着保障分布式系统各个节点数据和状态一致的作用。

本文分析卫星互联网存在的安全挑战,在多层卫星互联网架构下引入区块链技术,通过区块链实现信息防篡改和资源信息共识,保证卫星网络与地面网络之间的安全接入和节点资源的安全调度。

1 相关研究进展

1.1 卫星网络的安全

针对卫星网络的安全问题,张志强等^[8]提出一种基于轨道分簇的低轨卫星网络密钥更新算法,该算法依据卫星的运行轨道对低轨卫星网络进行分簇,通过密钥动态分发保证低轨卫星网络密钥的安全性。余春东等^[9]从卫星网络的攻击监测方面进行研究,提出一种基于安全标签的安全监控模型,该模型可以实现对多种攻击行为的有效监测和响应。在卫星网络的路由安全方面,严开宇等^[10]提出一种基于区块链的卫星自组织网络安全路由方法,该方法能够应对路由操纵攻击,对受攻击节点能及时进行检查、隔离,提高卫星网络的安全性。在卫星网络的通信安全方面,马煜^[11]提出一种基于区块链的星间通信网络安全加密控制系统,采用基于区块链的分布式数字化身份加密技术,能够有效地提高安全网络加密系统的加密深度。这些工作从密钥更新、攻击检测、路由安全等不同方面对卫星安全提出有效的方案,但是没有考虑多层卫星场景下的卫星网络安全。

1.2 基于区块链的网络安全

XU等^[12]研究实用拜占庭容错(Practical Byzantine Fault Tolerance, PBFT)算法在物联网节点通信中的应用,设计基于区块链的物联网安全数据传输结构。在车联网中,HU等^[13]提出一种基于区块链的车联网(Internet of Vehicle, IoV)架构,给出一种基于时间序列和Gossip协议的高效拜占庭共识算法BCA-TG,以提高复杂环境下的通信安全性和节点认证效率。为了解决5G网络中用户设备(User Equipment, UE)移动导致的频繁认证问题,CHEN等^[14]提出一种基于区块链技术的5G安全认证方案,采用APG-PBFT算法生成接入点组(Access Point Group, APG)。UE在APG中被认证之后,通过广播机制在组内共享认证结果,不需要多次重复认证。LIN等^[15]提出一种基于区块链的隐私感知分布式收集导向(Blockchain based Privacy aware Distributed Collection oriented, BPDC)策略,用于在箱内网络(Network in Box, NIB)与6G的集成中保护数据聚合的安全性。LI等^[16]提出一种基于区块链的AI应用数据安全方案,并证明区块链用于确保AI应用数据安全的有效性。DAI等^[17]针对下一代无线通信网络提出一种区块链和深度强化学习结合的缓存方案,能够保证资源安全,提高系统效益。

虽然目前已经有区块链在通信网络安全中应用的研究,但是缺乏区块链在多层卫星互联网中的应用研究。区块链具有分布式和不可篡改的特性,适合应用在链路开放的卫星互联网中,为卫星互联网提供安全保障。本文通过分析卫星互联网面临的安全风险,提出基于区块链的安全管理架构。

2 卫星互联网架构与安全风险分析

典型的卫星互联网架构包括卫星网络层、地面基础设施层两部分,如图1所示。卫星网络层包括地球静止轨道(Geostationary Earth Orbit, GEO)卫星、中地球轨道(Medium Earth Orbit, MEO)卫星和低地球轨道(Low Earth Orbit, LEO)卫星,卫星之间通过光链路进行通信。地面基础设施层包括卫星的地面接收站、地面基站、控制中心、数据中心等设施,卫星与地面之间主要通过微波进行通信。不同于以往卫星星座集中于单层部署,LEO-MEO-GEO多层卫星联合部署,协同提供服务成为发展趋势,随之而来的是多层卫星互联网管理的安全问题。

卫星网络作为地面网络的补充,能够解决地面网络部署时覆盖范围有限的问题,但是卫星网络与传统地面网络之间的异构特征会引发安全问题。异构特征具体表现为网络设备部署差异、通信信道差异、业务安全需求

