基于区块链的频谱设备网络中防御拜占庭攻击的分布式共识机制

杨健[1]，陈曦[2]，丁国如[3]，赵杭生[4]，张林元[5]，孙佳琛[3]

（1. 国防科技大学第六十三研究所，江苏 南京 210007；2. 南京理工大学机械工程学院，江苏 南京 210094；
3. 陆军工程大学通信工程学院，江苏 南京 210007；4. 南京邮电大学通信与信息工程学院，江苏 南京 210003；
5. 江南计算技术研究所，江苏 无锡 214146）

摘 要：针对大规模、超密集部署移动互联网和物联网引发的精确频谱共享需求，基于区块链技术提出联网海量个人无线设备构成频谱设备网络：频谱管理服务器、移动基站、个人无线设备形成云计算与边缘计算相结合的频谱设备网络架构，以频谱数据获取、频谱区块添加、频谱数据传输、频谱数据采集的激励构成了基于区块链的频谱设备网络的基本运行机制，通过感知节点共识融合、验证节点共识验证、簇头节点共识确认，在一定置信度下的假设检验判断是否有恶意感知节点发动伪造频谱数据的拜占庭攻击。仿真结果表明分布式共识机制在防御恶意感知节点伪造频谱数据的拜占庭攻击上的有效性和可靠性。

关键词：区块链；频谱设备网络；分布式共识机制；拜占庭攻击

中图分类号：TN92

文献标识码：A

doi: 10.11959/j.issn.1000−436x.2020044

Blockchain-driven distributed consensus mechanism in defensing Byzantine attack for the Internet of spectrum device

YANG Jian[1], CHEN Xi[2], DING Guoru[3], ZHAO Hangsheng[4], ZHANG Linyuan[5], SUN Jiachen[3]

1. 63rd Institute, National University of Defense Technology, Nanjing 210007, China
2. School of Mechanical Engineering, Nanjing University of Science and Technology, Nanjing 210094, China
3. College of Communications Engineering, Army Engineering University, Nanjing 210007, China
4. School of Telecommunication and Information Engineering, Nanjing University of Posts and Telecommunications, Nanjing 210003, China
5. Jiangnan Institute of Computing Technology, Wuxi 214146, China

Abstract: To meet the requirement of the precisely spectrum sharing triggered by large-scale and ultra-dense deployment of mobile internet and internet of things, a framework based on blockchain technology for networking the massive personal wireless devices to form the Internet of spectrum device (IoSD) was proposed. The architecture of cloud with edge computing was proposed as the architecture of IoSD, which consists of spectrum management server, mobile base station, and personal wireless devices.The mechanism of spectrum data acquisition, spectrum block appending, spectrum data transmission, and spectrum sensing incentive, consist of basic operational mechanism of IoSD.The distributed consensus mechanism, including fusion consensus among sensing-nodes, verification consensusamong checking-nodes, and confirmation consensus among head-nodes, was applied to determine whether the spectrum data was falsified by the Byzantine attack of malicious sensing-nodesunder the hypothesis test of certain confidence. The simulation results show the effectiveness and robustness of proposed distributed consensus mechanism in preventing spectrum sensing data falsification by the malicious nodes.

Key words: blockchain, Internet of spectrum device, distributed consensus mechanism, Byzantine attack

---

收稿日期：2019−07−04；**修回日期**：2020−02−16

通信作者：陈曦，chenxi@njust.edu.cn

基金项目：国家自然科学基金资助项目（No.61871398, No.61931011）；江苏省杰出青年基金资助项目（No.BK20190030）；中国博士后科学基金资助项目（No.2018M633769）；装备预研领域基金资助项目（No.61403120304）

Foundation Items: The National Natural Science Foundation of China (No.61871398, No.61931011), The Natural Science Foundation for Distinguished Young Scholars of Jiangsu Province (No.BK20190030), China Post-Doctoral Science Funded Project (No.2018M633769), Equipment Advanced Research Field Foundation (No.61403120304)

1 引言

移动互联网和物联网的蓬勃发展进一步加剧了频谱资源紧缺的现状[1-2]，频谱共享被广泛认为是一种近期可实现的缓解频谱资源紧缺现状的有效途径[3]。随着移动通信网络向更高频段寻求可用频谱资源的拓展[4]，物联网的网络节点和设备越来越呈现出超密集部署的趋势[5]，频谱共享需要在更精准的时间划分、更宽的频谱范围、更细粒度的地理区域及更精准的功率控制上实现[6]。这种更加精确的频谱共享一方面需要更长时间、更宽频谱及更广地理范围的频谱数据支撑，另一方面需要进一步提高频谱数据在时域、频域、空域的分辨率以满足更精确的频谱共享需求。

然而，当前频谱数据采集与频谱策略推理的分离使精确频谱共享无法实现。频谱使用设备并不“了解”所在区域的电磁环境状况，只能按照既定的方案使用频谱资源；频谱管理机构集中管理频谱监测设备，得到离散的、碎片化的、稀疏的频谱数据，但频谱使用设备缺乏获取这些频谱数据的渠道，因此，精确的频谱共享一方面需要整合频谱使用设备和频谱监测设备，打通频谱数据的沟通渠道；另一方面需要促使海量具有频谱感知功能的频谱设备加入，拓展频谱数据在时域、频域、空域上的覆盖率，提高频谱数据在时域、频域、空域的分辨率水平，支撑频谱共享以更精确的方式实现。

区块链技术的出现为实现更高效的动态频谱管理提供了可能。区块链是一种公共分类账，按时间顺序记录所有交易，通过共识机制确保交易记录的不可篡改性。普遍认为，区块链技术可以帮助动态频谱管理改进安全性和提供激励机制，从而达到更有效的动态频谱管理[7-9]。美国联邦通信委员会（FCC, Federal Communications Commission）的发言人Rosenworcel在2018移动世界大会上的演讲中说到，基于区块链的动态频谱共享将是6G迈向太赫兹频率的关键技术，通过分布式数据库支持频谱共享接入，降低系统管理开销的同时提升频谱效率[10]。此外，文献[11]引入了区块链作为安全分类账来记录由授权用户发起的频谱拍卖信息，所有用户参与频谱交易的验证和维护。文献[12]基于区块链提出了一种安全的协作频谱感知动态频谱接入系统，通过协作频谱感知探索频谱接入机会，通过频谱拍卖分配频谱接入机会，并将所有频谱拍卖信息安全地存储在区块链中。上述工作均采用公有的区块链架构，所有用户参与区块链维护，有的虽然采用智能合约激励次级用户执行高效、有序的频谱感知[13]，但仍需网内所有用户参与共识，有的通过云与边缘计算结合的网络结构完成挖矿[14-15]，降低了区块链中挖矿的能耗，但本质上仍是类似于比特币系统的工作性证明共识机制，共识结果是有分叉的和概率性的。因此，安全、高效的共识机制设计是基于区块链的频谱共享中的开放性课题。

文献[16]提出集成频谱使用设备和频谱监测设备，构成基于云的频谱设备网络，使频谱监测设备获取的频谱数据能够直接用于指导频谱使用设备以恰当的方式使用频谱资源。然而，专业化的频谱监测设备价格高、数量少，日常监测往往只能得到频域上不连续、时域上碎片化、空域上稀疏的频谱数据，难以实现对时域、频域、空域的充分覆盖，无法为精确的频谱共享提供足够的频谱状态信息支撑。

幸运的是，随着个人无线设备（如智能手机、平板电脑、车载无线设备等）智能化水平的提高，越来越多的传感器被配置到个人无线设备上，使个人无线设备具备了可观的频谱感知能力[17]。如果能够促使海量的个人无线设备加入频谱设备网络，将大大提高时域、频域、空域的频谱数据覆盖水平[18]。然而，海量个人无线设备加入频谱设备网络，以充分覆盖时域、频域、空域的海量频谱数据为精确频谱共享提供支撑时，会带来很多新的问题。首先，基于云的集中式网络结构不再适用于管理海量的个人无线设备。海量个人无线设备的数据交互将产生巨大的时延，数据同步将导致过于复杂的处理架构和帧结构，因此，采用分布式的网络结构和异步的处理架构将是频谱设备网络管理海量个人无线设备的必然选择。然后，频谱数据的采集和共享均需消耗个人无线设备的能量。由于采用电池供电，个人无线设备一般对能量消耗敏感，因此，需要设计专门的激励机制，激励个人无线设备将有限的能量投入近似于“公益”的频谱数据采集中。最后，分布式的网络结构和异步的处理架构往往要求开放的数据处理与融合方式。在激励机制的驱动下，少数恶意的个人无线设备倾向于通过伪造的频谱数据“牟取”不当利益，因此，必须针对恶意个人无线设备伪造频谱数据（SSDF, spectrum sensing

data falsification）的拜占庭攻击设计防御机制，确保频谱数据的质量。

针对以上问题，本文提出了一种基于区块链的分布式频谱设备网络架构，设计了一种防御恶意用户伪造频谱数据拜占庭攻击的共识机制，使频谱数据能够被频谱设备网络更广泛地收集，更高效、更安全地存储和流通，以支撑精确频谱共享的实现。本文创新点主要体现在以下 3 个方面。

1) 提出一种云计算与边缘计算结合的分布式频谱设备网络结构，集成海量个人无线设备构成频谱设备网络。个人无线设备同时作为频谱使用设备和频谱感知设备，频谱管理服务器在频谱设备网络云端发布频谱感知任务、回收频谱数据、发放任务奖励。个人无线设备与移动基站在频谱设备网络边缘采集频谱数据、验证频谱数据、将频谱区块添加至频谱区块链，支撑频谱数据更高效地存储和流通。

2) 定义“频谱币”作为专门的数字货币，用于激励个人无线设备采集频谱数据，频谱币在频谱设备网络中发行和流通，可用于购买额外的频谱使用权、流量和带宽，支撑频谱数据更广泛地收集。

3) 面向恶意用户伪造频谱数据的拜占庭攻击，提出一种分布式共识机制，通过感知节点间共识融合、验证节点间共识验证、簇头节点间共识确认这 3 个共识过程剔除伪造频谱数据并添加至频谱区块链，仿真结果证明了该共识机制防御 SSDF 拜占庭攻击的有效性和稳健性，支撑频谱数据更加安全地存储和流通。

2　基于区块链的频谱设备网络

2.1　区块链及其关键技术

区块链是一种公共分类账，它按时间顺序记录所有交易，通过共识机制确保交易记录的不可篡改性，其特点包括不可篡改性、去中心化、永久性和匿名性。该公共分类账记录了网络节点之间发生的每笔交易的细节，而不涉及任何可信的中心节点，所有相关节点的分类账副本是同步的，从而降低了系统因故障而宕机的风险[19]。驱动区块链运行的关键技术主要有以下几种。

去中心化存储。区块链以去中心化的方式在不同物理地址的多个网络节点进行数据的共享与同步，且区块链网络的相关节点均拥有完整的区块链数据副本，各节点依靠共识机制独立对等地保证存储数据的一致性，也通过去中心化存储来确保区块链数据的安全性，即只有得到区块链网络中大多数节点的共识才能实现对已有数据的篡改，即“51%攻击”。