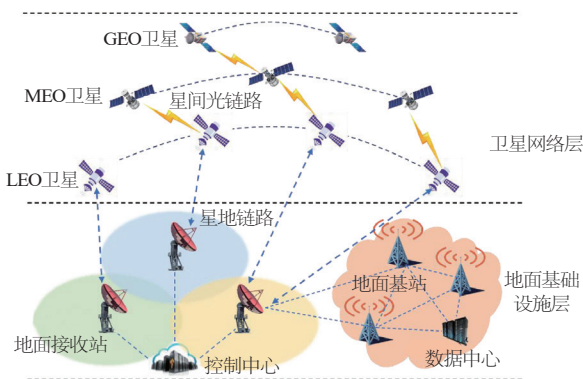


图1 卫星互联网架构

差异。在设备部署上,卫星网络设备部署成本高,并且受限于空间环境,设备维护困难,相较于地面网络难以实现故障恢复。在通信信道上,星间链路和星地链路依赖无线信道,地面基站长距离传输数据主要采用有线信道,信道差异导致部分通信协议无法兼容融合网络。在业务安全需求上,卫星网络除了满足普通用户需求外,还需要为科研等提供服务。不同业务的安全要求和敏感程度不同,卫星网络与地面网络的融合需要满足更加多样化的业务安全需求。

在卫星网络层,除地球静止轨道卫星外,其他轨道的卫星均围绕地球做高速相对运动。卫星网络的网络拓扑处于不断变化的状态,卫星与地面的链路需要频繁切换。动态拓扑中平衡网络负载、高效、安全路由的需求,给路由协议带来挑战;另外,链路切换带来了接入认证的问题。卫星网络不同于地面节点,太空中的卫星计算能力、存储、能源、带宽等资源均受到较大限制。卫星网络无法像地面网络那样部署复杂的软件防火墙,甚至,硬件层面的安全防护。一旦遭遇非法接入,卫星网络将更容易受到破坏。因此,卫星网络与地面网络的安全接入尤为重要。

与传统地面网络相比,卫星网络还具有信道开放、节点暴露的特点。卫星信道的可用频带宽,但传输功率受限、信噪比较低。星间链路采用光链路,在卫星系统实际的工作状态中,卫星信道处于开放的状态,卫星及其信道均未受到封闭保护,更易受到星间串扰、信息拦截等。卫星节点暴露在宇宙空间,易受到宇宙空间垃圾碎片的影响。卫星光链路的开放性,导致数据传输过程中面临未经授权的访问和窃听的风险,传输数据可能被劫持、篡改。因此,保障节点接入的安全、传输数据的可信对卫星网络的整体运行、卫星网络的整体安全显得尤为关键。

3 基于区块链的安全管理架构

针对LEO-MEO-GEO多层卫星联合部署的发展趋势,为了进一步提高多层卫星网络的安全性,保障卫星网络与地面网络的安全接入和卫星节点资源的可靠管理,本节在卫星互联网的管理中引入区块链技术,提出基于区块链的多层卫星互联网安全管理架构。

3.1 安全架构设计

区块链作为一种新兴的分布式安全技术,由于其匿名、不可篡改、可追溯等特点,迅速应用于各个领域。本小节提出的基于区块链的安全管理架构如图2所示,主要包含合约层、共识层和数据层。

合约层主要包括智能合约。智能合约通过提前设定触发条件,以脚本代码的形式运行在系统上。智能合约的触发条件在确认后不能更改,当满足设定的条件时,智能合约将自动触发^[8]。通过智能合约可以实现卫星网络管理的自动化。

共识层负责节点接入验证和资源数据的更新和验证,保证接入网络的节点为合法节点,以及维护节点间资源信息的一致性,确保共识过程的安全。针对多层卫星网络的拓扑特征,本小节提出分层拜占庭容错(Hierarchical Byzantine Fault Tolerant, HBFT)共识算法。对比传统共识算法,HBFT算法有更高的共识效率。

数据层的功能是存储节点认证信息和网络资源信息,确保节点认证信息和资源信息不会被篡改。卫星网络的资源信息以资源模型的形式存储在区块链中。除了存储节点的认证信息和资源信息,区块链的每个块还包含数字签名、时间戳、当前区块的哈希值和前一个区块的哈希值。区块链是一种链式数据结构,每个区块都包含前一个区块的哈希值,并且区块链存在多个副本,想要篡改区块链上的信息必须同时篡改所有区块的全部副本。这在分布式系统中几乎不可能实现,因此区块链具有不可篡改的特性,能够保证链上信息的安全性。

当有新的卫星节点请求加入卫星网络时,合约层会发起共识请求对卫星节点身份进行认证,网络中所有节点共识通过后会更新数据层区块链的链上数据,最后合约层允许新节点加入卫星网络。当地面站请求与卫星网络建立连接时,首先需对比区块链中的数据进行检索,查看是否有该地面站的认证信息。如果已经通过认证则允许建立连接,否则需要经过节点共识。当卫星网络资源再分配需要进行资源信息更新时,同样需要经过网络节点共识,才能产生新区块进行资源更新。

3.2 资源模型

系统中的资源信息以数学方法,将网络资源整理融

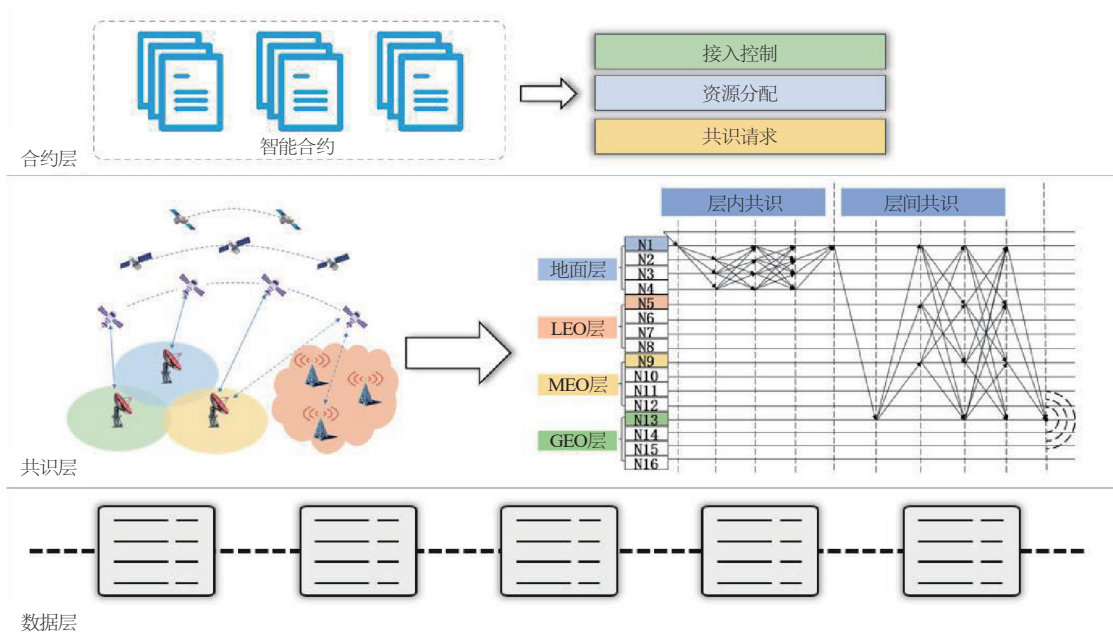


图2 基于区块链的安全管理架构

合为统一的资源模型。局部资源信息的变化需要经过系统全局的共识一致。资源信息存储在区块链中,由系统中所有节点维护。系统中的资源包含两类,第一类是节点资源 $R_i=(b_i, st_i, c_i, t_i, sta_i)$,其中 b_i 代表第 i 个节点的通信带宽, st_i 代表存储容量, c_i 代表计算能力, t_i 代表节点的信任值, sta_i 代表节点状态,当节点正常工作时 sta_i 值为1,当节点故障时 sta_i 值为0。节点的信任值由式(1)表示,其中 a 、 b 、 c 为权重系数,三者之和为1。 T 代表节点通信的平均时延,节点之间的通信不稳定会破坏系统的稳定性,不同节点的通信时延可能导致节点之间数据状态不一致。通信时延越长,越不利于正常共识。 P 代表节点作为主节点的频率,共识过程中的主节点会消耗更多的通信资源,并且长时间固定的主节点容易遭到针对性攻击,不利于系统的安全运行。因此,为了平衡资源消耗,保证系统稳定性,如果该节点在最近的时间周期中是主节点,在信任值评估时会当作减分项。 E 代表节点作恶次数,作恶行为主要包含两方面:一是节点的通信响应时延超过设定阈值的行为,即在 $2T_a$ 阈值内没有响应相邻节点的通信, T_a 是相邻节点之间正常通信的时延;二是在共识过程中篡改共识内容导致数字签名验证或哈希验证失败的行为。评估变量 G_i 由式(2)表示,用于评估节点 i 的资源权重,其各项系数之和为1。