非对称加密。区块链采用哈希算法和非对称加密来确保区块链数据的完整性和数据的安全传输。哈希算法用于产生区块链中各个区块的头信息，并通过在区块头中包括的前一区块的头信息实现区块之间的连接，同时通过 Merkle 树对区块中的具体数据进行结构化组织并将概要信息存入区块头。节点通过私钥加密的数字钱包（类似于银行账户）来进行交易，节点可通过私钥生成签名访问自己的数字钱包并认证交易，而对应的公钥作为地址公布在网络上。

共识机制。共识机制用于解决分布式系统的一致性问题，在中本聪的比特币系统中，区块链采用一种称为“工作性证明”的共识机制进行状态更新。节点（矿工）通过大量计算竞争在 10 min 内找到小于目标区块哈希值的目标值来获得对目标区块的记账权，一旦某个节点找到该目标值，就将其在网络中公开，其他节点通过签名来验证该目标值，通过这种方式在互不信任的节点之间达成共识[20]。随着区块链技术的发展，目前区块链系统可分为公有链、私有链和联盟链，同时也衍生出实用拜占庭容错（PBFT, practical Byzantine fault tolerance）、工作性证明(PoW, power of work)、权益证明（PoS, power of stake）等多种共识机制[21]。

智能合约。智能合约是以数字形式定义的一组承诺，以及履行这些承诺的协议。区块链网络为智能合约提供了可信的执行环境，区块链的智能合约是一段代码，一旦某个事件触发智能合约中的条款，代码就自动执行，不需要依赖第三方或中心化机构，这极大地提高了执行效率和准确性。

2.2　频谱设备网络

集成智能手机、平板电脑、智慧家居设备、车载无线设备等异构的个人无线设备，海量的个人无线设备融合后并没有产生中心控制节点，而是形成了分布式的网络结构。频谱设备网络通过云计算与边缘计算相结合的方式降低频谱数据的传输时延和数据传输能耗，频谱管理服务器、移动基站、个人无线设备形成三级的频谱设备网络结构，如图 1 所示。频谱设备网络包含多个频谱管理服务器，按区域管理频谱设备网络，频谱管理服务器部署在云

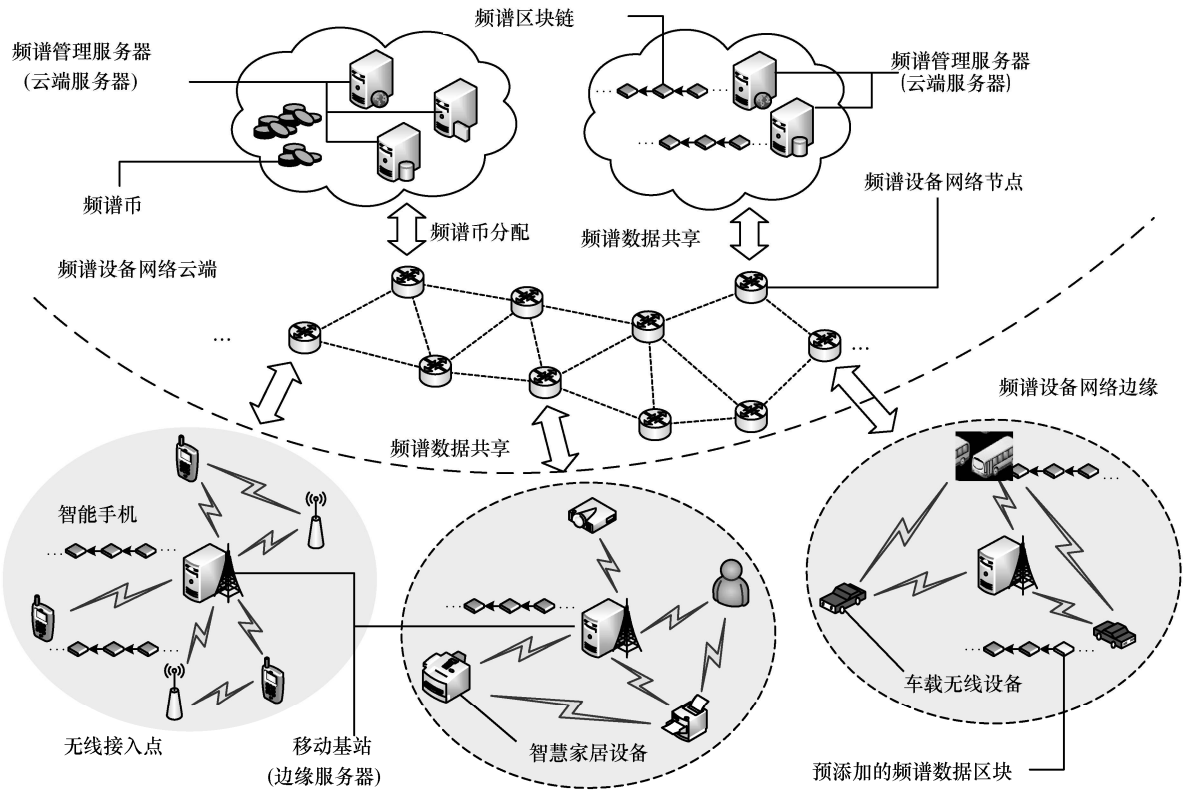


图1　云计算与边缘计算结合的分布式频谱设备网络架构

端，负责发布频谱感知任务和提出任务要求；移动基站部署在频谱设备网络边缘，直接与个人无线设备进行数据交互；个人无线设备是频谱设备网络的末端，既是频谱使用设备，也是频谱感知设备，个人无线设备通过贡献频谱数据获得频谱币，可用来购买额外的频谱使用权、流量和带宽。

由于本文涉及较多节点类型，为便于读者理解，简要介绍如下。

1) 感知节点：个人无线设备在执行频谱管理服务器发布的频谱数据采集任务时，被称为感知节点。

2) 簇头节点：若干个人无线设备以簇的形式共同执行频谱管理服务器发布的频谱数据采集任务时，领导该任务完成的个人无线设备被称为簇头节点。

3) 验证节点：个人无线设备通过分布式共识验证频谱子区块是否符合频谱数据采集任务要求时，被称为验证节点。

2.3　频谱区块的添加

如图2所示，从个人无线设备采集频谱数据，到形成频谱区块，并添加到频谱区块链中，历经4个步骤，详述如下。

步骤 1　频谱管理服务器发布频谱数据采集任务，感知节点采集频谱数据。

频谱管理服务器部署在频谱设备网络云端，定期发布频谱数据采集任务，提出包括采集时间要求、频段范围限制、地理区域限定等的频谱数据采集任务要求，频谱数据采集任务对频谱设备网络中所有服务器和节点可见。在频谱管理服务器发布频谱数据采集任务的同时，频谱设备网络自动产生并预存相应的频谱币作为频谱数据采集任务的完成奖励。

分布式部署的个人无线设备根据自身的行动计划、电池电量、地理位置决定是否响应频谱数据采集任务。响应任务的个人无线设备数量与任务规定的地理区域有关，如果任务限定在无人的沙漠或者戈壁，可能没有设备响应任务，则频谱数据采集任务失效；如果任务限定在偏僻的远郊，可能只有寥寥数台设备响应任务；如果任务限定在繁华的城区，可能有数十台甚至上百台个人无线设备响应任务，这些个人无线设备自发地形成若干个簇，每个簇包含一个簇头节点和若干感知节点，感知节点在簇