$$t_i = e^{-(aT+bP+cE)} \quad (1)$$

$$G_i = sta_i(ab_i + \beta st_i + \gamma c_i + \delta t_i) \quad (2)$$

第二类资源为系统级资源 $S=(Spe, At)$,其中 Spe 为系

统整体频谱资源的分配情况, At 为系统中所有节点的认证信息。随着卫星互联网的发展,频谱资源已经成为卫星网络中最重要的资源。通过基于区块链的频谱资源管理,能够实现空闲频谱资源共享,在保证资源安全的同时提高资源利用率。系统中经过认证的节点信息会存储在区块链中,在进行链路切换时系统认证通过的节点无须重复认证,只需要检索链上的认证信息即可建立链路。

通过资源模型 $M=\{R, S\}$,使系统节点之间对节点认证信息和资源信息的标准达成一致。资源信息按资源模型的形式存储在区块链中,由系统节点共同维护;当有节点请求接入网络或者资源变动时,需要所有节点达成共识,可有效防止伪造攻击,提高安全性;并且通过统一的资源模型,方便资源调配和优化。

3.3 分层拜占庭共识算法

共识算法是指在分布式系统中,使全局对局部的某种处理达成一致的算法。共识算法的性能表现直接影响整个分布式系统的运作。共识算法是区块链系统的核心。在卫星互联网中,共识算法需要满足低时延、高吞吐量的需求。目前常用的共识算法有工作量证明(Proof of Work, PoW)算法、PBFT算法等。

PoW算法在区块链的应用始于NAKAMOTO^[4]在2008年提出的比特币。NAKAMOTO提出一种去中心化的数字货币,无须第三方来记录交易,系统中的节点权利平等。数字货币的交易信息保存在区块链上,区块链

由系统全部节点共同维护。产生的交易信息由矿工打包成区块添加到区块链上。每个区块通常包含约2 000笔交易的信息。矿工通过PoW共识算法获得挖矿权利,即更新区块链账本的权利。矿工挖矿的过程就是系统共识的过程。将区块头进行两次SHR256运算就能得到当前这个区块的哈希值^[19]。在SHR256算法中不论输入什么值,总能得到一个256位的哈希值,输入只要略微变动,输出就完全不同;并且SHR256算法正向运算十分容易得到结果,逆向运算则只能通过穷举法求解。只要一个节点计算出满足要求的随机数和哈希值,其他节点就能够迅速验证。这种算法计算开销大,消耗大量资源,并且共识效率低,并不适合用于资源受限的卫星网络。

PBFT算法是由CASTRO等^[20]提出的算法。在PBFT算法中有两类节点,主节点和一般节点。算法分为5个阶段进行。当主节点收到请求后,将“预准备”信息广播给所有节点进行共识;节点收到“预准备”信息,如果同意共识则向其他节点广播“准备”信息;节点收到包含自己在内的 $2f+1$ ($3f \geq N_u$, N_u 为节点总数)条“准备”信息后向其他节点广播“提交”信息;节点收到包含自己在内的 $2f+1$ ($3f \geq N_u$, N_u 为节点总数)条“提交”信息后,标记共识通过,并向请求节点发送“回复”信息。当系统节点数量增多时,算法的共识效率会显著降低。PBFT算法不适用于节点数量多的多层卫星互联网架构。

针对多层卫星网络的拓扑特征,为了提高共识效率,本文提出HBFT共识算法。算法分为层内共识和层间共识两个阶段,以避免所有节点同时参与共识过程,降低算法的验证复杂度。HBFT算法的共识过程如图3所示。层内共识可分为以下5个步骤。

(1) 有新的节点请求加入网络或网络中有资源变动时,资源变动节点/请求接入节点发起共识请求,其他节点对请求进行验证。

(2) 请求节点所在层的主节点 N_1 验证请求签名是否有效,如果请求无效则直接丢弃并记录作恶行为;请

求验证通过则将共识业务广播给地面层的其他节点。同时, N_1 将在本地记录共识业务的哈希值用于后续的哈希验证。

(3) 地面层的其他节点接收到主节点的广播消息后,如果同意请求节点的认证请求,则向其他节点发送投票消息,并将共识业务的哈希值存储在本地。

(4) 当节点收到 $l+1$ 及以上(即当前层一半以上的节点)的投票后,节点将当前的共识服务标记为预采纳,并广播二次投票消息给层内所有节点,进行共识投票的二次验证。其中 $2l \geq M_d$, M_d 为层内共识节点总数。

(5) 当节点收到 $l+1$ 及以上二次投票消息后,节点将当前的共识业务标记为采纳,并将状态反馈给主节点。至此,层内共识过程结束。

层内共识通过后,共识请求达成局部共识,地面层主节点 N_1 会将共识业务转发给层间共识的主节点 N_{13} ;然后进入层间共识,层间共识步骤与层内共识步骤相同。参与层间共识的节点与参与层内共识的节点不同,参与层间共识的节点为当前各层的主节点。层间共识通过后系统就认证请求达成一致,层间共识的主节点将共识结果广播给网络中的所有节点,并更新链上记录。至此,一次完整的共识过程就结束了。

HBFT算法共识流程如图4所示,当有节点资源变动或者节点请求接入时,节点会发起共识请求。网络中的节点收到共识请求后,根据节点的信任值,选取出每层的主节点和层间的主节点,然后进行层内节点之间的共识。层内共识通过后,层内主节点将共识请求转发给层间的主节点;每层的主节点之间进行层间共识,两个共识阶段都通过则同意节点的资源变动请求/接入请求,更新区块链上的资源信息和节点的信任值。如果层内共识或层间共识任一阶段共识失败,则直接结束共识,并更新相关节点的信任值。

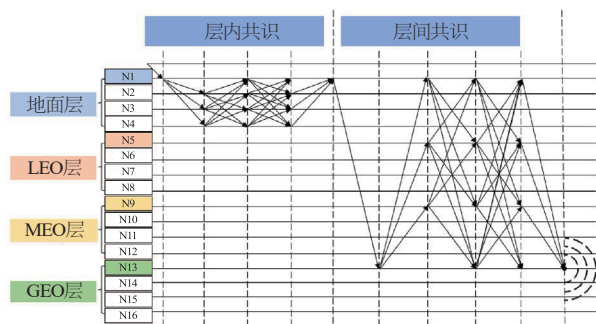


图3 HBFT算法的共识过程

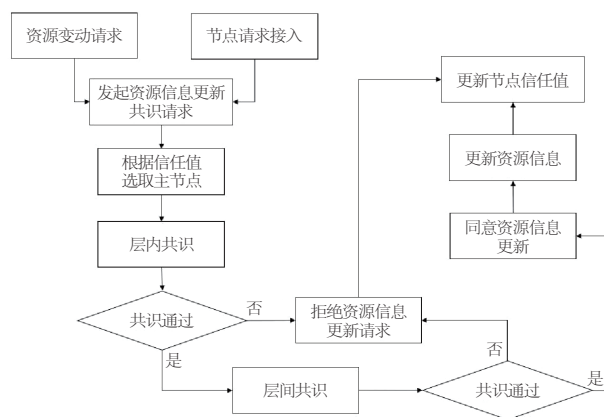


图4 HBFT算法共识流程

4 性能分析

为了验证HBFT算法的性能表现,本文从吞吐量、时间开销、算法稳定性、计算开销4个方面进行仿真实验。仿真实验运行的硬件环境:CPU型号为Intel Core i9-9900K,配置32GB内存,软件环境为Ubuntu 18.04.4 LTS。每组实验均设置46个虚拟节点,包含7个地面层节点、24个LEO层节点、12个MEO层节点和3个GEO层节点。受限于硬件环境,仿真实验中为一台主机模拟多个节点,故仿真结果不代表实际应用中算法的性能,在实际部署中,算法性能整体表现会有所提高。

4.1 吞吐量

在多层卫星网络架构下,网络具有覆盖范围广、节点数量多的特点。系统对共识机制的吞吐量有很高的要求。共识算法需要在有限的时间内完成尽可能多的共识业务。PBFT共识算法因其相对较高的吞吐量得到广泛应用。为了评估HBFT共识算法的吞吐量性能,设置10组吞吐量对比仿真实验,将HBFT共识算法的吞吐量性能与PBFT、PoW共识算法的吞吐量性能进行比较,分别统计3种不同共识算法在有限时间内可以完成的共识业务数量。其中PoW算法的计算难度为20,即需要计算得到随机数使得区块头的哈希值前20位为0,才能完成一次共识。