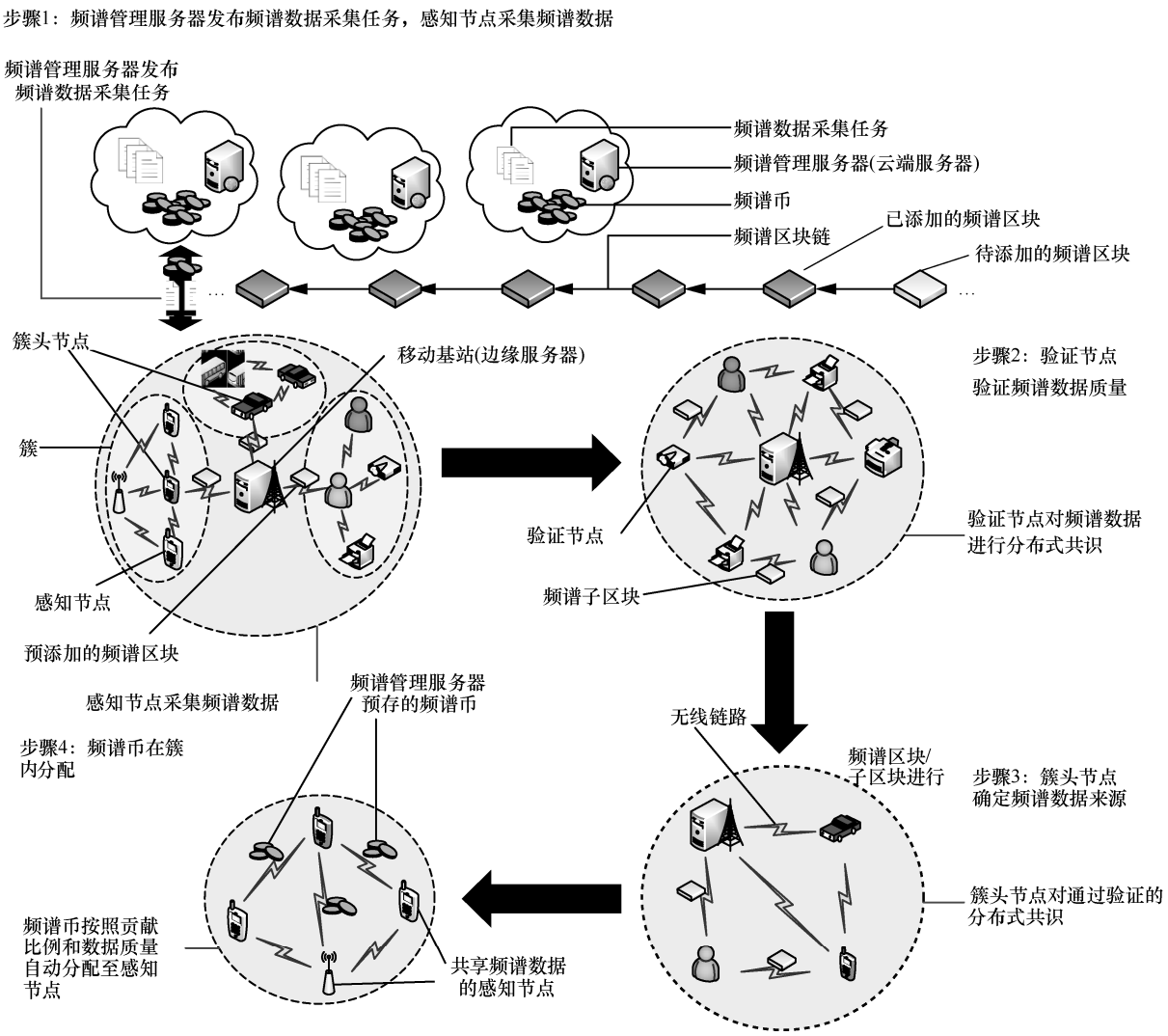


图 2　个人无线设备采集频谱数据、形成频谱数据、添加到频谱区块链的过程按步骤划分区域

头节点的领导下采集频谱数据，并对所采集的频谱数据进行分布式共识，形成一致的频谱子区块。

在基于区块链的众包、群智感知等应用中，簇的形成和簇头节点的选取受到研究者们的关注。文献[22]根据历史数据共享结果为节点评分，簇内得分最高的节点成为簇头节点；文献[23]设计了一种基于信誉值的簇头节点选取机制，根据数据共享质量为节点赋予信誉值；文献[24]利用模糊理论选取簇头节点，根据地理位置、服务能力计算节点与感知任务的匹配程度，匹配程度最高的节点成为簇头节点。簇头节点的选取和簇的形成是保证频谱数据采集效率和准确性的关键环节，本文根据地理位置以及与感知任务的匹配程度进行簇头节点的选取和簇的形成[25]。假设感知节点 A 发现频谱管理服务器发布的频谱数据采集任务后，在任务规定预设的最少簇内节点数量和最多簇内节点数量之间随机确定一个数值（假设为 N_c）作为簇内节点数量，然后，感知节点 A 向周围广播邀请信息（CFD, cluster formation demand），邀请其他感知节点加入簇，共同完成频谱数据采集任务，其中，CFD 包括频谱数据采集任务要求和簇内节点数量。可能有多个感知节点同时向周围广播 CFD，假设感知节点 B 收到了多个感知节点广播的 CFD，则感知节点 B 按照接收信号功率对 CFD 排序，向队列中具有最大接收信号功率的感知节点（假设为感知节点 A）发送加入回复信息（CFR, cluster formation reply）。当感知节点 A 收到 CFR 时，将对 CFR 计数，按照接收信号功率对感知节点排序，向队列中的前 N_c 个感知节点发送加入确认信息（CFA, cluster formation acknowledgement），并向队列中的其他感

知节点发送加入拒绝信息（CFN, cluster formation non-acknowledgement）。若感知节点 B 收到 CFA，则加入该簇；若感知节点 B 收到 CFN，则不加入该簇。当频谱数据采集任务规定的簇形成时间截止时，符合频谱数据采集任务要求（如簇内节点数量）的簇执行频谱数据采集任务，与频谱数据采集任务中心地理位置匹配程度最高的感知节点成为各个簇的簇头节点。

簇头节点下载距离最近的边缘服务器（移动基站）公钥，用该公钥产生的签名加密频谱子区块，并上传至该边缘服务器，边缘服务器利用私钥产生的签名解密得到频谱子区块。频谱设备网络的每个设备（包括边缘服务器、云端服务器）都拥有一对密钥，即公钥和私钥，公钥作为地址公布在网上，任何节点均可下载并产生签名加密频谱数据；私钥保存在设备端产生签名解密频谱数据。

步骤 2　验证节点验证频谱数据质量。

簇头节点通过边缘服务器发布频谱子区块验证任务，同时在频谱设备网络预存频谱币作为验证奖励（验证奖励只需少量的频谱币，但当节点成为簇头节点时，需保证拥有足够的频谱币作为验证奖励）。边缘服务器附近的其他个人无线设备自主响应验证任务，成为验证节点。验证节点通过分布式共识验证频谱子区块是否符合频谱数据采集任务要求。一种极端情况是没有频谱子区块通过验证，表明频谱数据采集任务失败，此时预存的频谱币被频谱设备网络回收。完成验证任务后，频谱数据网络将簇头节点预存的频谱币释放给参与验证任务的验证节点。

步骤 3　簇头节点确定频谱数据来源。

簇头节点对通过验证的频谱子区块进行分布式共识，以确定哪一个频谱子区块被添加到频谱区块链中，提供该频谱子区块的簇将获得一部分频谱币。各簇簇头节点通过分布式共识得到共识结果，将 Q^* 与各簇所提供的原始频谱数据相比，差异最小的频谱数据被认为是该频谱子区块的提供者，获得频谱币奖励。需要注意的是，簇头节点之间分布式共识的结果与各簇头节点提供的频谱子区块之间存在误差，误差最小的频谱子区块将被添加到频谱区块链中。簇头节点之间的分布式共识激励个人无线设备努力提高频谱数据质量，只有最符合任务要求的频谱子区块才能被添加到频谱区块链中，使簇内的感知节点获得相应的频谱币。

若干频谱子区块以 Merkle 树结构组织成为频谱区块，频谱区块的结构如图 3 所示。每个频谱区块在区块头中包含前一区块的地址（该地址通过哈希算法加密），直到第一频谱区块（创始频谱区块）的前一区块的地址（该地址通过哈希算法加密），并按时间顺序首尾相接成为频谱区块链。

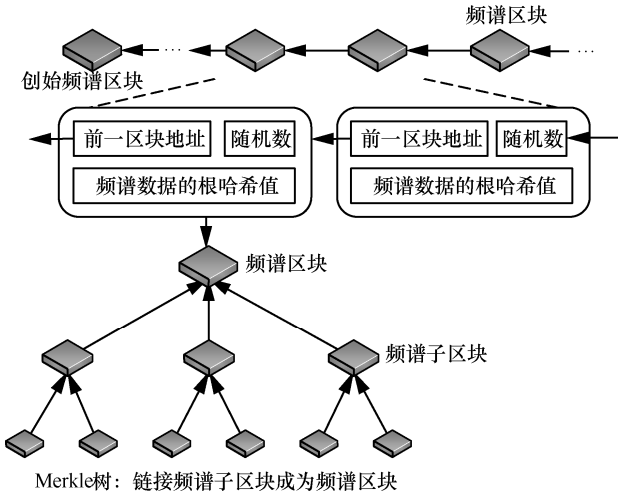


图 3　频谱区块的结构

步骤 4　频谱币在簇内分配。

当频谱区块被添加到频谱区块链中成为正式频谱区块后，频谱设备网络预存的频谱币释放至提供该频谱区块的簇，并根据各簇对频谱区块的贡献比例和数据质量将频谱币分配至各簇。根据所提频谱设备网络和频谱区块链的运行机制，每产生 M GB 符合要求的频谱数据，频谱设备网络即发行 S 个频谱币。假设某频谱数据采集任务将产生 X MB 频谱数据，频谱设备网络发行并预存 $\frac{SX}{2^{10}M}$ 频谱币，其中，簇 1、簇 2、…、簇 n 依次贡献了 x_1、x_2、…、x_n MB 的频谱数据，则当 X MB 频谱数据被添加到频谱区块后，簇 1、簇 2、…、簇 n 依次分配得到 $\frac{SX_1}{2^{10}M}$、$\frac{SX_2}{2^{10}M}$、…、$\frac{SX_n}{2^{10}M}$ 频谱币。各簇再根据各感知节点对频谱子区块的贡献比例和数据质量将频谱币分配至感知节点。续前例，从簇 1、簇 2、…、簇 n 分配得到的 $\frac{SX_1}{2^{10}M}$、$\frac{SX_2}{2^{10}M}$、…、$\frac{SX_n}{2^{10}M}$ 频谱币中扣除簇头节点预先付出的 c %作为验证奖励后，频谱币在各簇内平均分配，假设簇 1、簇 2、…、簇 n

内分别含有 N_1、N_2、…、N_n 个节点，簇 1、簇 2、…、簇 n 内节点（包括感知节点和簇头节点）依次分配得到 $\frac{S\,x_1(1-c\%)}{2^{10}N_1M}$、$\frac{S\,x_2(1-c\%)}{2^{10}N_2M}$、…、$\frac{S\,x_n(1-c\%)}{2^{10}N_nM}$ 频谱币。注意到，频谱币根据簇和感知节点对频谱数据的贡献比例和数据质量在簇间和簇内自动分配。

频谱管理服务器对个人无线设备进行准入许可之后，个人设备加入频谱设备网络，将频谱管理服务器和边缘服务器视为频谱区块链的记账人，每个频谱区块的添加由记账人共同决定，因此，频谱区块链实质上为一种联盟链。

2.4　频谱数据的获取

采集频谱数据形成频谱区块链，以更长时间、更宽频谱、更广地理范围的频谱大数据支撑精确的频谱共享。频谱数据具有明显的大数据特征，假设用 1 bit 来表示 100 m×100 m 范围内、频率分辨率为 100 kHz、时间分辨率为 100 ms 的频谱状态，那么 100 km×100 km 的地理范围、0~5 GHz 的频谱范围、一个星期的时间跨度内累计的频谱数据量将达到

$$\frac{7\text{ days}}{1\text{ week}}\times\frac{24\text{ hours}}{1\text{ day}}\times\frac{3600\text{ seconds}}{1\text{ hour}}\times\frac{1\text{ second}}{100\text{ ms}}\times\frac{5\text{ GHz}}{100\text{ kHz}}\times\frac{100\text{ km}\times100\text{ km}}{100\text{ m}\times100\text{ m}}\times1\text{ B}=3.024\times10^{17}\text{ B/week}=3.024\times10^{5}\text{ TB/week}$$

并且，频谱数据量不仅随着地理范围、频谱范围、时间跨度的扩大而增加，还将随着空间分辨率、频率分辨率、时间分辨率的提高而增加，海量频谱数据的处理和存储是频谱设备网络面临的重要挑战之一。

云计算以集中方式处理和存储频谱数据，显然已不再适合集成了海量个人无线设备、综合了海量频谱数据的频谱设备网络。移动边缘计算是新兴的计算模型，它将云计算及其服务扩展到网络边缘，采用集中式与分布式相结合的网络结构。将移动边缘计算应用于分布式的频谱设备网络，个人无线设备、移动基站、频谱管理服务器形成三级网络结构。如图 4 所示，在频谱设备网络云端，移动基站和频谱管理服务器以集中的方式进行组网和管理；在频谱设备网络边缘，个人无线设备和移动基站以分布的方式进行组网和管理。具体而言，个人无线设备在本地采集频谱数据，并对频谱数据进行预处理，从而大大减少了需要交互的频谱数据量；边缘服务器（移动基站）依托个人无线设备在网络边缘完成频谱区块验证和添加；当新频谱区块添加至频谱区块链后，边缘服务器将新频谱区块的索引上传至频谱设备网络的云端，方便用户查询和下载。

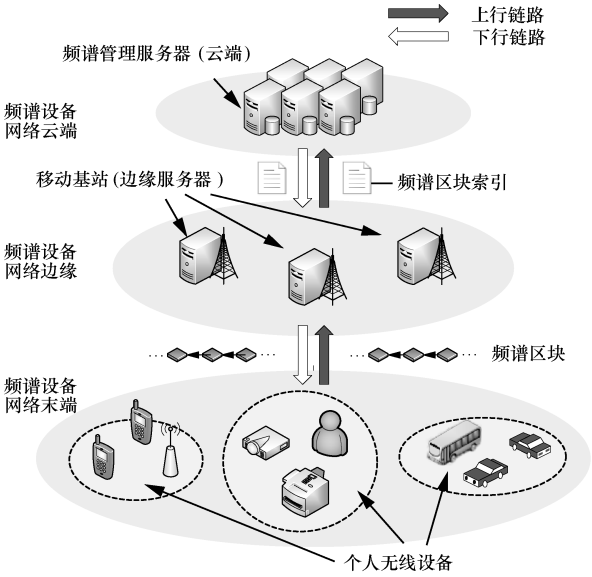


图 4　频谱设备网络的三级网络结构

区块大小已成为影响区块链网络吞吐率、交易时延、可容纳节点数量，进而影响区块链网络可扩展性的关键因素之一[26]。文献[27]证明了要保证区块链网络 90%节点的吞吐率，区块链的大小不应超过 4 MB，因此，为了保证频谱设备网络中节点的吞吐率，频谱区块大小应小于 4 MB。研究者在缩减区块大小方面进行了诸多尝试，文献[28]提出了区块分片技术，将较大的区块数据分为更小、更快、更易于管理的子区块；文献[29]提出区块仅保留区块头，将数据量大的区块体存放在边缘服务器，使用户可以通过查询区块头找到区块体的存放地址，而用户与边缘服务器之间的沟通则通过专门的数据传输信道进行。借鉴文献[29]的策略压缩频谱区块链的大小，具体是，新的频谱区块添加到频谱区块链之后，提供该频谱区块的簇头节点将频谱数据信息写入区块体，用哈希算法生成频谱数据信息的摘要，并用自己的私钥对此摘要信息加密，上传至最近的边缘服务器，其他用户可用该簇头节点的公钥解密摘要信息，以验证频谱数据未被修改，具体见 2.5 节。边缘服务器收到频谱区块体后，通过非对称加密的方式将频谱区块体的存放地址发送给该簇头节点，该簇头节点将频谱区块的基本信息，如数据采集时间、数据采集地点、设备参数等数据采集信息、区

块体存储地址等关键信息写入区块头，区块头被添加到频谱区块链中成为频谱区块。这样，频谱区块链仅保存区块头信息，大大降低了频谱区块链的数据量。

尽管上述方法大大压缩了频谱区块链的数据量，然而，边缘服务器的存储空间也是有限的，频谱数据的日积月累必将填满边缘服务器的存储空间；其次，频谱区块体的日积月累也将导致频谱区块链数据量的增加。为此，频谱区块链需要随时间流逝定期丢弃一部分频谱区块，同时删除存放在边缘服务器的频谱区块体，保证频谱区块链的数据量总体保持不变。

在精确频谱共享中，绝大部分频谱数据（本文为频谱区块和子区块的形式）在本地产生、在本地使用，较少有跨地域的频谱数据使用需求。当用户需要使用本地的频谱数据支撑精确频谱共享时，个人无线设备接入最近的边缘服务器查询并下载所需的频谱区块；当个人无线设备需跨地域（异地）使用频谱数据支撑精确频谱共享时，个人无线设备向频谱管理服务器（云端）提出申请并预存频谱币，云端的频谱管理服务器根据频谱区块索引匹配距离最近的验证节点，并向个人无线设备发送该频谱区块索引，个人无线设备下载该验证节点的公钥，验证节点配合将所需频谱区块传输给个人无线设备，个人无线设备完成下载后确认，验证节点获得频谱币奖励。

2.5 频谱数据的传输

个人无线设备之间或个人无线设备与边缘服务器/云端服务器之间通过频谱设备网络以非对称加密的方式传输频谱数据/频谱币。频谱设备网络的每个设备（包括边缘服务器和云端服务器）均拥有一对密钥，即公钥 $\mathrm{key}^{\mathrm{public}}$ 和私钥 $\mathrm{key}^{\mathrm{private}}$，公钥作为公布在网上，任何节点均可下载并加密频谱数据；私钥保存在设备终端解密频谱区块。

频谱设备网络可以通过非对称加密的方式传递数据。例如，当节点 A 需要将频谱数据 Data 传输给节点 B 时，首先查询并下载节点 B 的公钥 $\mathrm{key}_{\mathrm{B}}^{\mathrm{public}}$，用公钥 $\mathrm{key}_{\mathrm{B}}^{\mathrm{public}}$ 加密频谱数据 data 得到交易 $\mathrm{record}_{\mathrm{data}}$，如式(1)所示。

$$\mathrm{record}_{\mathrm{data}} = \mathrm{RSA}(\mathrm{data}, \mathrm{key}_{\mathrm{B}}^{\mathrm{public}}) \tag{1}$$

其中，$\mathrm{record}_{\mathrm{data}}$ 是加密后得到交易记录，RSA 为非对称加密算法。当节点 B 收到交易后，用自己的私钥 $\mathrm{key}_{\mathrm{B}}^{\mathrm{private}}$ 解密交易 $\mathrm{record}_{\mathrm{data}}$，得到频谱数据 Data，如式(2)所示。

$$\mathrm{data} = \mathrm{DSA}(\mathrm{record}_{\mathrm{data}}, \mathrm{key}_{\mathrm{B}}^{\mathrm{private}}) \tag{2}$$

频谱设备网络也通过非对称加密的方式验证频谱数据未被修改。当节点 B 向边缘服务器上传频谱数据 data 时，节点 B 用哈希算法生成频谱数据 data 的摘要，如式(3)所示。

$$\mathrm{digest}_{\mathrm{data}} = \mathrm{hash}(\mathrm{data}, \mathrm{key}_{\mathrm{B}}^{\mathrm{public}}) \tag{3}$$

节点 B 使用私钥 $\mathrm{key}_{\mathrm{B}}^{\mathrm{private}}$ 对 $\mathrm{digest}_{\mathrm{data}}$ 加密，生成数字签名，如式(4)所示。

$$\mathrm{sign}_{\mathrm{digest}} = \mathrm{RSA}(\mathrm{digest}_{\mathrm{data}}, \mathrm{key}_{\mathrm{B}}^{\mathrm{private}}) \tag{4}$$

节点 B 将数字签名 $\mathrm{sign}_{\mathrm{digest}}$ 附在频谱数据 Data 之后，上传至边缘服务器。其他节点可以在边缘服务器查看该频谱数据 Data，用节点 B 的公钥 $\mathrm{key}_{\mathrm{B}}^{\mathrm{public}}$ 解密数字签名 $\mathrm{sign}_{\mathrm{digest}}$，得到频谱数据的摘要 $\mathrm{digest}_{\mathrm{data}}$，如式(5)所示。

$$\mathrm{digest}_{\mathrm{data}} = \mathrm{RSA}(\mathrm{sign}_{\mathrm{digest}}, \mathrm{key}_{\mathrm{B}}^{\mathrm{public}}) \tag{5}$$

再对频谱数据使用哈希算法，如式(6)所示。

$$\mathrm{digest}'_{\mathrm{data}} = \mathrm{hash}(\mathrm{data}, \mathrm{key}_{\mathrm{B}}^{\mathrm{public}}) \tag{6}$$

将得到的结果与频谱数据摘要对比，若两者一致，即 $\mathrm{digest}'_{\mathrm{data}} = \mathrm{digest}_{\mathrm{data}}$，说明频谱数据未被修改过。

2.6 频谱数据采集的激励机制

频谱设备网络通过“频谱币”及相应的配套策略激励个人无线设备采集频谱数据。频谱币是在频谱设备网络中发行和流通的数字货币，由频谱设备网络发行，仅在频谱设备网络中流通，可用于购买额外的频谱使用权、流量和带宽等。

频谱币的定价策略。频谱币的定价与频谱区块挂钩，规定每个频谱区块包含 M GB 的频谱数据，即每产生 M GB 符合要求的频谱数据，频谱设备网络即发行 S 个频谱币。依托频谱设备网络产生的频谱数据发行相应数量的频谱币，即频谱币的发行与频谱数据量锚定[30]。每当频谱管理服务器发布频谱数据采集任务时，频谱设备网络根据产生的频谱数据量发行相应数量的频谱币。

频谱币自动发行和自动支付策略。频谱数据采集任务的发布与频谱币的发行是相互独立的，频谱管理服务器发布频谱数据采集任务，频谱设备网络发行频

谱币，以这种方式避免频谱管理服务器操纵频谱币的发行速度和频谱币的价格。当频谱数据被添加到频谱区块链成为新的频谱区块后，频谱设备网络根据各簇和各感知节点在频谱区块中的贡献比例和数据质量自动将频谱币分配到各簇和各感知节点。

3　防御拜占庭攻击的共识机制

分布式的网络结构和异步的处理架构往往要求开放的数据处理与融合方式，在频谱币激励机制的驱动下，少数恶意的个人无线设备倾向于通过伪造频谱数据的方式牟取不当利益，因此，需要针对恶意个人无线设备伪造频谱数据的拜占庭攻击设计专门的防御机制，确保频谱数据的质量。

在频谱数据添加的过程中，恶意个人无线设备伪造频谱数据的拜占庭攻击主要发生在步骤 1，恶意感知节点并没有进行频谱感知，因为频谱感知需要消耗个人无线设备的能量和时间，而恶意感知节点却希望通过提供伪造的频谱数据来获取频谱设备网络的频谱币奖励，即“不劳而获”，防御该拜占庭攻击要求频谱设备网络能够检测出恶意感知节点伪造的频谱数据。针对频谱设备网络分布式、无中心的特点，提出一种分布式共识机制，检测恶意感知节点伪造频谱数据的拜占庭攻击。

本文所提出的防御拜占庭攻击的共识机制以验证节点在一定置信度下的假设检验判断感知节点是否伪造频谱数据进行拜占庭攻击。该机制借鉴了 Ripple 协议[31]，属于实用拜占庭容错（PBFT, practical Byzantine fault tolerance）[32]的变种，包括感知节点共识融合、验证节点共识验证、簇头节点共识确认这 3 个步骤。

在步骤 1 频谱数据的添加过程中，感知节点在簇头节点的领导下采集频谱数据，并通过分布式共识形成一致的频谱子区块。令 node_{ij}^{s} 表示簇 i 的第 j 个感知节点，node_{ij}^{s} 首先采集频谱数据，再根据邻接图接收邻居感知节点 n 的频谱数据 $x_{in}(k)$，按式(7)将自身的频谱数据由 $x_{ij}(k)$ 迭代更新为 $x_{ij}(k+1)$。

$$x_{ij}(k+1)=x_{ij}(k)+\eta\sum_{n\in\mathcal{N}_j}(x_{in}(k)-x_{ij}(k)) \tag{7}$$

其中，可表示步长。则有

$$0<\eta\leqslant\left(\max_j\left|\mathcal{N}_j\right|\right)^{-1}\triangleq\frac{1}{\Omega} \tag{8}$$