吞吐量仿真实验结果如图5所示,从图中可以看出,在1~10 s之间,每组实验表现最优的算法均为HBFT算法。HBFT算法的吞吐量性能约为PBFT算法的1.85倍。由于PoW算法在每个共识业务中都需要计算大量的哈希值,因此PoW算法的吞吐量是3种算法中最低的。PBFT算法复杂度为 $O(n^2)$,因此吞吐量性能不如HBFT。

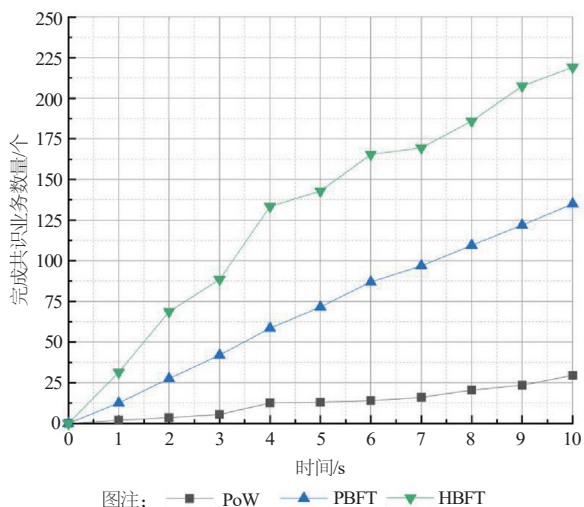


图5 吞吐量仿真实验

从吞吐量性能来看,HBFT算法的性能最好。这表明HBFT算法比其他共识算法更适合于高吞吐量的多层卫星互联网场景。

4.2 时间开销

本小节进行时间开销仿真实验。时间开销是指共识算法完成一定数量的共识业务所花费的时间。时间开销是共识算法综合性能的直观体现。

时间开销的仿真结果如图6所示。在业务量为50~500个的情况下,PoW算法在3种算法中花费的时间总是最高的。由于算法复杂度较高,每轮共识需要所有节点进行多次信息交互,因此PBFT算法在时间开销方面的性能不佳。HBFT算法采用分层机制,节点分阶段进行共识,降低验证的复杂度,因此在时间开销上表现最优。

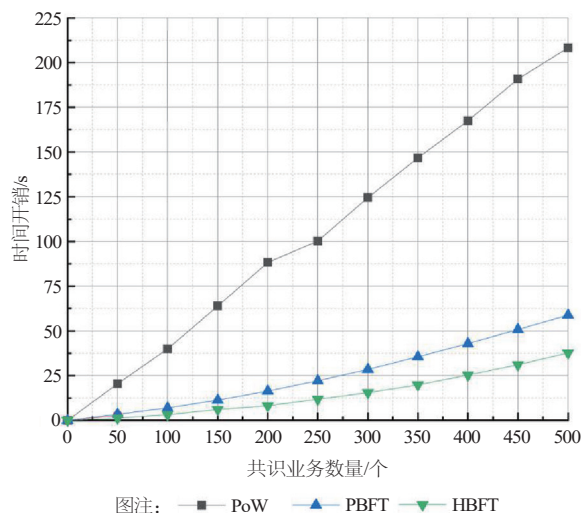


图6 时间开销仿真结果

从时间开销的角度来看,HBFT算法在减少时间开销、降低共识时延方面具有重要意义。

4.3 算法稳定性

在实际应用中,希望完成共识的时间是可预测的,即要求共识算法的时间开销在较小的范围内波动。因此,本小节进一步分析这3种算法的稳定性。通过算法完成共识业务花费时间的波动程度来评估算法的稳定性。每个算法在相同数量的共识业务下运行5次,根据5次时间开销之间的差异计算算法的稳定性参数。计算公式为

$$\sigma_n = \sqrt{\frac{1}{5} \sum_{i=1}^5 (T_i - t)^2} \quad (3)$$

σ_n 代表算法在不同业务量下的稳定性参数, σ_n 越低表

示算法越稳定。其中 t 为5次实验的平均时间开销， T_i 为每次实验的时间开销。

算法稳定性仿真结果如图7所示，从图中可以看出，在不同数量的共识业务实验中，PoW算法的稳定性总是最差的，稳定性波动较大。这是由PoW算法的不确定性造成的。因为SHR256算法的输出是不可预测的，所以在PoW算法中无法提前预知何时能计算出满足要求的随机数，这使得算法完成时间不可预测。在多层卫星互联网架构中，共识算法的时间开销需要可控，即能提前预估完成共识所需的时间，这对整个网络的稳定性至关重要。PoW算法不能满足稳定性要求。在3种共识算法中，PBFT算法的稳定性最好，HBFT算法稳定性与PBFT算法相近。综上，PBFT和HBFT共识算法的稳定性性能表现都很优秀，这两种算法的稳定性与PoW算法相比波动较小，都能够满足多层卫星互联网稳定性的要求。