其中，$\mathcal{N}_j$ 为节点 node_{ij}^{s} 的邻居，$\left|\mathcal{N}_j\right|$ 表示节点 node_{ij}^{s} 的度，Ω 为频谱设备网络邻接矩阵 $\boldsymbol{G}$ 的最大度，且 $x_{ij}(0)=\mathrm{data}_{ij}$。频谱数据分布式共识的迭代更新也可以写成如式(9)所示的矩阵形式。

$$\boldsymbol{x}(k+1)=\boldsymbol{P}\boldsymbol{x}(k) \tag{9}$$

其中，$\boldsymbol{P}=\boldsymbol{I}-\eta\boldsymbol{L}$，$\boldsymbol{I}$ 为单位矩阵，$\boldsymbol{L}$ 为邻接矩阵 $\boldsymbol{G}$ 的拉普拉斯变换。共识过程迭代进行，直到簇内感知节点的频谱数据均收敛至共同值 x^*。定理 1 保证了迭代过程的收敛性[33]。

定理 1　簇内的感知节点通过式(10)来更新频谱数据。

$$x_{ij}(k+1)=x_{ij}(k)+u_{ij}(k) \tag{10}$$

其中，$u_{ij}=\eta\sum_{n\in\mathcal{N}_j}(x_{in}(k)-x_{ij}(k)),\ 0<\eta\leqslant\frac{1}{\Omega}$，则可得以下结论。

① 在任何初始状态下，都可以渐进地达成共识。

② 共识算法的迭代过程将渐进地收敛到 $x^*=\frac{1}{n}\sum_{i=1}^{n}x_i(0)$。

定理 1 的证明如附录所示。当簇内的状态迭代更新完成时，簇内的感知节点和簇头节点形成一致的频谱数据 data_i。

簇头节点将频谱数据（包括感知节点位置信息、邻接矩阵信息）打包成频谱区块体，用哈希算法生成频谱数据信息的摘要，如式(11)所示。

$$\mathrm{digest}_{\mathrm{data}_i}=\mathrm{hash}(\mathrm{data}_i,\mathrm{key}_{\mathrm{head}}^{\mathrm{public}}) \tag{11}$$

用自己的私钥对此摘要信息进行加密，如式(12)所示。

$$\mathrm{sign}_{\mathrm{digest}}=\mathrm{RSA}(\mathrm{digest}_{\mathrm{data}_i},\mathrm{key}_{\mathrm{head}}^{\mathrm{private}}) \tag{12}$$

将加密后的信息上传至最近的边缘服务器，其他任何节点均可访问该频谱区块体 data_i，用簇头节点的公钥 $\mathrm{key}_{\mathrm{head}}^{\mathrm{public}}$ 解密数字签名 $\mathrm{sign}_{\mathrm{digest}}$，得到频谱区块体的摘要 $\mathrm{digest}_{\mathrm{data}_i}$，如式(13)所示。

$$\mathrm{digest}_{\mathrm{data}_i}=\mathrm{RSA}(\mathrm{sign}_{\mathrm{digest}},\mathrm{key}_{\mathrm{head}}^{\mathrm{public}}) \tag{13}$$

再对频谱区块体使用哈希算法，如式(14)所示。

$$\mathrm{digest}'_{\mathrm{data}_i}=\mathrm{hash}(\mathrm{data}_i,\mathrm{key}_{\mathrm{head}}^{\mathrm{public}}) \tag{14}$$

得到的结果与频谱区块体的摘要对比，若两者一致，即 $\mathrm{digest}'_{\mathrm{data}_i}=\mathrm{digest}_{\mathrm{data}_i}$，说明频谱区块体未被修改过。此时，其他节点确认频谱区块体未被修改，可以放心访问。将簇内感知节点之间共识机制伪代码总结为感知节点共识融合协议，如协议 1 所示。

协议 1 感知节点共识融合协议

1) 频谱管理服务器(server)发布频谱数据采集任务($\text{task}_{\text{sensing}}$)： $\text{server} \xrightarrow{\text{task}_{\text{sensing}}} \text{network}_{\text{SD}}$

2) 频谱设备网络($\text{network}_{\text{SD}}$)预存频谱币($\text{coin}_{\text{sensing}}$)： $\text{network}_{\text{SD}} \xrightarrow{\text{coin}_{\text{sensing}}} \text{network}_{\text{SD}}$

3) 初始化： node_{ij}^{s} 表示簇 i 的第 j 个感知节点， $i=1,2,\cdots,N_C$ ， $j=1,2,\cdots,N_i$ ， node_i^H 表示簇 i 的簇头节点

4) while $T_{\text{start}}<k\leqslant T_{\text{stop}}$ // T_{start} 和 T_{stop} 分别为频谱数据采集的开始时间和终止时间

5) for i=1: N_C

6) for j=1:N_i

7) while $\sum_{n=1}^{N_i}(x_{ij}-x_{in})^2 \geqslant \Delta X_i$

8) do $x_{ij}(k+1)=x_{ij}(k)+\eta\sum_{n\in N_j}(x_{in}(k)-x_{ij}(k))$

9) end for

10) end for

11) 频谱数据 data_i 生成摘要： $\text{digest}_{\text{data}_i}=\text{hash}(\text{data}_i,\text{key}_{\text{head}}^{\text{public}})$

12) 对摘要信息加密： $\text{sign}_{\text{digest}}=\text{RSA}(\text{digest}_{\text{data}_i},\text{key}_{\text{head}}^{\text{private}})$

13) 将 data_i 和 $\text{digest}_{\text{data}_i}$ 上传至边缘服务器： $\text{node}_i^H \xrightarrow{\text{data}_i+\text{sign}_{\text{digest}}} \text{edge}_i$

14) 向频谱设备网络预存频谱币： $\text{node}_i^H \xrightarrow{\text{coin}_{\text{checking}}} \text{network}_{\text{SD}}$

随后，边缘服务器 edge_i 发布频谱区块验证任务，附近的其他个人无线设备自主响应验证任务，成为验证节点。验证节点根据频谱数据子区块提供的信息在验证节点本地进行共识验证，目的是检查频谱数据中是否存在恶意感知节点伪造的频谱数据。验证节点通过共识验证得到每个频率的共识结果 $x_i^{\dagger}$ 和在 $1-\alpha$ 置信度下的置信区间 $[\Delta_{\min},\Delta_{\max}]$ ，如果 $x_i^{\dagger}\in[\Delta_{\min},\Delta_{\max}]$ 则认为感知节点没有伪造频谱数据，频谱数据通过共识验证；否则，认为感知节点伪造了频谱数据，共识验证失败。将验证节点之间共识机制的伪代码总结为验证节点共识验证协议，如协议 2 所示。

协议 2 验证节点共识验证协议

1) 簇头节点 node_i^H 通过边缘服务器 edge_i 发布频谱数据验证任务 $\text{task}_{\text{checking}}$ ： $\text{edge}_i \xrightarrow{\text{task}_{\text{checking}}} \text{network}_{SD}$

2) 边缘服务器 edge_i 附近的个人无线设备响应验证任务，成为验证节点， node_m^C 为第 m 个验证节点， $m=1,2,\cdots,M_C$

3) while $k<T_{\text{checking}}$ ， T_{checking} 为数据验证的终止时间

4) for m=1: M_C

5) 验证节点下载频谱数据并解密数字签名： $\text{digest}_{\text{data}_i}=\text{RSA}(\text{sign}_{\text{digest}},\text{key}_{\text{head}}^{\text{public}})$

6) 对频谱区块体使用哈希算法： $\text{digest}'_{\text{data}_i}=\text{hash}(\text{data}_i,\text{key}_{\text{head}}^{\text{public}})$

7) if $\text{digest}_{\text{data}_i}$=$\text{digest}'_{\text{data}_i}$

8) 验证节点模拟得到共识结果： $\text{node}_m^C \xrightarrow{\text{Consensus}} x^{\dagger}$

9) if $x_i^{\dagger}\in[\Delta_{\min},\Delta_{\max}]$ ，验证节点认为频谱数据通过验证： $\text{node}_m^C \xrightarrow{\text{Pass}} \text{edge}_i$

10) else $\text{node}_m^C \xrightarrow{\text{No Pass}} \text{edge}_i$

11) end if

12) else $\text{node}_m^C \xrightarrow{\text{Error}} \text{edge}_i$

13) end if

14) end for

15) if $\text{num(Pass)}\geqslant\gamma\%$ //如果验证节点中认为频谱数据通过验证的数量高于 $\gamma\%$

16) $\text{edge}_i \xrightarrow{\text{Pass}} \text{data}_i$

17) else $\text{edge}_i \xrightarrow{\text{No Pass}} \text{data}_i$

18) end if

19) 频谱设备网络向参与验证任务的验证节点释放频谱币： $\text{network}_{\text{SD}} \xrightarrow{\text{coin}_{\text{checking}}} \text{node}_m^C$

随后，簇头节点对通过验证的频谱子区块进行分布式共识，以确定哪一个频谱子区块被添加到频谱区块链中，提供该频谱子区块的簇将获得一部分频谱币。各簇簇头节点通过分布式共识得到共识结果 Q^* ，将 Q^* 与各簇所提供的原始频谱数据相比，差异最小的频谱数据被认为是该频谱子区块的提供者，获得频谱币奖励。将簇头节点之间共识机制总结为簇头节点共识确认协议，如协议 3 所示。

协议 3 簇头节点共识确认协议

1) 初始化： node_i^h 为通过验证的簇头节点， $i=1,2,\cdots,N_{C_0}$

2) for i=1:N_{C0}

3) while $\sum_{n=1}^{N_{C0}}(x_i-x_n)^2\geqslant\Delta X$

4) do $x_i(k+1)=x_i(k)+\eta\sum_{n\in N_i}(x_n(k)-x_i(k))$

5) end while

6) end for

7) 差异最小的被认为是频谱数据子区块的提供者：$x(j)=\arg\min_i \left|x_i-Q^*\right|$

8) 预存的频谱币对该簇自动分配：$\text{network}_{\text{SD}} \xrightarrow{\text{coin}_{\text{sensing}}} \{\text{node}_i^h, \text{node}_{ij}^S\},\ j=1,2,\cdots,N_j$

4　性能仿真

通过实验仿真测试本文设计的共识机制对恶意感知节点伪造频谱数据的拜占庭攻击的防御性能。

4.1　参数设置

考虑频谱设备网络中小尺度授权用户的场景，如图 5 所示。一个授权用户发射机 PU 位于坐标原点 (0 m, 0 m)，发射功率为 P_t=1~10 W (30~40 dBm)。100 个个人无线设备随机分布在以坐标原点为中心、边长为 5 km 的方形区域内，随机自发地形成 C=6 个簇，每个簇包含 7~13 个个人无线设备、一个簇头节点和若干个感知节点。授权用户信号经瑞利衰落后被感知节点接收，环境噪声的功率谱密度为−174 dBm/Hz[34]，大尺度路径衰落系数为 4，小尺度瑞利衰落系数为 1，感知节点通过本地频谱感知采集频谱数据，感知节点的接收授权用户信号的信噪比与授权用户发射功率、感知节点的位置和传播路径相关。区域内其他个人无线设备以 50%的概率参与共识验证，成为验证节点，其余个人无线设备为一般节点，不参与共识验证。验证节点在 α=0.05或α=0.1 的置信度下对频谱数据进行共识验证，并通过边缘服务器将验证结果反馈给各簇头节点，验证节点获得簇头节点预存的频谱币作为验证奖励，簇头节点对通过共识验证的频谱数据进行分布式共识，确定频谱数据的来源，即确定哪一个频谱子区块被添加到频谱区块链。