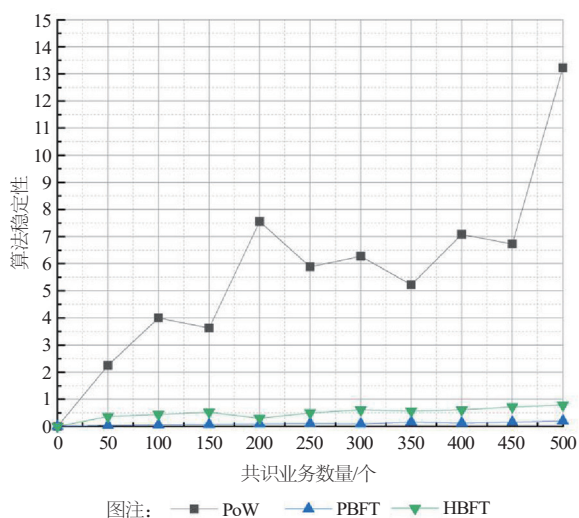


图7 算法稳定性仿真结果

4.4 计算开销

在多层卫星互联网架构中，计算能力是节点非常重要的资源，需要尽可能降低共识算法的计算开销。本节进行计算开销的仿真实验。

在运行这些共识算法仿真的同时每20 ms记录一次CPU占用数据。共识结束后，计算出共识算法运行期间的平均CPU占用率。CPU占用率能直观反映算法的计算开销。

不同算法的CPU平均占用率见表1，从中可以看出，PoW算法几乎占用所有CPU资源，其消耗的计算资源最多，远远高于其他两种算法。值得一提的是，在实际的PoW共识算法的应用中，消耗算力资源的同时会带来大量的电力消耗，因而PoW算法不适用节点数量多的多层

卫星网络架构。HBFT算法的CPU占用率最低，共识算法的低计算开销可以促进系统整体资源优化。HBFT算法由于采用分层共识，不需要所有节点同时共识，因而计算开销低。PBFT算法由于所有节点需要同时参与共识，共识中节点之间的频繁交互会增加CPU的负担，造成计算开销大。

表1 不同算法的CPU平均占用率

算法	CPU平均占用率
PoW	99.99%
PBFT	81.99%
HBFT	42.91%

综合来看，HBFT算法在每次仿真实验中都表现出优异的性能，尤其是吞吐量和计算开销等关键性能指标。HBFT算法高吞吐量、低计算开销的特点非常适合多层卫星网络架构。PoW算法吞吐量低、计算开销大，其并不适合资源受限的多层卫星互联网架构。PBFT算法由于计算开销高、可扩展性较差，也不适用于多层卫星互联网架构。

参考文献：

- [1] 郑小勇. 卫星互联网综述[J]. 科技资讯, 2007, 5(12): 45-46.
ZHENG X Y. Overview of satellite internet[J]. Science & Technology Information, 2007, 5(12): 45-46.
- [2] Internet World Stats. World internet users and 2021 population stats[Z]. 2021.
- [3] 李刚. 卫星互联网时代的技术攻坚者[J]. 科学中国人, 2020(19): 62-64.
LI G. Technological crusaders in the era of satellite internet[J]. Scientific Chinese, 2020(19): 62-64.
- [4] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[Z]. 2008.
- [5] 宋波, 刘铮, 冯云霞, 等. 基于区块链技术的医联体系统架构研究[J]. 计算机测量与控制, 2020, 28(9): 196-201.
SONG B, LIU Z, FENG Y X, et al. Research on architecture of medical alliance based on block chain technology[J]. Computer Measurement & Control, 2020, 28(9): 196-201.
- [6] 刘明瑶, 余益民. 基于区块链与零知识证明的物流隐私保护研究[J]. 软件导刊, 2021, 20(5): 153-157.
LIU M Y, YU Y M. Logistics privacy protection based on blockchain and zero knowledge proof[J]. Software Guide, 2021, 20(5): 153-157.