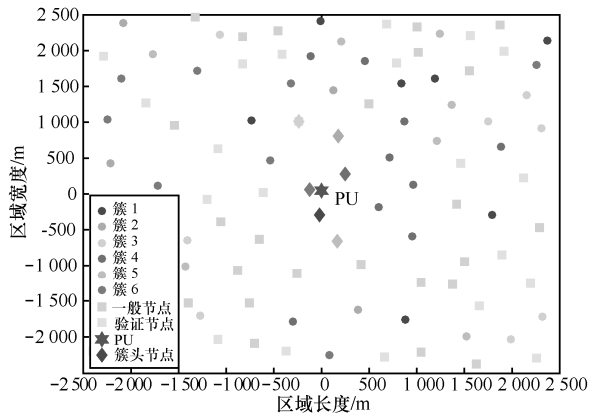


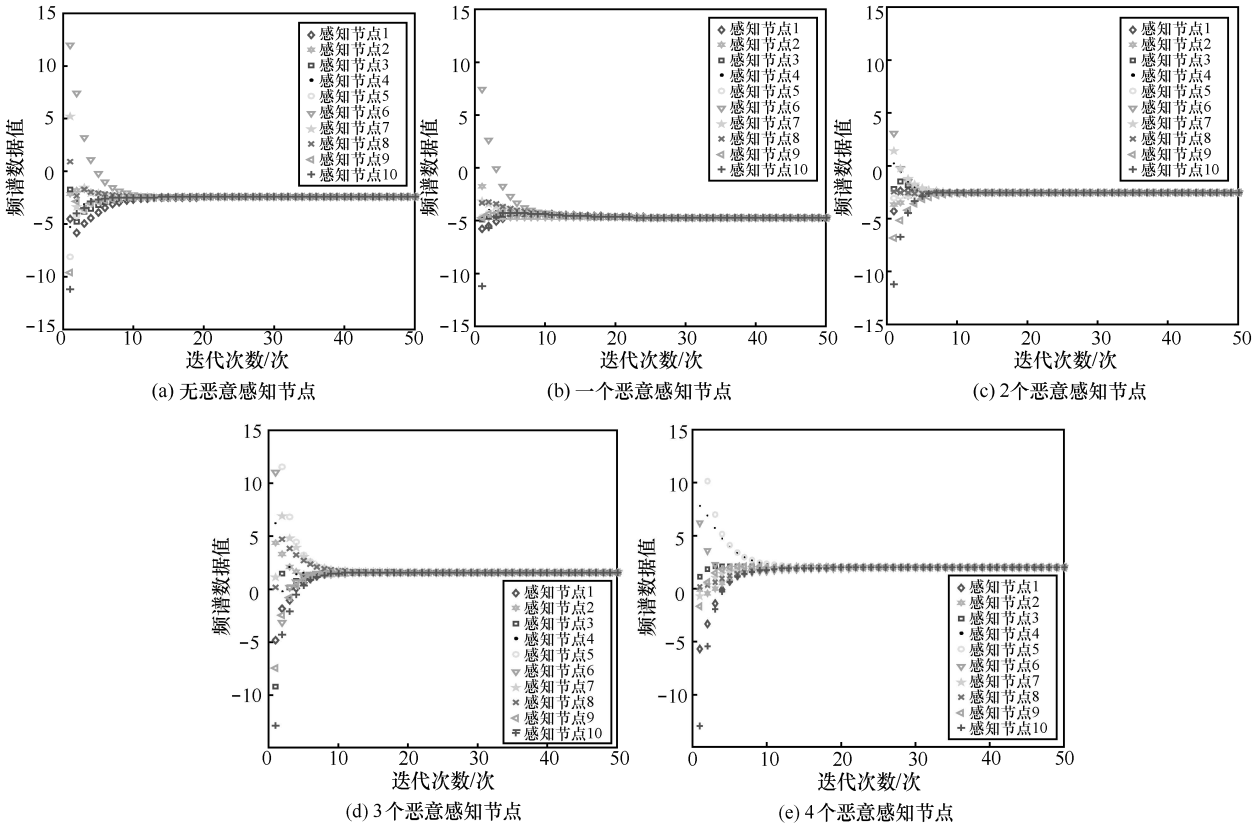
图 5　100 个个人无线设备和一个授权用户的频谱设备网络场景

假设簇内恶意感知节点的数量总体上小于或等于诚实感知节点的数量，以簇 4 为例，即簇内包含 1~4 个恶意感知节点。恶意感知节点以 P_{attack} 的概率发动伪造频谱数据的拜占庭攻击，所伪造的频谱数据为区间 $[x_{\min}(k), x_{\max}(k)]$ 内的随机值，其中，$x_{\min}(k)$ 和 $x_{\max}(k)$ 分别为 k 时刻接收邻居感知节点发送的频谱数据最小值和频谱数据最大值。

4.2　共识机制性能分析

图 6(a)~图 6(e)分别仿真了簇 4 在无恶意感知节点和包含 1~4 个恶意感知节点时对频谱数据进行分布式共识的过程，可见无论簇内有无恶意感知节点，均能通过簇内感知节点之间的分布式共识对频谱数据值达成一致。当簇 4 在无恶意感知节点时达成共识，其值可以视为分布式共识的真实值；当簇 4 包含恶意感知节点时，感知节点通过分布式共识得到的频谱数据值与真实值之间的差异随着恶意感知节点数量的增多而增大。在此基础上，对簇 4 无恶意感知节点和包含 1~4 个恶意感知节点的情况进行 1 000 次 Monte-Carlo 仿真，统计簇内感知节点达成分布式共识时频谱数据值的分布，如图 7(a)~图 7(e)所示，可见在无恶意感知节点时，达成共识时频谱数据值在很小的区间内（如图 7(a)所示的 [−1.853 5, −1.849 0]）形成正态分布；当簇内包含恶意感知节点时，达成共识时频谱数据值仅较集中地分布在若干个离散点。从图 7(b)~图 7(e)来看，达成共识时频谱数据值的分布符合上述的观察结果，即达成共识时频谱数据值与真实值之间的差异随着恶意感知节点数量的增多而增大。由文献[34]可知，分布式共识的收敛速度由 λ_2 决定，λ_2 为 $\boldsymbol{L}$ 第二小的特征值，称为图的代数连通性。在恶意用户数量逐渐增多的过程中，邻接矩阵 $\boldsymbol{G}$ 不变，$\boldsymbol{L}$ 作为 $\boldsymbol{G}$ 的拉普拉斯变换也不变，因此分布式共识的收敛速度并不会随着恶意用户数量的增多而变慢。

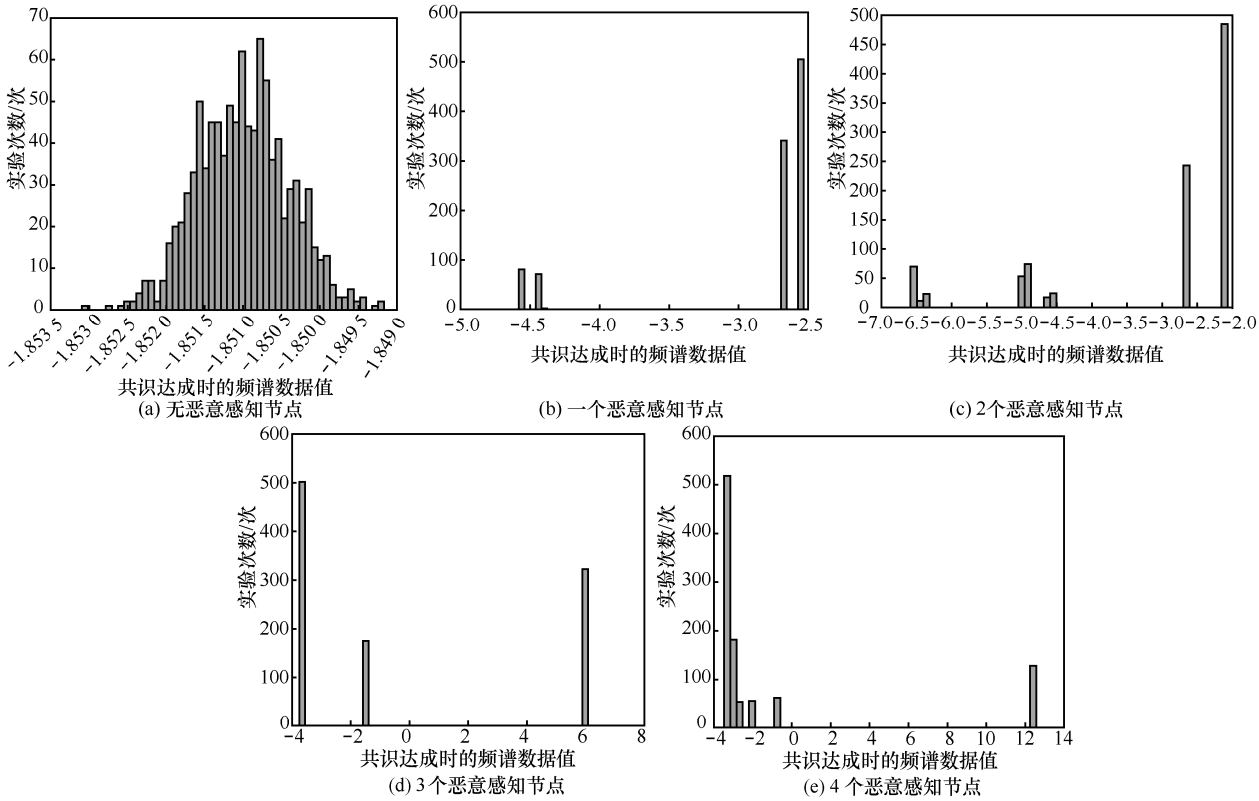
簇内感知节点通过分布式共识对频谱数据达成共识后，簇头节点将频谱数据和簇内邻接矩阵信息非对称加密，通过边缘服务器发送给验证节点，验证节点根据邻接矩阵信息对频谱数据进行共识验证，确定感知节点是否伪造频谱数据。验证节点在 α=0.05或 α=0.1 的置信度下对频谱数据进行共识验证的结果如图 8(a)和图 8(b)所示。若达成共识时的频谱数据（实线）落入 $1-\alpha$ 置信度下的置信区间 $[\Delta_{\min}, \Delta_{\max}]$，即认为感知节点没有伪造频谱数据，通过共识验证；