- [7] SUN S, DU R, CHEN S D, et al. Blockchain-based IoT access control system: towards security, lightweight, and cross-domain[J]. IEEE Access, 2021, 9: 36868-36878.
- [8] 张志强, 张永健, 王宇, 等. 低轨卫星网络中基于轨道分簇的密钥更新算法[J]. 电子与信息学报, 2010, 32(3): 687-692.
ZHANG Z Q, ZHANG Y J, WANG Y, et al. Rekeying algorithm based on orbital cluster in the LEO satellite network[J]. Journal of Electronics & Information Technology, 2010, 32(3): 687-692.
- [9] 余春东, 马雅琪, 贾潞汀, 等. 卫星网络中基于安全标签的安全监控模型: CN108234499A[P]. 2018-06-29.
SHE C D, MA Y Q, JIA L T, et al. Security monitoring model based on security label in satellite network: CN108234499A[P]. 2018-06-29.
- [10] 严开宇, 张艺, 章小宁, 等. 基于区块链的卫星自组织网络 BATMAN安全路由方法: CN113259940A[P]. 2021-08-13.
YAN K Y, ZHANG Y, ZHANG X N, et al. Satellite ad hoc network BATMAN secure routing method based on block chain: CN113259940A[P]. 2021-08-13.
- [11] 马煜. 基于区块链的星间通信网络安全加密控制系统设计[J]. 计算机测量与控制, 2021, 29(3): 171-175.
MA Y. Design of inter satellite communication network security encryption control system based on blockchain[J]. Computer Measurement & Control, 2021, 29(3): 171-175.
- [12] XU L C. Design and implementation of Internet of Things information security transmission based on PBFT algorithm[C]// Proceedings of 2020 International Conference on Computer Engineering and Application (ICCEA). Piscataway: IEEE Press, 2020: 201-205.
- [13] HU W, HU Y W, YAO W H, et al. A blockchain-based Byzantine consensus algorithm for information authentication of the Internet of vehicles[J]. IEEE Access, 2019, 7: 139703-139711.
- [14] CHEN Z L, CHEN S Z, XU H, et al. A security authentication scheme of 5G ultra-dense network based on block chain[J]. IEEE Access, 2018, 6: 55372-55379.
- [15] LIN H, GARG S, HU J, et al. A blockchain-based secure data aggregation strategy using sixth generation enabled network-in-box for industrial applications[J]. IEEE Transactions on Industrial Informatics, 2021, 17(10): 7204-7212.
- [16] LI W W, SU Z, LI R D, et al. Blockchain-based data security for artificial intelligence applications in 6G networks[J]. IEEE Network, 2020, 34(6): 31-37.
- [17] DAI Y Y, XU D, MAHARJAN S, et al. Blockchain and deep reinforcement learning empowered intelligent 5G beyond[J]. IEEE Network, 2019, 33(3): 10-17.
- [18] CHRISTIDIS K, DEVETSIKIOTIS M. Blockchains and smart contracts for the Internet of Things[J]. IEEE Access, 2016, 4: 2292-2303.
- [19] 陈汇文, 郭东超, 李莉, 等. 数字加密货币网络拓扑结构特征分析[J]. 电子技术与软件工程, 2020(20): 232-236.
CHEN H W, GUO D C, LI L, et al. Analysis of network topology characteristics of digital cryptocurrency[J]. Electronic Technology & Software Engineering, 2020(20): 232-236.
- [20] CASTRO M, LISKOV B. Practical Byzantine fault tolerance and proactive recovery[J]. ACM Transactions on Computer Systems, 2002, 20(4): 398-461.

[作者简介]



朱睿杰 (1988-), 男, 博士, 郑州大学副教授, 硕士生导师, 主要研究方向为6G天地一体化信息网络、机器学习等。



张玉东 (2000-), 男, 郑州大学信息工程学院硕士生, 主要研究方向为区块链技术、卫星网络安全等。



魏雅婷 (1999-), 女, 郑州大学信息工程学院硕士生, 主要研究方向为卫星网络故障定位、卫星网络安全等。



席超 (1988-), 男, 航天恒星科技有限公司高级工程师, 主要研究方向为卫星通信与卫星运行控制、卫星定位与导航等。