(a) 无恶意感知节点　(b) 一个恶意感知节点　(c) 2个恶意感知节点

(d) 3个恶意感知节点　(e) 4个恶意感知节点

图 6　簇内频谱数据进行分布式共识的过程



(a) 无恶意感知节点　(b) 一个恶意感知节点　(c) 2个恶意感知节点

(d) 3个恶意感知节点　(e) 4个恶意感知节点

图 7　达成共识时频谱数据值的分布

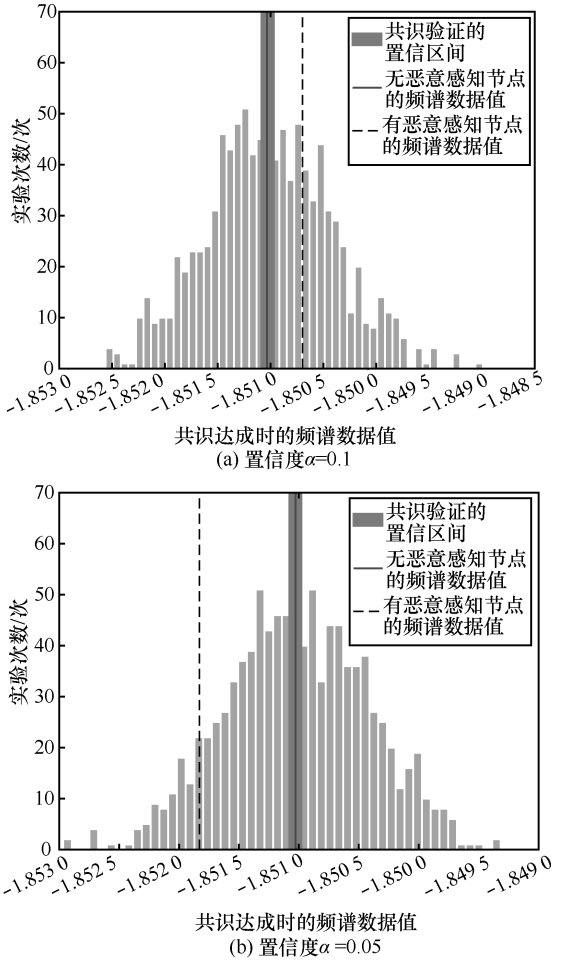


图 8　验证节点对频谱数据进行共识验证

若达成共识时的频谱数据值（虚线）落入$1-\alpha$置信度下的置信区间$[\Delta_{\min},\Delta_{\max}]$之外，即认为感知节点伪造了频谱数据，共识验证失败。当置信度由α=0.05变为α=0.1时，共识验证的置信区间增大。为评估所提共识验证对拜占庭攻击的防御性能，定义 2 种概率：虚警概率 P_{f}和漏警概率 P_{m}。虚警表示无恶意感知节点或恶意感知节点未发动拜占庭攻击时，达成共识时频谱数据因落在置信区间$[\Delta_{\min},\Delta_{\max}]$之外而未通过共识验证。漏警表示恶意感知节点发动了拜占庭攻击，达成共识时频谱数据因落入置信区间$[\Delta_{\min},\Delta_{\max}]$而通过共识验证。虚警概率 P_{f}和漏警概率P_{m}直接反映了共识机制对恶意感知节点伪造频谱数据的拜占庭攻击的防御性能。

授权用户发射机取 1~10 W (30~40 dBm)的发射功率，验证节点对频谱数据值进行共识验证，得到授权用户在不同发射功率下共识验证的虚警概率 P_{f}和漏警概率 P_{m}，仿真结果是在α=0.05或α=0.1下通过 1 000 次 Monte-Carlo 仿真得到的平均水平。漏警概率 P_{m}与授权用户发射功率 P_{t}的关系如图 9 所示。从图 9 可以看出，漏警概率 P_{m}随着授权用户发射功率 P_{t}的增加而降低，说明授权用户发射功率 P_{t} 的增加提高了共识验证的区分度；漏警概率 P_{m}随着恶意用户数量的增加而降低，说明恶意用户数量的增加也提高了共识验证的区分度；随着置信度α从 0.1 降低到 0.05，共识验证的置信区间$[\Delta_{\min},\Delta_{\max}]$将缩小，使漏警概率 P_{m}进一步降低。虚警概率P_{f}与授权用户发射功率P_{t}的关系如图10所示。从图 10 可以看出，虚警概率 P_{f}随着授权用户发射功率 P_{t} 的增加而降低，说明授权用户发射功率 P_{t} 的增加提高了共识验证的区分度；恶意用户数量和置信度α对虚警概率 P_{f}的影响不大，但总体来说，虚警概率 P_{f}随恶意用户数量的增加而降低，说明恶意用户数量的增加也有助于提高共识验证的区分度；当置信度α从 0.1 降低到 0.05，共识验证的置信区间$[\Delta_{\min},\Delta_{\max}]$将缩小（如图 8 所示），可能使一部分无

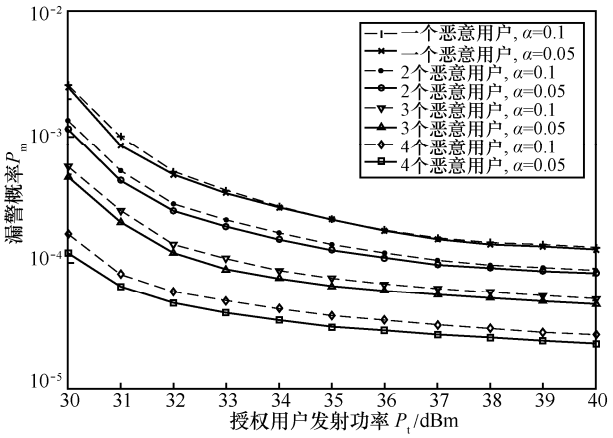


图 9　漏警概率 P_{m}与授权用户发射功率 P_{t}的关系

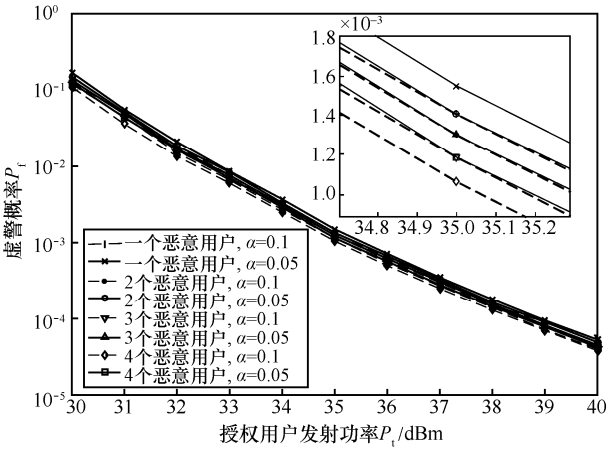


图 10　虚警概率 P_{f}与授权用户发射功率 P_{t}的关系

恶意感知节点的频谱数据落入置信区间$[\Delta_{\min},\Delta_{\max}]$之外，导致虚警。综合不同授权用户发射功率$P_t$、不同恶意感知节点数量和置信度$\alpha$=0.05或$\alpha$=0.1下的漏警概率$P_m$和虚警概率$P_f$，得到漏警概率$P_m$、虚警概率$P_f$与授权用户发射功率$P_t$的关系如图 11 所示。

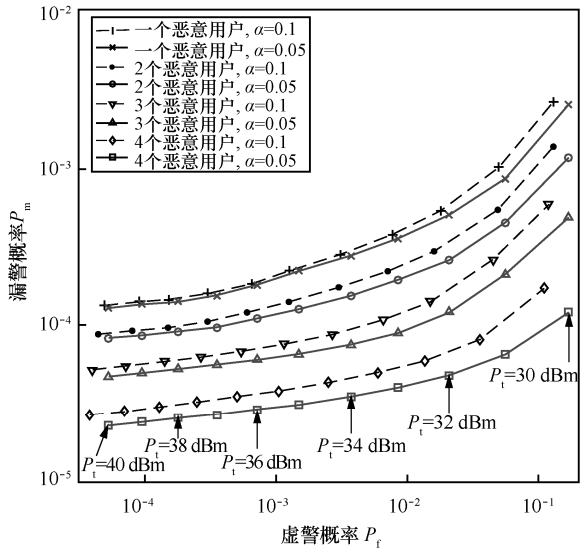


图 11 漏警概率P_m、虚警概率P_f与授权用户发射功率P_t的关系

最后，簇 1~簇 6 的簇头节点对通过共识验证的频谱数据进行分布式共识（这里，假设簇 1~簇 6 的频谱数据均通过共识验证），如图 12 所示，共识过程表明簇头节点 6 的初始频谱数据值与频谱数据共识值（实线）误差最小，因此确定簇 6 提供的频谱子区块被添加到频谱区块链，根据簇 6 内感知节点对频谱子区块的贡献比例，频谱设备网络将频谱币自动分配至簇 6 内各感知节点。

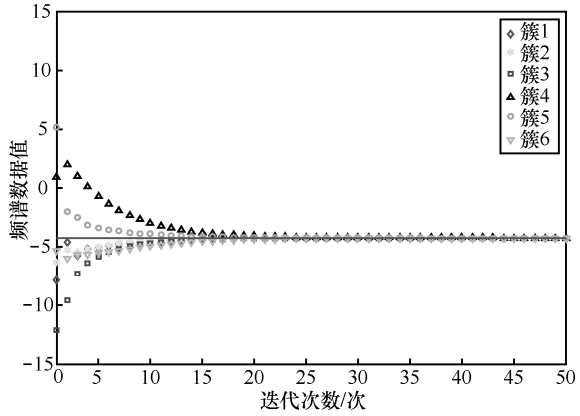


图 12 簇头节点通过分布式共识确定频谱数据来源的过程

本文所提共识机制属于 PBFT 的变种[32]，借鉴了 Ripple 协议[31]，将其与主流共识机制（如 PoW、PoS）进行比较，如表 1 所示，其中，n 为网络中的节点数量。

表 1 本文共识机制与主流共识机制的比较

比较项	PoW	PoS	PBFT	Ripple
区块链类型	公有链	公有链	联盟链	联盟链
交易时延	高	低	低	低
交易吞吐率	7 笔/秒	100 笔/秒	100 笔/秒	1500 笔/秒
交易终结类型	概率性	概率性	确定性	确定性
是否需要挖矿	是	是	否	否
对恶意攻击的抵御能力	50%以下的算力	50%以下的权益	$\leqslant\left\lfloor\frac{n-1}{3}\right\rfloor$	$\leqslant\left\lfloor\frac{n-1}{5}\right\rfloor$

实际上，PoW 中的搜索空间是无限的，因此也导致 PoW 的吞吐率较低；PoS 的搜索空间有限，但存在矿工挖矿并寻求其他矿工的一致性验证过程，导致 PoS 的吞吐率仍然不高。本文所提共识机制没有 PoW、PoS 等典型共识机制中的“矿工”挖矿过程，这一点将大大提高频谱设备网络的吞吐率，代价是对恶意攻击的抵御能力低于 PoW 和 PoS。

5 结束语

针对大规模、超密集部署移动互联网和物联网带来的精确频谱共享需求，提出了基于区块链技术联网海量个人无线设备构成频谱设备网络。采用云计算与边缘计算结合的频谱设备网络架构，频谱管理服务器在频谱设备网络云端发布频谱感知任务、回收频谱数据、发放任务奖励，个人无线设备既是频谱使用设备又是频谱感知设备，在频谱设备网络边缘分布式地采集频谱数据构成频谱区块链、获得频谱币奖励，频谱设备网络通过感知节点共识融合、验证节点共识验证、簇头节点共识确认的分布式共识机制防御恶意节点伪造频谱数据的拜占庭攻击。频谱设备网络以频谱数据获取、频谱区块添加、频谱数据传输、频谱数据采集的激励作为网络运行的基本策略。仿真结果表明，分布式共识防御恶意节点伪造频谱数据的拜占庭攻击的有效性和可靠性。基于区块链的频谱设备网络利用区块链技术去中心化存储、非对称加密、分布式共识等关键技术，使联网的海量个人无线设备贡献频谱数据、支撑精确频谱共享成为可能。下一步，将面向精确频谱共享，在区块链技术框架下对频谱数据的获取、频谱区块的添加、频谱数据的传输、频谱感知的激励等频谱设备网络运行基本策

略做进一步的研究。

附录　定理 1 的证明

结论①的证明见文献[35]，下面主要证明结论②。

考虑到 $\boldsymbol{L}$ 为邻接矩阵 $\boldsymbol{G}$ 的拉普拉斯变换，则有 $\mathrm{rank}(\boldsymbol{L})=n-1$，证明见文献[36]，则 0 是 $\boldsymbol{L}$ 的特征值，令 $\boldsymbol{\gamma}=(\gamma_1,\gamma_2,\cdots,\gamma_n)$ 为 $\boldsymbol{L}$ 的左特征向量，则有 $\boldsymbol{\gamma}^{\mathrm{T}}\boldsymbol{L}=\boldsymbol{0}$，且有 $\dot{x}=-\boldsymbol{L}x$ [36]，则由

$$\dot{y}=-\boldsymbol{\gamma}^{\mathrm{T}}\boldsymbol{L}x=0 \tag{15}$$

可得 $y=\boldsymbol{\gamma}^{\mathrm{T}}x$ 为常数，进一步有

$$\lim_{t\to\infty}y(t)=y(0)=\boldsymbol{\gamma}^{\mathrm{T}}x(0) \tag{16}$$

以及

$$\boldsymbol{\gamma}^{\mathrm{T}}(\alpha\boldsymbol{1})=\boldsymbol{\gamma}^{\mathrm{T}}x(0) \tag{17}$$

求得

$$\alpha=\frac{(\boldsymbol{\gamma}^{\mathrm{T}}x(0))}{\sum_{i=1}^{n}\boldsymbol{\gamma}_i} \tag{18}$$

令 $\gamma=\boldsymbol{1}$ 可得

$$\lim_{t\to\infty}y(t)=y(0)=\frac{1}{n}\sum_{i=1}^{n}x_i(0) \tag{19}$$

表明共识算法的迭代过程将渐进收敛到

$$x^{*}=\frac{1}{n}\sum_{i=1}^{n}x_i(0) \tag{20}$$

证毕。

参考文献：

[1] AGIWAL M, ROY A, SAXENA N. Next generation 5G wireless networks: a comprehensive survey[J]. IEEE Communications Surveys & Tutorials, 2016, 18(3): 1617-1655.

[2] CHIANG M, ZHANG T. Fog and IoT: an overview of research opportunities[J]. IEEE Internet of Things Journal, 2016, 3(6): 854-864.

[3] ZHANG W, WANG C, GE X, et al. Enhanced 5G cognitive radio networks based on spectrum sharing and spectrum aggregation[J]. IEEE Transactions on Communications, 2018, 66(12): 6304-6316.

[4] RAPPAPORT T, SUN S, MAYZUS R, et al. Millimeter wave mobile communications for 5G cellular: it will work![J]. IEEE Access, 2013,(1): 335-349.

[5] QIU J, DING G, WU Q, et al. Hierarchical resource allocation framework for hyper-dense small cell networks[J]. IEEE Access, 2016(4): 8657-8669.

[6] DING G, WANG J, WU Q, et al. Cellular-base-station-assisted device-to-device communications in TV white space[J]. IEEE Journal on Selected Areas in Communications, 2016, 34(1): 107-121.

[7] LIANG Y. Dynamic spectrum management: from cognitive radio to blockchain and artificial intelligence[M]. Singapore: Springer Nature Press, 2020.

[8] DAI Y, XU D, MAHARJAN J, et al. Blockchain and deep reinforcement learning empowered intelligent 5G beyond[J]. IEEE Network, 2019, 33(3): 10-17.

[9] WEISS M, WERBACH K, SICKER D, et al, On the application of blockchains to spectrum management[J]. IEEE Transactions on Cognitive Communications and Network, 2019, 5(2): 193-205.

[10] ROSENWORCEL J. Remarks of commissioner jessica rosenworcel mobile world congress[R]. FCC, (2018-02-27)[2019-07-04].

[11] KOTOBI K, BILEN S. Secure blockchains for dynamic spectrum access: a decentralized database in moving cognitive radio networks enhances security and user access[J]. IEEE Transactions on Vehicular Technology Magazine, 2018, 13(1): 32-39.

[12] PEI Y, HU S, ZHONG F, et al. Blockchain-enabled dynamic spectrum access: cooperative spectrum sensing, access and mining[C]//The IEEE Global Communications Conference. Piscataway IEEE Press, 2019: 1-6.

[13] BAYHAN S, ZUBOW A, WOLISZ A. Spass: spectrum sensing as a service via smart contracts[C]// The IEEE Symposium on New Frontiers in Dynamic Spectrum Access Networks. Piscataway IEEE Press, 2018: 1-10.

[14] JIAO Y, WANG P, NIYATO D, et al. Auction mechanisms in cloud/fog computing resource allocation for public blockchain networks[J]. IEEE Transactions on Parallel and Distributed Systems, 2019, 30(9): 1975-1989.

[15] XIONG Z, ZHANG Y, NIYATO D, et al. When mobile blockchain meets edge computing[J]. IEEE Communications Magazine, 2018, 56(8): 33-39.

[16] WU Q, DING G, DU Z, et al. A cloud-based architecture for the internet of spectrum devices over future wireless networks[J]. IEEE Access, 2016(4): 2854-2862.

[17] WU Q, DING G, XU Y, et al. Cognitive internet of things: a new paradigm beyond connection[J]. IEEE Internet of Things Journal, 2014, 1(2): 129-143.

[18] DING G, WANG J, WU Q, et al. Robust spectrum sensing with crowd sensors[J]. IEEE Transactions on Communications, 2014, 62(9): 3129-3143.

[19] PUTHAL D, MALIK N, MOHANTY S, et al. The blockchain as a decentralized security framework[J]. IEEE Consumer Electronics Magazine, 2018, 7(2): 18-21.

[20] NAKAMOTO S. Bitcoin: a peer-to-peer electronic cash system[EB]. Biton, 2020.

[21] PUTHAL D, MALIK N, MOHANTY S, et al. Everything you wanted to know about the blockchain: its promise, components, processes, and problems[J]. IEEE Consumer Electronics Magazine, 2018, 7(4): 6-14.

[22] KANG J, YU R, HUANG X, et al. Blockchain for secure and efficient data sharing in vehicular edge computing and networks[J]. IEEE Internet of Things Journal, 2018, 6(3): 4660-4670.

[23] DELGADO S, TANAS C, HERRERA J. Reputation and reward: two sides of the same bitcoin[J]. Sensors, 2016, 16(6): 776-798.

[24] AN J, YANG H, GUI X, et al. TCNS: node selection with privacy protection in crowd sensing based on twice consensuses of blockchain[J]. IEEE Transactions on Network and Service Management, 2019, 16(3): 1255-1267.

[25] GUO C, PENG T, XU S, et al. Cooperative spectrum sensing with cluster-based architecture in cognitive radio networks[C]// IEEE 69th Vehicular Technology Conference. Piscataway IEEE Press, 2009: 1-5.

[26] WU M, WANG K, CAI X, et al. A comprehensive survey of blockchain: from theory to IoT applications and beyond[J]. IEEE Internet of Things Journal, 2019, 6(5): 8114-8154.

[27] CROMAN K, DECKER C, EYAL I, et al. On scaling decentralized blockchains[C]//International Conference on Financial Cryptography and Data Security. Berlin: Springer, 2016:106-125.

[28] LUU L, NARAYANAN V, ZHENG C, et al. A secure sharding protocol for open blockchains [C]//The 2016 ACM SIGSAC Conference on Computer and Communications Security. NewYork: ACM Press, 2016: 17-30.

[29] AETERNITY, Aternity blockchain[M]. Hess: Aeternity Publisher, 2017.

[30] MIHAYLOV M, JURADO S, AVELLANA N, et al. NRGcoin: virtual currency for trading of renewable energy in smart grids[C]// 11th International Conference on the European Energy. Krakow, 2014: 1-6.

[31] SCHWARTZ D, YOUNGS N, BRITTO A. The ripple protocol consensus algorithm[M]. Ripple Labs Inc White Paper, 2014.

[32] CASTRO M, LISKOV B. Practical byzantine fault tolerance[J]. Operating System Design and Implementation, 1999(99): 173-186.

[33] OLFATI R, FAX J, MURRAY R. Consensus and cooperation in networked multi-agent systems[J]. Proceeding of the IEEE, 2007, 95(1): 215-233.

[34] SHELLHAMMER S, TAWIL V, CHOUINARD G, et al. Spectrum sensing simulation model[S]. IEEE 802.22-06/0028r10, 2006.

[35] GODSIL C, ROYLE G. Algebraic graph theory[M]. Graduate Texts in Mathematics. Berlin: Springer-Verlag Press, 2001.

[36] OLFATI R, MURRAY R. Consensus problems in networks of agents with switching topology and time-delays[J]. IEEE Transactions on Automatic Control, 2004, 49(9): 1520-1533.

[作者简介]

杨健（1984− ），男，安徽铜陵人，博士，国防科技大学在站博士后，主要研究方向为电磁频谱管理、频谱预测、认知物联网、频谱态势等。

陈曦（1984− ），女，江苏徐州人，博士，南京理工大学副研究员，主要研究方向为电磁频谱管理、认知无线电、频谱预测、智能弹药与毁伤等。

丁国如（1986− ），男，河南新乡人，博士，陆军工程大学副教授，主要研究方向为认知无线网络、大规模 MIMO、机器学习、大数据分析等。

赵杭生（1962− ），男，浙江杭州人，博士，南京邮电大学研究员，主要研究方向为电磁频谱管理、认知无线电、频谱服务、频谱态势等。

张林元（1991− ），男，山东临清人，博士，江南计算技术研究所工程师，主要研究方向为电磁频谱态势感知、安全数据融合等。

孙佳琛（1994− ），女，江苏南通人，陆军工程大学博士生，主要研究方向为频谱数据分析、无线通信、认知无线电等。